Business Analytics:

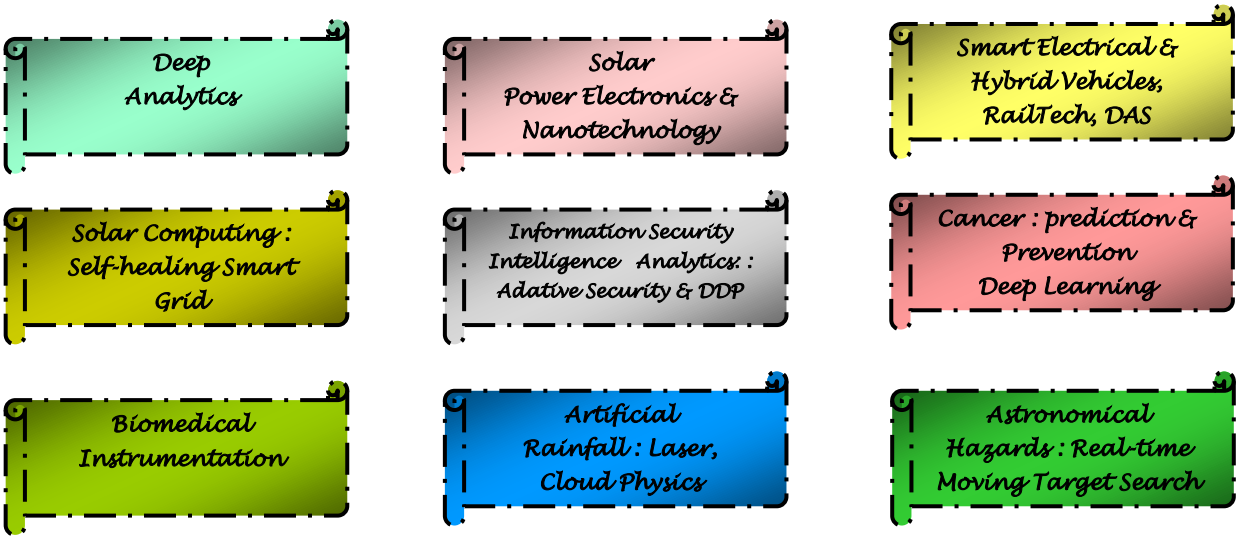
Technology for Humanity

3rd Edition, 2019

By

Sumit Chakraborty

Suryashis Chakraborty



FREE eBooks

WHOEVER
WHENEVER
WHEREVER
YOU ARE

INSTANTLY DOWNLOAD THESE MASSIVE BOOK BUNDLES

CLICK ANY BELOW TO ENJOY NOW

3 AUDIOBOOK COLLECTIONS

Classic AudioBooks Vol 1 ▪ Classic AudioBooks Vol 2 ▪ Classic AudioBooks Kids

6 BOOK COLLECTIONS

Sci-Fi ▪ Romance ▪ Mystery ▪ Academic ▪ Classics ▪ Business

Preface

Deep analytics does not only mean statistics or data mining or big data analytics, it is a complex multi-dimensional analysis through '7-S' model based on rational, logical and analytical reasoning from different perspectives such as scope, system, structure, staff-resources, skill-style-support, security and strategy. This book presents a deep analytics model through a consistent and systematic approach and highlights its utility and application for reasoning ten technology innovations today: (1) solar power electronics & Nanotechnology, (2) Electrical and hybrid vehicles : smart batteries , (3) RailTech: DAS, security & safety, (4) Emerging digital technology, (5) Solar computing : Self-healing mechanism for a smart grid, (6) Information Security Intelligence (ISI) Analytics : Adaptive security and dynamic data protection for IIOT, SCADA & ICS (7) Cancer prediction & prevention mechanism: deep learning, (8) Biomedical instrumentation, (9) Artificial rainfall & cloud physics and (10) Real-time moving target search for astronomical hazards.

The reality is that every stakeholder is impacted by the challenges and opportunities of innovation ecosystems today. The concept of deep analytics is still relatively new; it has now emerged as a powerful tool for business analytics and a real world theme in the modern global economy. The target audience of this book includes academic and research community, corporate leaders, policy makers, administrators and governments, entrepreneurs, investors, engineers, producers and directors interested in production of documentary films, news and TV serials. We are excited to share the ideas of deep analytics with you. We hope that you will find them really value adding and useful and will share with your communities. It is a rational and interesting option to teach deep analytics in various academic programmes of various Business Management programmes (e.g. Technology Management, Information Technology, Information Systems, Management Information Systems (MIS), Strategic Management and Analytics for BBA, MBA, PGDM, PGDBM) and also Electrical and Electronics Engineering (e.g. B.Tech, M.Tech, B.E.E., M.E., Ph.D.).

This e-book is the summary of electronic version of 3rd edition dated 15 August'2019; Price: $250 (per copy). This book contains information obtained from authentic sources; sincere efforts have been made to publish reliable data and information.

Thanks and regards.

Sumit Chakraborty, Fellow (IIM Calcutta), Bachelor of Electrical Engineering (JU)
Suryashis Chakraborty
Business Analytics Research Lab, India
15.08.2019

Content

CHAPTER 1 : DEEP ANALYTICS - TECHNOLOGY for HUMANITY

1. INTRODUCTION : DEEP ANALYTICS

Figure 1.1 : **Deep Analytics**

Deep analytics is an intelligent, complex, hybrid, multi-phased and multi-dimensional data analysis system. The basic steps of computation are data sourcing, data filtering / preprocessing, data ensembling, data analysis and knowledge discovery from data. The authorized data analysts select an optimal set of input variables, features and dimensions (e.g. scope, system, structure, security, strategy, staff-resources, skill-style-support) correctly being free from malicious attacks (e.g. false data injection, shilling); input data is sourced through authenticated channels accordingly. The sourced data is filtered, preprocessed (e.g. bagging, boosting, cross validation) and ensembled. It is rational to adopt an optimal mix of quantitative (e.g. regression, prediction, sequence, association, classification and clustering algorithms) and qualitative

(e.g. case based reasoning, perception, process mapping, SWOT, CSF and value chain analysis) methods for multi-dimensional analysis. The analysts define intelligent training and testing strategies in terms of selection of correct soft computing tools, network architecture – no. of layers and nodes; training algorithm, learning rate, no. of training rounds, cross validation and stopping criteria;. The hidden knowledge is discovered from data in terms of collective, collaborative, machine, security and business intelligence. The analysts audit fairness and correctness of computation and also reliability, consistency, rationality, transparency and accountability of the analytics.

Deep analysis (e.g. in memory analytics) can process precisely targeted, complex and fast queries on large (e.g. petabytes and exabytes) data sets of real-time and near real-time systems. For example, deep learning is an advanced machine learning technique where artificial neural networks (e.g. CNN) can learn effectively from large amount of data like human brain learn from experience by performing a task repeatedly and gradually improves the outcome of learning. Deep analytics follows a systematic, streamlined and structured process that can extract, organize and analyze large amounts of data in a form being acceptable, useful and beneficial for an entity (e.g. individual human agent, organization or BI information system). It is basically a specific type of distributed computing across a number of server or nodes to speed up the analysis process. Generally, shallow analytics use the concept of means, standard deviation, variance, probability, proportions, pie charts, bar charts and tabs to analyze small data set. Deep analytics analyze large data sets based on the concepts of data visualization, descriptive and prescriptive statistics, predictive modeling, machine learning, multilevel modeling, data reduction, multivariate analysis, regression analysis, logistic regression analysis, text analysis and data wrangling. Deep analytics is often coupled with business intelligence applications which perform query based search on large data, analyze, extract information from data sets hosted on a complex and distributed architecture and convert that information into specialized data visualization outcome such as reports, charts and graphs. In this book, deep analytics has been applied for technology management system (TMS).

Technological innovations are practical implementation of creative novel ideas into new products or services or processes. Innovations may be initiated in many forms from various sources such as firms, academic institutions, research laboratories, government and private enterprises and individual agents. There are different types of innovations from the perspectives of scope, strength, weakness, opportunities, threats and demands from the producers, service providers, users, service consumers and regulators.

Innovation funnel is a critical issue in technology management; innovation process is often perceived like a funnel with many potential ideas passing through the wide end of a funnel but very few become successful, profitable, economically and technically feasible products or services through the development process [24]. Deep analytics is an intelligent method and consulting tool that is essential for effective management of top technological innovations today [Figure 1.1]. It is basically an integrated framework which is a perfect combination or fit of seven dimensions. Many technological innovation projects fail due to the inability of the project managers to recognize the importance of the fit and their tendency to concentrate only on a few of these factors and ignore the others. These seven factors must be integrated, coordinated and synchronized for the diffusion of top technological innovations globally [16,53].

Deep Analytics Mechanism [DAM]

****

Agents: Single or a group of data analysts;

System : Technology Management System /* Technology for humanity*/

Moves:

- Adopt a hybrid approach : quantitative $\oplus$ qualitative;
- Optional choices :
  - Collaborative analytics /* agents : multiple data analysts*/
  - Big data
  - Predictive modelling

Objectives: Evaluate an emerging technology for innovation, adoption and diffusion;

Constraints: Availability of authenticated and correct data, time, effort, cost;

Input: Technical data (D_t), Business data (D_b); /* Entity : An emerging technology for humanity*/

Procedure:

- Source data (D_t, D_b);
- Filter data;
- Ensemble data;

- Analyze data → select choice
  - Choice 1: qualitative analysis (Perception , Case based reasoning, SWOT, TLC);
  - Choice 2: quantitative analysis (Prediction, Simulation);
  - Choice 3 : Hybrid (quantitative ⊕ qualitative);
- Multi-dimensional analysis → KDD (S_1, S_2, S_3, S_4, S_5, S_6,S_7); /* S_1: Technology scope, S_2: System, S_3 : Structure, S_4: Technology security, S_5: Strategy, S_6: Staff-resources, S_7: Skill-style-support; KDD: Knowledge discovery from data */

Revelation principle:

- Define information disclosure policy → preserve privacy of strategic data.
- Verify authentication, authorization and correct identification in data sourcing.
- Audit fairness, correctness, reliability, consistency and rationality of analytic computation.

Payment function : Compare a set of technologies based on cost benefit analysis.
Output: Technology intelligence (collective, collaborative, security, machine, business);

****

Deep analytics is essential to understand the nature of a technological innovation and identify the gaps between as-is and to-be capabilities in a systematic and compelling way. It reasons seven dimensions under three major categories: (a) Requirements engineering schema: scope [S_1]; (b) Technology schema : system [S_2], structure [S_3], security [S_4] and (c) Technology management schema : strategy [S_5], staff-resources [S_6] and skill-style-support [S_7] [Figure 1.1]. This chapter analyzes each dimension briefly and reasons nine cases of top technology innovations today in chapters [2-10] applying the tool of deep analytics. The basic building blocks of our research methodology include critical reviews of existing works on technology management and case based reasoning. We have reviewed various works on technology management [1-33,53]. We have collected the data of nine cases from various technical papers and secondary sources. Chapter 11 concludes the work.

a. RESEARCH METHODOLOGY AND OPEN AGENDA

The basic objective of this book is to explore a set of fundamental questions on technology management:

- **Scope : What is technology swing? What is the scope of a technology innovation?**
- **System: What are the basic schema and dominant design of a system associated with a technology innovation?**
- **Structure: What are the basic elements of the system architecture associated with a technology innovation? How to represent the structure correctly and transparently through multi-dimensional simulated modeling such as digital twins?**
- **Security: What do you mean by technology_security? How to verify the security intelligence of a system associated with a technology innovation?**
- **Strategy:**
  - **What are the strategic moves of technology innovation, adoption and diffusion?**
  - **What is the outcome of technology life-cycle analysis?**
  - **How to compare an emerging technology with the existing old technologies through SWOT analysis?**
  - **What are the technology spillover effects?**
  - **What are the blind spots and critical success factors?**
- **Staff - resources: How to exercise ERP and SCM in a technology innovation project? What should be the talent management strategy?**
- **Skill-style-support:**
  - **What are the skills, leadership style and support demanded by a technological innovation? How to manage technology innovation projects efficiently through resource and time constrained, stochastic, adaptive multi-objective and multimode project scheduling algorithms?**
  - **What should be the shared vision, common goals and communication protocols?**

- **How to ensure a perfect fit among '7-S' elements?**
- **What type of organization structure is essential for various types of technology innovations?**

We have adopted two approaches to develop '7-S' model of deep analytics for technological innovation management. The first approach is learning-before-doing. We have reviewed relevant literature on technology management and have defined an initial framework of the deep analytics. We have reviewed on top emerging technologies today from the technical reports of Gartner, IEEE, MIT and other sources. We have observed that today, technology management demands a rational balanced approach for the benefits and sustainabilities of the humanity globally. There is too much focus on information and communication technology; but less focus on other critical domains such as biomedical and electrical engineering, nanotechnology, earth and space science.

Next, we have selected ten potential strategic technologies for humanity. which have significant impact on our society globally. The most of these technologies are at emergence phase of TLC; the others are passing through growth phase. As a part of learning-by-doing approach; we have analyzed these nine cases using '7-S' model and have backtracked to redefine the initial framework of deep analytics. We have found out several open research agendas: (a) Should We consider any additional elements for the proposed deep analytics which can streamline the evolution and diffusions of various technological innovations effectively? For instance the deep analytics may be 10-S model instead of 7-S in figure 1.1. (b) Is it practically manageable to consider too many elements simultaneously? Should we consider resources instead of staff – resources? Should we decompose sixth element into skill, style and support separately? Should we position the element 'system' centrally or 'strategy' in figure 1.1? (c) There are ${}^{7}C_{2}$ links (such as S1-S7, S2-S7,S3-S7,S4-S7, S5-S7, S6-S7....) among 7-S elements of the deep analytics; what are the implications of these links on complex technological innovations? There may be other various types of links considering ${}^{7}C_{3}$,${}^{7}C_{4}$,${}^{7}C_{5}$ and ${}^{7}C_{6}$ combinations (S1-S2-S3, S4-S5-S6-S7 ....). (d) How do these elements of deep analytics impact technological innovation in terms of technology trajectory, spillover, dominant design and organizational learning process? (e) How to foster creativity, problem solving capability, learning rate, generalizability, convergence and stopping criteria in organizational learning? What are the major constraints and barriers against nine cases of technological innovations? There are several open issues of debate on the concept of deep analytics. It is an interesting observation from this book that we are living in 21st century today; but we could not reach the point of saturation at present; extensive R&D efforts are still pending for the sustainability of human civilization in the coming future.

2. SCOPE

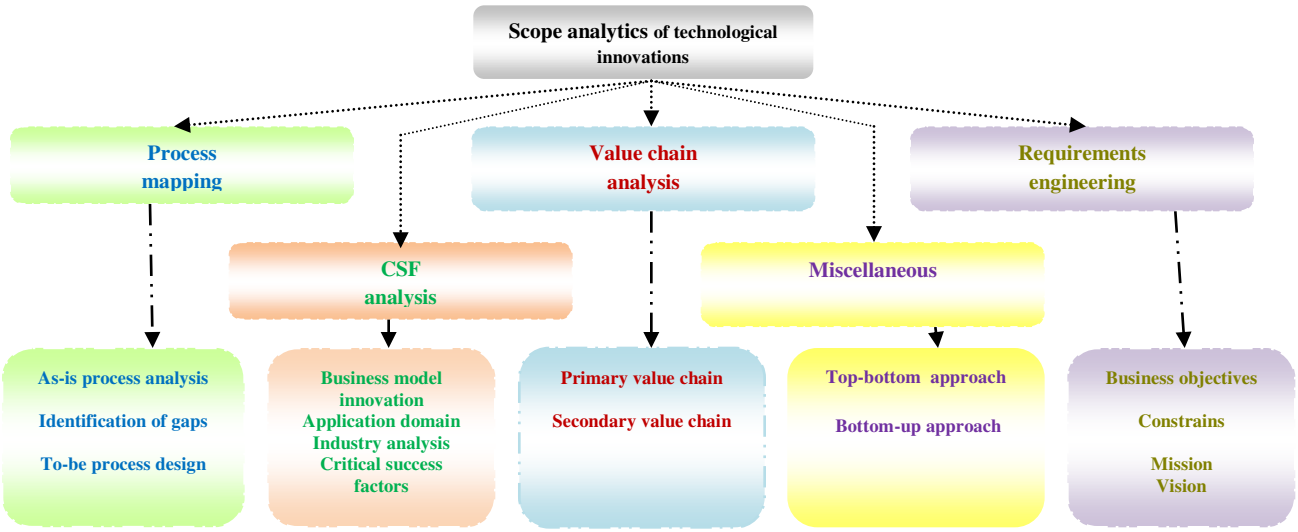


Figure 1.2 : Scope analytics

Technological innovation is basically associated with new product development and new process innovation, act and initiatives of launching new devices, methods or materials for commercial and practical applications. It is one of the most critical competitive drivers in many industries such as information and communication technologies, high technology manufacturing and life-science. Deep analytics explores miscellaneous issues of top technological innovations today such as dynamics of innovation, innovation strategy and implementation process; the impact of globalization of markets and advanced information and communication technologies, computer sided design, computer aided manufacturing, flexible manufacturing system, economic feasibility, economies of scale and short production run; technology life cycle, technology diffusion; social, environmental and economic effects, negative effects of technological changes; R&D fund allocation strategy; pace, advantages and disadvantages of innovation, critical success factors, causes of failure; cost optimization and differentiation. Technological innovations are essential to create new business models. But, many innovation projects fail to make profit due to various reasons such as scope creep or ill-defined scope analysis.

The first element of deep analytics is scope [Figure 1.2]. The scope of a technology innovation project should be explored through various scientific and systematic methods such as process mapping, critical success factors (CSF) analysis, value chain analysis, analysis of business objectives, constraints, mission and vision and top-down and bottom-up approaches. Process mapping analyzes a set of critical issues: what is as-is process? How to identify gaps of as-is process? How to innovate to-be process? What are the inputs, outputs, mechanism and constraint for each task associated with a business process? How to configure process flow diagram? The basic objective of CSF analysis is to identify a set of critical success factors through business model innovation, application domain and industry analysis.

The scope of a technology innovation project is explored based on CSFs. The basic objectives of value chain analysis is to find out a set of critical parameters: what is value; it may be product differentiation, cost leadership or improved quality of services? How to define value in a technology innovation? What are the activities associated with primary and secondary value chain? Primary activities add value to a product and service directly such as manufacturing and supply chain management; secondary value chain activities (e.g. HR, Maintenance) support primary value chain activities. Top bottom approach analyzes business plans and goals of a firm, defines the basic needs of a system and explores the scope of technology innovation projects. On the other side, bottom up approach analyze as–is system, identifies gaps and explores the basic needs or scope of a project.

The scope of a technological innovation should be explored through industry analysis and also external environment and various stakeholders associated with the value chain. In this connection, Porter's six force model is useful to assess the bargaining power of the customers and suppliers, role of compliments, threats of new entrants and substitutes and competition. The internal environment should be accessed through SWOT analysis, identification of core competencies and rigidities, dynamic capabilities, potential strength and opportunities of sustainable competitive advantages. The scope should be also explored in terms of strategic intent, vision, mission and goals from different perspectives such as process innovation, organization learning, financial performance and customer satisfaction.

The scope of technological innovations may be analyzed from the perspectives of product or process innovation, radical or incremental, architectural or component and competence enhancing or destroying innovation. Product innovations occur in the outputs of a firm as new products or services. Process innovations try to improve the efficiency of business or manufacturing process such as increase of yield or decrease of rejection rate. Component or modular innovation changes one or more components of a product. Architectural innovation changes the overall design of a system or the way the components of a system interact with each other. Radical innovation is new and different from prior solutions. Incremental innovation makes a slight change of existing product or process.

We have explored a set of innovative concepts such as technology for humanity, cancer genomics, separating chromosomes, DNA computing, large scale cheap solar electricity and photovoltaics technology, solid state batteries, synthetic cells, next generation predictive, collaborative and pervasive analytics, big data analytics, adaptive security and dynamic data protection, smart transformers, applied AI and machine learning, deep learning, assisted transportation, Internet of Things (IoT), cloud computing and cloud streaming, Internet of bodies, Blockchain and distributed ledger technology, homomorphic encryption, crash-proof code, social indexing, gestural interfaces, social credit algorithms, advanced smart material and devices, activity security protection, virtual reality, chatbots, automated voice spam prevention, serverless

computing, edge computing, real-time ray tracing, digital twins, tablets and mobile devices in enterprise management, innovative mobile applications and interfaces for a multichannel future, human computer interface, context aware computing and social media, enterprise app stores and marketplaces, in-memory computing, extreme low energy servers and strategic global sourcing.

3. SYSTEM

The second element of deep analytics is system [Figure 1.3]. A system is a complex grouping of interrelated parts i.e. machines and agents; it can be decomposed into a set of interacting sub-systems. A system may have single or multiple objectives; it is designed to achieve overall objectives in the best possible way. It is possible to analyze a system from the perspectives of system state, complexity, model, environment, system dynamics, cause effect analysis, feedback loop, physical and information flows and policy decisions [35-41]**.** A system may be open or closed loop. A hard system has clearly defined objectives, decision making procedures and quantitative measures of performance. It is hard to define the objectives and qualitative measures of performance and make decisions for a soft system. The state of a system at a specific time is a set of relevant properties of the system. The complexity of a system can be analyzed in terms of number of interacting elements, number of linear and nonlinear dynamic relationships among the elements, number of goals or objectives and number of ways the system interacts with its environment. A model is an abstraction of real system. A model is isolated from its environment through model boundaries. A model may be static or dynamic, linear or non-linear based on functional relationship among various variables in a model.

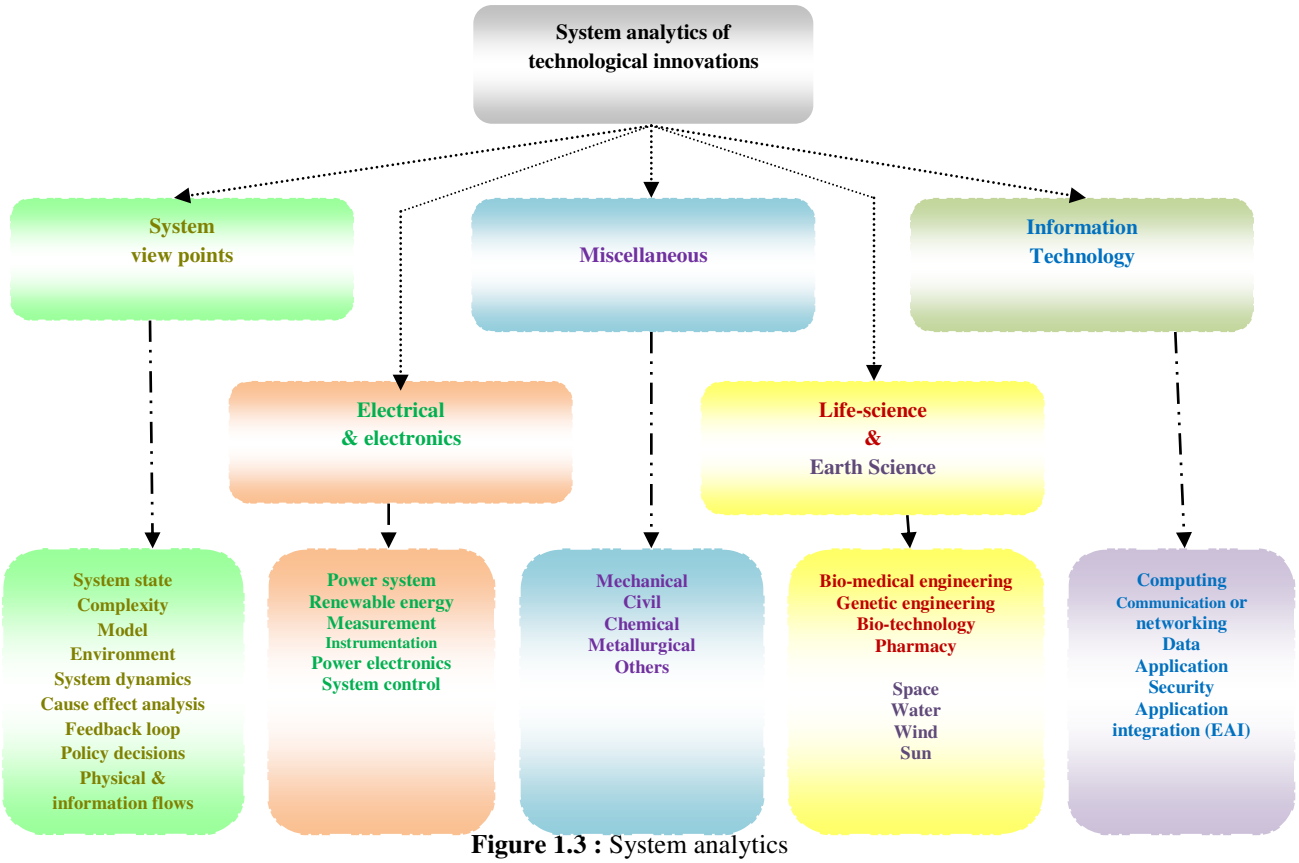


Figure 1.3 : System analytics

A complex system can be analyzed from the perspectives of different branches of engineering and technology such as information and communication technology, electrical and electronics, mechanical, civil, chemical, metallurgical, biotechnology, genetic engineering, pharmacy and others. IT system can be analyzed in terms of computing, communication or networking, data, application and security schema and also application integration (EAI). An electrical system may have various subsystems such as power system, renewable energy, photonics, system control, power electronics, machines, measurement &

instrumentation, illumination and high voltage engineering. A complex system may be associated with various domains of earth science such as space science, water, wind and solar power.
The basic objectives of system analytics are to analyze complex, dynamic, non-linear and linear interactions in various types of systems and design new structures and policies to improve the behavior of a system. A system is associated with a problem oriented model; the basic building blocks of system dynamics are cause effects analysis, positive and negative feedback loops and physical and information flows. The basic functions of system analytics include defining a problem and model boundary, building model, testing and validation of a model, model analysis, evaluation of policy alternatives and recommendation of most viable R&D policy related to technological innovations [42].

4. STRUCTURE

The third element of deep analytics is structure i.e. the backbone of a system associated with a specific technological innovation [Figure 1.4]. What are the basic elements of the system architecture associated with a technology innovation? It has two critical viewpoints: system architecture and organization structure. The first one considers technological aspects of the system architecture in terms of topology, smart grid and various components of industrial control system such as SCADA, Expert system, DCS, PCS, SIS, BAS and EMS. The topology of a system should be analyzed in terms of nodes, connectivity, type of connections such as P2P or multipoint, layers, interfaces between layers and organization of layers.
For example, OSI model is a layered framework for the design of communication networks of information systems. It has seven layers from bottom to top : physical, data link, network, transport, session, presentation and application layers. A data communication system has five basic components such as message, sender, receiver, transmission medium and protocol. On the basis of nodes and links, the physical topology of a communication network can be classified into four categories such as mesh, ring, star and bus. The second viewpoint is organization structure – what type of structure is suitable for specific technological innovation; it may be functional, divisional, matrix or network structure. Is there any link between technology and organization structure? It depends on the characteristics of business model.
Another view of structure should be explored in terms of organization structure, size of a firm, economies of scale in R&D, access to complementary resources such as capital and market, governance mechanisms and organizational learning. There are various types of organization structure such as divisional and networked models. The efficiency and creativity of innovation model is closely associated with different types of structural dimensions such as formalization, standardization, centralization, decentralization and loosely coupled networks within and between firms. Global firms should consider several critical factors such as knowledge, resources and technological diffusion to conduct R&D activities.

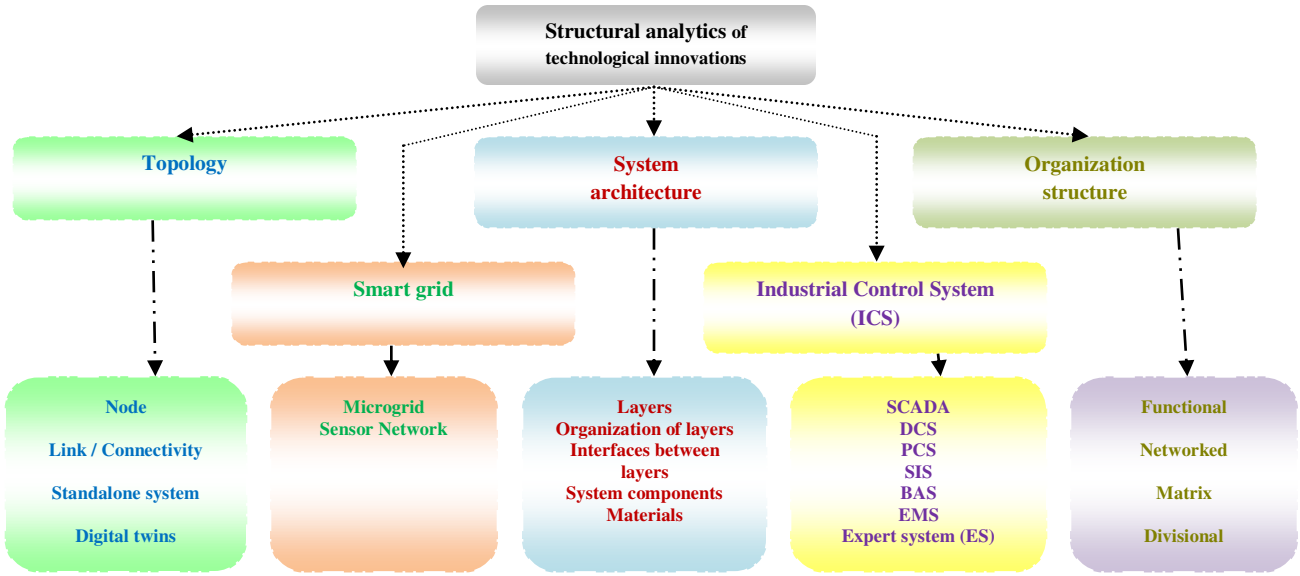


Figure 1.4: Structure analytics

How is it possible to represent the structure of a system associated with a technology innovation correctly and transparently? Digital twins may be an interesting solution; it integrates the concept of industrial IoT, AI, machine learning and software analytics to optimize the operation and maintenance of physical assets, systems and manufacturing processes. A digital twin is the digital replica of a living or non-living physical entity (e.g. physical asset, process, agent, place, system, device); it is expected to bridge and support data sharing between the physical and virtual entities. Digital twins can learn from multiple sources such as itself through sensors, historical time series data, experts and other nodes of the networking schema of the system and get updated continuously to represent real-time status, working conditions or positions.

The concept of digital twins are expected to be useful for manufacturing, energy (e.g. HVAC control systems), utilities, healthcare and automotive industries in terms of connectivity, digital traces and product life-cycle management. The concept can be used for 3D modeling to create digital companions of the physical objects i.e. an up-to-date and accurate copy of the properties and states of the objects (e.g. shape, position, gesture, status, motion) based on the data collected by the sensors attached to the system. It may be useful for the maintenance of power generation equipment such as turbines, jet engines and locomotives; monitoring, diagnostics and prognostics to optimize asset performance and utilization through root cause analysis and to overcome the challenges in system development, testing, verification and validation for automotive applications. The physical objects are virtualized and can be represented as digital twin models seamlessly and closely integrated in both physical and cyber spaces. Digital twins should represent the structure of a product innovation intelligently through various phases of the product life-cycle.

Another interesting technology for exploring innovative structure is **V-commerce** through virtual (VR), mixed (MR) and augmented reality (AR). A virtual entity may not exist physically but created by software in a digital environment. VR and AR are sophisticated, creative and powerful tools to show complex structures and offer a complete computerized digital experience by integrating AI, computer vision, graphics and automation in various applications such as manufacturing, retail, healthcare, entertainment, furniture and interior decoration.

5. SECURITY

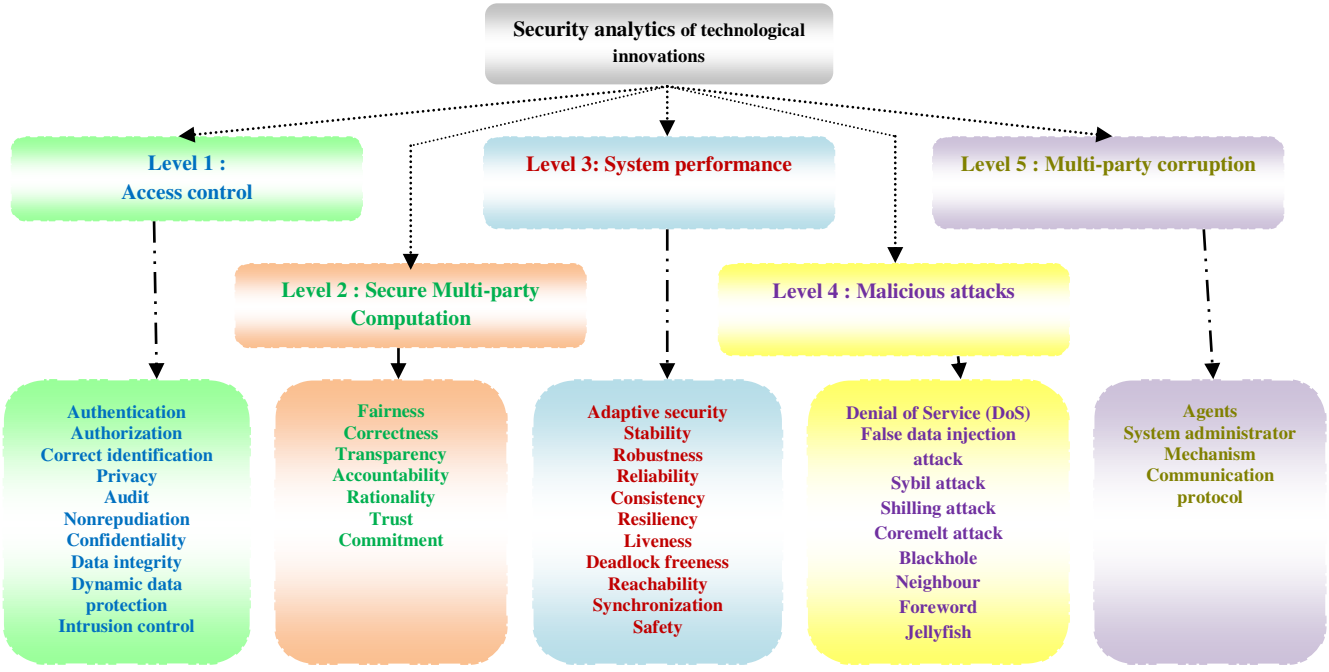


Figure 1.5 : Security analytics

The fourth element of deep analytics is security. **What do you mean by technology_ security?** A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion and. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks.

Let us explain the objectives of adaptive security architecture in depth. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The systems demand continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

How to verify the security intelligence of the system associated with an emerging technology? It is essential to verify security intelligence of a technological innovation collectively through rational threat analytics at five levels : L1, L2, L3, L4 and L5 (Figure 1.5).. The basic building blocks of the security element are an adversary model and an intelligent threat analytics. An adversary is a malicious agent who attacks a system or a protocol; the basic objectives are to cause disruption and malfunctioning of a secure system. The security element should be analyzed in terms of the assumptions, goals and capabilities of the adversary. It is also crucial to analyze the adversary model in terms of environment, location, network, resources, access privileges, equipments, devices, actions, results, risks, reasons and motivations of attacks and probable targets (i.e. why the adversary attacks and to obtain what data).

Let us consider the security of an information system innovation. At level L1, it is required to verify the efficiency of access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, non-repudiation and data integrity. For any secure service, the system should ask the identity and authentication of one or more agents involved in a transaction. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries.

After the identification and authentication, the system should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication.

Privacy is the primary concern of the revelation principle of an information system; the issue of secure private communication can be addressed through the concept of cryptography, digital signature, signcryption and secure multiparty computation. The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. Data integrity ensures that data is protected from unauthorized modifications or false data injection attack. The system should provide public verifiability so that anyone can verify the integrity of the data. Redundancy of data is a critical issue which is resulted through replication across the writers.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. But there are other different types of security concerns. At level L2, it is required to verify the efficiency of secure multiparty computation associated with a technological innovation in terms of fairness, robustness, correctness, transparency, accountability, trust and commitment. A protocol ensures correctness if the sending agent broadcasts correct data and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with the commitment, honesty and rational reasoning on payment function, trust and quality of service. Fairness ensures that something

will or will not occur infinitely often under certain conditions. The recipients expect fairness in private communication according to their demand plan, objectives and constraints. The sending agent expects fairness from the recipients in terms of true feedback and commitment on confidentiality of data. As per traditional definition of fairness of secure multi-party computation, either all parties learn the output or none. The system must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. In fact, accountability is also associated with collective intelligence. Transparency is associated with communication protocols, revelation principle and automated system verification procedures. For example, a mechanism should clearly state its goal to define a policy. There exist an inherent tension between transparency and privacy. A fully transparent system allows anyone to view any data without any provision of privacy. On the other side, a fully private system provides no transparency. Privacy can be achieved using cryptographic techniques at increased cost of computation and communication. Is it possible to trade-off privacy vs. transparency? Is it possible to provide public verifiability of its overall state without disclosing information about the state of each entity? Public Verifiability allows anyone to verify the correctness of the state of the system.

Next, it is required to verify the system performance at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety. The performance of a system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Safety is a critical requirement of any system whether it may be mechanical, electrical, electronics, information technology, civil, chemical, metallurgical or instrumentation engineering. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. Another important issue is robustness of a system. The delivery of the output should be guaranteed and the adversary should not be able to threaten a denial of service attack against a protocol.

At level L4, it is required to assess the risks of various types of malicious attacks by adversaries on a system such as Denial of Service (DoS), false data injection attack, sybil attack, shilling attack, coremelt attack (or network traffic congestion), blackhole, neighbor, node deletion, rushing and jellyfish attacks. At level L5, it is required to assess the risks of various types of corruptions such as agents (e.g. sending agent, receiving agents), system administrator, communication protocol and payment function of a mechanism associated with a technological innovation.

For example, prevention and detection are traditional approaches to the security of a system. In today's world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt cloud based solutions and open application programming interfaces also. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture.

Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

6. STRATEGY

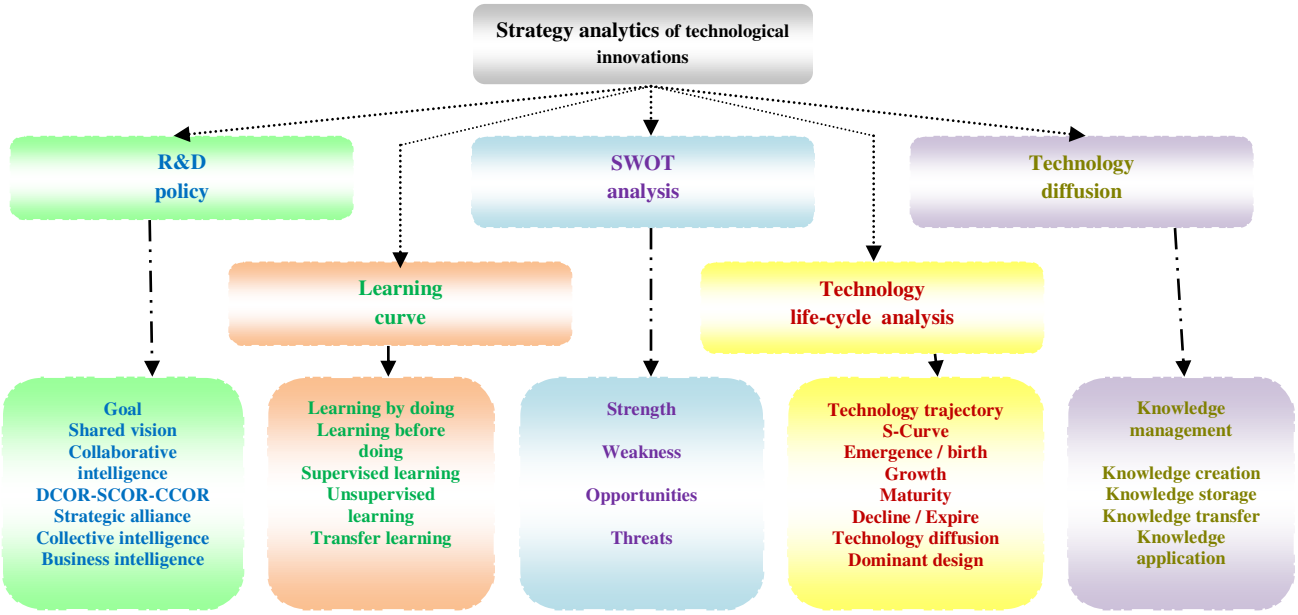


Figure 1.6: Strategy analytics

The fifth element of deep analytics is strategy [Figure 1.6]. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovations are closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of top innovations today. Diffusion is the movement of molecules from high density zone to low density zone of a solution. Can an emerging technology diffuse in the same way globally? What is the pressure acting on technology diffusion? Is the external pressure natural or artificial? Another analogy is osmosis where the molecules move from low density zone to high density zone through a barrier? Can the emerging technology spread and move from low to high density zone smoothly like osmosis or reverse osmosis?

Technological innovation is closely associated with R&D policy and organizational learning strategies in new product development and process innovation. There are various strategies of learning such as learning-by-doing and learning-before-doing [6,7]. Learning by doing is effective in semi-conductor manufacturing and bio-technology sectors which demand low level of theoretical and practical knowledge. On the other side, learning-before-doing is possible through various methods such as prototype testing, computer simulations, pilot production run and laboratory experiments. It is effective in chemical and metallurgical engineering where deep practical and theoretical knowledge can be achieved through laboratory experiments that model future commercial production experience.

Let us explore the role of deep analytics on technological innovation. It is interesting to analyze the impact of different learning strategies and timing of technology transfer on product development performance, process re-engineering and R&D cost of top technological innovations. It is important to compare the effectiveness of various types of learning strategies in terms of cost, quality and time. It is also critical to analyze the relationship between process innovation and learning curve in terms of dynamic cost reduction and improvements in yield. In case of learning-by-doing, it is possible to acquire knowledge of new process development in specific production environment. But, some knowledge may be lost when a new process is transferred to commercial production environment. It is also interesting to analyze the impact of dedicated process development facilities, geographic proximity between R&D lab and production plant and the duplication of equipment between development and production facilities on practical implementation, speed and effectiveness of top technological innovations. It is essential to identify the critical success

factors (e.g. resource allocation, ERP and SCM strategies) that influence the rate of learning and superior performance.

6.1 SWOT Analysis

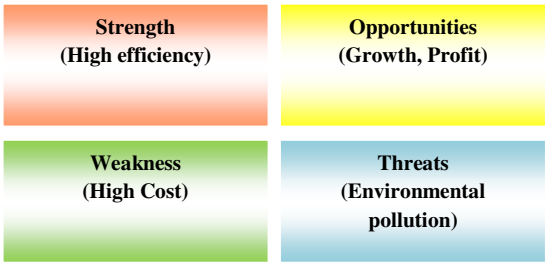


Figure 1.7 : SWOT Analysis

It is rational to evaluate strength, weakness, opportunities and threats of a technological innovation [Figure 1.7]. There may be major and minor strengths and weaknesses. Strength indicates positive aspects, benefits and advantages of a strategic option. Weakness indicates negative aspects, limitations and disadvantages of that option. Opportunities indicate the areas of growth of market and industries from the perspective of profit. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses.

6.2 Technological life-cycle analysis

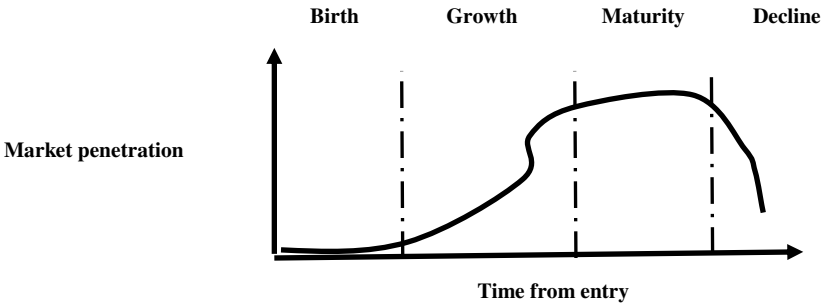


Figure 1.8 : Technology life–cycle analysis

Deep analytics evaluate and explores top technological innovations in terms of technology life-cycle, technology trajectory, S-curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, each technology emerges, grows to some level of maturity and then declines and eventually expires [16, Figure 1.8]. It is essential to evaluate the status of each technological innovation through TLC analysis. Some technologies may have relatively long technology life-cycle; others never reach a maturity stage. Emergence of new technologies follows a complex nonlinear process. It is hard to understand how the technology life-cycle interacts with other technologies, systems, cultures, enterprise activities and impacts on society. All technologies evolve from their parents at birth or emergence phase; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early phases, it adapts and forwards to its intended environment with the emergence of competitors. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. The final stage is decline and phase out or expire; all technologies eventually decline and are phased out or expire at a substantial cost. TLC may have other different types of phases such as acquisition, utilization, and phase-out and disposal; preparation or initiation, implementation and operation; organization, directive, delegation, coordinate, collaborative, and dissolution; acquisition; emergence, diffusion, development, and maturity.

Let us consider the analysis of the performance of a new technology vs. effort; it is basically an S-curve. Initially, it is difficult and costly to improve the performance of a new technology. The performance begins to improve with better understanding of the fundamental principles and system architecture. Finally, the technology approaches its inherent limits with diminishing returns. Next, let us analyze the adoption of a new technology over time which is also an S curve. Initially, a new technology is costly for the adopters due to various uncertainties and risks. Gradually, this new technology is adopted by large segments of the market due to reduced cost and risks. Gradually, the diffusion of new technology slows with the saturation of market or due to the threats imposed by other new technologies.

The rate of improvement of a new technology is often faster than the rate of market demand over time; the market share increases with high performance. Technological change follows a cyclical pattern. The evolution of a technology passes through a phase of turbulence and uncertainty; various stakeholders of a supply chain explore different competing design options of the new technology and a dominant design emerges alongwih a consensus and convergence of structure. Then, the producers try to improve the efficiency and design of products based on stable benchmark of the industry. The dominant design considers an optimal set of most advanced technological features which meet the demand of the customer, supply and design chain in the best possible way.

Technology trajectory is the path that a technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of top innovations today. How to manage evolution of technological innovation? The nature of innovation shifts markedly after a dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow an S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by technologies. Technology diffusion indicates how new technologies spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards.

7. STAFF-RESOURCES

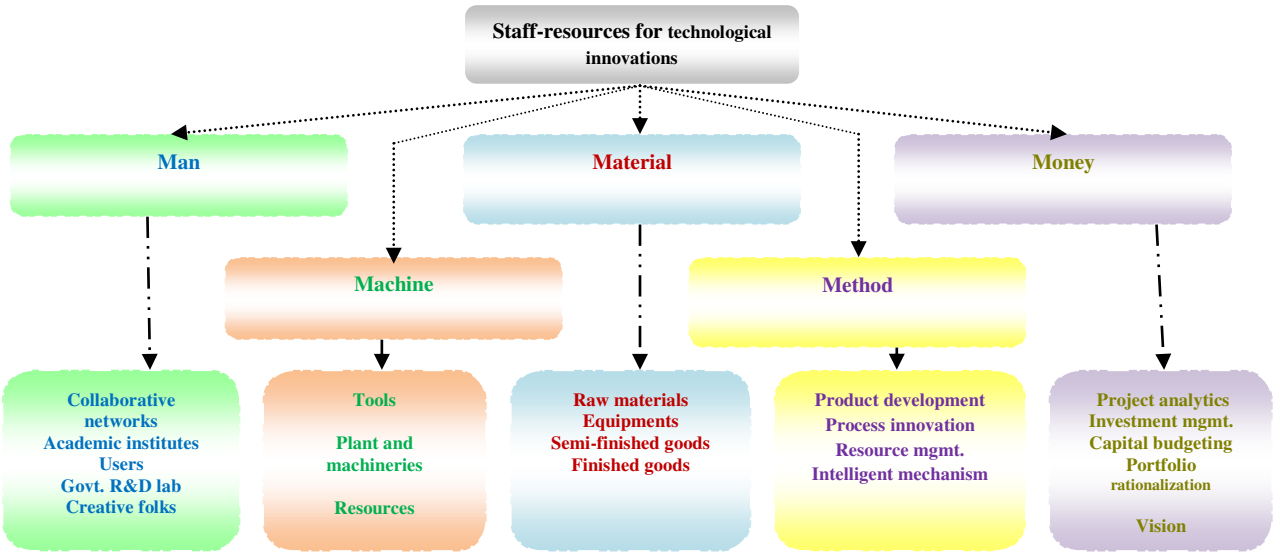


Figure 1.9 : Staff-resources analytics

Figure 1.9 outlines the sixth element of deep analytics i.e. staff-resources in terms of 5M – man, machine, material, method and money [23,54]. 'Man' analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive and performance evaluation. 'Machine' analyzes the basic aspects of tools and automated / semi-automated / manual machines; 'material' analyzes planning of raw materials,

equipments, semi-finished and finished goods. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure. Finally, 'money' highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

It is crucial to analyze dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion such as 5M i.e. man, machine, material, method and money; dominant design factors, effects of timing and mode of entry. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment.

Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers or clients or private nonprofit organizations may innovate new products or services based on their own needs. Many firms set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities define sound research mission and vision and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators).

A complex technological innovation often needs collaborative intelligence to manage the gap between demand and supply of a specific set of capabilities, skills and resources [29]. It is possible to control cost, speed and competencies of technological innovations through efficient sharing mechanisms. It is rational to share the cost and risks of new innovations through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem. There are different modes of collaboration such as strategic alliance, joint ventures, technology licensing, outsourcing and collective research organizations. Collaborative networks are other sources of innovation. Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms [34]. But, it may be hard to control the development of product and process innovation protecting IP of proprietary technologies. The critical success factors of collaborative networks may be the right selection of innovation partners having strategic and resource fit, transparent and flexible monitoring and governance process so that the innovation partners understand their rights and obligations. .

Technological innovation demands the motivation and commitment of creative people. For example, the evolution of electronics and communication technology has been possible because of the involvement of the creative and efficient engineers and scientists in related domains. Most of top technology innovations are not trivial problems; need useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. The impact of knowledge on creativity is double-edged. Lack of knowledge is a major constraint to the original contribution in a technological innovation. But, extensive knowledge may be biased and trapped in existing logic and paradigms. It is difficult to conclude that moderate knowledge is adequate for creativity. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routines, performance evaluation, compensation, reward and incentive policy, social processes and contextual factors.

7.1 Resource Allocation Analytics

When the capacity of a firm is more than the total demand of a set of technological innovation projects, the resource manager may like to allocate the required resources such as fund or capital to each project using suitable resource allocation model. However, when the capacity is less than total demand, the resource manager would have to find the combination of projects, which would fit the resource allocation model and

give maximum benefit. There are three different types of resource allocation protocols: linear, proportional and selective allocation.

***Linear allocation*:** It is an equal sharing of the pain i.e. shortage of capacity of capital among a set of projects. If that pain exceeds the actual demand of a project, then the project becomes passive. The project P_i is allocated $q_i = d_i - (1/n) \max (0, \sum_{i=1}^{n} d^*_i - C)$ where n is the number of active projects, C is the capacity of capital of the client.

***Proportional allocation* :** The project P_i is allocated $q_i = \min \{d^*_i, C.d^*_i/(\sum_{i=1}^{n} d^*_i)\}$. Here, n is the number of active projects and C is the total capacity of capital of the client. If the demand is more, more capital will be allocated to that project proportionately.

Selective allocation : It is basically priority based portfolio rationalization where the capital is allocated as per the priority of a set of technological innovation projects. It is an interesting problem to find the allocation of the projects while maximizing the utility of the client under capacity constraints. This is basically a knapsack problem. Let $\{(u_1,d^*_1),(u_2,d^*_2), ..,(u_n,d^*_n), C\}$ be an instance of the *knapsack problem* – C is the knapsack capacity i.e. total capacity of capital of the client; (u_i,d^*_i) are respectively the utility and demand of capital of the project i. The goal is to choose a subset of projects of maximum utility with total demand of capital at most C. According to this resource capacity allocation strategy, all the projects are not treated equally. In case of any shortage of capacity, several projects may become infeasible. The projects are ranked based on utility and priority and the capital is allocated as per the rank of the projects.

The business analysts should consider a financial investment framework for optimal resource allocation and project portfolio rationalization along two dimensions: strategic objective and technology scope [Figure 1.10]. There are four cells: transformation, experiments, process improvements and renewal [52]. Most of the technology innovation projects fall in transformation and experiments cells. The basic objectives of transformation projects are growing need of application integration, end-to-end business process re-engineering and improved support. It demands process change. But, during economic downturn, it may be a costly option. The expected benefits are efficient customer service, greater accuracy and long-term growth. The basic objectives of experiments are to adopt new business models using new technology; the expected benefits are change of organization structure, infrastructure and business process improvements. The basic objective of process improvement is to yield more profit from improved operational performance. The process owner or a functional unit realizes benefits such as short term profitability. The basic objective of renewal is to replace old shared technology with new cost effective powerful technology maintaining the existing infrastructure and keeping it cost effective. The expected benefits are improved maintainability, reduced support and efficient capacity utilization.

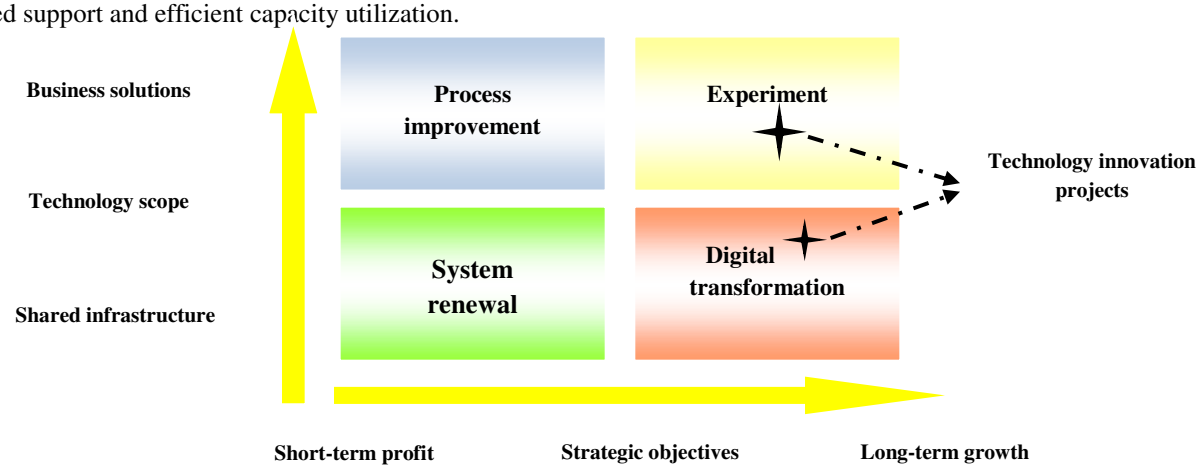


Figure 1.10 : Financial Investment Framework

Resource allocation and mobilization are two critical aspects of project management. It is possible to call different types of logic such as linear, proportional and selective resource allocation (as stated above)

subject to shortage of capacity. Each strategic project defines a set of objectives, strategies and demand plans and then the resources are allocated to different projects according to the demand plans. It is basically the principle of management by objectives (MBO) which commits the reservation of different types of financial, non-financial and human resources. The sick projects may need new investment for turnaround and renewal; the star projects may need additional fund for continuous strategic growth; the emerging projects may need capital for appropriate technology management and skill development. The old dead assets should be divested; wastage of energy, utilities, materials and products should be minimized and existing capacity should be utilized intelligently.

The resources are generally allocated to different business units through various types of budgeting such as capital budgeting, performance budgeting, zero based budgeting and strategic budgeting. Capital budgeting is decided based on payback period, NPV, IRR and profitability index. Zero based budgeting evaluates the particular demand and need of each project. It involves identification of decisive projects, analysis of each decisive project, ranking of the demand of each project and then allocation of resources. Strategic budgeting asks a set of fundamental questions: What is the goal of a project in terms of performance and results? What are the key activities or tasks to be done to achieve the goal? The management should be cautious of the risk of resource allocation such as limited resource capacity, competition and past commitments.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support [Figure 1.11]. The workforce involved in top technological innovations are expected to develop different types of skills in technical, management and medical science domain such as research and development, knowledge management, new product development, process innovation, team management, design, protection of innovation, project management, supply chain management, sales and marketing, event management, construction, erection, testing, commissioning, product and service maintenance. The intellectual rights of technological innovations are protected through patents, trademarks, trade secrets and copyrights. The diffusion of the new technological innovation depends on the skills and capabilities of a group of firms in production, promotion and distribution of the new products and services globally.

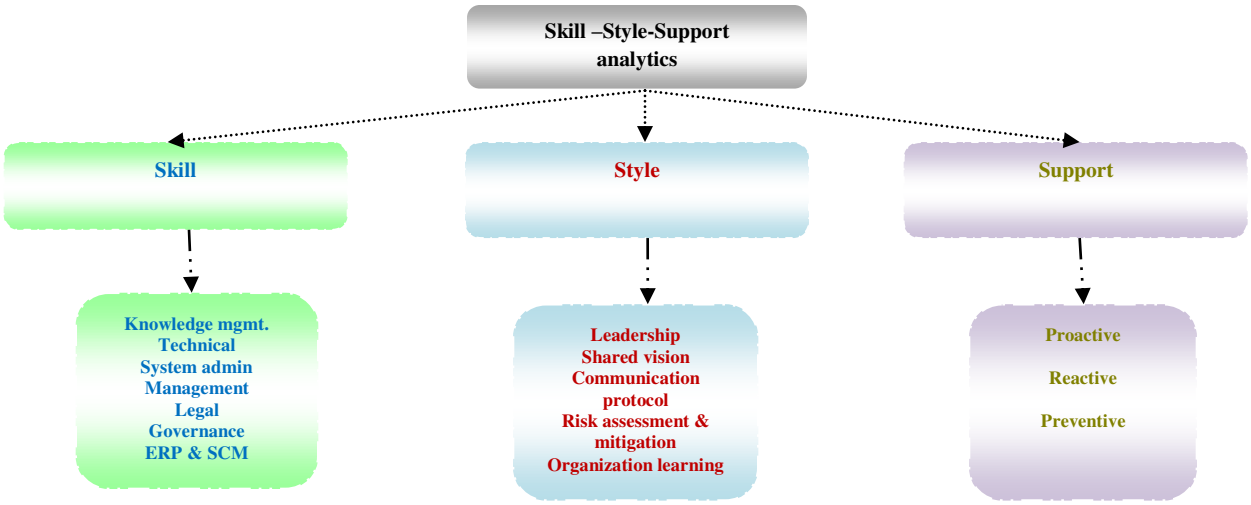


Figure 1.11: Skill-style-support analytics

The system administrators must have leadership skills in smart thinking, communication, coordination and change management. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and

application of knowledge in a transparent, collaborative and innovative way. The life-cycle of a technological innovation also depends on the intelligence of marketing strategies such as branding, promotion, advertising, launching time, pricing mechanism, product quality, profit margin, compatibility and market share. It is important to analyze market segmentation, cost of advertising and promotion, reach, information content and duration of exposure.

The diffusion of top technology innovations needs the support of great leadership style; they are not only industry leaders but also political one. The style is basically the quality of leadership; the great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. The leaders must be able to share a rational vision; mission and values related to top technology innovations among all the stakeholders honestly and appropriately in time. It is really challenging for the great leaders to implement top technological innovations physically and practically in the form of commercial products and services. They have to face and tackle threats from traditional industries. Top management must tackle the complexity of system implementation by developing a dedicated project team, a right mix of committed resources and talents like technical and business experts.

What should be the right organization model for top technological innovations? A traditional functionally centered organization model may not be suitable for supporting end-to-end business processes. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common, customer oriented goal. The business models of top technological innovations require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement. The structure of process enterprise requires a collaborative and cooperative work culture. Top innovations need proactive, reactive and preventive support for proper technology management.

8.1 Innovation Model

What should be the innovation model for effective diffusion of an emerging technology? Is it possible to adopt K-A-B-C-D-E-T-F model?

- ***Knowledge manager***: The innovators should acquire the basic and fundamental concept through a *differentiated* course work; classify the primary, secondary and tertiary focus areas. Mandatory courses: Innovation, creativity and research methodology; communication. The depth and breadth of the course works should be traded off rationally. It needs proper guidance.
- ***Activator***: The activators should initiate the innovation process by identifying a good research problem through scope analysis. Random selection of research problem should be avoided by evaluating the strength, experience and skill of the innovators. The research problem should have potential business intelligence and social benefits.
- ***Browser***: The browsers should search for information; investigate throughout the process and find relevant data or information to start innovation. They may review and analyze the existing works through traditional sources of research data (e.g. digital library, books, papers, journals, magazines, industry reports, you tubes) and also through webinars, social networking and attending seminars, workshops and conferences. Random search may result wastage of time; a systematic and planned / guided search process may lead to good results.
- ***Creator***: The creators should analyze the gap and think of to-be system; generate new ideas, concepts and possibilities and search for new solutions.
- ***Developer***: The developers should transform the ideas of the creation phase into good solutions; turn the ideas into deliverables, products and services. They should collaborate with different research forums, industries and experts during this phase.
- ***Executor***: The executors should implement and execute the roadmap of the innovation.

- ***Tester**:* The testers should do various types of experiments and laboratory works; verify system dynamics and monitor the performance of the deliverables. Advanced research laboratories are required for complicated testing and experiments.
- ***Facilitator***: The facilitators should define project plan, corporate governance policy, marketing plan, production plan, investment plan and cost-benefit analysis. They should be able to identify the revenue and profit making stream and fair, rational business intelligence. The government should provide financial assistance to the innovators in patent registration.

8.1 Project Management Skill & Style

Traditional approaches to project management focus on long-term planning and stability to mitigate various risks. But, complex technology innovation project management needs a mix of traditional and agile approaches to cope with uncertainties [43-49]. The intension driven role develops collaboration. The event driven role integrates planning and review with learning. The other important roles of the project managers are to prevent major disruptions and maintaining forward momentum continuously. They must acknowledge the emergence of a problem and then try to minimize the frequency and negative impact of unexpected events in a dynamic environment. They must be people, information and action oriented.

Traditional project management approach follows four steps such as definition, planning, execution and termination. But, no projects are so linear. Once project execution starts, reality may demand exception management i.e. the adjustment and amendment in the planning or definition phases. Each industry has a different profile of risk. Deep analytics is applicable to both adaptive and linear project management approaches for technology innovation. Many projects fail due to conventional approach which may not adapt to a dynamic business environment. It is very crucial to identify the scope of a project rationally through feasibility study and cost-benefit analysis. It is essential to identify the primary and secondary scopes through portfolio rationalization and analysis of priority, novelty, objectives and constraints of a set of projects. Perception based emotional and readymade thoughts may affect the correctness of scope analysis. Scope creep is a serious concern in project management. It is not a simple task to tackle uncertainties and complexities in time and resource constrained project management for top technological innovations.

Novelty indicates how intensely new innovations are crucial aspects of a project. A project should be assessed on the scale of sophistication of technology, which may be low, medium or high. Another critical factor is the complexity of the project in terms of product, service and process. Pace indicates the urgency of a project which may be normal, fast, time critical or blitz. Different projects have varying degrees of newness or novelty. A derivative product development project may have low risk and few future concerns. The new version of an existing product needs detailed analysis and market research.

Breakthrough product development projects face high risks. Each project is unique, but not in every respect and may have some common features. The uncertainty in a project is a measure of the mix of new and mature technology and existing knowledge base; it may arise from technological aspects, new service offering or new market segments. High technology projects are subject to time delays, cost overruns and risks of product failure. The complexity base measures three different types of complications within a project such as assembly (low), system (medium) and array (high). High complexity requires efficient coordination and integration among various phases and systems of a project. Pace indicates a sense of urgency and time sensitivity. The failure of time critical projects results from the violation of milestone deadlines and related opportunity loss; blitz projects are crisis projects with extremely urgent timing. There are various strategies for optimal pace management such as contingency plans, alternative solutions in parallel, resilient approach and business cases to manage emergency and to overcome uncertainties and unexpected surprises.

A technology innovation project may be delivered on time and budget through the efforts, skill and professionalism of the project managers. But, it may not meet the needs of the end customers due to uncertainty and misunderstanding. The basic objective of the deep analytics is to figure out the actual structure of a project as compared with the existing capabilities, the gap and the measure of project success in terms of efficiency, impact on the customer, impact on the team, business success and preparation for the future. It is rational to take both short and long term view of a project plan since success may change during the life-cycle of a project with the change of environmental parameters and information. Does anything change from a future point of view? Does a project have sufficient flexibility to adapt to new requirements

of a dynamic business environment? Are the incentives aligned properly with customer satisfaction, system performance, deadline and budget requirements? The deep analytics is useful to find the gaps between as-is and to-be requirements of a project, efficient resource planning, uncertainty and risk management. Correct use of deep analytics clearly highlights low-medium-high benefit opportunity and low-medium-high risk difficulty.
The feasibility and opportunities of a technology innovation project are estimated through real option, DEA, net present value (NPV) or internal rate of return (IRR). But, it is hard to compute discounted cash flows due to inherent risks and uncertainties associated with an innovation of new technology. Data envelopment analysis combines qualitative and quantitative measures; it is basically a multi-criteria decision making approach.

8.1.1 Project Analytics

Classical models of resource constrained project scheduling problems are not adequate to solve real world problems due to increased complexities and uncertainties. Intelligent project analytics are essential for complex, fuzzy, stochastic, multi-mode, time and resource constrained project scheduling problems with multiple objectives. This work explores how to apply the concept of intelligent deep analytics for project management. Efficient project management requires coordination and integration among various elements. It is essential to define the scope of a project correctly through feasibility study, priority and cost-benefit analysis.

8.1.2 Project Performance: KPIs and Data Visualization Strategy

It is essential for an efficient project manager to understand critical metrics and key performance indicators (KPI) and how to identify, measure, analyze, report and manage for the success of a project. KPIs and metrics are displayed in dashboards, scorecards and reports. Project metric is generic but KPI is specific. KPIs give early warning signs of poor project performance if the problems are not addressed appropriately [50]. The project success is measured in terms of time, cost, performance and customer satisfaction [51]. It is difficult to measure and monitor too many project performance metrics. Therefore, it is essential to consider optimal number of performance metrics and KPIs. It is possible to classify the performance metrics and KPIs into four categories.
Category 1 [Operation] : scope creep, project completion stage, flexibility, quality, cost, time, inventory, customer satisfaction; this category is associated with project success and element S_2 and S_3.
Category 2 [Finance] : revenue growth rate, cost reduction, profitability, ROI, payback period, NPV; this category is associated with element S_3.
Category 3 [Human Resources (HR)] : performance, productivity, capacity utilization, skill; this category is associated with element S_3.
Category 4 [Security intelligence] : It is essential to audit fairness and correctness (i.e. accuracy of estimate and measurement) of project plan computation and adjustment as per exceptions based on rationality.

9. TECHNOLOGY FOR HUMANITY

There are some interesting observations on the technology for humanity today.

- How do we define 'Technology for humanity'?
- "In modern society, there is very little discussion about what's needed to fundamentally improve our collective quality of life. How do we evolve our societies into something more productive, more rewarding and more in harmony with our natural environment? Emerging technologies can not only sharply improve the world in which we live, they can alter who we are as human beings, and in this way, they can forever shape and improve our quality of life. The next big tech trend is technology for humanity. It is difficult to find a roadmap from industry, government or academia of what future jobs and the economy might offer to people and what society might look like. By historic measures, future predictions are mostly incorrect. We need a better balance in our

thinking here. There is no reason why man and machine cannot work together, with humans at the controls. There is no reason why we cannot make decent investment returns and create meaningful jobs and new technologies, build communities, and respect the environment. It is definitely about putting the human back into technology-led globalization. 2019 is the year of moving past the hype of emerging tech and building out these technologies. Realistically this involves the critical role of humans in shaping emerging tech to improve the state of humanity. If technology is an enabler, then we need to aggressively deploy it to address the biggest issues concerning humanity with an emphasis on human agency Global goals are a universal call to action to end poverty, protect the planet and ensure that all people enjoy peace and prosperity, that's what we need to achieve with our human and technological superpowers. It is humanity and technology working together that will best solve these problems to meet the objectives. In order to attract the private investment capital to achieve this, we are going to have to better learn how to make acceptable risk-adjusted returns at the same time as eliminating hunger and poverty, creating employment diversity at decent wages, and cleaning up the planet. We can no longer reward behaviors and outcomes that put humanity, communities, and the planet in existential jeopardy. There's no point in arguing about a few percentage points better return on capital when half of the world is underwater." [Reference : Discussion at UN and World Econmic forums]

- How to define 'Sustainable Development Goals' for the sustainability of human civilization?
- Should we focus on a set of path breaking technologies based on top most priorities?
- Is there too much focus on the innovation of digital technology (e.g. ICT) ignoring the basic necessities of life? Can AI and Robotics solve all the problems of our universe?
- We can not deny the progress of technology today but are we at the point of saturation in innovation or lot of works are still pending? "Miles to go before I sleep... Miles to go before I sleep".....
- Can we fight against various types of natural disasters effectively such as flood, drought, earthquake, cyclone, storm, volcano and astronomical hazards effectively with existing technologies?
- Can we manage natural resources such as sunlight, wind, water, soil and others with existing technologies effectively? Pls. think, think, think.....

REFERENCES

1. P. Attewell. 1992. Technology diffusion and organizational learning: the case of business computing, Organ. Sci., 3(1).
2. Basalla, G. 1988. The Evolution of Technology, Cambridge University Press, New York.
3. E.M. Rogers. 1995. Diffusion of Innovations, 4th ed., Free Press, New York.
4. M.W. Cardullo.1996. Introduction to Managing Technology, Vol. 4, J. A. Brandon, ed., Engineering Management Series, Research Studies Press, Taunton, England.
5. D.I. Cleland and W.R. King. 1983. Systems Analysis and Project Management, McGraw-Hill, New York.
6. N.W. Hatch and D.C.Mowery. 1996. Process Innovation and Learning by Doing in Semiconductor Manufacturing. Research policy, 25, 1097-1119
7. G. P. Pisano. 1996. Learning-before-doing in the development of new process technology. USA .
8. W.B.Hirschmann. 1964. Profit from the learning curve. Harvard Business Review. 42(1)125-139,
9. M. Kilbridge, M. 1962. A model for industrial learning. Management Sci. 8.
10. G.P. Pisano. 1997. The Development Factory: Unlocking the Potential of Process Innovation. Harvard Business School Press, Boston, Massachusetts.
11. M.E.Porter. 1980. Competitive Strategy. Free Press, New York.
12. J.D.Teece, G, Pisano and A. Shuen. 1997. Dynamic capabilities and strategic management. Strategic Management . 18(7) 509-533.
13. P.Adler and K. Clark. 1991. Behind the learning curve. Management Science 37(3), 267-281.
14. K.Ulrich and S. Eppinger. 1995. Product Design and Development. McGraw-Hill, New York.
15. E.Hippel and M. Tyre. 1995, How the 'learning by doing' is done: problem identification in novel process equipment. Research Policy 24(1), 1-12.
16. Richard C. Dorf (Ed.).2000. Technology Management Handbook. Boca Raton: CRC Press.

17. R. Adner. 2006. Match Your Innovation Strategy to Your Innovation Ecosystem. Harvard Business Review. April.
18. R. Adner. 2002. When are technologies disruptive: a demand-based view of the emergence of competition. Strategic Management Journal 23(8): 667–688.
19. R. Adner and D. Levinthal D. 2001. Demand heterogeneity and technology evolution: implication for product and process innovation. Management Science 47(5):611–628.
20. R. Adner and P.Zemsky. 2002. Strategy dynamics through a demand-based lens: the evolution of market boundaries, resource rents, and competitive positions. INSEAD working paper series 2003/01/SM.
21. R.Adner and P.Zemsky. 2005. Disruptive technology and the emergence of competition. Rand Journal of Economics 36(2): 229–254.
22. J.M.Utterback and W. Abernathy. 1975. A dynamic model of process and product innovation. Omega **3**(6):639–656.
23. B. Wernerfelt. 1984. A resource-based view of the firm. Strategic Management Journal **5**(2): 171–180.
24. M.A.Schilling. 2017. Strategic management of technological innovation. McGrawhill Education.
25. M.A.Schilling. 2015. Towards dynamic efficiency: Innovation and its implications for antitrust Antitrust Bulletin.
26. M. A. Schilling and C. E. Vasco. Product and Process Technological Change and the Adoption of Modular Organizational Forms. in Winning Strategies in a Deconstructing World, eds. R. Bresser,M. Hitt, R. Nixon, and D. Heuskel (Sussex, England: John Wiley & Sons, 2000), pp. 25–50.
27. H. A. Simon. 1973. Technology and Environment. Management Science 19 (1973), pp. 1110–21.
28. H. Chesbrough. 2003. Open Innovation: The New Imperative for Creating and Profiting from Technology, Harvard University Press, Boston.
29. M.A.Schilling and C.Phelps. 2007. Interfirm Collaboration Networks: The impact of Large-scale Network Structure on Firm Innovation. Management Science 53, pp. 1113–1126.
30. M. Boden. 1992. The Creative Mind: Myths and Mechanisms. New York: Basic Books, 1992.
31. R. J. Thomas. 1995. New Product Success Stories: Lessons from Leading Innovators , John Wiley & Sons, NY.
32. E. Roberts. 2001. Benchmarking Global Strategic Management of Technology. Research Technology Management, March–April, pp. 25–36.
33. M. Dodgson. 2000. The Management of Technological Innovation. Oxford University Press, NY.
34. A.B. Jaffe. 1986. Technological Opportunity and Spillovers of R&D: Evidence from Firms' Patents, Profits and Market Value. American Economic Review 76, pp. 984–1001.
35. J. Sterman. 1983. Economic vulnerability and the energy transition, Energy Systems and Policy 7(4), 259-301.
36. J.Sterman and J. Wittenberg. 1989. Path dependence, competition, and succession in the Stewart, I., Does God Play Dice? The Mathematics of Chaos. Cambridge, MA: dynamics of scientific revolution, Organization Science 10(3), 322-341
37. J.W.Forrester. 1985. The model versus a modeling process, System Dynamics Review 1(1), 133-134.
38. J.W. Forrester. 1968. Principles of systems. MIT Press, Cambridge.
39. D. Kim and P. Senge. 1994. Putting systems thinking into practice, System Dynamics Review lO(2-3), 277-290.
40. P. Senge. 1990. The Fifth Discipline: The Art and Practice of the Learning Organization. New York Doubleday.
41. P. Senge and J. Sterman. 1992. Systems thinking and organizational learning: Acting locally and thinking globally in the organization of the future, European Journal of Operational Research 59(1), 137-150. (eds.) (1994) Modeling for Learning Organizations. Portland, OR: Productivity Press.
42. P.K.J. Mohapatra and P. Mandal. 1989. System dynamics paradigm, Decision, 16(no. 4):251-266.
43. A. E. Plaza. 1994. Case-based reasoning: foundational issues, methodological variations and system approaches, AI Communication. 7 (1), March, 39–59.
44. D.B. Leake (Ed.). 1996. Case-Based Reasoning, MIT Press, Cambridge, MA, 1996.
45. T.W.Malone, R.Laubacher and C.Dellarocas. 2010. The Collective Intelligence Genome. MIT Sloan Management Review. Spring, volume 51, no. 3.
46. S.L.Epstein. 2015. Wanted : Collaborative Intelligence. Artificial Intelligence 221, 2015, 36 - 45.
47. Averbakh. 2010. Nash equilibria in competitive project scheduling. European Journal of Operational Research 205, 552–556.

48. W.Herroelen and R.Leus. 2005. Project scheduling under uncertainty: survey and research potentials. European Journal of Operational Research, 165, 289–306.
49. A.J.Shenhar. 2001. One size does not fit all projects : exploring classical contingency domains. Management Science. Vol. 47 no. 3, pp. 394 - 414. March.
50. H.Kerzner and C. Belack.2010. Managing Complex Projects, John Wiley & Sons and the International Institute for Learning (IIL) Co-publishers.
51. H.Kerzner, 2006. Project Management Best Practices; Achieving Global Excellence, Hoboken, NJ:John Wiley & Sons Publishers.
52. J.W.Ross and C.M.Beath. 2002. Beyond the business case: new approaches to IT investment. MIT Sloan Management Review. Winter.
53. R.H.Waterman, T.J.Peters and J.R. Phillips. 1980. Structure is not organization. Business Horizons. June.
54. S. Chakraborty and S.K. Sharma. 2007. Enterprise Resource Planning: An Integrated Strategic Framework. International Journal of Management and Enterprise Development, Volume 4, No. 5.

Exercise

1. **What is the technology swing and the scope of technology innovation?**
2. **What is the dominant design of this technology innovation?**
3. **What are the basic elements of the system architecture associated with the technology innovation? How to represent the structure correctly?**
4. **What do you mean by technology_security? How to verify the security intelligence?**
    a. **What are the strategic moves of technology diffusion? What is the outcome of technology life-cycle analysis?**
    b. **How to compare an emerging technology with the existing old technologies through SWOT analysis?**
    c. **What are the technology spillover effects?**
    d. **What are the blind spots and critical success factors?**
5. **How to exercise ERP and SCM in a technology innovation project? What should be the talent management strategy?**
6. **What are the skills, leadership style and support demanded by a technological innovation?**
7. **How to manage technology innovation projects efficiently?**
8. **What should be the shared vision, common goals and communication protocols?**
9. **How to ensure a perfect fit among '7-S' elements?**
10. **What type of organization structure is essential for various types of technology innovations?**

CHAPTER 2: SOLAR POWER ELECTRONICS & NANO SOLAR CELLS – DOMINANT DESIGN & TECHNOLOGY DIFFUSION MOVES

Abstract: This chapter is focused on the problem of global energy security and has explored a set of fundamental research agendas: What should be the strategic moves for the diffusion of solar technology? What should be the dominant design of solar power system in terms of structure and security? What is the scope of solar technology? What should be the right innovation model? What is the outcome of a rational SWOT analysis on various types of energy? What is the outcome of solar technology life-cycle analysis? Solar power electronics and nanotechnology based solar cells are two critical success factors of the dominant design of solar power system for the improvement of energy conversion efficiency and reduction of cost of solar energy generation. Are there any other interesting strategic moves in this connection? **Is it really possible to enhance the absorption capacity of solar cells by 1000 times using the concept of nanotechnology?** Is it possible to reduce the cost of solar panel by 50% of the present cost? Can we dream of K-A-B-C-D-E-T-F innovation model for fast diffusion of solar technology globally?
Photovoltaic (PV) is the most direct way to convert solar radiation into electricity and is based on the photovoltaic effect, which was first observed by Henri Becquerel in 1839. Solar power electronics is an interesting option in transformation of old and traditional energy system which requires fundamental rethinking and radical redesign of as-is energy policy and technology. The present work has analyzed the technology of solar power through deep analytics in terms of seven 'S' dimensions: scope (S_1), system (S_2), structure (S_3), security (S_4), strategy (S_5), staff-resources (S_6) and skill-style-support (S_7). Effective solar technology diffusion strategy demands a perfect fit, proper coordination and integration among these seven elements. It is clear from scope and SWOT analysis that solar power is a potential option of sustainable energy and business model innovations for the future as compared to other sources of energy. There are some technological constraints such as efficiency and cost of solar cells. Presently, solar power system is at the growth phase of technology life-cycle and it demands an intelligent and rational technology diffusion strategy through the support, commitment and involvement of efficient and creative innovators.

Keywords: Energy Security, Solar power electronics, Deep Analytics, Business model innovations, Technology diffusion, SWOT analysis.

1. INTRODUCTION

The basic objective of this chapter is to analyze the technology of renewable energy, more specifically solar energy. This is an interesting cross-fertilization between management science (e.g. business intelligence, technology management, entrepreneurship) and engineering science (e.g. photonics, power electronics, chemical engineering, electrical engineering, renewable energy and structural engineering). It is basically a modest effort to business model innovation and system implementation; it tries to explore a set of fundamental questions based on rational analytics: What are the intelligent moves in solar technology management? Who are the customers? What do they value? How is it possible to deliver value to the customers at optimal cost? What are the emerging application domains? What is the revenue model? What is the quality policy? What are the corporate social responsibilities? Can the business model generate significant number of new job opportunities in our society? Is the technology ready, feasible and practically implementable? What are the major constraints? What are the critical success factors?
The contribution of this work is that proper diffusion of solar technology at a fast speed requires effective coordination and integration among seven 'S' elements of the deep analytics. These moves must be integrated, coordinated and synchronized for effective diffusion of solar power technology. The scope analytics outline a set of interesting business model innovation in solar technology. The system intelligence is explored along five dimensions: smart materials innovation for photonic cell, power electronic circuit intelligence in terms of power amplifier, DC-DC boost converter, microinverter, energy storage, energy efficient load (e.g. LED, computing devices, motors) and topology (e.g. microgrid, standalone or hybrid system). The security intelligence is explored along four dimensions: switchgear, relay and earthing system and maximum power tracking based load manager. The strategic intelligence is associated with good

governance, good wishes in public policy, industry analysis, efficient enterprise resource planning, supply chain management and marketing efforts like strategic pricing, promotion, trust in communication, sales and distribution.

The business model requires the support of a functional organization structure enabled with advanced information and communication technology. The structure should have project, power generation, distribution, maintenance, revenue management, HR, SCM and finance cells. The structure is also important for effective knowledge management: creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The business model should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated staffs or HR workforce.

The workforce require different types of skills such as research and development, product design, sales, event management, project management, erection, testing, commissioning and service maintenance. One of the critical success factors is the style or quality of leadership in terms of motivation, commitment, support, coordination and excellent communication. The leaders must be able to share vision and values among all the stakeholders honestly and appropriately in time. It is really challenging to implement the solar power system physically and practically for global energy security. There are different threats from traditional industries: coal, oil and gas, thermal and nuclear power, local bias, power play and politics. It is essential to understand the intelligence of business modeling and system dynamics, fundamental rethinking and radical redesign of global energy trading. The traditional boundaries of electrical, power and consumer electronics and structural engineering industries must be redefined for future growth in a stable way. The research methodology adopted for this work includes literature review on solar energy, photonics and photovoltaic power electronics and case analysis.

This chapter is organized as follows. Section 1 defines the problem of solar power electronics, explains the motivation of the problem and the contributions of the work. Section 2-8 evaluate the technology of solar power through deep analytics in terms of seven 'S' dimensions: scope (S_1), system (S_2), structure (S_3), security (S_4), strategy (S_5), staff-resources (S_6) and skill-style-support (S_7). Section 2 explores a set of intelligent business model innovations on solar power. Section 3 outlines the challenges of photonic power electronics. Section 6 shows SWOT analysis, technology life-cycle analysis and technology diffusion strategy for solar power. Finally, section 9 concludes the work.

2. SCOPE

Entrepreneurial success depends on various factors. The *critical success factors* are associated with entrepreneurial motivation, creativity, business model innovation, rational and intelligent business plan, core competencies, new technology management, sustainable policy for economic growth, corporate social responsibilities, industry structure, government's support in terms of incentives and subsidies, dynamic role of entrepreneurial education institutes, business incubator, business cluster and good support of financial institutions. Let us first explore a set of innovative business models for solar power technology.

The people of today's world need energy security through emerging renewable technology, new business models and innovative applications. Presently, the global energy consumption is 10 TW per year and 30 TW by 2050. The solar energy plays a significant role in meeting the global energy demand in future. Solar power is useful for the growth of rural, urban, semi-urban and remote zone. The business models based on solar power can create significant number of new job opportunities in photovoltaic micro grid project, erection, installation, testing, commissioning and maintenance of standalone solar power system. Further, there are good opportunities of technology consulting in power electronics and product design and business consulting in global supply chain management. This section explores various types of innovative business models and applications of solar power electronics in terms of solar lighting system, solar power pack, consumer electronics and home appliances, solar charging for laptop and tablets, microgrid for rural electrification and solar water pumps for agriculture with some practical examples of business analytics. This section requires detailed cost benefit analysis based on current technical and commercial data.

Solar Lighting System **:** Solar power system can be used intelligently in various applications such as lighting of homes, religious places, tourist spots, streets, transportation management systems (e.g. airport, rail stations, bus stops, public toilets), educational institutes (e.g. schools, colleges, universities, research labs), healthcare institutes (e.g. public and private hospitals, health clinics, drug shops, pathological lab), office buildings of public and private firms, IT firms, hotels, restaurants, dairy firms, biotechnology firms and food processing units and space science. A typical solar lighting system can illuminate a house of 5

persons lighting 5 lamps for up to 5 hours daily. It can save the cost of 300 litres of Kerosene of about Rs. 10,000. The PV panel converts solar radiation into electrical power; the current is controlled by a charge controller or inverter and charges a battery. The battery supplies power to the connected load while switched on and illuminate.

***Solar Power Pack*:** A power pack consists of a set of solar panels which convert solar radiation into electrical energy and transmit the power to domestic load or battery bank through a smart inverter. The battery bank stores surplus power when the demand mismatches with the supply. The inverter interacts with PV panel, domestic load, grid and battery intelligently to ensure continuous and regular supply of power. The rating may vary between 100W upto a few KW. A 1 KW power pack can save fuel cost of Rs. 50,000 per annum approximately and can also save energy bill of Rs. 10000 per annum.

Consumer Electronics and Home Appliances: Solar cells can be used as economical power supplies with miscellaneous applications such as solar cookers, fans, mobile phones, watches, tablets, laptops, torches, emergency lamps, LED, calculators, radios, televisions, freezes, air conditioners, water heaters, cars and other different types of home appliances. Solar cells are generally used in *space vehicles*.

Solar water heater: A solar water heater consists of a collector, pipes and an insulated tank. The collector is made of glass tubes in evacuated vacuum tube system or metallic tubes in flat plate collector system. It gets heated in sunlight and the heated water reaches the top of a water tank. The relatively colder and denser water descends into the tubes and gets heated through a continuous Thermo-siphon cycling effect. A 100 LPD water heater provides 100 litres of hot water at 65°C and saves Rs. 5000 energy cost annually. The existing design needs a change in terms of mechanism, size and compactness. Solar power enable water purifier is expected to be attached with tube wells in urban and rural zone to ensure the supply of clean purified drinking water.

Solar Charging for Computing Devices and Mobile Phones: Solar charging of batteries has recently become very popular for laptops, tablets and mobile phones. The typical voltage output of a solar cell is 0.7 V. A solar panel may have eight cells connected in series producing 5.6 V at most. It can charge a single Li-ion battery used in cell phones to 4.2 V with a buck or step-down charger. It requires a boost step-up charger to charge a multicell Li-on battery of a laptop.

Solar Water Pumps for Agriculture : Let us analyze the technology of solar water pumps [58,59]. What is a solar pump and how is it different from conventional pumps? What are the various types of solar water pump? What are the differences between surface and submersible pumps? Is a DC pump more efficient than AC pump? What are the advantages? What are the disadvantages such as impact of cloudy and foggy days and natural disaster? What are the basic working principles, irrigation capacity and average discharge? What is the procedure of site selection, erection, testing, and commissioning and relocation procedures of solar pump? What is the outcome of cost-benefit analysis? What are the marketing, promotion, advertising, sales and distribution strategies? What are the outcomes of technology life-cycle analysis?

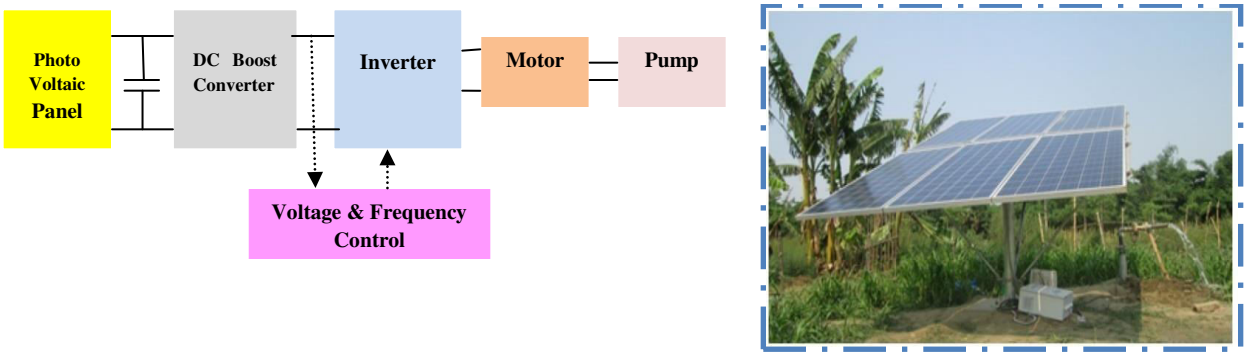


Figure 2.1: Solar water pump for agriculture

A solar water pump is a system powered by renewable solar energy [Figure 2.1]. It is used to extract water from various sources of water (e.g. lake, pond, river, borewell) for agriculture, irrigation and domestic drinking water applications (0.1-5 HP), municipal and rural community applications (15 - 100 litres of water per peak watt). For example, 2 HP and 7.5 HP pump may supply water to 2 and 10 acres of land respectively but this data may vary depending on the level of ground water and the type of irrigation required for a particular crop. A solar water pump can be used effectively for domestic application and irrigation (e.g. submersible, surface or deep well) in agriculture. It gets electrical power from solar array

wherein a number of solar modules are connected in series or parallel. The array converts solar radiation into electrical energy which is controlled by a variable frequency driver and enables the connected pump to draw water from ponds, rivers or bore-wells and distribute the same to green fields directly for agriculture or to tanks for storage through pipeline. Solar power can be used as the energy supply of cold storage or warehouses which are generally used to store food grains, fruits and vegetables and can reduce the cost of storage and wastage of perishable items significantly.

A solar pump may be of different types such as AC/DC and submersible / surface pumps. A submersible pump is used in a borewell having water level deeper than 15 meters; a surface pump may be used in an open well, pond and water level less than 10 meter. The basic components of the system include solar panels, motor pump set, electronic controllers and inverters. Solar panels supply DC to the motor; AC pump requires an inverter to convert DC into AC. DC pumps may have higher efficiency over AC pumps and do not have inverter for operation. But, DC pumps may have constraints in terms of cost, repair and maintenance services. The discharge rate may vary 15-20 Litres of water per peak watt depending on solar intensity, location and seasonal factors.

Solar water pumps offer many advantages as compared to conventional nonrenewable energy driven pumps such as cost of fuel and maintenance, low voltage regulation, power cut and environmental pollution (e.g. air, water, soil) problems. It can be installed at remote areas; it has fewer moving parts and less chance of wear and tear; the system needs minimal maintenance like cleaning of the panels on a regular basis. It is easy to operate and do not require lubricants. But, the pump may not work effectively during cloudy and foggy days; it need to the conventional grid. Solar panels may be damaged due to hail storm, cyclones and direct lightning strike (if no lightning arrester is used). Solar panels should be installed in areas free of shade, dust and dirt; should be easily accessible for cleaning and should be as close as possible to the pump and water source. It is interesting to exercise a comparative analysis on the cost of AC and DC solar water pumps of various suppliers, subsidies and promotional efforts initiated by the state and central governments of various countries globally.

Solar induction cooker [53-57]***:*** *Solar cooker* is an interesting emerging application; it may be a direct or indirect application. An indirect application is related to the use of induction cooker or microwave oven enabled with solar panel. Let us exercise SWOT analysis of solar induction cooker and conventional gas cooking oven / gas pipelines. Is it possible to explore the option of solar power enabled induction cookers at mass scale? Solar power enabled induction cooker should be a substitute of costly cooking gas. It is irrational to invest capital on new gas pipeline projects today in the age of induction cooker. Solar cooker uses the solar energy from direct sunlight to heat, cook or pasteurize food or drink. It is relatively inexpensive, reduces fuel cost, having simple technology and large solar cookers can cook for hundreds of people. Solar cookers have various advantages in terms of minimal fuel consumption, reduced danger of accidental fire, health and environmental pollution.

Figure 2.2: Solar cooker

There are many types of solar cookers such as parabolic, solar ovens and panel cookers [Figure 2.2]. The basic principle of solar cooker is based on concentration of sunlight, conversion of light into heat and trapping of heat. A mirrored surface with high reflectivity concentrate sun light on a small cooking area. It can produce high temperature like 65 - 400°C depending on the geometry of the surface. An alternative design of solar cooker concentrates sunlight on a receiver such as a cooking pan. The interaction between solar energy and the receiver material converts light to heat; it is maximized by materials which can conduct and retain heat. The convection of heat can be reduced by isolating the air inside and outside the cooker. Parabolic solar cookers concentrate sunlight to a single point which is focused on the bottom of a pot and can heat the pot quickly to very high temperature. Parabolic troughs are used to concentrate

sunlight for solar-energy. Spherical reflectors operate like paraboloidal reflectors and can attain temperatures above 290°C to cook meat, vegetable, soup, baking of bread and boiling water in minutes.
But, solar cookers are less useful in cloudy weather and near the poles and may take longer time to cook food. The alternative solution is the adoption of induction cooker which can be operated through solar power fed by PV panels. It is essential to design user friendly solar cooker which can be commercialized. The basic principle is to incorporate heating into material by photovoltaic effect and thermal treatment. An efficient solar cooker needs the boosting of only 30W which is generated by a small standalone solar panel of 75W.

Solar Microgrid for Rural Electrification: A smart *Microgrid* is an interesting option of rural electrification [Figure 2.3]. It consists of solar panels, power condition unit (PCU), distribution box (DB), battery system and loads. Its size depends on the load estimation and the number of PV panels and rating of solar cells. The PV panels comprise of a set of solar cells connected in series or parallel; they convert solar radiation into electrical power; the power flows from PV panels to PCU or power inverter; PCU controls, regulates and directs the power to various loads (e.g. domestic load, water pumps in Greenfield). The surplus power generated in the daytime is stored in the battery bank and may be utilized after the sunset. The typical energy demand of a rural house is approximately 3 units. For a village of 100 houses, a 5 KW microgrid may be useful. It can generate annual energy of Rs. 50000. It is an approximate calculation.
Let us consider the application of solar power for rural electrification: how solar power can illuminate the life of poor rural people. The innovative business model of solar power can save energy cost of rural people in domestic applications and agriculture. The peasants and farmers can reduce the cost of energy used in water pumps for irrigation in agriculture. It can improve the productivity required for green revolution. Many rural people suffer from road accidents and snake bites due to lack of adequate street light; the solar power can save them from those dangers in the form of solar torch. The rural students can study in the evening and night effectively using solar lamps. The rural people can save the cost of energy used for home appliances and domestic power supply. They are able to use modern electrical and electronics systems (e.g. home appliances, TV, music system, mobile phones, i-pod, computers, laptops, washing machines, freeze, induction cookers, microwave ovens etc.) through the use of solar power economically. In summer, they can feel comfortable using fans and air-conditioners and in winter, they can use room heaters and geezers. Rural market is a potential option for the growth of consumer electronics and electrical industries.

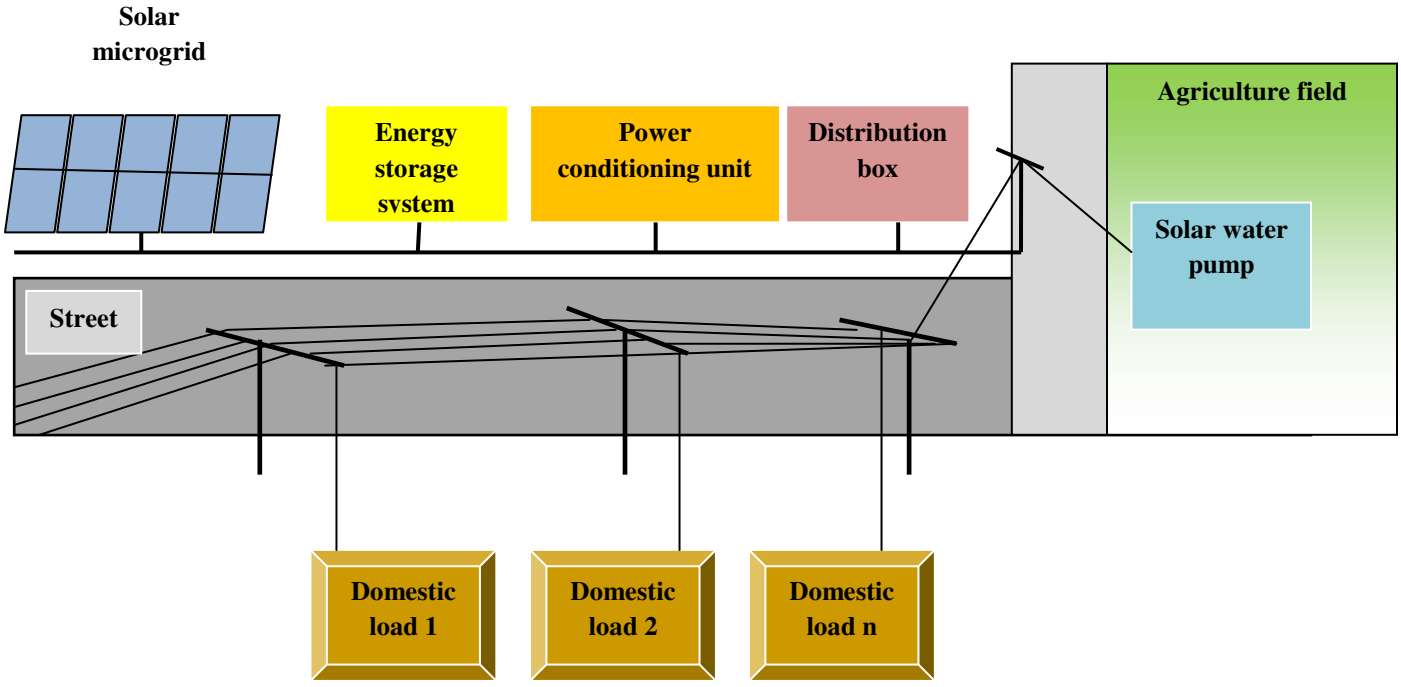


Figure 2.3: Solar microgrid for rural electrification

PV Panels or Solar Cells Manufacturing: The present global PV market is growing at about 40% per year and global PV production was about 11 GW in 2009 due to rapid reduction in production cost, technology improvement and market development reflecting the economy, reliability and versatility of solar energy. About 80% of the global PV production is based on c-Si and pc-Si wafer technologies. Major market segments comprise consumer applications, industrial systems, rural electrification in developing countries, microgrid and hybrid systems. The major markets exist in USA, European Union (e.g. Germany), Japan, China and Taiwan. The top ten producers of PV cells and modules are First Solar, Suntech Power, Sharp, Q-cells, Yingly Green Energy, JA Solar, Kyosera, Trina solar, Sunpower and Gintech. In future, a set of PV panels (or solar cells) manufacturing plants should be set up in India through joint ventures. Definitely, the new industrial units will be able to boost the growth of manufacturing industry in India.

The budding entrepreneurs must try to explore a set of fundamental questions based on rational analytics: Who are the customers? What do they value? How is it possible to deliver value to the customers at optimal cost? What are the emerging application domains? What is the revenue model? What is the quality policy? What are the corporate social responsibilities? Can the business model generate significant number of new job opportunities? Is the technology ready, feasible and practically implementable? What are the major constraints? What are the critical success factors? What are the business intelligence moves in solar technology management? How to make an effective business plan? What are the critical elements of an intelligent business plan? A good business model consists of four interlocking elements : customer value proposition in terms of target customers, jobs and product and service offerings; profit formula in terms of revenue model, cost structure, margin model and resource velocity; key resources such as people, technology, products, equipments, information, channels, partnerships, alliances and brand and key processes, rules, metrics and norms. A good business plan must have a set of common elements such as executive summary, the mission and vision of a company, organization structure, roles and responsibilities of management team, industry analysis, market, operation management strategy, marketing plan, financial plan, risks assessment and mitigation strategy. Many ventures fail due to lack of intelligence in defining a good business model and business plan.

The entrepreneurs need the support of business incubator, social network, business cluster and single window system from the ministry of MSME (Micro, Small and Medium enterprises). Entrepreneurial development institutes and MSME training institutes should focus on developing entrepreneurial skills in the domain of solar power electronics. A business incubator can nurture new ventures by providing them good guidance and support during start-up period. The entrepreneurs also need good network of technical experts and business development consultants. A business cluster may gain performance advantage through co-location, business relationships, right infrastructure and right skills. The aspiring entrepreneurs should be able to get all necessary permits and clearances by applying to a single agency of MSME ministry. The ministry of MSME should offer value adding incentive schemes and good mechanisms for access to debt, equity and venture capital, tax breaks, stimulating innovation, access to market and simplification of administrative burden and legal hassles. The policies should be correctly evaluated on regular basis. The rural banks and cooperative banks should launch innovative schemes (e.g. loan guarantee) to fulfill the needs of the budding entrepreneurs for rural electrification though smart Microgrids. Finally, the budding entrepreneurs must have commitment, determination, patience, tolerance of risk and uncertainty, creativity, self-reliance and motivation for successful ventures on solar power electronics.

3. SYSTEM

The design of solar power system should be smart, compact, cost-effective, reliable, robust, modular, standardized, flexible in terms of service maintenance and focused on high performance and efficiency. There are lot of scopes of improvement of the existing design of solar water heaters, pumps, lighting systems, cookers and other home appliances in terms of appearance, size, quality, cost and product performance. The customers are very much conscious about product's performance, quality of service, cost and values of a standalone solar power system. It is possible to obtain system intelligence through value engineering and value analysis, brainstorming, standardization of product design, excellent quality control practice and efficient supply chain management [Figure 2.4].

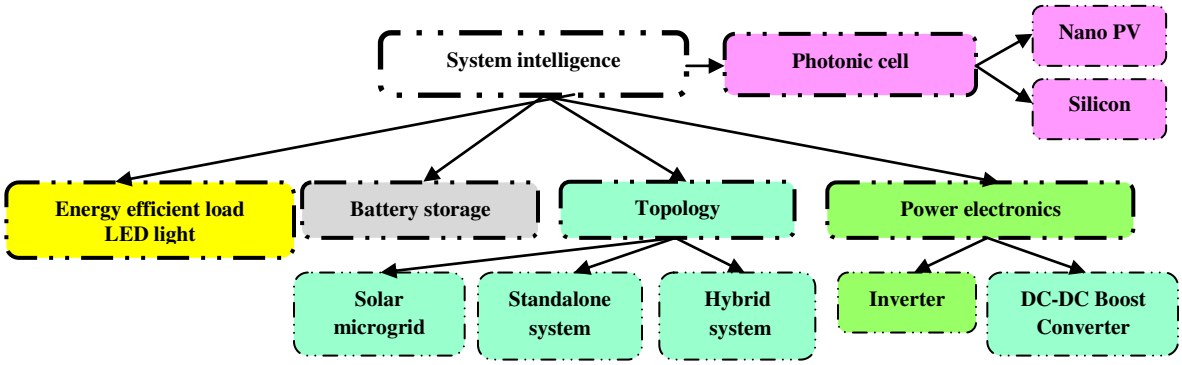


Figure 2.4 : System intelligence of solar power

3.1 Topology: One of the critical factors of system intelligence is topology of solar power system. There are different types of topologies such as standalone system, smart micro grid and hybrid system. Solar power is the modern trend of sustainable energy which requires flexible use of standalone, grid connected and hybrid system. The standalone systems are available in the form of innovative solar power enabled home appliance products such as solar cooker, lighting system, water pump, water heater and charger of computing devices. The basic components of a standalone rooftop system are solar or photovoltaic (PV) panel, inverter (optional for AC load), meter, protection relays and load. Smart Microgrids are intelligent electricity distribution networks that interconnect loads, distributed energy resources and energy storage systems within transparently defined electrical boundaries to act as a single controllable entity that can be grid connected or isolated. The system intelligence of a microgrid is associated with right sensing, communication, measurement and control technologies for effective generation and distribution of energy, self healing, stability analysis, fault analysis and load balancing mechanisms. Microgrid is an interesting and smart option of rural electrification. A hybrid system uses solar rooftop system and electrical grid alternatively according to the availability of power. There are issues of proper system integration, stability and load balancing with hybrid power system. It is logical to build an optimal number of solar thermal power plants and solar parks with medium and large capacities. But, standalone systems are also required in remote zones such as rural, forests, hilly and desert areas.

3.2 Photonic or Solar Cell

It is interesting to explore the dominant design of solar power system in terms of Nanotechnology based solar cells and solar power electronics. The system intelligence greatly depends on the innovation of smart materials and progress of mono and polycrystalline thin film photovoltaic technologies based on Si, semiconductors and nano PV. The efficiencies of Si and Ga As monocrystalline solar cell are relatively high. Thin film PV can reduce the cost of solar cells. CdTe and Cu (In,Ga)Se_2 thin-film solar cells have efficiencies of 21% and 20.5% respectively. The production cost of CdTe thin-film modules is about $0.76 per peak watt; the same of mono and polycrystalline wafer Si solar is around $1.50 per peak watt (in 2011). Silicon solar cells can be classified into crystalline and thin film cells. The maximum efficiency of a crystalline solar cell is around 25.6%; the thickness may be as high as 400 µm. Reduced reflection loss, better light trapping and improved contact area result better efficiency of crystalline solar cells. Thin film silicon solar cells have reduced thickness of 50 µm; thin films can be deposited on low cost base and the efficiency may vary between 10.5 % and 21.2% [7,9]. It is required to do similar type of analysis based on real up-to-date data.

The improved optical, chemical and electrical properties of nanomaterials can increase the efficiency of solar cells. Crystalline semiconductor III–V materials, polymeric materials, and carbon based nanostructures are used for third generation PV cells. Third generation PVs are based on nanostructure which can improve the efficiency of solar cells at relatively low cost. Quantum wells and quantum dots are used in crystalline solar cells to achieve high efficiencies. Quantum dots are nanometer sized crystallite semiconductors. These are artificial atoms improving the energy of the carriers. Nanocrystals increase the surface area of a solar cell and absorb more solar energy. The other options are rectifying antennas using wave property of light and organic solar cells. It is really challenging to improve the efficiency of solar cells and reduce the cost of production through various strategic moves such as carrier multiplication,

multi-junction cell structure, hot electron extraction, impurity and intermediate band devices. The carrier multiplication strategy increases the photocurrent generated by a solar cell and improves energy conversion efficiency by creating additional electron-hole pairs in PV devices. A multi-junction structure captures a large fraction of solar spectrum while minimizing thermal losses by stacking cells in the order of band gaps; its efficiency is 37.9%. It is essential to improve the efficiency of the solar cells through innovation of smart materials and explore economical manufacturing technology. A smart analytics needs up-to-date data on efficiency and cost of different types of solar cells.

A Photovoltaic (PV) system converts sunlight into electricity directly. The basic building block of a PV system is PV cell; a set of PV cells are grouped to form panels or arrays. The cells are connected in series to obtain large output voltage. It is possible to obtain large output current by increasing the surface area of the cells or by connecting cells in parallel. A PV cell is basically a semiconductor diode with its *p–n* junction exposed to sunlight. The rate of generation of electrical carriers depends on the flux of incident sunlight and the capacity of absorption of the semiconductor. The capacity of absorption depends on the temperature, semiconductor band gap, reflectance of cell surface, intrinsic concentration of carriers of the semiconductor, electronic mobility and recombination rate.

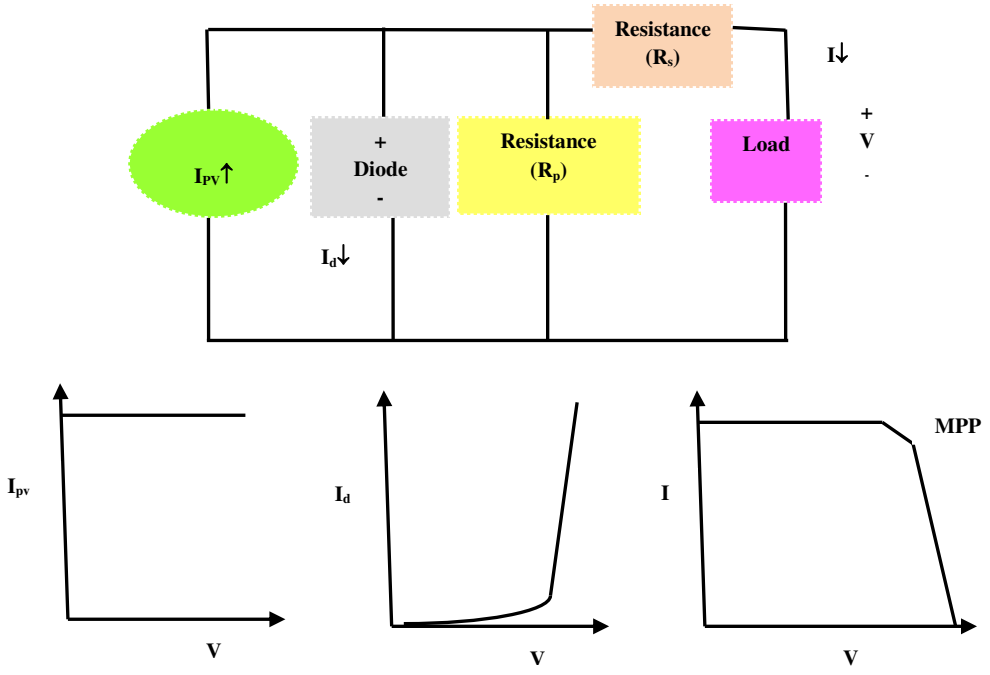


Figure 2.5 : Circuit of PV cell and Electrical Characteristics (I-V curve and MPP)

Figure 2.5 shows the equivalent circuit of a PV cell. The basic equation describes the current (I) – voltage (V) characteristic of the ideal PV cell is $I = I_{pv} – I_0 [\exp(qV/akT) – 1]$ where I_{pv} - current generated by the sun light , I - Shockley diode equation; I_0 - reverse saturation or leakage current of the diode, q - electron charge ($1.60217646 \times 10^{-19}$ C), k - Boltzmann constant ($1.3806503 \times 10^{-23}$ J/K), T (in Kelvin) - temperature of the *p–n* junction and *a* - diode ideality constant. A solar panel can generate its maximum voltage in full sunlight with no load; it is open circuit voltage of the panel. As the load of the solar panel increases, the output voltage decreases nonlinearly. The power output of a PV system depends on various factors such as module temperature, dirt and dust and DC to AC conversion. The output power of a PV system reduces as the module temperature increases. Dirt and dust on the solar module surface blocks some of the sunlight and reduces output (e.g. 7%). Some power is lost through DC to AC conversion in inverters (e.g. 10-12%).

Nano technology for solar cells : The basic objective of Nanotechnology is to reduce the cost per solar cell and improve the energy conversion efficiency. The emerging technology is looking for efficient solar cells at reduced cost which can change the economics of energy market. The scope of nanotechnology may

be explored in terms of nanoparticles, nanotubes, nanowhiskers as antireflective coating, multi-junction solar cells (MJSC), dye sensitized solar cells (DSSC) and quantum dot solar cells (CdSe QD). The technology of solar cells has been evolving through three generations: first generation having *crystal silicon cells* dominating the market, second generation having *amorphous silicon thin film cells* at reduced cost and third generation adopting *nanotechnology* with a mix of flexible and printable substrates and electronically conducting nanomaterials.

The structure of nanoparticles determines what range of frequencies they can resonate at or accept plasmon energy levels : roughly 575 - 9000 nm or 2.25 - 0 eV for nanoshells, 475 - 1400 nm or 2.6 - 1.0 eV and 600 -1200 nm or 2.2 - 1.25 eV for nanocubes. In dye-sensitized solar cells, electrons pass through a TiO_2 layer and gather on fluorine-doped SnO_2 of a glass surface. In CdSe QD system, the split and transfer process occurs between a polymer and CdSe dots, which provide tunnels to the electrodes. TiO_2 only collects 5% of the solar spectrum with a bandgap of 3.2 eV. TiO_2 can be doped with N. Antireflection (AR) coating and quantum wells can also improve the energy conversion efficiency. Multi-junction cell allows the absorption of larger range of wavelengths in the solar spectrum through stacking of solar cells of different band gaps in series. A 3-junction solar cell can have about 40.7% efficiency under 240-sun illumination.

3.3 Power Electronics

3.3.1 DC-DC Boost Converters [35,36, 37, 38, 43, 44]

A DC chopper can be used as a DC converter to step up or step down a fixed dc voltage. The chopper can also be used for switching mode voltage regulators and for transferring energy between two dc sources. But, harmonics are generated at the input and load side of chopper and the harmonic can be reduced by input and output filter. A chopper can operate on either fixed or variable frequency. A simple step-up boost converter is comprised of dc input voltage source V_S, boost inductor L, controlled switch S, diode D, filter capacitor C and load resistance R [Figure 2.6, 2.7] . When S is on, the current in the boost inductor increases linearly. The diode D is off at the time. When S is turned off, the energy stored in the inductor is released through diode to RC circuit. The switch is operated with a duty ratio $\delta = t_{on} / (t_{on} + t_{off}) = t_{on} / T$; $T = 1/f$, f : switching frequency; The average value of the output voltage is $V_O = \delta.V_S$.$V_S.\delta.T = (V_O - V_S)(1 - \delta)T$; DC voltage transfer function $M_V = V_O/V_S = 1/ (1-\delta)$; the output voltage is always greater than the input voltage. The boundary value of inductance : $L_b = (1 - \delta)^2\delta R$; $C_{min} = \delta.V_O/(V_r R.f)$; a large filter capacitor is required to limit the output voltage ripple.

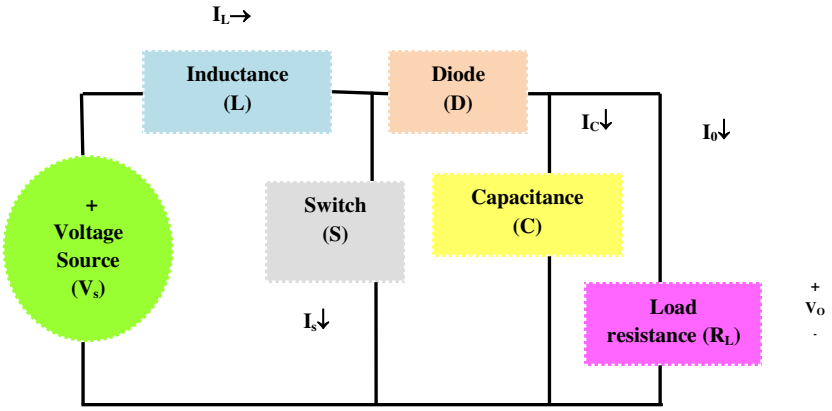


Figure 2.6 : DC boost converter – simple circuit

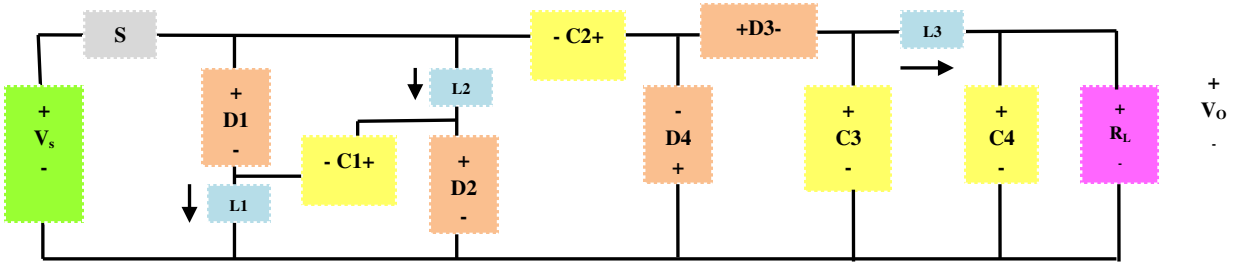


Figure 2.7 : DC-DC boost converter – complex circuit

Let us perform the strength and weakness analysis of a DC-DC boost converter. Solar panels convert sun irradiation into electrical energy using photovoltaic effect. The output voltage of a solar panel varies based on solar irradiation and temperature; it is not possible to connect sophisticated electrical and electronic load with PV panels for this reason. So, the circuit requires a reliable and efficient DC-DC boost converter with constant step-up voltage. Here, the critical success factors are converter configuration, control mechanism, integration with power utilities, output limitation, efficiency, sensors and complex control algorithm. The cost of converter is approximately 15% of the system cost. But, there are various constraints such as reduction in gain, decreased output voltage, complex control schema, less efficiency and increased cost, variable PV power irradiation and load.
The possible solution may be high output voltage DC-DC boost converter with MPPT algorithm based on PI controller. A PV module with parallel connection of a set of panels can obtain high current. For a PV panel, power capacity is about 100-300W, MPPT Voltage range is 15-40V, DC-DC boost converter is used for step up conversion of low voltage of a PV panel. The circuit a DC-DC boost converter consists of static switch, diodes, capacitors, inductors and load resistance. The important design parameters are input voltage, inductance, capacitance, load resistance, duty ratio, switching frequency. The other variables are supply voltage load voltage, supply current and load current.

3.3.2 Maximum Power Point Tracking [MPPT]

What are the strategic options to obtain maximum available solar power from PV panels?

- DC-DC boost converter with high gain may be connected with an inverter;
- Series / parallel connection of arrays of solar panel;
- Maximum power point tracking algorithm (MPPT) based on PI control;
- The power output of solar systems increases with the use of efficient sun tracking methods such as polar axis and azimuth / elevation types. AI based solar tracking policy may consider various factors such as forecasted weather conditions, energy consumption and complex closed-loop PI control logic.

***Power Amplifier*:** The system intelligence of a solar power system is highly correlated to the design and topology of power electronic circuit. The energy conversion efficiency of a photonic solar cell is low (e.g. 20%). Therefore, a solar power system needs the support of a power amplifier. It is a new concept. Let the input power of a power amplifier is p; the output of the amplifier should be P = k.p where k is a constant greater than 1. Recently, Mitsubishi Electric Corporation has developed a prototype gallium nitride high electron mobility transistor amplifier with 100W output power for satellite communications. Generally, voltage and current amplifiers are used in boost converter. A voltage amplifier can raise the voltage generated by solar panels in poor light condition.
Is DC-DC boost converter considered as equivalent to power amplifier? What is boosted V or I? P=VI; If I $\uparrow$ and V = constant then P$\uparrow$; If V $\uparrow$, I $\uparrow$; then P $\uparrow$; but increased I results overheating of electrical and electronic devices. P= Constant; if V $\uparrow$then I$\downarrow$. If V$\uparrow$ and I = constant then P$\uparrow$; in case of PV power generation with voltage operation mode, high output voltage DC-DC boost converter maximizes the output of PV panel. Let us consider circuit intelligence of maximum power point tracking schema.
The solar power system requires the support of an intelligent load manager for effective monitoring of voltage (V), frequency (f), current (I), power (P), energy (E) and maximum power point tracking (MPPT). Maximum Power Point Tracking (MPPT) techniques find the voltage V_{MPP} or current I_{MPP} automatically at which a PV cell should operate to obtain maximum power output P_{MPP} under a given temperature and irradiance [Figure 2.8]. There are different MPPT techniques such as hill climbing, Kalman filtering and perturb and observe (P&O) methods. Hill climbing is related to a perturbation in the duty ratio of the power converter and P&O involves perturbation in the operating voltage of the solar cell. There are differences among various MPPT techniques in terms of complexity, number of sensors, convergence speed, cost, effectiveness, implementation hardware and use of soft computing based microcontrollers (e.g. Fuzzy Logic, Artificial Neural Network).

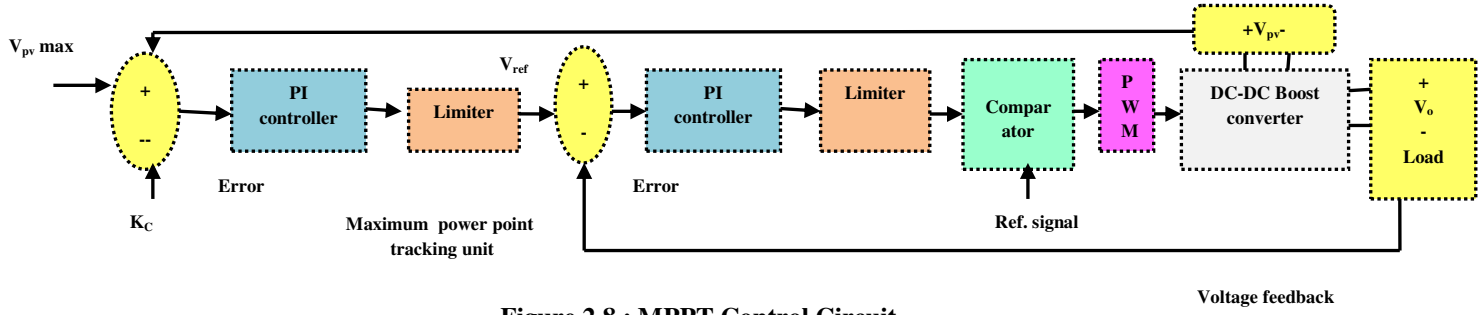


Figure 2.8 : MPPT Control Circuit

Voltage control mode is considered to maximize power generation by PV panel. For example, MPPT may be set at 10V to attain maximum power 500W. The circuit for MPPT consists of two voltage sensor feedback, two P-I controllers, two limiters and a signal compensator [35,36]. The feedback voltage from PV panel is compared with maximum reference voltage and obtained error is regulated through a P-I controller to obtain the output reference voltage. It is the maximum fixed output voltage reference for the converter. The feedback from DC load voltage is compared with the reference voltage to obtain the error which is then applied to another P-I controller to compensate the error. The signal of P-I controller defines the duty ratio δ for PWM mode. δ is then compared with a ramp-signal to generate pulses for static switch of the converter circuit. The proportional and integral gain of PI controller are fine-tuned to maintain MPPT under variable irradiation and load.

3.3.3 Solar micro-inverter

Inverters convert from DC to AC while rectifiers convert from AC to DC. Many inverters are bi-directional; operate in both inverting and rectifying modes. A standalone PV system operates at 110/240V AC with 50/60 Hz frequency. Inverters operate at 12, 24, 48, 96, 120 or 240V. An inverter for a stand-alone PV system should have sinusoidal output voltage, voltage and frequency within allowable tolerance limits, good voltage regulation and high efficiency at light loads. Inverters use semiconductor devices such as metal oxide semiconductor field effect transistor (MOSFET) and insulated gate bipolar transistors (IGBT). These devices are used in units up to 5 KVA and 96V DC. They have the advantage of low switching losses at higher frequencies. Voltage Source Inverters (VSI) and Current Source Inverters (CSI) are usually used in standalone PV applications. They can be single phase or three phase and use square wave, quasi-square wave, and pulse width modulation techniques.

The topologies, control method (e.g. pulse width modulation [PWM], boundary conduction mode [BCM], discontinuous conduction mode [DCM]) and soft switching methodologies using MOSFETs and IGBTs are the basic elements of circuit intelligence in power electronic inverters and converters. A PV ac module is called *microinverter* which has benefits in terms of maximum power point tracking efficiency, low manufacturing cost, safe and simple installation procedure. Module integrated converters or microinverters (MICs) are designed to interface a single, low-voltage (e.g. 25–40 V) panel to the ac grid. Such converters provide benefits in terms of ease of installation, system redundancy, and increased energy capture in partially shaded conditions. An energy storage block can be used in a series connected path with the line interface block providing independent control over the capacitor voltage, soft-switching devices and full four quadrant operation with the grid. Several factors must be considered while selecting or designing an intelligent inverter for solar power system such as power conversion efficiency, electrical losses, rated power, duty rating, input voltage, voltage regulation, voltage and current protection, frequency and power factor.

A solar micro-inverter converts DC from a single solar panel to AC. The combined output from several microinverters is fed to the electrical grid. Solar panels produce DC voltage that depends on module design and lighting conditions. For example, panels using 6-inch 60 cells can produce a nominal 30 volts. The panels are connected in series to produce 300 - 600 V DC. The inverter converts this DC voltage into 110V / 230VAC, 50 Hz; microinverters are typically rated between 190 and 220 W and can tune the output of PV panel. Microinverters contrast with conventional string inverters having advantages simplicity in system

design, space utilization, cooling and safety. Even small amount of shading, debris or snow lines on any one solar panel or a complete panel failure do not reduce the output of the entire array disproportionately. Each microinverter harvests optimum power through maximum power point tracking. The efficiency of a panel's output is strongly affected by the load. Inverters use MPPT to ensure optimal energy harvest by adjusting the applied load. Microinverters may not need large transformers; large electrolytic capacitors can be replaced by thin-film capacitors.

Module integrated converters or microinverters (MICs) can be used for single-phase grid-tied photovoltaic applications with a topology that places the energy storage block in a series-connected path with the line interface block [31-34, Fgure 2.9]]. It can interface a single low voltage 25-40V PV panel to an AC grid. This design provides various types of benefits such as soft-switching for all semiconductor devices, independent control over capacitor voltage and full four-quadrant operation with the grid, ease of installation, system redundancy, and increased energy capture in partially shaded conditions. A third-port topology places energy storage buffer block in series with the line voltage interface. The topology achieves high efficiencies with its continuous constant power operation.

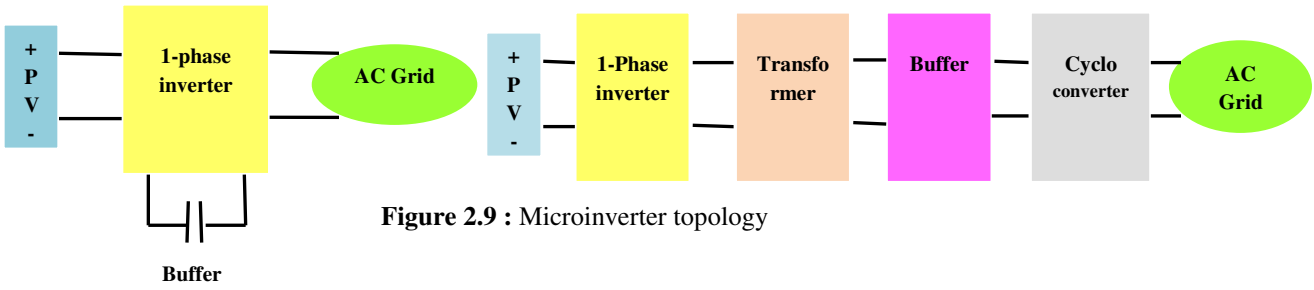


Figure 2.9 : Microinverter topology

The circuit consists of four functional blocks of the converter: (1) high-frequency resonant inverter, (2) transformation stage, (3) energy buffer and (4) cycloconverter. Each is connected in series, with a common high frequency resonant current linking them together. This topology allows bidirectional power flow in each block and it is possible to reduce heavy conduction loss through soft switching techniques. Typical rating of a microinverter is 100W,32V input, 240V output, 95% efficiency. In the classification of inverter topology, the location and the operation of energy storage buffer within the converter are two important parameters. Single stage topologies (e.g. flyback, ac-link) place capacitance in parallel with PV panel. The second option is two complete cascaded conversion stages with energy storage at an intermediate dc bus. Generally electrolytic capacitors are used for dc energy storage due to high energy density, but suffer from long-term failure rates.

Photovoltaic Grid-Tied-Interleaved Flyback Microinverters can achieve high efficiency in wide load range by intelligent control strategies such as Boundary conduction mode (BCM) and discontinuous conduction mode (DCM) [Table 1]. In this case loss analysis plays a critical role in estimation of efficiency of flyback microinverters. The dominant losses at heavy load include conduction loss of the power MOSFETs, diodes and transformer; the dominant losses at light load include gate driving loss, turn-off loss of power MOSFETs and transformer core loss.

Parameters	BCM	DCM
Control	Complex	Easy
Loss (high load) load	High	Low
Peak current	Yes	No
Power transfer	High	Low
THD (Total harmonic distortion)	Low	High

Table 1 : Comparison of BCM and DCM Control of Flyback Microinverter

3.4 Energy Storage System: The output of solar photovoltaic system varies significantly depending on the time of a day, weather and shading conditions. The system requires a stable energy source and it should be

dispatched at request. It demands an efficient energy storage system for solar power system in the form of batteries. There are different options for integrating an energy storage system into a solar PV system such as PV to grid (dc to ac), PV to battery (dc to dc), battery to grid (dc to ac), and battery/PV to grid (dc to ac). An intelligent converter can be used for both single phase and three phase PV battery application. The system is expected to have improved efficiency, reduced weight, volume and cost and minimum number of conversion stages. Li-ion battery can be used for solar energy storage system. It requires a constant current constant voltage charging algorithm. The battery should be charged at a set current level until it reaches its final voltage.

3.5 Load : The system intelligence is associated with energy efficient loads and mechanisms. Energy consumption is a critical concern since energy dissipation results thermal problems in electrical and electronic devices. Energy is a critical design constraint of electrical and electronic system. There are various strategies of minimizing energy consumption in computing devices such as power down mechanisms and dynamic speed scaling in variable speed processors. The display of computing devices 9 e.g. laptops, tablets) turns off after some period of inactivity. A computing device transitions to a standby or hibernate mode if it remains idle for a while. Intelligent task scheduling can save energy consumption in micro-processor enabled devices. Today, LEDs are widely used as energy efficient lighting or illumination systems. A simple standalone solar power system is easily compatible with light load such as LED, fans, TV and energy efficient motors and computing devices. In agriculture, the pumps and motors should be efficient to reduce the consumption of energy. The design and selection of electrical and electronics equipments should focus on energy efficiency through intelligent algorithms and operating mechanisms.
The system intelligence depends on good design and sizing of PV cells, power conditioning system, inverters and converters, battery management system. Technology management for solar power electronics requires discriminatory, fair and rational pricing mechanisms, incentive and subsidy policy, economies of scale of mass production, strategic cost reduction, product life-cycle management, quality policy and intelligent cost-benefit analysis. Solar power electronics face two critical constraints which should be improved through innovation, strategic alliance and intelligent technology management in future : high cost of production and low efficiency in conversion of sun light into electrical energy. It is essential to explore intelligent business models and applications of solar power such as rural electrification, agriculture and solar cooker. It can be a blue ocean space in energy business.

4. SECURITY

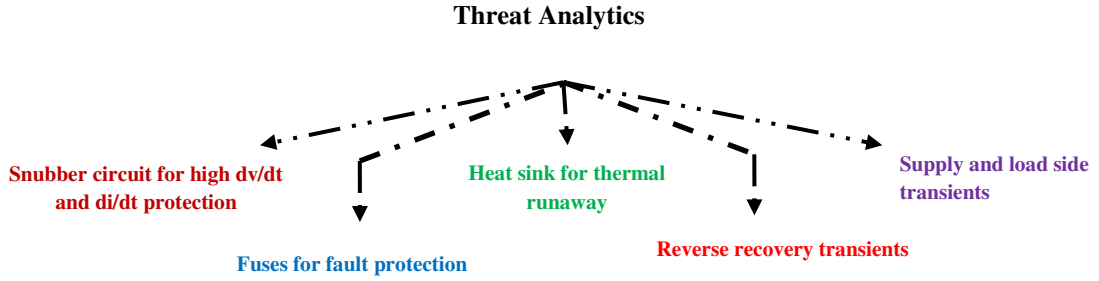


Figure 2.10: Threat analytics

Let us first consider the protection of power electronic circuit used in solar power system. The threat analytics analyzes the power electronics circuit from five different perspectives: snubber circuit for high dv/dt and di/dt protection, fuses for fault protection, thermal runaway by heat sinks, reverse recovery transients, supply and load side transients [Figure 2.10]. Voltage transients are caused in converter circuit due to reverse recovery process of power electronic devices and switching actions in the presence of circuit inductance. Short circuit faults may result excessive current flow in power electronic circuit.. Overheating may occur due to losses in semiconductor devices; it must be dissipated sufficiently and effectively for operating the device within upper temperature limit otherwise it may affect the reliability and consistency of power electronic circuit. Fuses are used for overcurrent protection. Power converters may develop short circuit or faults and the resultant fault currents must be cleared quickly. Fast acting fuses are normally used to protect semiconductor devices. As the fault current increases, the fuse opens and clears the fault current in few milliseconds. It is essential to select the location of fuse in the power electronic circuit; generally a

fuse is connected in series with each device. A fuse is selected based on the estimation of fault current. A fuse must carry continuously the device rated current; it must be able to withstand voltage after arc extinction; peak arc voltage must be less than peak voltage rating of the device.
Next, let us consider cooling by heat sink. Heat is generated due to on state and switching losses in power electronic devices. The heat must be transferred from the power electronic devices to a cooling medium to maintain junction temperature within specified range. Convection cooling is commonly used in industrial applications. It is rational to consider a set of important design parameters of heat sink such as contact area between device and heat sink, correct mounting pressure of the device on the heat sink, material (e.g. Al), size, and thermal resistance of power devices. Let us consider a power electronic circuit where a voltage source is connected in series with three resistances. $T_j = P_a(R_{jc}+ R_{cs}+R_{sa})$; T_j : junction temperature, P_a :average power loss, R_{jc} : resistance from junction to case; R_{cs} : thermal resistance from case to sink, R_{sa} : resistance from sink to ambient; T_a : Ambient temperature
Let us consider the protection through snubber circuit. It limits di/dt and dv/dt; since transients may occur in power electronic circuit. $di/dt = I_L/t_r = I_{Cs}/t_r$; during turn on collector current rises. $dv/dt = V_s / t_f = V_{cc}/t_f$, during turn off, collector emitter voltage must rise in relation to the fall of I_c. Snubber circuit protects the power electronic circuit within allowable limit of di/dt and dv/dt. Inductor L_s limits di/dt; it is a series snubber. RC snubber is normally connected across a semi-conductor device to limit dv/dt within maximum allowable rating. There are three types of snubber circuit : polarized (Resistance R limits forward dv/dt); reverse polarized (Resistance limits discharge current of the capacitor) and unpolarized (semiconductor devices are connected in parallel).

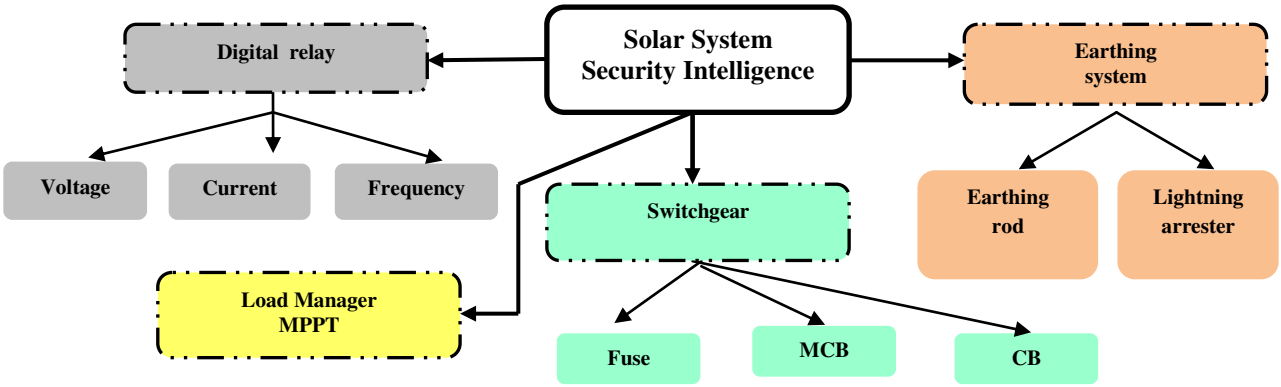


Figure 2.11 : Security schema for a solar system

Finally, we consider the risk of transients. There are three types of transients - reverse recovery transients, supply side transients and load side transients. In case of supply side transients, a transformer is normally connected to the input side of converters. Under steady state conditions, an amount of energy is stored in the magnetizing inductance L_m of transformer and switching off the supply produces a transient voltage at the input of the converter. A capacitance C is connected across the secondary of a transformer to limit transient voltage and a resistance is connected in series with C to limit transient voltage oscillation. In case of load side transient voltage, under normal condition, an amount of energy is stored in the supply and leakage inductance of the transformers. When the load is disconnected, transient voltages are produced due to the energy stored in the inductance. In case of reverse recovery transients,
Let us consider a circuit where voltage source Vs is connected with an inductance L, capacitance C and resistance R and a diode D_m is connected across C and R. Due to reverse recovery time t_r and recovery current I_r, an amount of energy is trapped in the circuit inductance and transient voltage appears across inductance. In addition to dv/dt protection, snubber circuit limits peak transient voltage across inductance. The snubber also limits peak transient voltage across device. The values of snubber circuit R and C are selected so that the circuit is slightly underdamped. The peak reverse voltage depends on damping ratio and current. The energy stored in inductance L is transferred to the snubber capacitance C and is mostly dissipated in snubber resistance. $L.di/dt + R.i + (1/C). \int i\ dt + v_c(t=0) = V_s; V = V_s - L.di/dt$; $i(t=0) = I$; $v_c(t=0)=0$
The intelligence in selection of protective system and load monitoring depends on the complexity of system topology, scalability of operation and cost. A standalone solar power system may be protected by a digital

relay having features of over voltage, over current, over frequency, under voltage, under frequency, earth fault and short circuit protection. Additionally, the system should be equipped with switchgear devices like fuse, miniature circuit breaker (MCB), earthling system and simple switches. The power electronic circuit should be protected appropriately. Less harmonic should be injected by inverters to avoid heating, thermal losses and damage of consumer electronics and home appliances. Photovoltaic inverters must be able to withstand overloading for short term to take care of higher starting currents from pumps and refrigerators. The other protection issues are related to over/under voltage and frequency, short circuit, surge protection, low idling and no load losses, low battery voltage disconnect and low audio and radio frequency noise. A solar park should be protected by heavy duty equipments such as air circuit breakers (CB), MCCBs, isolators, lightning arresters (LA), power control panels and sophisticated digital relays [Figure 2.11]. The cost of the protection system and load manager is a function of scalability of operation and complexity of the system configuration.

5. STRUCTURE

The structure element analyzes solar power system in terms of smart microgrid, various topologies such as AC coupled, DC coupled and ACDC coupled hybrid microgrids [Figure 2.12], AC/ DC sources and loads, renewable energy system (e.g. PV or solar power system), capacity and access oriented energy storage system, stand alone and grid connected operation mode, power management strategies and control schemes for both steady state and transient conditions.

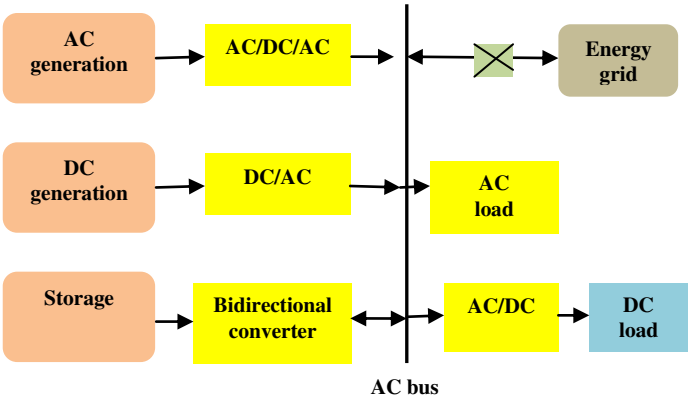


Figure 2.12 (a): AC coupled hybrid microgrid

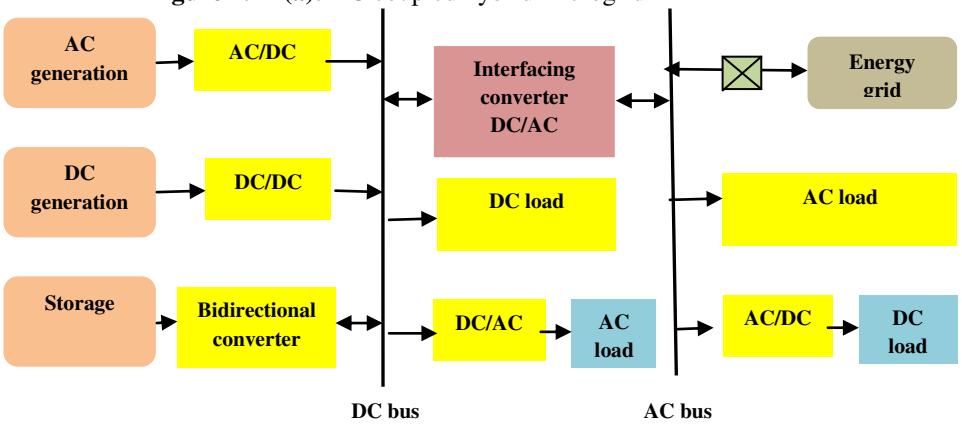


Figure 2.12 (b): DC coupled hybrid microgrid

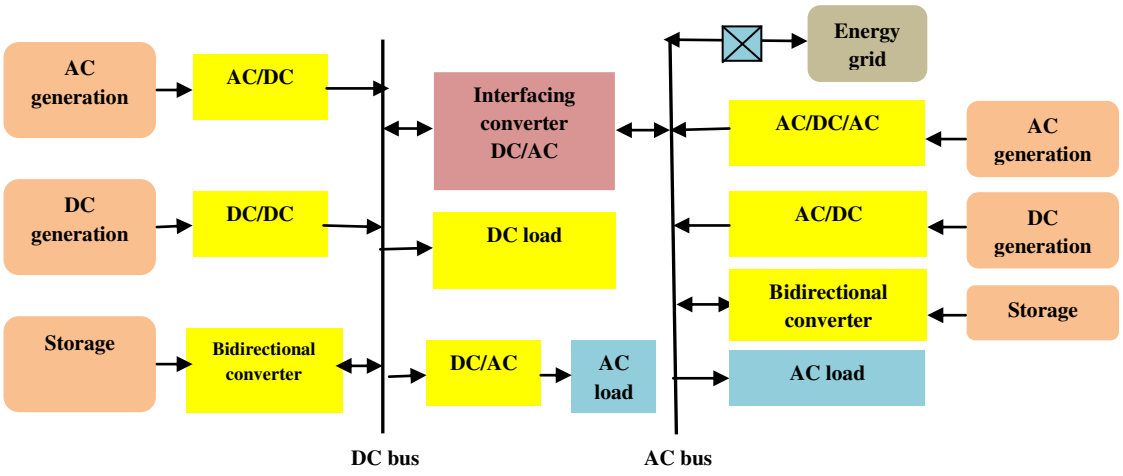


Figure 2.12 (c): AC-DC coupled hybrid microgrid

Smart grids are considered as next generation power systems which interconnect a set of microgrids consisting of Distributed generations (DGs) and renewable energy (RE) resources (e.g. solar, wind, tidel, clean alternative energy sources. Hybrid AC/DC microgrid contains both AC/DC power sources and AC/DC loads. It can be classified into three categories based on how the sources and loads are connected to the system and how AC and DC buses are configured into low and high frequency AC-coupled, DC-coupled and AC-DC-coupled microgrids [38-43]. In AC-coupled hybrid microgrids, DGs and SEs are connected to the common AC bus through their interfacing converters. In DC-coupled hybrid microgrids, DGs and SEs are connected to the common DC bus and an Interfacing Converter (IFC) links DC and AC buses. In AC-DC-coupled hybrid microgrids, DGs and SEs are connected to DC and AC buses and the buses are linked by Interlinking Converter (ILC). The basic objective of energy management is to match demand and supply of power optimizing cost (e.g. fuel, capital and maintenance costs), voltage and frequency regulations and real-time power dispatching among different power sources in micrograms. Microgrid architectures can be classified utility, industrial, commercial and remote type based on applications. The following table 2 compares various structures of microgrids based on a set of evaluation parameters such as topology, structural complexity, operation mode, control schema, power management strategies, cost and benefits [35-50].

Comparison parameters	AC coupled hybrid microgrid	DC coupled hybrid microgrid	AC-DC coupled hybrid microgrid
Topology	DGs and SEs are connected to AC bus through interfacing converters.	DGs and SEs are connected to the common DC bus, and an Interfacing Converter (IFC) is used to link the DC and AC buses.	DGs and SEs are connected to DC and AC buses, where these buses are linked by Interlinking Converter (ILC); most promising microgrid structures in the near future.
Complexity of structure	Simple, dominant structure, multiple port converters may be used.	Simple structure; multiple-port power converters may be used	Complex structure
Operation mode	Stand alone and grid connected ; transition between two modes should be seamless and smooth.	Stand alone and grid connected	Stand alone and grid connected
Control strategy	Simple, the power control can be realized by current or voltage control.	Complexity : medium; central control scheme, uses optimization techniques to adjust	Complex, Requires high coordination for voltage and power control between AC and DC subsystems; focus on DC

		set-points of each source.	and AC bus voltages and frequency control, power balance within DC and AC subsystems
Power management strategy	Grid connected operation mode : dispatched and undispatched output power; standalone : ac bus voltage and frequency control	Complexity : medium; Grid connected operation mode : dispatched and undispatched output power; standalone mode : ac and dc bus voltage control	Complexity : high; Grid connected operation mode : dispatched and undispatched output power; standalone mode : ac and dc bus voltage control
Cost	May be cost effective	May be cost effective	May be slightly costly
Benefits	Cleanness, simple technologies, increasing demands for electrical energy and exhaustible nature of fossil fuel demands efficient solar microgrids.	emerging new semiconductor devices use silicon carbide and gallium nitride for improved performance of power electronic switches.	Higher flexibility and reliability, improves overall efficiency and reduces the system cost with reduced number of power converters

Table 2 : Comparison of power management strategies

Hybrid DC- and AC-Coupled Microgrids integrate a variety of DER units into existing distribution system. It connects the distributed energy storage systems like batteries and fuel cells to bidirectional AC-DC converters and PV systems connected through DC-DC Boost converters. Microgrids can be classified into single and two stages power conversion systems [Figure 2.13]. In single-Stage power conversion systems, a transformer is used for isolation or voltage conversion . It is a very simple structure having high efficiency, small size and weight and reduced cost. Two-Stage Power Conversion is the most common configuration for all electronically coupled DER units and it consists of a DC-DC converter for energy sources with DC output voltage or an AC-DC converter for energy sources with AC output voltage with a grid-connected DC-AC converter. The converter on the energy source side extract the maximum power from the primary energy source and the grid side converter is controlled to follow grid requirements. Multilevel converter reduces the cost and improves the efficiency of power conversion systems.

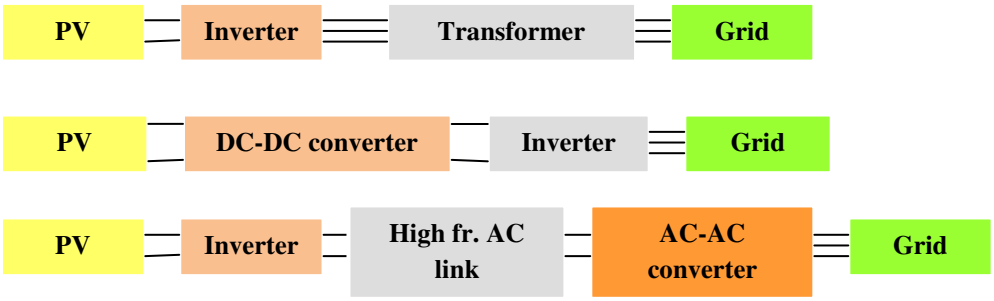


Figure 2.13 : (a) single stage and (b,c) two-stage power conversion system for PV system

A power electronics enabled microgrid consists of a static transfer switch (STS), distributed critical and noncritical loads, multiple DER units with various power electronics interfaces, protection devices and measurement, monitoring, and control units. DC microgrids are used in telecommunication systems, electric vehicles office buildings, commercial facilities, Photovoltaic (PV) and fuel cell system. HFAC Microgrids are generally used in distributed power systems for military and aircraft systems working in single-phase 400 Hz. It is an interesting agenda to explore the use of solar power for DC microgrids application.

Microgrid is the basic building block of the future flexible, reliable and smart power grid with increased penetration of Distributed Energy Resources (DER) such as solar or PV panels. The entire architecture of future electrical power system may consider three possible concept models : Microgrids, ICT driven Active Networks and the Internet. Microgrid paradigm interconnects multiple customers to multiple DER units including DG and Distributed Storage (DS) units and form an intentional or non-intentional energetic

island in the electrical distribution network. The customers and DER units can operate in parallel with the main grid and supports a smooth transition during abnormal grid conditions. The evolution and rapid development of efficient power electronics technology improves the transient response, Digital Signal Processors (DSP) reduce the processing time and support complex control algorithms and efficient power electronic converters enable cost-effective and flexible control, power management and energy flows efficiently. The aforesaid structural analysis explores the vision of an efficient solar microgrid or solar park for rural electrification and agricultural application.

6. STRATEGY

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as SWOT analysis, technology life-cycle analysis, R&D policy, learning curve, shared vision, communication protocol and knowledge management strategy.

6.1 SWOT Analysis

The technology of solar power is related to the problem of energy security. The people in today's world are faced with significant challenges in energy sector such as shortage of energy, high cost of power generation and distribution, power distribution loss, environmental pollution, greenhouse gas emission and rural electrification. We must set an efficient national and global energy policy to promote the development of a sustainable energy system which should be viable environmentally, socially and economically based on solar power. The sustainability in energy not only requires the development of renewable energy but also promotes the use of energy efficient system such as LED lighting system which slows down the growth of energy demand and promotes the concept of clean energy that can cut down the usage of fossil fuel significantly.

Let us first do the SWOT analysis on solar power. Renewable energy uses natural energy sources such as sun, wind, water, earth's heat and plants. There are different types of renewable energy such as solar, wind, hydropower, ocean or tidal, geothermal and bio-energy. Clean and green renewable energy technologies turn these fuels into electricity, mechanical, heat and chemical energy. It is basically an initiative of natural resource planning (NRP), a specific case of ERP. The world has limited supply of fossil fuels; there are critical issues of environmental pollution, safety and problem of waste disposal, rapid growth of energy demand. The use of thermal and nuclear power cause global warming which in turn results increase in sea level, flood, drought, heat wave and different types of natural disaster. Air pollution is one of the most dangerous killers worldwide – more than alcohol, sugar and kidney failure. The main cause of air pollution is the burning of fossil fuels. The crisis of global warming is associated with rising seas, catastrophic flood, devastating heat waves, changing heat structure of the atmosphere, unprecedented hurricanes, summer storms and smog. These events clearly show how the traditional old power plant engineering technologies are affecting the climate and weather globally. Renewable energy is plentiful and the technologies are improving rapidly. Solar technologies convert the infinite power of the sun into heat, light and power. Solar electricity or photovoltaic (PV) technology converts sunlight directly into electrical energy. Solar energy is a potential option for sustainable global energy demand. The PV market is growing rapidly.

National energy policy should be redefined since solar energy is an alternative source of energy and a substitute of traditional sources of energy such as thermal, hydel and nuclear power. It is essential to define a clear vision on renewable sources of clean energy such as solar power and set up relevant advanced research institutes to ensure energy security. Sufficient capital has been already invested on thermal, diesel and hydel power. The initial investment on hydel power plant is very high. It is not a good option for hot and dry zone where there is scarcity of water (e.g. drought in Brazil). The tribal workforce should be relieved from hard mining career (e.g. coal) in future. The nuclear power is very expensive due to shortage of fuel (e.g. Uranium). The coastal zones need several solar and wind power plants; it may be a hybrid system. **Land may not be a constraint for the adoption of solar power; there is large barren land in rural zone, coastal areas, desert, hills, plateau and forests. The barren land may be utilized for solar park.** It is possible to adopt 'million roof program with solar power'. It is possible to make strategic alliance with reputed solar energy vendors and manufacturers of Germany, Japan, USA, China and Israel for fast and efficient implementation of solar power system. It is possible to build many solar parks but it is also required to promote intelligent standalone solar power system. This change in energy policy is not a simple, trivial problem. The people expect more dynamic and active performance from Solar Energy

Society and Rural Electrification Corporation Limited. It is required to define an intelligent solar energy policy, imports of PV modules and anti-dumping strategy.
The strong points of solar power are direct conversion of solar radiation into electricity, no mechanical moving parts, no noise, no high temperatures, no pollution. PV modules have a very long life-time, the energy source i.e. the sun is free, ubiquitous, and inexhaustible. PV is a very flexible energy source, its power ranges from microwatts to megawatts. Solar power can boost the growth of various types of industries like photovoltaic cells or modules, power electronics devices (e.g. power amplifiers, converters and inverters), battery and energy storage devices, intelligent load managers with power tracking capabilities, smart micro-grid, steel and aluminum structures. It can reduce the cost of power generation, transmission and distribution and power distribution loss significantly. But, there are few constraints of this technology such as low efficiency of solar cell, maintenance, cleaning of dust, dirt and moisture from solar panels and the negative impact of natural disasters like storm, rainfall and snowfall.

6.2 Technology Life-cycle Analysis

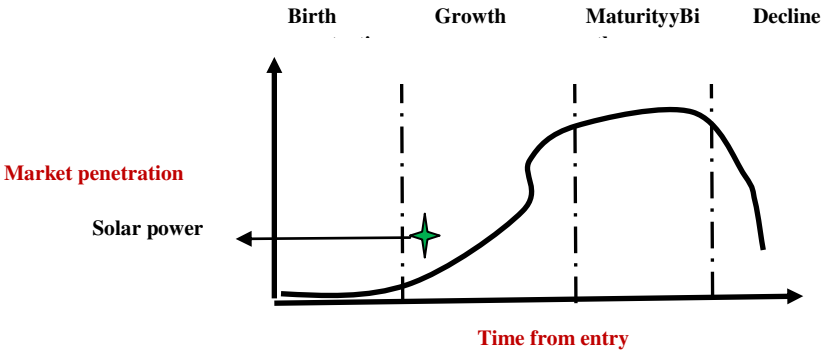


Figure 2.14 : Technology life–cycle analysis

Deep analytics evaluate and explores top technological innovations in terms of technology life cycle, technology trajectory, S-curve, technology diffusion and dominant design. Technology trajectory is **t**he path that the solar technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors on solar technology trajectory today. How to manage the evolution of this technological innovation? The nature of innovation may shift after a dominant design emerges. At present, the solar technology is waiting for the dominant design. The diffusion indicates how new solar technologies will spread through a population of potential adopters. It is controlled by the characteristics of innovation, economic environment and the adopters like innovators, early adopters, early majority, late majority and laggards.
At present, the technology of solar power is at growth phase of technology life-cycle [Figure 2.14]. It has come out from the emergence phase. It is interesting to understand how the life-cycle of solar technology is interacting with other technologies, systems, social impact, life-style and culture. The solar technology has been evolving from its parents such as other branches of electrical power system and electronics engineering; they are interacting with each other to form complex technological ecologies. The parents are adding their technological DNA which are the basic building blocks of new product development. A new development of solar technology must be nurtured properly since many technologies had perished at the emergence phase due to inherent constraints, uncertainties and risks. Next phase is growth; the solar technology has survived its early phases, it is adapting to various challenges of business model innovations and is forwarding to its intended environment with the emergence of competitors. It is basically the question of struggle for existence and survival for the fittest of the dominant design.
Initially, it may be difficult and costly to improve the performance of new solar technology; it may be costly for the adopters due to various uncertainties and risks. The performance is expected to improve with better understanding of the fundamental principles and system architecture. Gradually, this new technology may be adopted by large segments of the market due to reduced cost and risks. The rate of improvement of the new solar technology may be faster than the rate of market demand over time; the market share is expected to increase with high performance. The evolution of the solar technology is now passing through a

phase of turbulence and uncertainty; various stakeholders of the supply chain are exploring different competing design options and a dominant design is expected to emerge in near future through the consensus and convergence of the system intelligence. Then, the producers will try to improve the efficiency and design of solar power systems based on stable benchmark of the industry. The dominant design must consider an optimal set of most advanced technological features which can meet the demand of the users, supply chain and design chain in the best possible way.

6.3 Quantitative Analysis: It is essential to exercise intelligent quantitative analysis through business analytics and technical analytics based on up-to-date technical and business data. Both types of analytics are closely associated. The scope of business analytics should be explored in terms of installed power generation capacity: Energy type, capacity (MW/GW), Period (year); PV market analysis based evolution of PV modules production : The basic parameters for this analysis may be energy sources (e.g. solar, wind, tidel, thermal, hydel, nuclear), market share, zone and growth rate; SWOT analysis; Period (year), zone, PV production; Top PV cell production companies, Period (year), MW; Type of PV cell, MW and PV Module comparison based on efficiency, and power rating.
The scope of technical analytics should be explored through advanced experimental set up and graphical data visualization techniques.

- Solar cell
    - Cost vs. efficiency analysis : solar cell type (e.g. 1st, 2nd, 3rd generation), material (Si, III-V, II-VI, I, III, VI, Nano PV), , cost , energy conversion efficiency;
    - V-I characteristics : short circuit, open circuit, MPP at different irradiation and temperature
    - P-V characteristics for equivalent series and parallel resistance
    - Absolute error vs. voltage
    - Company, device, size, efficiency (%), Power (MW);
    - PV cell material, optimal absorption, band gap (minimum and maximum eV);
    - Deposition time vs. evaporation rate
- Power electronic circuit performance analysis:
    - DC-DC boost converter
        - Performance analysis: input voltage, input current, input power, output voltage, output current, output power, duty ratio, efficiency (%), ripple (%)
        - Transient performance analysis : time (S) vs. output voltage (V), time (S) vs. output current (A) under varying load and irradiation;
        - Converter type (classical, proposed), output voltage, output current;
        - Simulation testing analysis : input voltage, inductance, capacitance, load resistance, duty ratio, switching frequency;
        - MPPT analysis : PV panel rating, rated voltage, rated current, rated power, open circuit voltage, short circuit voltage, short circuit current, MPPT;
        - Duty ratio vs. output voltage graph;
        - 3-D Radar plot of performance measurement: output voltage (V), output current (A) and efficiency (%);
        - PV panel output analysis : voltage (V) vs. current (A), voltage (V) vs. power (W);
    - Photovoltaic module integrated Inverter or micro-inverter
        - Performance comparison of various types of micro-inverters : topology (series buffer, parallel buffer, flyback, boost, AC Link), energy storage, input voltage (V), rated power(W), efficiency, reactive power, complexity (low, medium, high);
        - Input voltage, output voltage, output power, line frequency;
        - Switching frequency, buffer voltage, inductance, capacitance, transformer turns ration, MOSFET rating, resonant inductance and capacitance;
        - Waveform analysis : current, voltage, line phase vs. current, line phase vs. phase shift, line voltage phase angle vs. impedance, line phase vs. efficiency; current waveform of flyback inverter under BCM and DCM control, input and output waveform, PV voltage vs. PV current, PV voltage vs. PV power, PV voltage and

current under half and full load conditions, grid voltage and current under half and full load conditions;
        - Comparative analysis on BCM and DCM in terms of switching frequency, power transfer, peak current sensing, loss analysis under high and low load, efficiency vs. output power
- Battery performance analysis in terms of battery capacity, nominal voltage, minimum battery voltage, maximum discharge current, maximum charging voltage, maximum charging current, steady state and transient analysis;
- Temperature profile of solar cooker (Time vs. Temperature)

6.4 Shared vision : Efficient change management is one of the most critical success factors in solar system implementation. It ensures that an organization and its workforce are ready, willing and able to embrace the new business processes and systems. The change management is a complex process. The change should occur at various levels: system, process, people and organization. Communication is the oil that ensures that everything works properly in solar system implementation. Management's honest determination to exert and maintain its right to decide within a policy of fairness and openness is essential for successful change management. An efficient leader creates understanding among his workforce through intelligent corporate communication.

6.5 Communication protocol : It is essential to communicate the scope of solar power to the common people, corporate sector, public policy makers, state and central governments, academic and research community through popular broadcast communication channels (e.g. TV, radio, social media, social networking sites, SMS, MMS, corporate web portals etc.) and adoption of rational and intelligent programmes, advertising and promotions. It is also possible to make innovative and creative documentary films on solar power evolution and broadcast the same to the academic and research community through school and college education systems and YouTube channels. It is rational to focus on introduction of courses on renewable energy and solar power in academic programmes of Electrical and Electronics Engineering (e.g. B.Tech, M.Tech, B.E.E, M.E., Ph.D.) and also business management (e.g. Technology Management, Strategic Management and Business Analytics for BBA, MBA, PGDM, PGDBM).

6.6 The goal : The strategic intelligence is associated with good governance, good wishes in public policy, industry analysis, efficient enterprise resource planning, supply chain management and marketing efforts (e.g. pricing, promotion, trust in communication, sales and distribution). Let us first consider *pricing strategy*. The diffusion of solar power requires a rational, discriminatory and fair pricing mechanism, incentive and subsidy policies. Industrial power play may be a serious threat against the adoption of solar energy. Existing power generation, transmission and distribution companies are comfortable with traditional thermal power technology. The coal, oil and gas industries are also not comfortable with the emerging trends of renewable sustainable energy. They do not want to save precious fossil fuels and oil. That is why, the old power generation and distribution firms are not serious in R&D and deployment of solar power system globally. Solar power is a real transformation initiative and the old firms are trying to resist against this change. Our society needs fundamental rethinking and radical redesign of energy policy. The pricing policy of solar power system (e.g. energy service charge, price of standalone solar power systems) should have necessary *competitive intelligence* to conquer the aforesaid threats.
Next, let us consider the *promotional strategy*. An intelligent marketing strategy is essential for proper technology management and enhancement of the awareness of new solar technology. The trade fairs and energy summits are expected to perform live product demonstration and interactive brainstorming sessions; audio and video display of solar power plants and standalone systems already in use in various places of the world; invite national and international technical experts and scientists from industry and academic institutions; invite energy policy makers, consultants, engineers, students, strategists, architects, construction and infrastructure project managers, entrepreneurs, traders, venture capitalists, banking & financial institutions (e.g. NABARD, national banks); invite Business Intelligence analysts to discuss possible growth roadmap and publish smart product catalogues and brochures. Event management plays an important promotional strategy; various workshops, conferences and seminars should encourage exchange of innovative ideas among the experts. There are other important initiatives such as training sessions for the workforce of construction and infrastructure firms, power generation, transmission and distribution companies and contractors; advertisements in popular business and industry magazines and daily

newspapers; intelligent broadcast through TV, radio and corporate communication channels; pilot projects in villages, hilly areas, forests and deserts and active involvement of gram panchayat and municipal corporations in solar power system implementation programmes.
Another critical strategy is related to *production process and supply chain management of solar cells*. Sustainable photovoltaics need the production of next-generation smart materials, devices and manufacturing processes suitable for global needs, environment and resource availability, advanced manufacturing process and multi-scale modeling and reliability. Solar energy integration is a critical issue; it is essential to identify and assess key technical, economic, environmental, and policy barriers in the adoption of solar power globally. For correct road mapping and assessment, it is required to analyze market research, policy and technical data, solar energy integration, storage and multi-scale (10 - 500 kW) concentrating solar power systems.

7. STAFF-RESOURCES

The sixth element of deep analytics is staff-resources. The sources of solar power innovation should include R&D units of renewable energy and powergrid corporation, electrical, power electronics, photonics and power plant departments of engineering institutes, technology management department of management institutes and collaborative networks. Creativity is the underlying process for solar power innovation which should promote new ideas through shared vision, intellectual abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics. It demands the motivation and commitment of intelligent and creative people to look at the problems in unconventional ways.
For instance, we are enjoying today the innovation of internet and wireless mobile communication technology due to hard work, commitment and involvement of the great talents in electronics and telecommunication engineering. Similar type of involvement and commitment is essential from electrical and electronics engineering, photonics and renewable energy sectors globally. Organizational creativity should be fostered through intelligent human capital management, talent acquisition and retention strategy, complex and tacit knowledge management strategy, organization structure, corporate culture, routine and incentive policy. What should be the right organization structure and innovation model for the evolution of solar technology? Is it possible to improve the efficiency of innovation model through various structural dimensions such as formalization, standardization and centralization? It is an open research agenda.
The business model of solar power should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated staffs or HR workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for the diffusion of new technology. New skill should be developed in erection, testing, commissioning, operations, maintenance and trading of solar power system. The business model requires the support of a good human resource management system for talent acquisition and retention, skill development, training, career growth planning, incentive, reward, recognition and payment function.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforce involved in solar power innovation are expected to develop different types of skills in technical (e.g. photonics, photovoltaic and renewable energy, power plant, power electronics, electrical and electronics), technology management and system administration such as research and development, maintenance support, knowledge management, system design and project management (e.g. erection, testing and commissioning). The system administrators must have multiple leadership skills like smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of solar power innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management can tackle the complexity of system implementation by developing an efficient team through group dynamics.
It is essential to develop skills in development of solar power system through proper coordination among design, supply and customer chain and R&D, production and marketing functions. The basic objectives are to maximize fit with the needs of the users, ensure quality assurance, minimize time to

market, sales and distribution and control product development cost. It may be an interesting initiative to make the suppliers and the users involved in the development process.
The workforce involved in solar power trading should develop different types of skills such as research and development, product design, sales, event management, project management, erection, testing, commissioning and service maintenance. An effective innovation model requires the support of a knowledge repository in the form of a digital library which should extract good up-to-date data from top journals and magazines on solar power electronics and solar energy. The list of journals and magazines includes Energy and Environmental Science, Advanced Energy Materials, Progress in Photovoltaics: Research and Applications, Annual Review of Chemical and Bimolecular Engineering, Nano Energy, Renewable and Sustainable Energy Reviews, IEEE Transactions on Sustainable Energy, IEEE Transactions on Power Electronics, Polymer Reviews, Solar Energy Materials and Solar Cells, Solar Energy, Renewable Energy, Environmental Research Letters, IET Renewable Power Generation and Journal of Photonics for Energy.
What should be the ideal organization model for solar power trading? A traditional functionally centered organization model may be suitable for supporting end-to-end business processes. The business model of solar power requires the support of a functional structure enabled with advanced information and communication technology. The structure should have project, design, power generation, distribution, maintenance, revenue management, human resource management, supply chain management and finance cells. The business model requires a collaborative and cooperative work culture.
Technology management is not a trivial simple problem. The model of solar power innovation encompasses over multiple domains like electrical engineering, power electronics, materials science, structural engineering, physics, photonics, chemistry, chemical engineering, nano-technology and business analytics. National and international technical experts and scientists from industry and also academic institutions should exercise knowledge management through a collaborative platform. The energy policy makers, consultants, engineers, technicians, strategists, construction professionals, architects, infrastructure project managers, entrepreneurs, traders, venture capitalists, banking and financial institutions should provide necessary support to the industrial member organizations and trade fair committees and organizers. The social media, news and TV broadcast can play a responsible role for general awareness of the public and government and promotion of the technology globally.

The diffusion of solar power technology requires the support of great leadership style; they are not only industry leaders but also political one. The style is basically the quality of leadership; the great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. The leaders must be able to share a rational vision, mission and values related to solar energy among all the stakeholders honestly and appropriately in time. It is really challenging for great leaders to implement the solar power system physically and practically to ensure global energy security. They have to face and tackle threats from traditional industries (e.g. coal, oil and gas, thermal and nuclear power), selfish local bias, power play and politics. They must understand the intelligence of business modeling and system dynamics associated with solar energy, they must do fundamental rethinking and radical redesign of global energy trading system. Top management can tackle the complexity of system implementation by developing a strong project team, which should be a right mix of dedicated resources like technical and business experts.

8.1 Innovation Model

What should be the innovation model for effective diffusion of solar power technology? Is it possible to adopt K-A-B-C-D-E-T-F model?

- ***Knowledge manager***: The innovators should acquire the basic and fundamental concept through a *differentiated* course work; classify the primary, secondary and tertiary focus areas. Mandatory courses: Innovation, creativity and research methodology; communication. The depth and breadth of the course works should be traded off rationally. It needs proper guidance.
- ***Activator***: The activators should initiate the innovation process by identifying a good research problem through scope analysis. Random selection of research problem should be avoided by evaluating the strength, experience and skill of the innovators. The research problem should have potential business intelligence and social benefits.

- ***Browser***: The browsers should search for information; investigate throughout the process and find relevant data or information to start innovation. They may review and analyze the existing works through traditional sources of research data (e.g. digital library, books, papers, journals, magazines, industry reports, you tubes) and also through webinars, social networking and attending seminars, workshops and conferences. Random search may result wastage of time; a systematic and planned / guided search process may lead to good results.
- ***Creator***: The creators should analyze the gap and think of to-be system; generate new ideas, concepts and possibilities and search for new solutions.
- ***Developer***: The developers should transform the ideas of the creation phase into good solutions; turn the ideas into deliverables, products and services. They should collaborate with different research forums, industries and experts during this phase.
- ***Executor***: The executors should implement and execute the roadmap of the innovation.
- ***Tester:*** The testers should do various types of experiments and laboratory works; verify system dynamics and monitor the performance of the deliverables. Advanced research laboratories are required for complicated testing and experiments.
- ***Facilitator***: The facilitators should define project plan, corporate governance policy, marketing plan, production plan, investment plan and cost-benefit analysis. They should be able to identify the revenue and profit making stream and fair, rational business intelligence. The government should provide financial assistance to the innovators in patent registration.

9. CONCLUSION

This chapter has explored the potential of solar power through Deep Analytics '7-S' model. It is clear from scope and SWOT analysis that solar power is a potential option of sustainable energy and business model innovation for the future as compared to other sources of energy. Solar power is at the growth phase of technology life-cycle. The technology is still not matured; there are several constraints such as efficiency of solar cell and cost of solar panels. It is possible to extend the scope of solar power in battery charging of electric vehicles (reference: chapter 3) and drones. It may be very useful and economical to adopt solar power driven water pumps in agriculture, warehouses, cold storages and other innovative applications. The ultimate success of any innovation effort no longer depends on a single element alone. It is important to understand the customers and competition and also to recognize and align the critical partners in the innovation ecosystem. It is essential to identify the blind spots of solar technology which are efficient solar cell, power electronics circuit and business model innovation.

REFERENCES

1. R.H.Waterman, T.J.Peters and J.R. Phillips. Mckinsey & Company. Structure is not organization. Business Horizons. June'1980.
2. M.W.Johnson, C.M.Chritensen and H.Kagermann. Reinventing your business model. Harvard Business Review. Decmber'2008.
3. M.Hammer. Process management and the future of six sigma. MIT Sloan Management Review, Vol. 43, No. 2, pp.26–32.2002.
4. S.Chakraborty and S.K.Sharma. Enterprise Resource Planning: an integrated strategic framework. International Journal Management and Enterprise Development, Vol. 4, No. 5, 2007.
5. R.Roy. Entrepreneurship. Oxford University Press. 2008.
6. G.Boyle. Renewable Energy. 2nd Edition. Oxford University Press. 2004.
7. Department of Energy, USA. Renewable energy: an overview. March'2001.
8. F.Kreith and D.Y.Goswami (edited). Handbook of energy efficiency and renewable energy. CRC Press. 2007.
9. B.K.Bose. Power Electronics and Motor Drives. Advances and trends. Elsevier. 2006.
10. S.K.Mazumder. High-Frequency Inverters: From Photovoltaic, Wind and Fuel Cell Based Renewable and Alternative Energy DER/DG Systems to Energy-Storage Applications. University of Illinois, USA. 2010.

11. X.Yang, Y.Song, G.Wang and W.Wang. A comprehensive review on the development of sustainable energy strategy and implementation in China. IEEE Transactions on Sustainable Energy, volume 1, no. 2, July'2010.
12. H.M.Upadahyaya, T.M.Razykov and A.N.Tiwari. Thin film PV Technology. In F.Kreith and D.Y. Goswami (Edited). Handbook of energy conservation and renewable energy. CRC Press, NY,USA. 2007.
13. T.M.Razykov,B.Rech and A.N.Tiwari (Edited). Special issue on thin film PV. Solar Energy, N6. 2004.
14. S.B.Kjaer, J.K.Pedesen and F.Blaabjerg. A review of single phase grid connected inverters for photovoltaic modules. IEEE Transactions Industrial Application. Volume 41, no. 5, pp. 1292-1306, Sep / Oct'2005.
15. ABB online document : Distributed energy storage product presentation. 2010.
16. U.S. Department of Energy. Solar Energy Grid Integration System Energy Storage (SEGIS-ES).May'2008.
17. S.J.Chiang, K.T.Chang and C.Y.Yen. Residential photovoltaic energy storage system. IEEE Transactions on Industrial Electronics. vol. 45, no. 3, pp 385-394, June'1998.
18. R.W.De Doncker, C.Meyer, R.U.Lenke and F.Mura. Power electronics for future utility applications. IEEE 7th International conference Power Electronics Drive System. November'2007.
19. F. Katiraei, R. Iravani, N. Hatziargyriou and A. Dimeas. Microgrids management. IEEE Power Energy Magazine, vol. 6, no. 3, pp. 54–65, May/Jun. 2008.
20. M. Marinelli, F. Sossan, G. T. Costanzo and H. W. Bindner. Testing of a Predictive Control Strategy for Balancing Renewable Sources in a Microgrid. IEEE Transactions on Sustainable Energy.
21. J.Charias. Maxium power solar converter. Microchip.
22. R.Faranda and S.Leva. A comparative study of MPPT techniques for PV system. 7th WSEAS International Conference on Application of Electrical Engineering, Norway, July,2008.
23. T.Esram and P.L.Chapman. Comparison of photovoltaic array maximum powerpoint tracking techniques. IEEE Transactions on Energy Conversion. Vol. 22, No.. 2, June 2007.
24. J.Charais. Maximum power solar converter. Microchip Technology Incorporation. 2010.
25. RIB, Italy. Solar amplifier. Code ACG9125.
26. J.Falin and W.Li. A boost-topology battery charger powered from a solar panel. Texas Instruments. www.power.ti.com.
27. http://www.MitsubishiElectric.com
28. http://www.tatapowersolar.com
29. http://www.msme.gov.in
30. http://www.ediindia.org, www.nabard.org
31. S. B. Kjaer, J. K. Pedersen, and F. Blaabjerg. A review of single-phase grid-connected inverters for photovoltaic modules. *IEEE Trans. Ind. Appl.*, vol. 41, no. 5, pp. 1292–1306, Sep./Oct. 2005.
32. S. B. Kjaer, J. K. Pedersen, and F. Blaabjerg. Power inverter topologies for photovoltaic modules-a review. in *Proc. 37th IAS Annu. Ind. Appl. Conf. Meet. Rec.*, 2002, vol. 2, pp. 782–788.
33. F. Blaabjerg, R. Teodorescu, M. Liserre and A. V. Timbus. Overview of control and grid synchronization for distributed power generation systems. *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1398–1409, Oct.2006.
34. B. J. Pierquet. *Designs for Ultra-High Efficiency Grid-Connected Power Conversion*. Ph.D. dissertation, Dept. Electric. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, 2011.
35. P.Sanjeevikumar, E.Kabalci, A.Iqbal, H.Abu-Rub, O.Ojo. Control Strategy and Hardware Implementation for DC-DC Boost Power Conversion Based on Proportional-Integral Compensator for High Voltage Application. *Engineering Science and Technology: An International Journal* (*JESTECH*), Dec.2014.
36. P.Sanjeevikumar, A.Iqbal, H.Abu-Rub, M.Bishal. Implementation and control of extra high voltage dc-dc boost converter. *7th IET Intl. Conf. on Sustainable Energy and Intelligent System,* IET-SEISCON'13,Chennai, India. 2013.
37. F.Blaabjerg, F.Iov, T.Kerekes, R.Teodorescu. Trends in power electronics and control of renewable energy systems. *14th Int. Power Electron. & Motion Control Conf.,* 2010.
38. J. M. Guerrero, F. Blaabjerg, T. Zhelev, K. Hemmes, E. Monmasson,S. Jemei, M. P. Comech, R. Granadino, and J. I. Frau. Distributed generation: Toward a new energy paradigm. IEEE Ind. Electron. Mag., Vol. 4, No. 1, pp. 52-64, Mar. 2010.

39. R. Lasseter. Smart distribution: Coupled microgrids. IEEE Proc., Vol. 99, No. 6, pp. 1074-1082, Jun. 2011
40. M. Barnes, J. Kondoh, H.Asano, J. Oyarzabal, G. Venkataramanan, R. Lasseter, N. Hatziargyriou, and T. Green. Real-world microgrids – an overview. Proc. IEEE SoSE, pp. 1-8, 2007.
41. N. Hatziargyriou, H. Asano, R. Iravani and C. Marnay. Microgrids. IEEE Power Energy Mag., Vol. 6, No. 4, pp. 78-94, Jul./Aug. 2007.
42. F. Katiraei, R. Iravani, N. Hatziargyriou and A. Dimeas. Microgrids management. IEEE Power and Energy Mag., Vol. 6, No. 3, pp. 54 -65, 2008.
43. A. Timbus, M. Liserre, R. Teodorescu, P. Rodriguez, and F. Blaabjerg. Evaluation of current controllers for distributed power generation systems. IEEE Trans. Power Electron., Vol. 24, No. 3, pp. 654-664, 2009.
44. M. Kazmierkowski, R. Krishnan, and F. Blaabjerg. Control in Power Electronics. London, U.K.: Academic, 2002.
45. N. Pogaku, M. Prodanovic and T. Green. Modeling, analysis and testing of an inverter-based microgrid. IEEE Trans. Power Electron., Vol. 22, No. 2, pp. 613-625, 2007.
46. P. Kundur, Power system stability and control. New York: McGraw-Hill, 1994.
47. J. Lopes, C. Moreira and A. Madureira. Defining control strategies for microgrids islanded operation. IEEE Trans. Power Syst., Vol. 21, No. 2, pp. 916-924, May 2006.
48. M. H. Nehrir, C. Wang, K. Strunz, H. Aki, R. Ramakumar, J. Bing, Z. Miao, and Z. Salameh. A Review of Hybrid Renewable/Alternative Energy Systems for Electric Power Generation: Configurations, Control, and Applications. *IEEE Trans. Sustain. Energy*, vol. 2, no. 4, pp. 392–403, Oct. 2011.
49. K. Kurohane, T. Senjyu, A. Yona, N. Urasaki, T. Goya, and T.Funabashi. A hybrid smart AC/DC power system. *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 199–204, 2010.
50. K. T. Tan, P. L. So, Y. C. Chu, and M. Z. Q. Chen. Coordinated Control and Energy Management of Distributed Generation Inverters in a Microgrid. *IEEE Trans. Power Delivery*, vol. 28, no. 2, pp. 704–713, Apr. 2013.
51. C. T. Rodríguez, D. V. de la Fuente, G. Garcerá, E. Figueres, and J. A. G. Moreno. Reconfigurable Control Scheme for a PV Microinverter Working in Both Grid-Connected and Island Modes. *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1582–1595, Apr. 2013.
52. Sh. Jiang, W. Wang, H. Jin, and D. Xu. Power Management Strategy for Microgrid with Energy Storage System. in *Proc. 2011 IEEE IECON- 37th Annual Industrial Electronics Society Conf.*, pp. 1524-1529.
53. International Standard for Testing Solar Cookers ASABE Standard S580 Dr. Paul A. Funk, Avinashilingam University, Coimbatore, India, January 1997.
54. S. C. Mullick, T. C. Kandpal, and A. K. Saxena. Thermal test procedure for box-type solar cookers,*Solar Energy*, vol. 39, no. 4, pp. 353–360, 1987.
55. S. K. Philip and H. N.Mistry. Solar cooker testing: "a suggestion for change in BIS standards, *SESI Journal*, vol. 5, pp. 17–22,
1995.
56. S. K. Philip, T.K.Chaudhuri and H. N.Mistry. Testing of solar box cookers, in *Proceedings of the 3rd International Conference on Solar Cookers Use and Technology*, Coimbatore, India, 1997.
57. S. B. Joshi and A. R. Jani. Photovoltaic and Thermal Hybridized Solar Cooker. Hindawi Publishing Corporation ISRN Renewable Energy Volume 2013, Article ID 746189.
58. http://www.indiawaterportal.org accessed on 15.08.2018
59.http://mnre.gov.in/□le-manager/UserFiles/Schemefor-Solar-Pumping-Programme-for-Irrigation-and-Drinking-Water-under-offgrid-and-Decentralised-Solar-applications.pdf accessed on 15.08.2018.
60. Trombly, J., "Technology solutions: Nano-PV set to accelerate solarenergy use," *Environ. Sci. Technol*., 38, pp. 376–376A, 2004.
61. Catchpole, K. R., "Nanostructures in photovoltaics," *Phil. Trans. Math. Phys. Eng. Sci.*, 364, pp. 3493–3503, 2006.
62. Tsakalakos, L., "Nanostructures for photovoltaics," *Mater. Sci. Eng*., 62(6), pp. 175–189, 2008.
63. Green, M., "Silicon photovoltaic modules: A brief history of the first 50 years," *Prog. Photovolt.*, 13, pp. 447–455, 2005.
64. Jadhav, M. V., Todkar, A. S., Gambhire, V. R., and Sawant, S. Y., "Nanotechnology for powerful solar energy," *Int. J. Adv. Biotechnol. Res*.,
2, pp. 208–212, 2011.

65. Honsberg, C. B., Barnett, A. M., and Kirkpatrick, D., "Nanostructured solar cells for high efficiency photovoltaics," in *Photovoltaic Energy Conversion, IEEE 4th World Conference*, Hawaii, USA, 2006.
66. Nozik, A. J., "Nanoscience and nanostructures for photovoltaics and solar fuels," *Nano Lett*., 10(8), pp. 2735–2741, 2010.
67. Green, M. A., Emery, K., Hishikawa, Y., and Warta, W., "Solar cell efficiency tables (Version 34)," *Prog. Photovolt. Res. Appl.*, 17, pp. 320–326, 2009.
68. Goetzberger, A., Hebling, C., and Schock, H., "Photovoltaic materials, history, status and outlook," *Mater. Sci. Eng. R Rep.,* 40, pp. 1–46, 2003.
69. Banerjee, S., Misra, M., Mohapatra, S. K., Howard, C., Mohapatra, S. K., and Kamilla, S. K., "Formation of chelating agent driven anodized TiO2 nanotubular membrane and its photovoltaic application,"*Nanotechnology*, 21, pp. 145201, 2010.
70. Jadhav, M. V., Todkar, A. S., Gambhire, V. R., and Sawant, S. Y.,"Nanotechnology for powerful solar energy," *Adv. Biotech*. *Res*., 2(1),pp. 208–212, 2011.

Exercise

1. **Explain the technology of solar power. Justify it as a technology for humanity. What is the scope and emerging applications of this technology?**
2. **What is the dominant design of the technology?**
3. **What are the basic elements of the system architecture?**
4. **What do you mean by technology security? How to verify the security intelligence?**
5. **What are the strategic moves of technology innovation, adoption and diffusion for solar power? What is the outcome of technology life-cycle and SWOT analysis?**
6. **How to manage resources for this innovation project?**
7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
9. **Discuss the evolution of nanotechnology for solar cells.**
10. **Design an intelligent power electronic circuit for solar power system.**

CHAPTER 3: ELECTRICAL & HYBRID VEHICLES - SMART BATTERIES & CHARGING MECHANISM

Abstract: Sustainable transportation infrastructure demands widespread adoption of electric vehicles (EVs) and renewable energy sources. The use of EVs is growing due to increasing technological success of complex and reliable hybrid vehicles; technological diffusion of Li-ion batteries and increasing willingness of society, political world and the automobiles market due to increasing environmental air pollution, global warming and fuel consumption and high stress on the storage of fossil fuels. This chapter analyzes the technological innovation of electrical and hybrid vehicles through deep analytics. The dominant design includes smart batteries. The chapter is organized as follows. Section 1 defines the scope of the technology. Section 2- 7 analyses the other six elements of the technological innovation: system, structure, security, strategy, staff-resources, and skill-style-support. Section 2 presents a mechanism for battery charging of electrical and hybrid vehicles. Section 5 highlights SWOT analysis and technology life-cycle analysis. Section 8 concludes the work.

Keywords: Electrical vehicles, Hybrid vehicles, Smart batteries, Smart transformers, Battery charging mechanism, Solar power, Security and safety, Mobile communication, IoT

1. SCOPE

Let us first focus on the scope of the technological innovation on electrical vehicles which includes E-bus, E-truck, E-scooter, E-bike, E- bicycle, E-Taxi and E-private car [1,2,4,14]. The scope can be extended to E-steamer/ launches / ships, electric trains (e.g. metro rail, mono rail, local trains) and small aircrafts (e.g. helicopters, hovercrafts, fighter planes, military aircrafts, HY4 plane free of carbon emission and driven by serial hybrid powertrain such as fuel cell and alternative energy sources like solar cell). It is interesting to develop power management system of the aircrafts which select appropriate energy sources as per the demand of aircraft and the propeller engine. Vehicles can be powered by internal combustion engine using gasoline, diesel or gas or electric drives. The critical success factors of vehicle manufacturing industry are sustainable, environment friendly design, improvements in power train systems, fuel processing and power conversion technologies.

Vehicles can be classified based on various types of synthetic fuels such as hydrogen, biodiesel, bioethanol, dimethylether, ammonia and electricity via electrical batteries : conventional gasoline vehicle (petrol or diesel, ICE), hybrid vehicle (gasoline fuel, electrical drive, rechargeable battery), electric vehicle (high capacity electrical battery, electrical drive), hydrogen fuel cell vehicle (high pressure hydrogen fuel tank, fuel cell, electrical drive), hydrogen internal combustion vehicle (high-pressure hydrogen fuel tank and ICE) and ammonia fueled vehicle (liquid ammonia fuel tank, hydrogen-fueled ICE). In case of electrical or hybrid vehicles, electricity may be produced from renewable energy sources or natural gas.

It is an interesting option to perform a comparative analysis among various type of vehicles based on a set evaluation parameters such as vehicle price, fuel cost, maintenance cost, economic attractiveness, driving range, energy and power features, safety, sustainability, fuel consumption, reduction in emission and environmental impact. The trading agents often try to trade-off miscellaneous critical factors such as vehicle performance, improved performance of fuel cell or batteries, cost, governmental subsidies and environmental pollution issues. It has been found that hybrid and electrical vehicles have many advantages than the other types of vehicles in terms of high fuel price and environmental pollution, the economics and environmental impact depends significantly on the source of electrical energy. If the electricity is generated from renewable energy sources, electric car is even better than hybrid vehicles [10-13]. Nickel metal hydride and Li-ion batteries have shown improved performance as compared to old lead-acid batteries.

1.1 Requirements Engineering of Vehicles

What should be the vision for the vehicles in future [15-19]? The requirements should be defined from several perspectives. It is essential to transform the design principles of the conventional vehicles. The traditional design is based on petrol and diesel engines for energy, internal combustion engine for power, manual control and independent standalone operation. The vision for the future vehicles may be based on

electrical and hybrid system, light, clean, safe, fun and fashionable design, mobile communication, and Internet of Things (IoT). The design of the vehicles should promote mobile Internet and IoT enabled by electronic tags and sensors and seamless connection to IoT; the basic objectives are efficient traffic management and reduced travel time by collecting, processing and sharing big data. The electrical and hybrid vehicles should be integrated with smart power grid having clean renewable energy sources (e.g. solar, wind and hydroelectric power), dynamic pricing mechanism and optimal balance between supply and demand of electrical energy. The vehicles should be designed with real-time control capabilities, mobile connectivity and onboard intelligence for optimal utilization of road and parking space and traffic congestion control.

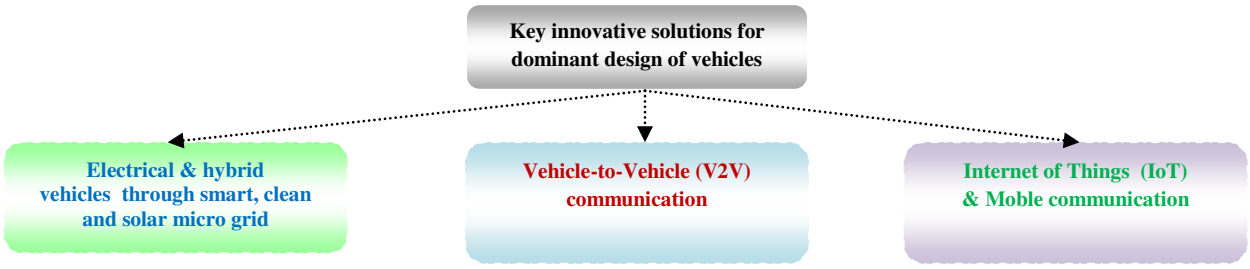


Figure 3.1 : Requirements engineering for dominant design of vehicles

The automobiles market demands fundamental rethinking, radical redesign and reinvention of vehicles of the future. The enabling technologies should be developed in terms of dominant design and converged for proper diffusion of electrical and hybrid vehicles globally. The expected benefits of converging innovative solutions should be explored in terms of lower cost, sustainable economic growth and prosperity, enhanced freedom, mobility, safety, zero emissions, use of clean renewable energy to fight against air pollution, climate change and global warming, minimal traffic congestion, increased roadway throughput, fun, entertainment and autonomous driving.

2. SYSTEM

BEVs are the simplest type of EV using electrical power from a single source of battery to power one or more electric motors. A single electric motor is connected to the front axle through a simple gearbox; a series of four hub motors may be attached to each wheel. The battery has many cells combined into modules and the modules are grouped into packs through series and parallel connections. Fo example, 100 Li-ion series connected batteries with cell voltage of 3.6V can produce 360 V. The battery pack is the largest and most expensive component of the BEV; it is readily removable and swappable. Typically, EVs have higher initial costs, lower fuel costs, lower external costs, higher insurance costs, lower maintenance and repair costs. The cost of EV system depend on various types of elements such as size of key components (e.g. batteries, fuel cells, electric motors), desired performance, driving range, energy efficiency, cost of key materials for EV components (e.g. Li for batteries, platinum for fuel cells and carbon fiber for pressure vessels), life-cycle of key components, the impact of technological learning and economies of scale on manufacturing cost, energy use of EV, technology, design of the power train, drive cycle and weight; cost of energy (e.g. fuel production, distribution and delivery costs, insurance and maintenance cost [5-9].

There are various types of battery charging methods such as normal, induction, semi-fast and fast charging [Figure 3.2]. Normal charging uses standard domestic socket, can be used anywhere but is limited in power. Semi-fast charging allows a higher charging power (up to 22 kW), suitable for most EVs. Fast charging needs a more expensive infrastructure. Inductive charging does not use plugs and cables and suitable for specific applications. The basic requirements of the technological innovation of EVs include availability of efficient electric energy storage devices or batteries and recharging infrastructure to transfer electric energy from the distribution grid to the battery.

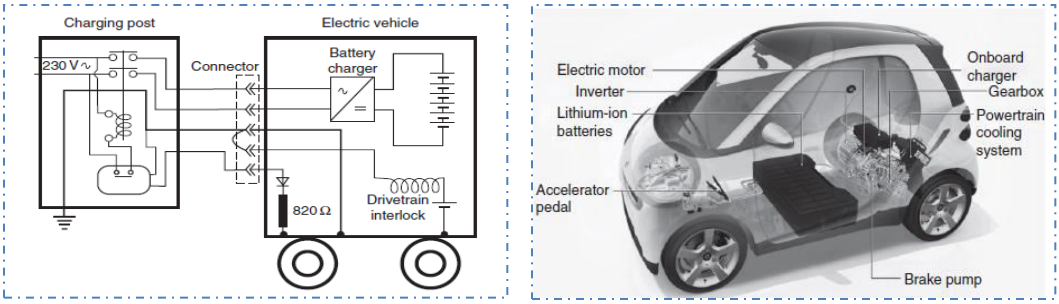


Figure 3.2 : Electrical vehicles charging system

EVs may also need intelligent communication protocol for vehicle identification and billing, charge cost optimization and grid load optimization. The value chain associated with electrical vehicles has various processes such as component production, cell production, module production, pack assembly, vehicle integration, use, reuse and recycling [Figure 3.3]. Typically, NCA (Li-Ni-Co), NCM (Li-Ni-Mn), LMO (Li-Mn spinel), LTO (Li-Titanate), Li ion Phosphate (LFP) technologies are used to make EV batteries. It is possible to do a comparative analysis of various types of batteries based on materials of anodes and cathodes, safety, performance,, cost, life-span, specific energy and specific power ([3], Figure 3.4)

2.1 Smart Batteries: Smart batteries are essential part of the dominant design of electrical and hybrid vehicles; Smart batteries should have higher energy density and tolerance to higher temperatures; should avoid the use of dangerous toxic materials, should be nonflammable and safe to use and should withstand higher voltage. Smart batteries are expected to be simple in design, cheaper and lighter in weight as compared to present batteries; won't need liquid cooling; the batteries should be long lasting, fire-proof and should permit faster charging. Existing battery technology for EVs is very expensive and has limitations in terms of poor system performance at low temperature, impact of pressure, breakage due to mechanical stress and risks of dendrites.

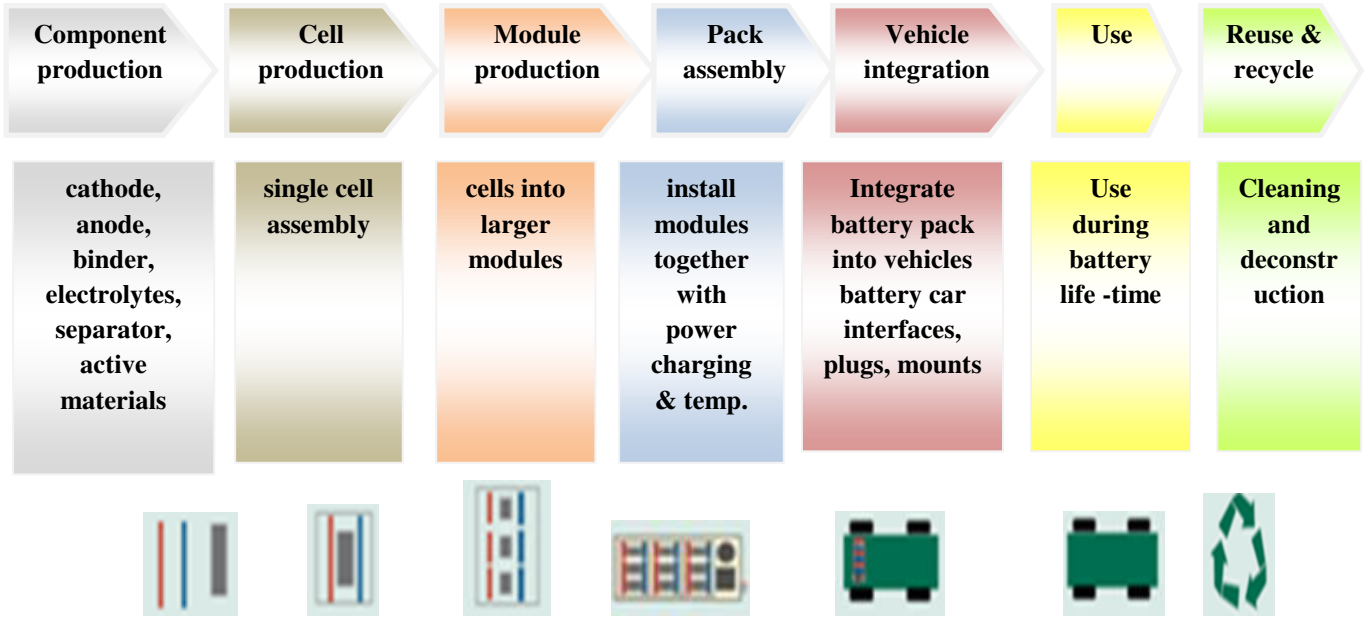


Figure 3.3: Value chain analysis of EV batteries

EVs can be classified into non-hybrid vehicles (ICE) drive), hybrid electric vehicle (micro, mild, full, plug-in), extended range EV (EREV), BEV and fuel cell electric vehicle (FCEV). The hybrid solution obtains reduction of consumption and emissions; heat engines are operated more efficiently; electric power accumulators and electric motors allow energy recovery during braking and its use for traction purposes. In

case of series hybrid vehicles, the electric motor supplies power to the wheels. In case of parallel hybrid vehicles, both the heat engine and the electric motor supply power to the wheels. In case of series-parallel hybrid vehicles, the heat engine can drive the wheels directly.

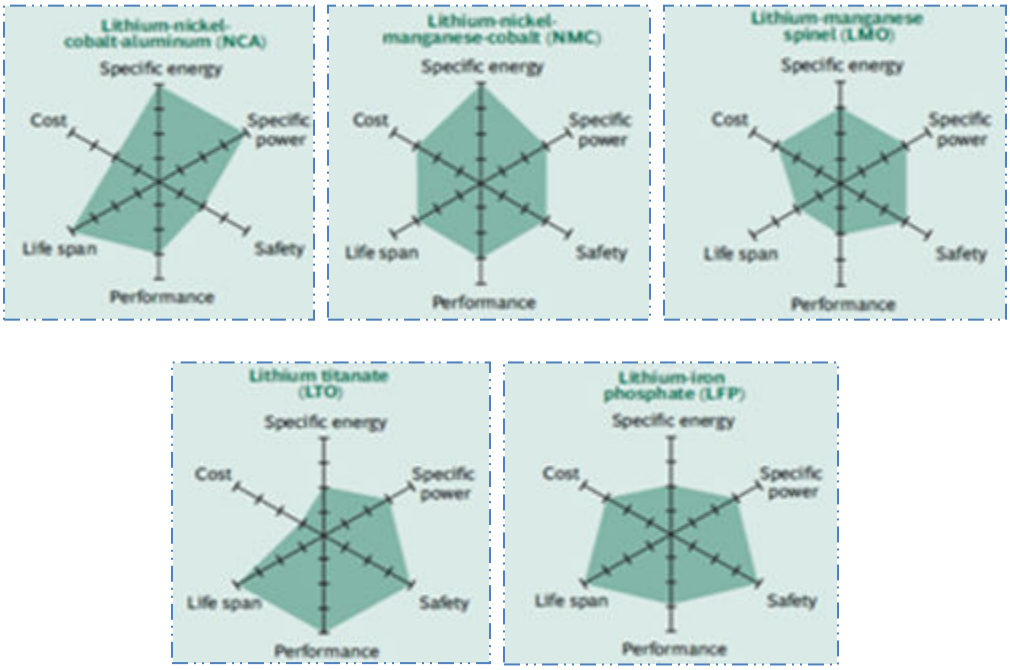


Figure 3.4 : Comparative analysis on batteries

2.2 Electrical Vehicle's Battery Charging Mechanism

Let us analyze the battery charging mechanism of electrical and hybrid vehicles. The basic objective is to develop an efficient market mechanism or market interface where the trading agents i.e. the service consumers of electrical vehicles and the service providers of battery charging stations act rationally and negotiate a flexible and intelligent service contract on the replenishment of charged batteries based on approximate estimation of their preferences in EV charging scenario. The market mechanism is expected to maximize the utilities of the trading agents through efficient resource allocation subject to the constraints of time and cost and limited supply of electrical energy. Traditional auction mechanism may not be an interesting option in this business model.

++

Agents : Service consumer (B), Service provider (S);
Input: Demand plan of B, Supply plan of S;
System: Electrical / hybrid vehicles, batteries, battery charging stations,
Objectives: minimize mismatch between demand and supply plans of charged batteries;
Constraints: time, cost, technology;
Strategic moves : Select optimal resource allocation heuristics.

- FCFS (First Come First Served)
- Most Requests First (MRF)
- Longest Waits First (LWF)
- Selective resource allocation for emergency load
- Linear allocation
- Proportional allocation

Protocol: The agents settle single or multiple intelligent service contracts.

- Collaborative planning, forecasting and replenishment (CPFR)
- Swing option
- Push pull

- Group buying

Payment function: verify business intelligence of service contracts in terms of (pay per use, payment mode, payment terms);
Security intelligence:

- verify security intelligence in terms of rationality, fairness, correctness, transparency and accountability;
- B and S preserve privacy of SC contract as per revelation principle;

Output: Battery charging service contract.

++

Collaborative planning, forecasting and replenishment (CPFR) is a strategic tool for comprehensive value chain management. This is an initiative among all the stakeholders of the supply / service chain in order to improve their relationship through jointly managed planning, process and shared information. The ultimate goal is to improve the position of the battery charging service provider in the competitive market and the optimization of its own value chain in terms of optimal inventory, improved sales, higher precision of forecast, reduced cost and improved reaction time to customer demands. The interplay between trust and technology encourages the commitment of collaboration among the trading agents.
Let us consider a specific scenario of multi-party negotiation in battery charging of electrical vehicles. *Swing option* is a specific type of supply contract in trading of stochastic demand of a resource such as charged battery for electrical / hybrid vehicles. It gives the owner of the swing option the right to change the required delivery of a resource through short time notice. It gives the owner of the swing option multiple exercise rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, $i \in [1,2,..,n]$, $1 \leq t_1 \leq t_2 \ldots \leq t_n \leq T$ at which a fixed number of $d_0$units of a resource may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where $g \leq n$ is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0. There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function for violating local or global constraints. In this contract, the primary negotiation issue may be a discriminatory pricing plan which depends on the negotiation of a set of secondary issues such as up-swing limit, down-swing limit, maximum total demand, minimum total demand, penalty function and number of swings for a specific period.

3. STRUCTURE

The third element of deep analytics is structure. The new automotive DNA is expected to be developed through proper integration of electrical drives and connected vehicle technologies. The design principles are based on electrical drives with electrical motors for power, renewable solar energy for battery charging and electronic systems for control. Hybrid EVs may use batteries and electric motors to improve the efficiency of mechanically driven vehicles. Smart vehicles are expected to be lighter, more conducive to electrical drives and renewable sources of energy to avoid air pollution. The computing schema should be able to estimate price and incentives for regulating demand and supply of electrical energy. Smart vehicles should be able to communicate wirelessly with each other and with roadway infrastructure and activities through global positioning system (GPS) technology and digital maps. Intelligent vehicle-to-vehicle (V2V) communication protocols should be able to avoid collision and crashes.

SL No.	Structural components	Technology schema
1.	Mechanical system	Mechanical components, transmission, brakes
2.	Electrical & Electronics system	Power supply, battery charger, batteries, inverter,

		motor
3.	Battery charging station	Normal, induction, fast and semi-fast charging
4.	Information & communication technology	Digital transformation : Computing, networking, data, application and security schema, intelligent communication protocol

Table 3.1 : Structural analysis of electrical and hybrid vehicles

The topology of smart vehicles has been analyzed in terms of a set of sub-systems or modules, connectivity, type of connections, layers, interfaces between layers and organization of layers. The structure of EVs has three major components: mechanical system (e.g. brakes, wheel), electrical and electronics system (e.g. battery charging) and information & communication systems (e.g. driver advice system) [Table 3.1]. The sensors collect data from various systems and provide the inputs to DAS. DAS analyzes the sensed data and shows the output (e.g. alerts, advice) to the driver. Figure 3.5 shows typical structure of a hybrid EV.

It is essential to adopt a new automotive DNA which can transform the design principles of smart vehicles. The structure of traditional vehicles is mechanically driven and powered by ICE, energized by petrol and diesel, mechanical control system and operated in standalone mode. The new structure is expected to be more flexible, automated and simple to use. Another important part of the structure is mobile Internet; it is the backbone of communication schema which should enable the vehicles to share real-time and location-specific big data for optimal traffic management, minimal and more predictable travel time and no distraction of driving. The vehicles should be integrated with IoT and may be considered as nodes in mobile networks. The structure is expected to be less expensive to own and operate and should have light weight and less space. The integration of a set of transformative ideas should optimize the benefits, positive impacts and side effects in terms of design direction, energy, environment, safety, congestion and access inequality. These enabling technologies have been getting matured and converged gradually for practically feasible and large scale production.

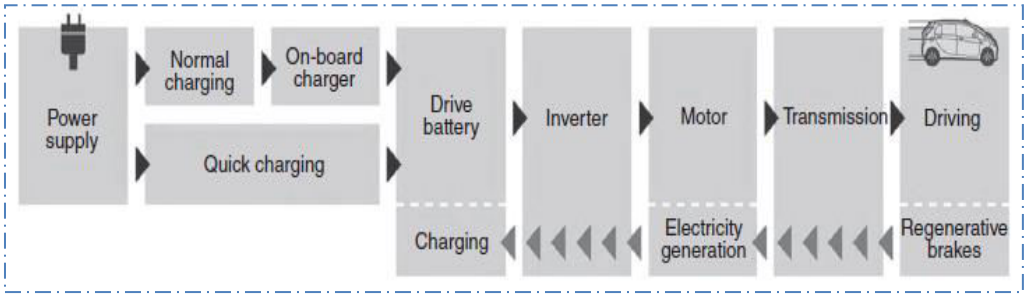
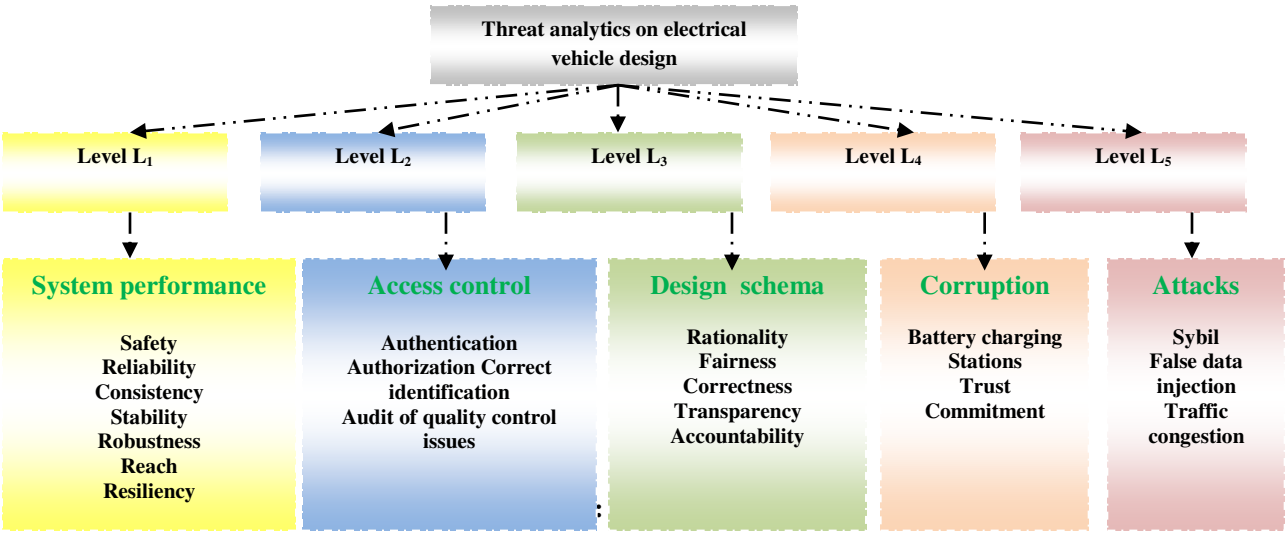


Figure 3.5 : Typical structure of hybrid EV

3.1 Smart Batteries: Smart batteries are an essential part of electrical and hybrid vehicles; let us explore and analyze the scope, system, security and strategy of smart batteries for EVs. Solid State Batteries (SSB) may be the future of EVs. Alternatively, EVs can use batteries having Li-ion, Ni-metal hydride (NiMH) and electric double layers ultra capacitors led by Li-ions. SSB is an emerging technology that uses solid electrodes and solid electrolyte such as ceramics (oxides, sulfides and phosphates)**,** glass and solid polymers**.** Solid state batteries are safer with higher energy densities but at higher cost. Li-ion batteries use liquid or polymer electrolytes. SSB is generally used in pacemakers, RFID and wearable devices. Presently, the technology of SSB is being developed at Tesla, Toyota, Dyson (Sakti 3), Caterpillar (Fisker), Swiss Fraunhofer institute, Cambridge University; the technology has been diffusing globally. Toyota has planned to use solid state batteries in EVs by 2020. The challenge is to explore a solid conductive material fit for large batteries. Solid Power and Volkswagen are also investing to build high capacity manufacturing plants of SSB.

4. SECURITY



It is essential to design electrical / hybrid vehicles in terms of security at various levels – L_1, L_2, L_3, L_4 and L_5[Figure 3.6]. Level L_1 verifies system performance in terms of safety, reliability, consistency, stability, robustness and reach. The other critical design issues are also associated with resiliency, reachability, deadlock-freeness, synchronization and interactive intelligent communication among electrical / hybrid vehicles. Solid-state battery technology has higher energy density and tolerance to higher temperatures; may avoid the use of dangerous toxic materials, nonflammable and safer; can withstand higher voltage and longer life-cycle and support faster recharging rate. The safety of electrical / hybrid vehicles depends on access control at level L_2 in terms of authentication, authorization of the drivers, correct identification of the system components and audit of quality control issues. The security schema is also designed and verified at level L_3 in terms of fairness, correctness, transparency, accountability, trust and commitment. The safety of the electrical / hybrid vehicles may be threatened at level L_4 through the corruption of various stakeholders such as car manufacturers, drivers, passengers and battery charging station supervisors. The design of the vehicles is expected to assess and mitigate the risks of various types of attacks at level L_5 such as false data injection, sybil, shilling and traffic congestion.

5.1 Real-Time Fault Diagnostics [RTFD]

It is essential to monitor and detect the faults of a complex real-time system such as electrical and hybrid vehicles; assess the chance of various types of faults and explore efficient and reliable fault detection and isolation methods based on artificial intelligence. The basic building blocks of real time fault diagnostics are soft computing and AI methods such as knowledge based expert system, model based system, if-then rule based system, artificial neural network (ANN), fuzzy logic, genetic algorithm (GA), decision tree and Bayesian network. The monitoring of real time system, faults detection, diagnosis and correction may happen at process and functional levels based on quantitative and qualititative performance metrics. Real-time fault diagnostics are basically condition monitoring systems having three core components: data logging and event recording system, event recording and data analytics and online health monitoring system. The first component can detect faults (e.g. change in logic and operation time), can give hard evidence of accidents and other abnormal conditions caused by malfunctioning of system and also can record the performance and status of critical equipments and operations in the form of digital data. The second component may have intelligent data analytics (e.g. statistical analysis, sequence mining) and remote access to critical data. The third component is basically knowledge based expert system which can collect digital and analog data from various critical equipments, analyze sensed data, compare with an inbuilt database of healthy and simulated faulty operational modes, flag alarms and recommend diagnosis to the drivers and maintenance workforce. Automated system verification is essential for scalability and

robustness in fault diagnosis. The basic building blocks of RTFD are three automated system verification algorithms based on time failure propagation graph (TFPG), fault tree analytics and failure mode effects analysis; these analytics have been discussed in details in the next chapter 6.

Security Intelligence Verification Mechanism

- Call real time fault diagnostics.
  - Graph Analytics
  - Fault Tree Analytics
  - FMEA Analytics
  - Data logging and event recording analytics
  - Event recording and data analytics
  - Online health monitoring analytics
- Call ***threat analytics***
  - assess risks of single or multiple threats on EVs; analyze performance, sensitivity, trends, exception and alerts.
  - what is corrupted or compromised: agents, communication schema, data schema, application schema, computing schema ?
  - **time:** what occurred? what is occuring? what will occur? assess probability of occurrence and impact.
  - **insights**: how and why did it occur? do cause-effect analysis.
  - **recommend** : what is the next best action?
  - **predict** : what is the best or worst that can happen?
- Verify **security intelligence** of EVs at levels L1, L2, L3, L4 and L5;

Level 1 [L1-access control]:

- authentication, authorization, correct identification, privacy, audit; confidentiality, data integrity, non-repudiation;
- private view of data through role based access control
- assess the risk of privacy attack;

Level 2 [L2-computing and communication schema]: fairness, correctness, transparency, accountability, trust, commitment, rationality;

Level 3 [L3-system performance]: robustness, consistency, liveness, reliability, resiliency, deadlock freeness, lack of synchronization, safety and reachability;

Level 4 [L4-malicious attacks] **:** detect the occurrence of any malicious attack on the EVs.

- coremelt or network traffic congestion
- rushing attack
- sybil attack
- false data injection attack
- poor QoS, information leakage, physical attacks on the drivers

Level 5 [L5-business intelligence]**:** audit flaws in payment function computation.

5. STRATEGY

The fifth element of deep analytics is strategy. This element should be analyzed from different perspectives such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovation is closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of the technology of electrical and hybrid vehicles through logical and analytical reasoning.

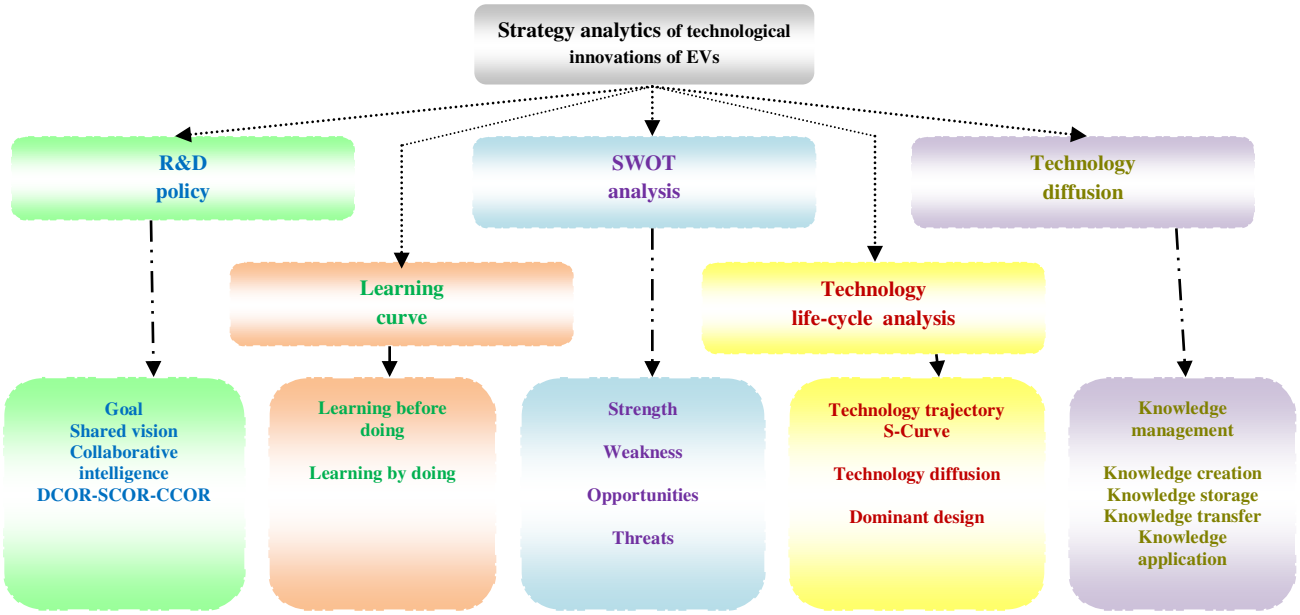


Figure 3.7: Strategy analytics

The technological innovation is closely associated with R&D policy and organizational learning strategies in new product development and process innovation. There are various strategies of learning such as learning by doing and learning before doing. Learning by doing is effective in those technologies which demand low level of theoretical and practical knowledge. On the other side, learning before doing is possible through various methods such as prototype testing, computer simulations, pilot production run and laboratory experiments. It is effective for the innovation of EVs where deep practical and theoretical knowledge can be achieved through laboratory experiments that model future commercial production experience.

Let us explore the role of deep analytics on technological innovation of EVs. It is interesting to analyze the impact of different learning strategies and timing of technology transfer on product development performance, process re-engineering and R&D cost of this technological innovation. It is important to compare the effectiveness of various types of learning strategies in terms of cost, quality and time. It is also critical to analyze the relationship between process innovation and learning curve in terms of dynamic cost reduction and improvements in yield. It is essential to identify the critical success factors (e.g. resource allocation, ERP and SCM strategies) that influence the rate of learning and superior performance.

5.1 SWOT Analysis

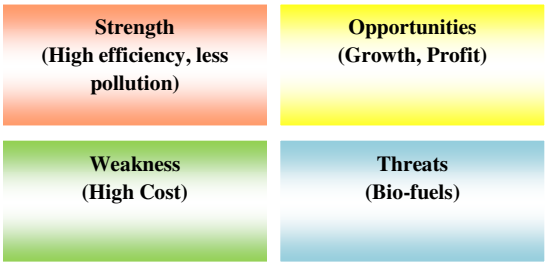


Figure 3.8 : SWOT Analysis

It is rational to evaluate strength, weakness, opportunities and threats of the technological innovation on electrical and hybrid vehicles [Figure 3.8]. There may be major and minor strengths and weaknesses. Strength indicates positive aspects, benefits and advantages of EVs. Weakness indicates negative aspects, limitations and disadvantages of the technology. Opportunities indicate the areas of growth of the market of

EVs and industries from the perspective of profit. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses.

Let us first do SWOT analysis on EV technology and explain the strength of EVs. Wide spread adoption of electrical and hybrid vehicles can limit the environmental pollution of conventional fuel based transportation and can reduce dependence on oil (e.g. petrol and diesel). Intelligent supply chain contracts and switching stations may increase driving. The adoption of electrical vehicles is safe, reliable and consistent. Rational policy intervention is expected to consider battery purchase subsidies and R&D for advancement of battery techniques in terms of safety, system performance, cost, life-span, specific energy and specific power. Sustainable green transportation is a critical research agenda of government, environmentalists, industry and academics; green fuel (electrical, biofuel, hydrogen, natural gas) can limit environmental pollution and oil dependence.
Next, let us talk about the weakness of EV technology. The transition from conventional gasoline vehicles to EVs poses several challenges. Increase in adoption of EVs may create unprecedented strains on the existing power generation, transmission and distribution infrastructure. Renewable energy is typically intermittent which may result a potential mismatch between supply and demand. There are other constraints such as range anxiety and high battery cost that may limit consumer adoption. It is rational to adopt novel switching station based solution. Electrical and hybrid vehicles can use standardized batteries that when depleted can be switched for fully charged batteries at switching station. The consumers can pay for miles driven and don't pay for upfront battery purchase. In case of range anxiety, an EV may have insufficient range to reach its destination. It demands technological advancement and high energy storage capacity of batteries.
Next, let us explore the opportunities and threats of EV technology. Transportation sector is a significant contribution to environmental pollution. Geopolitical uncertainties often result increased vulnerabilities of oil based transportation infrastructure. The adoption of electrical vehicles is expected to result the growth of electrical drives, hybrid vehicles, renewable energy (e.g. solar microgrid, wind, tidel), power plants, standardized batteries and electrical battery charging stations. This business model requires an efficient payment function and market clearing mechanism. It is not rational to buy batteries; rather it should be replenished at battery charging stations. EVs require adequate supply of electrical energy; thermal power may not be an interesting option from the perspectives of environmental pollution.

5.1.1 SWOT analysis on Smart Batteries

Let us exercise SWOT analysis on Li-ion and solid state batteries. Electrical vehicles may be dearer to buy but cheaper to run. But there are issues of range and rate of efficient battery charging mechanism. Electrical batteries may be the game changer in the innovation of electrical and hybrid vehicles technology. Solid state batteries replace the wet electrolyte of lithium ion batteries with a solid electrolyte. Current lithium-ion batteries are flammable and produce heat and have short life span; constant charging and discharging slowly erodes the performance of the battery. Smart batteries are expected to be simple in design, cheaper and lighter in weight as compared to present Li-ion batteries; won't need liquid cooling; the smart batteries should be long lasting, fire-proof and should permit faster charging.
Let us discuss the limitations of existing battery technologies of EVs. SSBs are generally very expensive; those batteries have other limitations such as poor system performance at low temperature, impact of pressure, breakage due to mechanical stress and risks of dendrites. Li metal dendrites from the anode piercing through the separator and growing towards the cathode in the form of crystal like structure. Generally, solid Li anodes in SSBs replace graphite anodes in Li-ion batteries for higher energy densities, safety, and faster recharging time. Solid Li anode experiences the formation of Li dendrites due to the reactivity of the metal. Li dendrites penetrate the separator between the anode and cathode to prevent short circuits. The penetration of Li dendrites into the separator may cause short circuit, overheating, fire or explosion from thermal runaway propagation and reduction of columbic.
There are also financial barriers of existing battery manufacturing plant; they have to invest significantly on solid state batteries. There is a huge difference between a technology that works on a small scale and one that is ready for mass market production. Cars charge as they drive; EVs demand the support of smart batteries which should be cheaper, smaller in size, light weight, non-flammable, increased life cycle (say 2-10 years), higher capacity and fit for faster charging and long range. The industry is looking for a

sustainable, affordable and widespread energy conversion system. Is it possible to have a battery with two times the density of current batteries at 1/5 of the cost?

5.2 Technological life-cycle analysis

Figure 3.9 shows the technology life-cycle analysis of electrical and hybrid vehicles; presently, the technology is at emergence phase of S-curve. . The manner of the viewpoint depends on from where the viewer is located; each viewer may be seeing the same world but from a different perspective. The technology life-cycle starts with the establishment or emergence of birth phase where the product is introduced into its intended market. This phase is followed by growth, maturation and finally declining phases. No element in this universe exists eternally. Today, electrical vehicles have been getting launched in several sectors such as 'Toto' and electrical private cars; the technology is not matured yet.

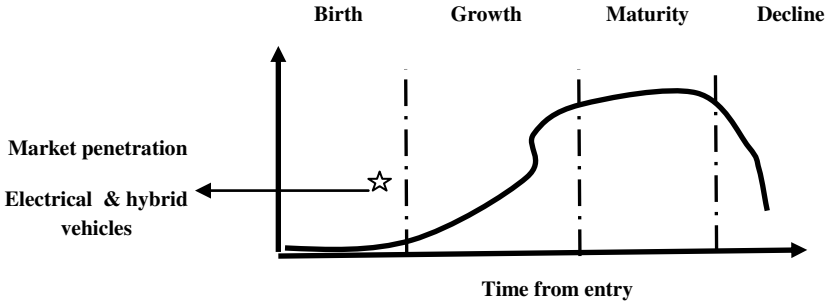


Figure 3.9 : Technological life cycle analysis

Deep analytics can evaluate and explore the technological innovation of EVs in terms of technology life-cycle, technology trajectory, S-curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, the technology of EVs has emerged and is now growing to some level of maturity It is essential to evaluate the status of each technological innovation through TLC analysis. Some technologies may have relatively long technology life-cycle; others never reach a maturity stage. Emergence of new technologies follows a complex nonlinear process. It is hard to understand how the technology life-cycle interacts with other technologies, systems, cultures, enterprise activities and impacts on society. All technologies evolve from their parents at birth or emergence phase; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early phases, it adapts and forwards to its intended environment with the emergence of competitors. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. The final stage is decline and phase out or expire; existing technologies of oil fuelled vehicles will eventually decline and are phased out or expire at a substantial cost.

Let us consider the analysis of the performance of a new technology vs. effort; it is basically an S-curve. Initially, it is difficult and costly to improve the performance of the new technology of EVs. The performance is expected to improve with better understanding of the fundamental principles and system architecture. Next, let us analyze the adoption of the technology over time which is also an S curve. Initially, the new technology of electrical and hybrid vehicles may be costly for the adopters due to various uncertainties and risks. Gradually, this new technology is expected to be adopted by large segments of the market due to reduced cost and risks.

The rate of improvement of the new technology may be faster than the rate of market demand over time; the market share increases with high performance. Technological change follows a cyclical pattern. The evolution of the new technology of EVs is passing through a phase of turbulence and uncertainty; various stakeholders of the supply chain are exploring different competing design options of the new technology and a dominant design is expected to emerge alongwih a consensus and convergence of structure. Then, the producers will try to improve the efficiency and design of the EVs based on stable benchmark of the industry. The dominant design of EVs must consider an optimal set of most advanced technological features which meet the demand of the customer, supply and design chain in the best possible way.

Technology trajectory is the path that the technology of EVs takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of this innovation today. How to manage the evolution of this technological innovation? The nature of innovation shifts markedly after a dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow an S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by technologies. Technology diffusion indicates how new technologies spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards.

6. STAFF-RESOURCES

Critical Success Factors for the Diffusion of Electrical & Hybrid vehicles

- Innovators : R&D units of automobile manufacturing companies; technology management departments of academic institutes, collaborative networks;
- Organizational creativity, organization structure, cooperative work culture, human capital management, talent management, knowledge management;
- Audit fairness in resource allocation (e.g. 5'M': man, machine, material, method, money), cost and quality control.

The sixth element of deep analytics is staff-resources. The sources of EVs innovation may be R&D units of automobiles manufacturing companies, mechanical, electrical and electronics departments of engineering institutes, technology management of management institutes and collaborative networks. Creativity is the underlying process for EV technology innovation which can promote new ideas through shared vision, intellectual abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics. It demands the motivation and commitment of the creative people to look at the problems in unconventional ways. Organizational creativity is closely associated with human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routine and incentive policy.

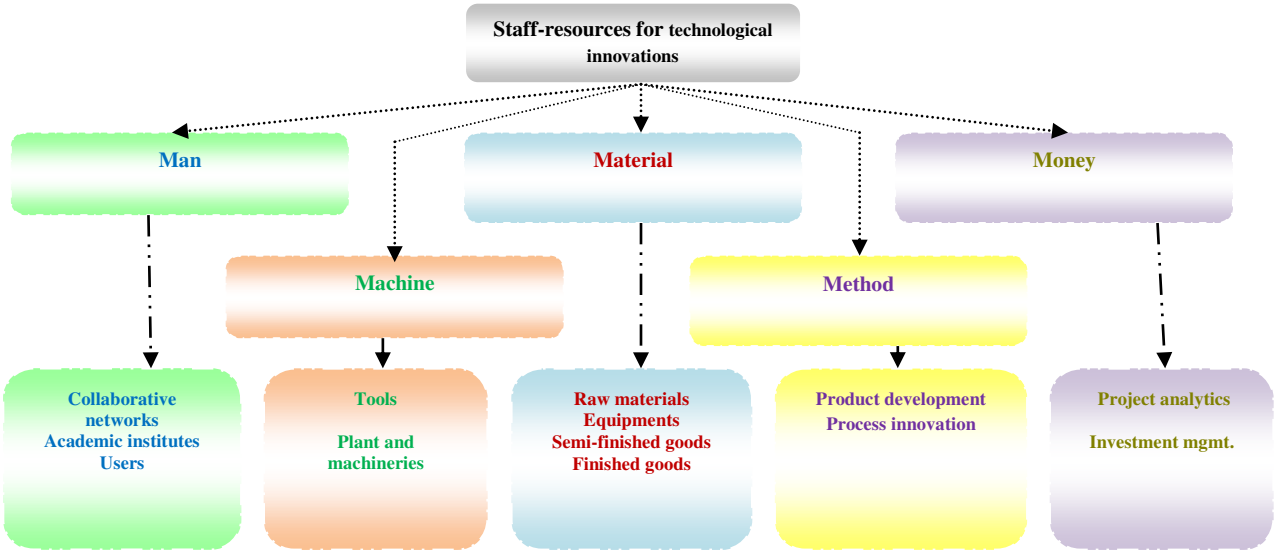


Figure 3.10 : Staff-resources analytics

Figure 3.10 outlines the sixth element of deep analytics i.e. staff-resources in terms of 5M – man, machine, material, method and money. 'Man' analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function,

compensation, reward, incentive and performance evaluation. 'Machine' analyzes the basic aspects of tools and automated / semi-automated / manual machines; 'material' analyzes planning of raw materials, equipments, semi-finished and finished goods. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure. Finally, 'money' highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion such as 5M i.e. man, machine, material, method and money; dominant design factors, effects of timing and mode of entry. This innovation demands the commitment of creative people. Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers may innovate based on their own needs. Many firms have set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities have defined mission and vision of research on EVs and are contributing through publication of research papers. The Governments of many developed and developing countries are also playing active roles in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators).

A complex technological innovation like EVs often needs collaborative intelligence to manage the gap between demand and supply of a specific set of capabilities, skills and resources. It is possible to control cost, speed and competencies of the technological innovation on EVs through efficient sharing mechanisms. It is rational to share the cost and risks of this new innovation through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem. There are different modes of collaboration such as strategic alliance, joint ventures, technology licensing, outsourcing and collective research organizations. Collaborative networks are other sources of innovation. Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms. But, it may be hard to control the development of product and process innovation protecting IP of proprietary technologies. The critical success factors of collaborative networks may be the right selection of innovation partners having strategic and resource fit, transparent and flexible monitoring and governance process so that the innovation partners understand their rights and obligations. .

The technological innovation of EVs demands the motivation and commitment of creative people. It is not a trivial problem; need useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. The impact of knowledge on creativity is double-edged. Lack of knowledge is a major constraint to the original contribution in a technological innovation. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time.

7. SKILL-STYLE-SUPPORT

Critical Success Factors for EVs Diffusion

- New skills developments for EV drivers, battery charging stations and traffic controller
  - Data visualization and data analysis Information and communication technology,
  - Battery charging
  - Coordination and integration in traffic control;
- Style : Project management by objectives, shared vision and goal setting;
- Support : proactive, reactive, preventive and breakdown maintenance of EVs system (e.g. mechanical, electrical, electronics and IT schema);
- Audit gaps in skills, style and support through rational talent acquisition, retention and training strategies.

The seventh element of deep analytics is skill-style-support. The workforce involved in EVs innovation are expected to develop different types of skills in technical (e.g. battery charging, solar power, hybrid vehicles), management and system administration domains such as research and development, maintenance support, knowledge management, system design, process innovation and project management. The system administrators should have leadership skill in smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of EVs innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management should be able to tackle the complexity of system implementation with the support of efficient teams.

It is essential to develop multiple skills in new EVs system development through proper coordination among design and supply chains. The basic objectives are to maximize fit with the needs of the drivers, ensure quality assurance and control R&D cost. It is an interesting option to get the suppliers and the drivers in the development process. It is really challenging to develop a complex EV system through a sound knowledge base and problem solving capability.

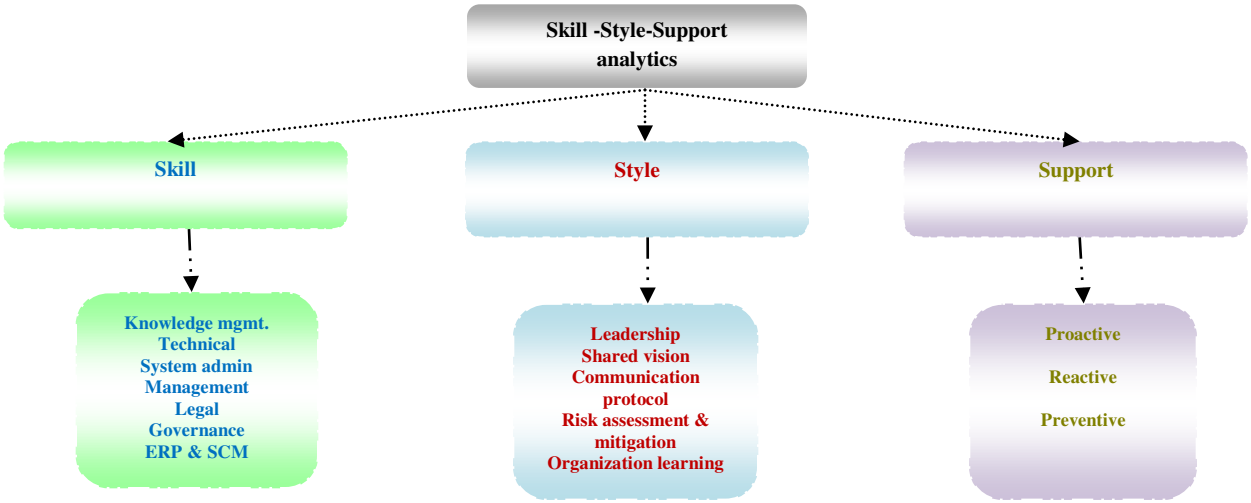


Figure 3.11: Skill-style-support analytics for EVs

What should be the right organization model for this technological innovation? A traditional functionally centered organization model may not be suitable for supporting end-to-end business processes. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common, customer oriented goal. The business models of EVs require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement. The structure of process enterprise requires a collaborative and cooperative work culture. Top innovations need proactive, reactive and preventive support for proper technology management.

8. CONCLUSION

What must be done to realize the future vision of EVs? It is essential to manage the fit among the design of EVs, energy and communication infrastructure and corporate governance; form coalition of the stakeholders; explore intelligent mechanisms and build a broad consensus around a common vision. There are critical issues such as purchasing dynamics and shared mobility. The preference of young generation has been changing. It is also essential to define a rational Govt. policy for the innovation, adoption and diffusion of EVs such as development of battery charging infrastructure, rationalization of profit margin of the manufacturers and dealers of EVs and reduction of tax. It is also necessary to stimulate the political support and consumer demand through SWOT analysis, what is at stake and what is possible, threats analysis and risk mitigation strategies. It may be interesting to launch a set of pilot projects at sufficient scale and investment to enable the integration of the key innovative solutions of electrical and hybrid vehicles. The aforesaid problem is an extremely complex issue in the world since we are not rich and blessed with adequate supply of natural resources in oil and gas sector; the situation demands proper coordination and integration among seven 'S' factors of deep analytics.

REFERENCES

[1] U.Eberle and R.V. Helmolt. 2010. Sustainable transportation based on electrical vehicle concepts : a brief review. Energy & Environmental Science, 3, 680-699.
[2] K. Girotra and S. Netessine. 2011. The electrical vehicle renaissance: Better place Inc. Teaching case. INSEAD.
[3] BCG report 2010. Batteries for electric cars. Challenges, opportunities and the outlook to 2020.
[4] V. Robu, E.H. Gerding, S. Stein, D.C. Parkes, A. Rogers & N.R.Jennings. 2013. An online mechanism for multi-unit demand and its application to plug-in hybrid electric vehicle charging. Journal of Artificial Intelligence Research, 48, 175-230.
[5] H.Stromberg, P.Andersson, S. Almgren, J. Ericsson, M. Karlsson & A. Nabo. 2011. Driver interfaces for electric vehicles. In Proceedings of the 3rd International Conference on Automotive User Interfaces and Interactive Vehicular Applications, AutomotiveUI '11, pp. 177-184, New York, NY, USA. ACM.
[6] C. Ahn, C.Li and H.Peng. 2011. Optimal decentralized charging control algorithm for electrified vehicles connected to smart grid. Journal of Power Sources, 196 (23), 10369 - 10379.
[7] K. Clement-Nyns, E. Haesen and J. Driesen. 2010. The impact of charging plug-in hybrid electric vehicles on a residential distribution grid. IEEE Transactions on Power Systems, 25 (1), 371- 380.
[8] C.M. Flath, J.P. Ilg, S. Gottwalt, H. Schmeck and C. Weinhardt. 2014. Improving electric vehicle charging coordination through area pricing. Transportation Science, 48 (4), 619-634.
[9] K. Hayakawa, E. Gerding, S. Stein and T. Shiga. 2015. Online mechanisms for charging electric vehicles in settings with varying marginal electricity costs. In 24th International Joint Conference on Artificial Intelligence (IJCAI), pp. 2610-2616.
[10] M. Granovskii, I. Dincer, M.A. Rosen, J. Power Sources 159. 2006. 1186.
[11] C. Zamfirescu, I. Dincer, J. Power Sources 185. 2008. 459.
[12] C. Zamfirescu, I. Dincer, Fuel Process. Technology. 90. 2009. 729.
[13] C. Handley, N. Brandon, R. Vorst, J. Power Sources 106. 2002. 344.
[14] P. Van den Bossche. 2003. The Electric Vehicle: Raising the Standards. Ph.D. Thesis, Vrije Universiteit Brussel.
[15] D.L.Burns, B. McCormick and C.E. Borroni-Bird. Vehicle of Change. 2002. Scientific American 287 : 64 – 73.
[16] L. Burns. 1993. Busy Bodies: Why Our Time-Obsessed Society Keeps Us Running in Place . New York : Norton.
[17] W.J. Mitchell. 1994. City of Bits: Space, Place, and the Infobahn .Cambridge, M ass. : MIT Press.
[18] W.J.Mitchell. 1999. E-topia . Cambridge, Mass. : MIT Press.
[19] W.J.Mitchell. 2004. Me++: The Cyborg Self and the Networked City . Cambridge, M ass. : MIT Press.
[20] R.L.Ackoff, J. Magidson and J.A. Herbert. 2006. Idealized Design: How to Dissolve Tomorrow's Crisis Today. Upper Saddle River, N .J. : Wharton School Publishing.
[21] R. Adams and T. Brewer. 2004. A Plan for 21st Century Land Transport. International Journal of Vehicle Design 35 (1/2) : 137 – 150.

[22] J.H.Ausubel, C. Marchetti and P. Meyer. 1998. Toward Green Mobility: Th e Evolution of Transport. ” European Review 6 (2) (1998): 137 – 156.
[23] G.Boyle, ed. 2004. Renewable Energy . Oxford University Press.
[24] G. Boyle, ed. 2007. Renewable Energy and the Grid: The Challenge of Variability . London : Earthscan Publications.
[25] G.Boyle, B. Everett, and J. Ramage. 2003. Energy Systems and Sustainability . Oxford University Press.
[26] R. Brandon. 2002 Auto Mobile: How the Car Changed Life. London : Macmillan .
[29] C.M.Christenson. 1997. The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail . Cambridge, Mass. : Harvard B usiness School Press.
[30] P. Droege. 2006. The Renewable City: A Comprehensive Guide to an Urban Revolution . Chichester : Wiley.
[31] P.Droege. 2008. Urban Energy Transition: From Fossil Fuels to Renewable Power . Oxford : Elsevier Science.
[32] S. Grava. 2003. Urban Transportation Systems . New York : McGraw-Hill.
[33] S.Henley. 2007. The Architecture of Parking . New York : Thames and Hudson.
[34] I.M. Hoffert , K. Caldeira , G. Benford , D. R. Criswell, C. Green , H. Herzog, A. K. Jain, H. S. Kheshgi , K. S. Lackner , J.S. Lewis , H. D. Lightfoot, W. Manheimer, J. C. Mankins , M. E. Mauel , L. J. Perkins , M. E. Schlesinger , T. Volk and T. M. L. Wigley. 2002. Advanced Technology Paths to Global Climate Stability: Energy for a Greenhouse Planet. Science 298 (5595) : 981 – 987.
[35] D.A. Kirsch. 2000. The Electric Vehicle and the Burden of History. New B runswick, N .J. : Rutgers University Press.
[36] Ladd , Brian. 2008. Autophobia: Love and Hate in the Automobile Age . Chicago : University o f Chicago Press.
[37] D. Mohan . 2008. Mythologies, Metros, and Future Urban Transport . TRIPP Report 08-01. New Delhi: Transportation Research and Injury Prevention Program.
[38] G. Mom. 2004. The Electric Vehicle: Technology and Expectations in the Automobile Age . Baltimore : Johns Hopkins University Press.
[39] R.A.Popa, H. Balakrishnan and A. J. Blumberg. 2009. VPriv: Protecting Privacy in Location-Based Vehicle Services. 18th USENIX Security Symposium. Montreal,August.
[40] M. Safdie and W. Kohn. 1998. The City After the Automobile: An Architect’s Vision . Boulder, C olo. : Westview Press.
[41] R. Strzelecki and B. Grzegorz eds. 2008. Power Electronics in Smart Electrical Energy Networks . London : Springer.
[42] J. Weinert, M.Chaktan and C. Cherry. 2007. The Transition to Electric Bikes in China and Key Reasons for Rapid Growth ” Transportation 34: 301 – 318 .
[43] M.A. Weiss, J. B. Heywood, E.M.Drake , A. Schafer and F.F. AuYeung. 2000. On the Road in 2020: A Life-Cycle Analysis of New Automobile Technologies. Energy Laboratory Report MIT EL 00-003. Energy Laboratory, MIT. October.

Exercise

- **Justify EVs & HVs as a technology for humanity. What is the scope of this technology?**
- **What is the dominant design of the technology?**
- **What are the basic elements of the system architecture?**
- **What do you mean by technology security? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion for EVs & HVs’? What is the outcome of technology life-cycle analysis and SWOT analysis of conventional and electrical vehicles?**
- **How to manage resources for this innovation project?**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among ‘7-S’ elements?**
- **Design a smart battery system for EVs / HVs.**

CHAPTER 4: RAILTECH SECURITY & SAFETY – DRIVER ADVICE SYSTEM WITH REAL-TIME FAULT DIAGONISTICS

Abstract: This chapter is focused on RailTech, an emerging technology in rail operation from the perspectives of intelligent management information systems. RailTech integrates intelligent Driver Advice System (DAS), traffic control centre (TCC) and real-time fault diagnostics (RTFD). The technology is analyzed through deep analytics along seven 'S' dimensions: scope (S_1), system (S_2), structure (S_3), strategy (S_4), security (S_5), staff-resources (S_6) and skill-style-support (S_7). It highlights technology life-cycle analysis on S-Curve and also shows SWOT analysis on three different types of RailTech system architectures. Finally, this work outlines the basic building blocks of real-time fault diagnostics in terms of a set of analytics: graphical analytics (GA), fault tree analytics (FTA) and failure mode effects analytics (FMEA). The core components of the graphical analytics include time failure propagation graph (TFPG), control, resources and data flows analytics. **What should be the top priority: high speed train or rail security and safety?**
Keywords : RailTech, Driver Advice System, Traffic control Centre, Real-time fault diagnostics, Fault tree analysis, FMEA, Time Failure Propagation Graph (TFPG), Control flow, Resource flow, Data flow

1. RAILTECH ANALYTICS

The basic objective of this section is to analyze RailTech which integrates Driver Advice System (DAS), traffic control centre (TCC) and real-time fault diagnostics (RTFD) for rail operations. The technology is analyzed through deep analytics along seven 'S' dimensions: scope (S_1), system (S_2), structure (S_3), security (S_4), strategy (S_5), staff-resources (S_6) and skill-style-support (S_7). In this work, RailTech is analyzed based on literature reviews on rail safety, driver advice systems and real-time fault diagnostics from the perspectives of management information systems (MIS) [1-28], extensive experience of rail travel of more than 100000 kilometers in last twenty five years and also summer training experience at Railways Corporation as part of graduation programme in Electrical Engineering.
The contributions and organization of the work are as follows. Section 1 explains the motivation of the problem. Section 2-8 analyzes RailTech through '7-S' deep analytics: scope (S_1), system (S_2), structure (S_3), strategy (S_4), security (S_5), staff-resources (S_6) and skill-style-support (S_7). Section 5 outlines the basic building blocks of real-time fault diagnostics in terms of a set of analytics: graphical analytics (GA), fault tree analytics (FTA) and failure mode effects analytics (FMEA). The core components of the graphical analytics include time failure propagation graph (TFPG), control, resources and data flows analytics. Section 6 highlights technology life-cycle analysis on S curve and also shows SWOT analysis on three different types of RailTech system architectures. Section 9 presents five cases related to rail security and safety. Section 10 concludes the work.

2. SCOPE [S_1]

RailTech Scope Analytics
Agents : Driver of train, Traffic controller at TCC, passengers;
Objectives:

- safe driving trading-off cost vs. comforts of the passengers through real-time fault diagnostics
- maintain schedule of train service approximately as far as possible
- improve energy efficiency of driving as per standard operating procedures
- optimal capacity utilization of limited rail infrastructure
- optimize train movements within limits and regulatory compliance
- ensure security, safety and comforts at optimal cost

Constraints : Technological complexity, application integration, cost

The ultimate goals of RailTech are to improve the performance of rail infrastructure and train services and minimize train delays which results decrease in capacity utilization, punctuality, reliability and safety. Increased capacity of infrastructure also causes secondary delays and increase in route conflicts. It is

essential to do analysis on various types of feedback and operational data for improving planning and control in rail operations and to monitor delays at stations using route conflicts, train and timetable data. Specifically, RailTech faces critical situations during natural disasters (e.g. flood, cyclone, storm, fog, mist and snowfall in winter). Deep analytics can find out chains of route conflicts, secondary delays, number of conflicts, time loss and delay jump.

RailTech safety and security is an emerging trend of top technological innovation today [42]. Railway technology is associated with a complex, distributed and integrated information system. We must monitor the performance of railways infrastructure globally and analyze political and social trends, principal technological advancement of condition monitoring system, driver advice system and real-time fault diagnostics; system complexity, R&D challenges and future vision of railway security and safety.

Condition monitoring is an important issue of RailTech safety. It is a common practice to compare relative benefits and limitations of various modes of transportation such as surface, rail and air in terms of traffic congestion, environmental pollution, safety, reliability, consistency, cost and capacity utilization. Traditionally, the security and safety of RailTech system is analyzed in terms of frequency of accidents, fire hazards, delay, punctuality, reliability, consistency, probability of injuries or fatalities due to derailing and track faults. Gradually, the system has been getting equipped with electronics, communication and information technology which increases the scope of automated fault detection and diagnosis. It is possible to improve punctuality, profit and revenue in rail operations and increase operational availability and reliability of key railway infrastructure through effective coordination and integration among DAS, TCC and RTFD.

3. SYSTEM [S_2]

RailTech System Intelligence

- advise a train driver the target arrival time along a specific route to satisfy the timetable and avoid conflicts with other trains;
- monitor the train's speed so that the advice is updated correctly and target time of the train is achieved;
- compute energy efficient speed/distance profile to achieve target time;
- advise a driver conflict free time target i.e. how far and fast a train can be driven safely within allocated and authorized movement hiding wider view of overall traffic management of rail network.
- **Computing schema**
    - track train movement
    - predict future train movement
    - conflicts detection and resolution
    - new target train timings to avoid conflicts
    - speed profiles and choice of advice to the driver
- **Networking schema**
    - 3G/4G/5G to DAS with built-in antenna
    - 3G/4G/5G with external antenna
    - 3G/4G/5G to a communication gateway onboard
    - Data communication via SMS
- **Data schema**
    - Explicit driving instructions : current speed target, time series analysis of train speed profile, advice to speed up or slow down;
    - Temporal information : train running status (early / delay), optimized speed profile to realize time table;
    - Decision support information : gradient profile, energy usage, position of other trains, conflict, traffic congestion;
    - Data mining: monitor a set of performance metrics such as primary and secondary delays, capacity utilization, route conflicts, traffic congestion, signaling errors and real-time train scheduling and time table.
- **Application schema :**
    - Provide advice to the train driver for running the train in a safe and efficient manner;

- Collect and recall from route knowledge the current and future speed targets such as infrastructure, regulation and operational factors;
- Select correct train speed to minimize delay and maximize safety;
- Monitor the speed of the train by collecting data from sensors, speedometer, noise and motion;
- Compare correct speed with train speed and compute speed gap;
- Speed control to minimize the difference between target required speed and actual train speed by changing the setting of the power or brake controller and considering train's response, gradients, curves and professional driving policy;
- Assist the driver to monitor the progress of a train continuously against a series of scheduled stops and understand if the train runs early or late between two timing points;
- Advice for any temporary speed restrictions within a route to give a perception of progress and recovery time to the driver;

The second element of the deep analytics is system. The system should be designed to satisfy multiple objectives subject to various constraints. The system should have clearly defined objectives, decision making procedures and quantitative measures of performance. The state of the system at a specific time is a set of properties of the system. The RailTech system is a complex grouping of interlinked components; it can be decomposed into a set of interacting schema such as computing, networking, data, application and security schema. Each schema can be outlined as stated above. DAS is basically an information system. The basic building blocks of the computing schema are a set of algorithms which compute critical system parameters. The networking schema is the communication system. The data schema processes data collected by the sensors and various measuring instruments. The application schema defines the basic features of driver advice system. The complexity of the system should be analyzed in terms of number of interacting elements, number of relationships among the elements, number of objectives and number of ways the system interacts with internal and external environment.

4. STRUCTURE [S_3]

RailTech System Architecture

- Driver advice system
  - Option 1 : DAS at TCC (Traffic Control Centre) /* refer figure 4.3*/
  - Option 2 : DAS Task shared between TCC and train /* refer figure 4.4*/
  - Option 3 : DAS tasks mainly onboard /* refer figure 4.5*/
- Railway system
  - track side infrastructure
  - vehicle or rolling stock
- Railway infrastructure assets
  - mechanical actuators (e.g. point machines, level crossing barriers, train stops, mechanical signals);
  - power supply equipment (e.g. substations, rectifiers, transformers);
  - track (e.g. rail, pads, sleepers, ballast, substructure);
  - signaling and telecoms (e.g. track circuits, interlockings, axle counters);
- Railway rolling stock
  - bogie : wheels, axles, suspension components;
  - traction and braking systems: motors, power electronics system, transformers, brakes;
  - auxiliary subsystems : doors; air conditioning system;
  - train communication bus (integrating the subsystems to a central controller);

The third element of deep analytics is structure i.e. the backbone of RailTech system. The topology of technology should be analyzed in terms of nodes, connectivity, type of connections, layers, interfaces between layers and organization of layers. RailTech structure has three major components: trackside infrastructure, rolling stock or vehicle and driver advice system. The aforesaid section outlines various components of rolling stock, infrastructure and DAS [42]. The sensors collect data from the track and

rolling stock and provide the inputs to DAS. DAS analyzes the sensed data and shows the output (e.g. alerts, advice, recommendations) to the driver and traffic control centre (TCC).

5. SECURITY [S_4]

Security Intelligence Verification Mechanism

- Call real time fault diagnostics for infrastructure and rolling stock monitoring through pattern recognition using artificial neural networks and knowledge based expert systems for fault detection and diagnosis.
    - Graph Analytics [section 5.1.1]
    - Fault Tree Analytics [section 5.1.2]
    - FMEA Analytics [section 5.1.3]
    - Data logging and event recording analytics
    - Event recording and data analytics
    - Online health monitoring analytics
- Call ***threat analytics***
    - assess risks of single or multiple threats on RailTech; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised: agents, communication schema, data schema, application schema, computing schema and RailTech System?
    - **time:** what occurred? what is occuring? what will occur? assess probability of occurrence and impact.
    - **insights**: how and why did it occur? do cause-effect analysis.
    - **recommend** : what is the next best action?
    - **predict** : what is the best or worst that can happen?
- Verify **security intelligence** of RailTech system at levels L1, L2, L3, L4 and L5;

Level1 [L1-access control]:

- authentication, authorization, correct identification, privacy, audit; confidentiality, data integrity, non-repudiation;
- private view of data through role based access control
- assess the risk of privacy attack;

Level2 [L2-computing and communication schema]: fairness, correctness, transparency, accountability, trust, commitment, rationality;

Level3 [L3-system performance] : robustness, consistency, liveness, reliability, resiliency, deadlock freeness, lack of synchronization, safety and reachability;

Level4 [L4-malicious attacks] **:** detect the occurrence of any malicious attack on the RailTech system.

- rail network delay due to coremelt or network traffic congestion
- rushing attack
- sybil attack
- false data injection attack
- other attacks: data integrity attack, node deletion, flaws in workflows, poor QoS, information leakage, physical attacks on the drivers by terrorists or malicious agents.

Level5 [L5-business intelligence]**:** audit flaws in payment function computation.

5.1 Real-Time Fault Diagnostics [RTFD]

The fourth element of deep analytics is security. Please refer to five test cases as discussed in section 9. We have analyzed those cases and outline the aforesaid security schema comprehensively. It is essential to monitor and detect faults of a complex real-time system; assess the chance of various types of faults and explore efficient and reliable fault detection and isolation methods based on artificial intelligence [30]. The basic building blocks of real-time fault diagnostics are soft computing and AI methods such as knowledge based expert system, model based system, if-then rule based system, artificial neural network (ANN), fuzzy logic, genetic algorithm (GA), decision tree and Bayesian network. It is possible to monitor real-time

system, faults detection, diagnosis and correction at process and functional levels through a set of quantitative and qualititative performance metrics.
Faults may occur due to various reasons such as failure of hardware components (e.g. sensors, triggers), environmental factors (e.g. noise) and flaws in software (e.g. algorithms, logic, coding, protocols, invalid and incorrect inputs and feedback, knowledge base, inference mechanism and knowledge representation). There are other constraints such as inconsistency in knowledge base and flaws in knowledge engineering, learning errors and data visualization. Traditionally, track geometry is monitored using accelerometers and camera; cracks in tracks are detected through non-destructive test; measurements are acquired through various sensors of specialist trains and data is analyzed on the train. If the value is above predetermined threshold, then it requires the effort of the experts to identify and diagnose the faults.
Real-time fault diagnostics are basically condition monitoring systems having three core components: (a) data logging and event recording system, (b) event recording and data analytics and (c) online health monitoring system [42]. The first component can detect faults (e.g. change in logic and operation time), can give hard evidence of accidents and other abnormal conditions caused by the malfunctioning of RailTech system and also can record the performance and status of critical equipments and operations in the form of digital data. On-Train Maintenance Recorder (OTMR) is equivalent to a black box and may use GPS and other sophisticated systems for real time data communication.
The second component may have intelligent data analytics (e.g. statistical analysis, sequence mining) and remote access to critical data. The second component may record door opening time, traction current and energy usage. Track based monitoring is useful for the verification of the performance of vehicles such as monitoring of wheel with strain gauge or fibre optic sensors and the monitoring of hot axles boxes.
The third component is basically knowledge based expert system which can collect digital and analog data from various critical equipments, analyze sensed data, compare with an inbuilt database of healthy and simulated faulty operational modes, flag alarms and recommend diagnosis to the drivers and maintenance workforce. Automated system verification is essential for scalability and robustness in fault diagnosis. The basic building blocks of RTFD are following three analytics the output of the same is fed to DAS.

5.1.1 Graphical Analytics [GA]

Call Graphical Analytics; Verify robustness and consistency of RailTech system performance;

- Time : Sense failure propagation in dynamic systems through [TFPG = F, D, E, M, ET, EM, DC, DS]; [section 5.1.1.1: TFPG]
  - TFPG transition system : S = (X,I,T); X= state variable, I - initial state, T - state transition;
  - F : failure nodes;
  - D : discrepancy nodes;
  - E : edges connecting all nodes;
  - M : system modes;
  - ET: E, a map that associates every edge with minimum and maximum time for the failure of propagation;
  - EM: E, a map that associates every edge with a set of modes either ON or OFF;
  - DC: D, a map defining the class of each discrepancy either AND or OR;
  - DS: D, a map defining monitoring status of discrepancy as either M (when discrepancy is monitored by alarm) or U (when the discrepancy is not monitored).
- Control flow [section 5.1.1.2 : Control Flow Analytics (CFA)]
- Resources flow [section 5.1.1.3 : Resources Flow Analytics (RFA)]
- Data flow [section 5.1.1.4 Data Flow Analytics (DFA)]

Detect, isolate and correct problems early and re-allocate resources as per demand.
Output :

- Timed Failure Propagation Graph (TFPG)
- System performance scorecard
- Data visualization : error trail / error trace / fault propagation path

The graphical analytics (GA) analyze RailTech System performance from the perspectives of four dimensions: time, control flow, resources flow and data flow. TFPG considers only time failure but ignores the other important aspects of vehicle diagnostics such as control, resources and data flows. RTFD is

expected to give a comprehensive view of system failure not only in terms of time delay but also flaws in control, data and resource flows. Sections 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 outline TFPG, CFA, RFA and DFA respectively. It is an interesting research agenda whether a single graph can show the propagation of different types of failures in system performance from the perspectives of time delay and flaws in resource, data and control flows simultaneously and comprehensively.

5.1.1.1 Time Failure Propagation Graph (TFPG)

Timed Failure Propagation Graph is a rich formalism and is used to model the occurrence and propagation of failure and their direct and indirect effects, Boolean combinations of faults, time delays, events and state transitions in the design of real-time fault diagnostics of a complex, autonomous and dynamic system [31-33]. There are several important issues: no critical state of a system should be ignored; no spurious and nonexistent sate should be considered for analysis; it is essential to perform fault detection, isolation and recovery, sense and compute time delays between events correctly and validate completeness and tightness of the graph through intelligent model checking algorithms. TFPG can model and reason the issues of spurious and missing alarms, intermittent faults and reduction of a large scale vehicle diagnostics system. It is an interesting open research agenda whether TFPG can verify performance of RailTech system in terms of reliability, consistency, liveness, safety, robustness, stability, deadlock freeness and reachability comprehensively.

A Timed Failure Propagation Graph is a directed graph model (Figure 4.1); the structure has a set of nodes (V) and edges (E) [34-39, 41]. The nodes represent failure modes (F) i.e. root events of the propagations of failure and discrepancies (D) i.e. possible deviations from nominal behavior caused by failure modes. Failure modes do not have any incoming edges; discrepancies must have at least one incoming edge and must be reachable from a failure mode node. Circular paths are possible. Edges (E) model the dependency between the nodes ($V = F \cup D$) and capture propagation of time delays; the edges can be activated or deactivated based on a set of operation modes (M). ET is a map that associates every edge with minimum and maximum propagation time (t_{min},t_{max}) of a failure. EM is a map that associates every edge with a set of modes in M. DC: D is a map defining the type of each discrepancy either AND or OR.

Is there any other type discrepancy apart from AND or OR such as NAND, NOR, NOT, XOR and loop? Section 5.1.1.2 gives an overview of various types of control flow patterns in RailTech system. DS: D is a map defining monitoring status of discrepancy as either M when (discrepancy is monitored by alarm) or U (when the discrepancy is not monitored). A TFPG transition system is represented by S = (X,I,T) where X is a set of state variables; I(X) is initial state, X' is next state of X and T represents transition relation. A state s of S is an assignment to the state variable of X. A trace of s is an sequence $\lambda := s_0,s_1,...s_n$ such that $s_o = I(X)$ and $(s_i,s_{i+1}) = T(X,X')$.

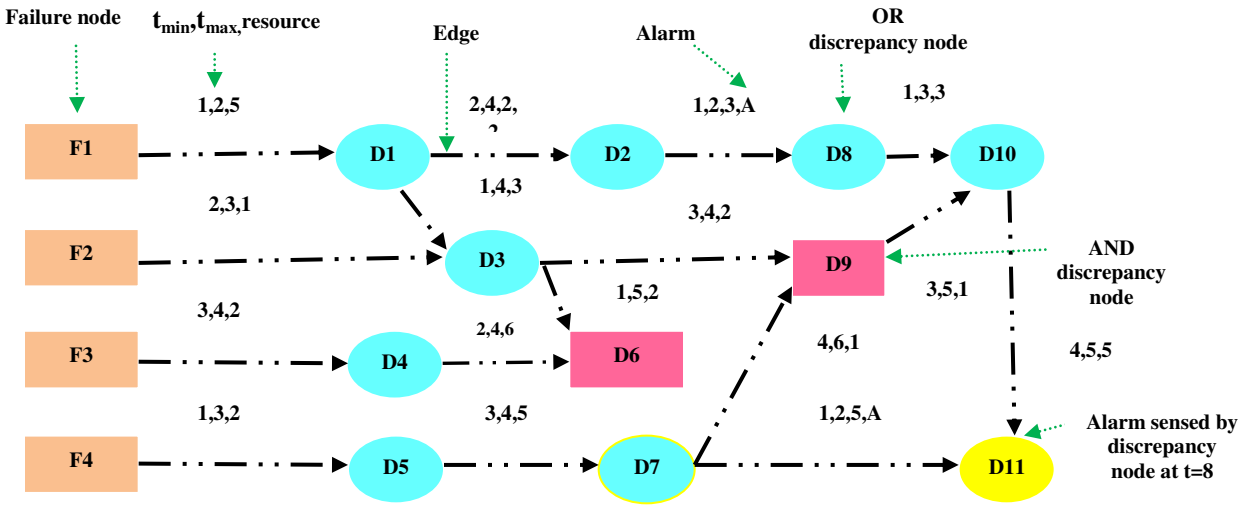


Figure 4.1: Time Failure Propagation Graph

5.1.1.2 Control Flow Analytics [CFA]

System : RailTech system (Mechanical, Electrical, Electronics, Information system : Driver Advice System [DAS], Communication system);
Assess risks: Verify correctness, reliability, consistency, liveness, deadlock freeness, synchronization and reachability in control flows.

- **Basic control flows** : Sequential, Parallel split, Synchronization, Exclusive choice, Simple merge;
- **Special branching and synchronization control flows**: Multi choice, Synchronizing merge, Multi merge, Discriminator, m-out-of-n join;
- **Structural control flows** : Loop, Implicit or explicit termination, Multiple instances;
- **State based control flows**: Deferred choices, Interleaved parallel routing, Milestone, Cancel;

Mitigate risks.

- Replace faulty components through proactive and reactive maintenance;
- Rectify circuit connectivity;
- Correct Boolean logic in electrical and electronic circuit: AND / NAND/ Exclusive OR/ NOR/ XOR/ XNOR/ NOT;

5.1.1.3 Resource Flow Analytics [RFA]

System : RailTech system (Mechanical, Electrical, Electronics, Information and Communication system), smart coaches;
Assess risks: Verify correctness, and fairness of resource management;

- **Resource planning:** sense demand supply mismatch.
- **Resource allocation** : automatic / semi-automatic execution, direct allocation, role based allocation, deferred allocation, authorization in allocation, separation of duties, case / exception handling, capability based allocation, history based allocation, organizational allocation, resource initiated allocation
- **Resource distribution** : Single / multiple resources distribution, early / late distribution, priority queue, autonomous resource allocation;
- **Resource mobilization**
- **Resource sharing**
- Resource delegation, escalation, deallocation, suspension, resumption, skip, redo, stateful / stateless reallocation, simultaneous / chained execution;

Mitigate risks:

- Optimal resource allocation (e.g. avoid shortage or surplus of resources such as fuel, safety stock)
- **Sensor based on board condition monitoring system**
    - Monitor health of critical system components (e.g. wheels) through sensors, CCTVs, smoke detectors, Fire extinguishers, IoT and integrated information system.
    - Real-time fault detection: Detect defects and major causes for derailments and delays and deterioration in tracks, running trains and other rail infrastructure.
    - Trade-off cost vs. comforts / luxury;

5.1.1.4 Data Flow Analytics [DFA]

System : RailTech system (Information and Communication schema of DAS)
Data elements: Single / multiple instance DAS operating environment data, Atomic and block task data, Boolean and numeric data, time series data;
Assess risks. Verify correctness, reliability and consistency of data schema.

- Data visibility
- Data interaction among various elements of DAS
- Data transfer between various components of networking, computing and application schema of DAS
- Data transformation
- Data based routing of various control flow patterns associated with DAS

- Data analysis / mining
    - ETL (Extract, Transform, Load) mechanism
    - Data cleaning and selection
    - Knowledge discovery from data
    - Data visualization

Mitigate risks:

- Sense flaws in data flow, streamline data management.
- Detect noise, missing, imprecise sensor data; clean data before analysis.

5.1.2 Fault Tree Analytics [FTA]

Call fault tree analytics;
Objectives : identification and analysis of conditions and factors that cause the occurrence of faults;
System verification mechanism : verify reliability and safety of RailTech system performance through top-bottom approach;

- Define fault tree structure based on system data, scope and applications related to RailTech System;
- Fault tree development, construction and evaluation;
    - Events
        - Basic event /* failure of a component */
        - External event /* normally expected to occur */
        - Undeveloped event /* insufficient data */
        - Conditioning event /* conditions that control logic gates */
    - Logic gates
        - AND gate /* o/p will occur only if all independent i/ps occur */.
        - Priority AND gate /* o/p occurs if the i/ps occur in a specific sequence specified by a conditioning event */
        - OR gate /* the o/p will occur if any i/p occurs */
        - Exclusive OR gate /* o/p will occur if exactly one i/p occurs */
        - Inhibit gate /* o/p will occur if i/p occurs under an enabling condition specified by a conditioning event*/
- Compute failure rate from fault tree analysis;

Output: FTA provides following output to the driver through automated data visualization tool.

- report
- error trail / error trace / fault propagation path

FTA is generally used as a diagnostic tool to understand the logic leading to a faulty state; does root cause and pareto analysis; evaluates, monitors and controls safety, consistency and reliability of a complex system. FTA is a deductive reasoning that analyses an undesired top level event and identifies fault configurations i.e. minimal cut sets; a cut set is a set of faults that represents a necessary, but not sufficient, condition that may cause an undesired state of a system. Event X occurs only if both events Y and Z occur. Event Y occurs if either event P or Q occurs. The standards, frequently used symbols, conventions, events and logic gates for fault tree diagrams can be found in [29].

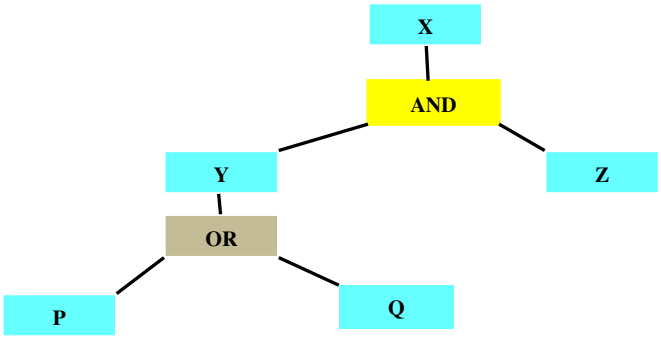


Figure 4.2: Fault tree

5.1.3 Failure Mode Effect Analytics [FMEA]

Call Failure Mode Effect Analytics (FMEA);
Objectives : identification and analysis of conditions and factors that cause the occurrence of faults;
Verify reliability and safety of RailTech system performance through bottom-up approach;
Output:

- FMEA Table: it highlights causality relationship between faults and undesired states or properties.
- Data visualization -error trail / error trace / fault propagation path;

Let us exercise a comparative analysis on TFPG, FTA and FMEA [29,40]. FTA is a deductive and top-down method which analyzes the effects of a fault and events on a complex system. FMEA is an inductive and bottom-up method which analyzes the effects of a single component on a system. FTA shows how a system is protected to single or multiple faults. It is not good at finding all possible faults of a system. FMEA is good at finding all possible faults exhaustively and their local effects. It is not good at finding multiple failures and their effects at a system level. FTA considers external events but FMEA does not consider it. TFPG allows fine grained and precise analyses that FMEA cannot do. FTA explores only subsets of propagation paths in response to specific events, TFPG presents a more comprehensive and integrated view of failure in a complex and dynamic system.

6. STRATEGY [S_5]

Strategic moves for RailTech diffusion

- Real-time fault diagnostics using fault tree analytics, FMEA and TFPG
- Automated verification of security intelligence at multiple levels using deep analytics
- Distribution of intelligence
- Processing unit integration
- Integration of driver's interfaces, train positioning and communication schema
- Exchange of information between track and train
- SWOT and TLC analysis /* section 6.1*/

6.1 SWOT & TLC Analysis

Let us first analyze strength, weakness, opportunities and threats of RailTech innovation. There are opportunities of growth of the technology in various types of train services such as metro rail, local train and long distance train. But, the technological innovation may face various types of threats such as complexity, integration and digital transformation through sensors, information and communication technologies. It is hard to integrate the mechanical and information systems physically. Let us analyze three different types of system architectures in figures 4.3, 4.4 and 4.5 [26]. We have extended these architectures by incorporating the concept of real-time fault diagnostics. In each system architecture, the basic building blocks of RTFD are three analytics i.e. graph analytics (GA), fault tree analytics (FTA) and failure mode effects analytics (FMEA); the output of these analytics is fed to DAS. The core components of GA include control, resources and data flow analytics. In figure 4.3, DAS intelligence is deployed at TCC and the onboard system only displays advice information to the driver. The system can be implemented using existing driver interface without any additional system in the train. But, the scope of data displayed and dynamic update of compensating feedback to the driver is limited. This is an interesting practical and economic solution for possible DAS rollout in future.

In figure 4.4, DAS intelligence is shared between TCC and train. TCC computes various critical parameters like previous architecture. DAS definitions and displays are done onboard. The solution optimizes the exchange of information between TCC and onboard in real-time. But, the advice can be poor if the real characteristics of the train system differ significantly from the characteristics known by TCC. The computation should be done correctly where it is easier to access the required data.

In figure 4.5, DAS tasks are mainly onboard. DAS intelligence is implemented in the train. TCC computes a set of functions as mentioned previously. It can adjust speed and optimizes energy to drive the train based on advanced algorithms. The cost of communication between TCC and the train is reduced. But, there is risk of consistency of local optimization.

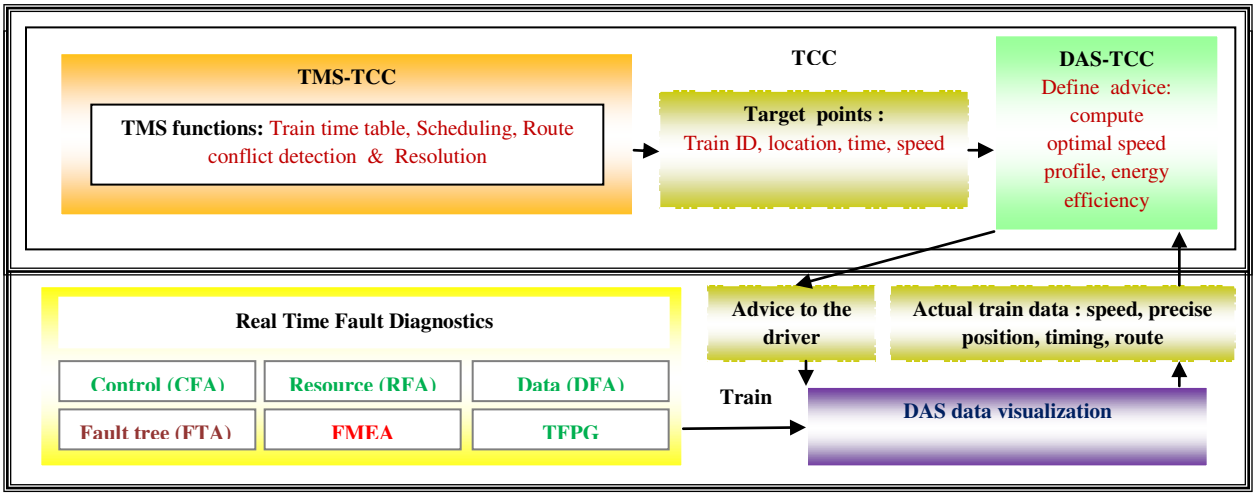


Figure 4.3 : DAS tasks done at Traffic Control Centre (TCC)

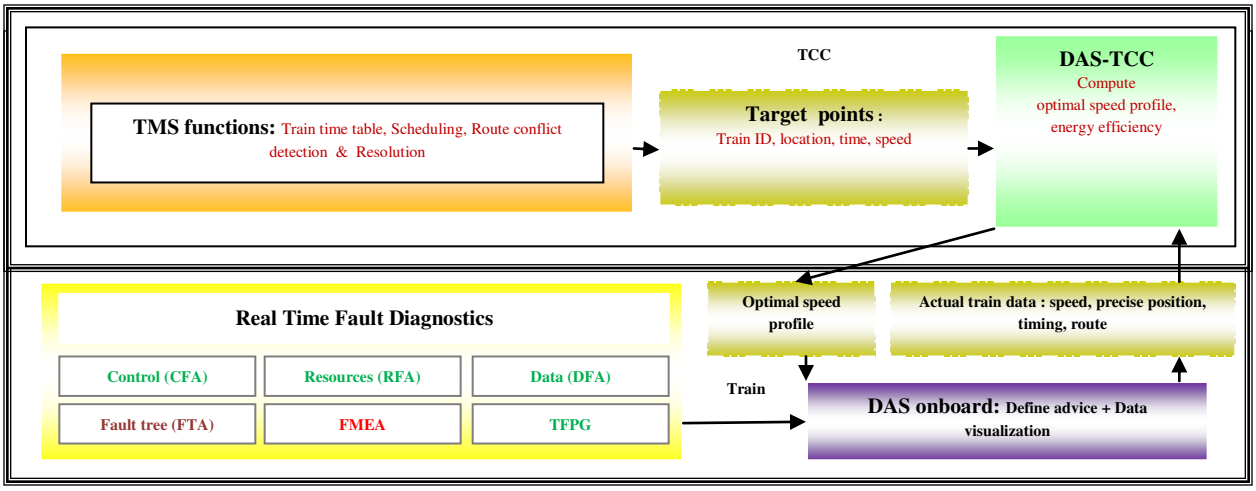


Figure 4.4: DAS tasks shared between the train and traffic control centre (TCC)

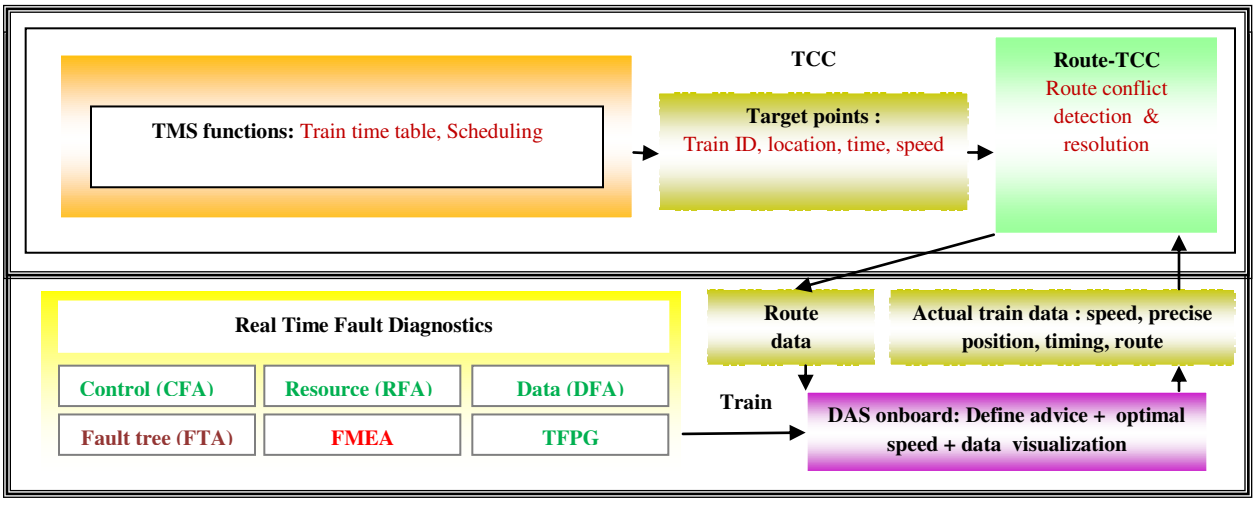


Figure 4.5 : DAS tasks mainly onboard in the train

6.2 Technology Life-cycle Analysis

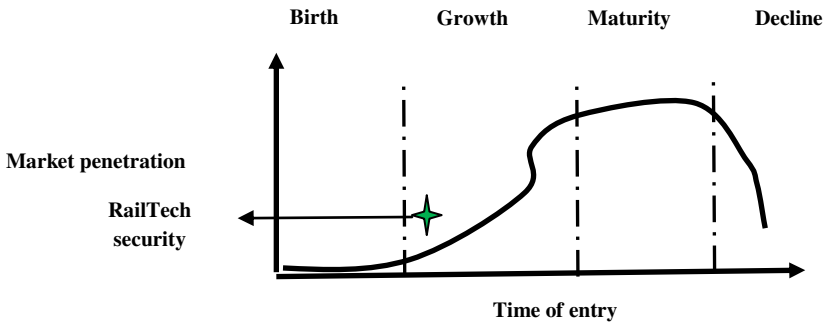


Figure 4.6 : Technology Life–cycle Analysis of RailTech

Figure 4.6 indicates approximate position of RailTech (as considered in this work) on S-curve of technology life-cycle. It is expected that RailTech will go through emergence, diffusion, development and maturity phases in this decade. At present, the technology is at growth phase of TLC. It is not a trivial task to evaluate and explore technology life-cycle in terms of S-curve, trajectory, diffusion strategy and dominant design of RailTech. It is hard to understand how RailTech interacts with other technologies, systems, cultures, enterprise activities and impacts on society.
Initially, it may be difficult and costly to improve the performance of the RailTech; the performance is expected to improve with better understanding of the fundamental principles and system architecture. The evolution of this technology passes through a phase of turbulence and uncertainty; various stakeholders associated with the system may explore different competing design options of the new technology and a dominant design will emerge through consensus and convergence of structure.

7. STAFF-RESOURCES [S_6]

Critical Success Factors for RailTech Diffusion

- Innovators : R&D units of Railways corporation; management information system (MIS) and technology management departments of academic institutes, collaborative networks;
- Organizational creativity, organization structure, cooperative work culture, human capital management, talent management, knowledge management;
- Audit fairness in resource allocation (e.g. 5'M': man, machine, material, method, money), cost and quality control.

The sixth element of deep analytics is staff-resources. The sources of RailTech innovation may be R&D units of Railways Corporation, MIS and IT units of engineering and management institutes and collaborative networks. Creativity is the underlying process for RailTech innovation which can promote new ideas through shared vision, intellectual abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics. It demands the motivation and commitment of the creative people to look at the problems in unconventional ways. Organizational creativity is closely associated with human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routine and incentive policy.

8. SKILL-STYLE-SUPPORT [S_7]

Critical Success Factors for RailTech Diffusion

- New skills developments for train drivers and traffic controller
  - Data visualization and data analysis (e.g. fault tree, FMEA, TFPG)
  - Information and communication technology,
  - Coordination and integration in traffic control;

- Style : energy efficient driving style, operation management by objectives, shared vision and goal setting;
- Support : proactive, reactive, preventive and breakdown maintenance of RailTech system (e.g. mechanical, electrical, electronics and IT schema;
- Audit gaps in skills, style and support through rational talent acquisition, retention and training strategies.

The seventh element of deep analytics is skill-style-support. The workforce involved in RailTech innovation are expected to develop different types of skills in technical (e.g. MIS, information and communication technology), management and system administration domains such as research and development, maintenance support, knowledge management, system design, process innovation and project management. The system administrators should have leadership skill in smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of RailTech innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management should be able to tackle the complexity of system implementation with the support of efficient teams.

It is essential to develop multiple skills in new RailTech system development through proper coordination among design and supply chains. The basic objectives are to maximize fit with the needs of the drivers, ensure quality assurance and control R&D cost. It is an interesting option to get the suppliers and the train drivers in the development process. It is really challenging to develop a complex RailTech system through a sound knowledge base and problem solving capability.

9. CASE ANALYSIS: RAIL SECURITY & SAFETY

Test case 1 (Fire in metro rail) : It was an incident of fire in metro rail of the metropolitan city Sidben.

19:02 : Trip of electrical connection near Masco station, suffocating black smoke was spreading rapidly inside the tunnel of metro rail.

19:03: The information was given to the fire brigade and police. The helpless passengers were trapped inside the locked and fully packed metro rail compartments; they were traumatized; it was a horrific experience; the time lasted for 55 minutes; the passengers tried to escape from the locked compartments by breaking glass windows but could not be successful; some passengers were injured in stampede; they called metro rail helpline, the public address system did not work; a passenger broke her leg; the metro rail boards and the state governments were involved in blame game; the metro rail board set up a committee. The metro rail wrecks are in dangerous conditions; there was no proper maintenance; anything from the rail compartment falling on the rail track might cause fire.

19:05: The metro rail employees started extinguishing fire by spraying water.

19: 14 : The electrical supply was disconnected in third rail.

19: 20 : The emergency rescue operation started.

19:55 : The rescue operation ended.

Deep analytics raised a set of important issues on the aforesaid accident in metro rail:

- Was the disaster management team ready to control the situation? What was the composition of disaster management team: NDRF, NSG and the employees of metro rail?
- What was the response time in such type of disaster? What are the devices and equipments available: jacket, gas mask, oxygen cylinders or anything else?
- What were the fire protection strategies? Can the employees of rail stations tackle small fire incidents? Can the fire brigade tackle major fire accidents? Are there water pipes in the tunnel for extinguishing fire?
- Is it possible to save the passengers from various acts of terrorism through the efforts of the police, military and NSG?
- Did the public address system work correctly in time?
- Was the logic of emergency door opening correct: was it a fully automated or manual system? Did the doors open only at station platforms?

- Was the maintenance problem considered as the root cause of the accident?
- Was there high risk of accidents in the metro rail? Who should be punished for the irresponsibilities? What was the accountability of higher authorities? Who took the responsibilities of any damage of the passengers?
- Why did not the driver drive the train towards next station from the spot of accident? Why did the train stop in the tunnel?
- Why did the emergency brake work? Was it due to the disconnection of power supply in train protection circuit?
- Was the driver able to contact the control room?
- Did the passengers get down before the disconnection of power supply in the third rail?
- Where were the train driver and guard during the time of accident?
- Was there any metro rail helpline number; how to contact the control room?

The possible risk mitigation strategies are expected to include several critical measures such as fire protection system, smoke detectors and CCTVs in each compartment, regulatory compliance on smoking inside running train, ban on carrying of hazardous materials (e.g. bombs, fireworks, explosives, kerosene, petrol and diesel) by the passengers, fire protection from the gas oven at pantry cars, use of induction cookers instead of gas ovens, announcements and alerts in time through public address system, automated air conditioning system in the tunnel, automated control of the velocity and direction of airflow to resist spreading of smoke and fire, automated airflow control system in the compartment after sensing smoke, footpath inside the tunnel, disconnection of power supply in third rail, fire caused by antisocialists and terrorists such as explosion or nerve gas attack and readiness of fire brigade and disaster management workforce.

Test case 2 (Fog and mist in winter) : It was winter in January'2018. Smith was pursuing his Doctoral programme at a management institute. He went to Delhi to present his paper at an International Conference. He was accompanied with his mother (50 years), wife (35 years) and son (3 years). It was a very cold night. Smith was returning to Howrah from Delhi by a superfast mail. The train started at 1 a.m. with a delay of 4 hours. The train arrived near Kanpur and stopped. The reason was poor visibility to the train driver due to dense fog and mist. The temperature was about 2 degree centigrade. The train could not start for about 4 hours till the sunrise in the morning. It was a horrible experience to Smith and his family members. They were in non-AC compartment. The kids inside the train compartment were crying and coughing in the severe cold weather. All the passengers and the driver were helpless at that night.

Test case 3 (Breakdown during journey): Smith was returning from Chennai to Howrah by a superfast express train. The train started at 23-45. At midnight, the train suddenly halted with heavy jerk. The passengers became frightened. The driver discovered that the gas pipe was broken. He replaced the gas pipe through shearing and welding operations in the darkness. The train was delayed by 1 hour. Was it possible to predict the poor health of the gas pipe in time?

Test case 4 (Act of terrorism): There were rail accidents with many casualties in country X due to various acts of terrorism. One case, the fishplates were taken out by the terrorists. There were five cases where the railway tracks were blown out with highly dangerous explosive bombs by the malicious agents. There were some horrific incidents of robbery and loot by the dacoits at night. There were also many incidents of theft of shoes and belongings of the passengers. Can automated check-in system at various rail stations ensure security and safety of the passengers? Do the passengers need protection by the armed security force and watchdogs during journey by rail?

Test case 5 (Healthcare problem during rail journey): There were frequent cases of allergic disorders, itching, skin rash, heart burning and food poisoning of the train passengers during long distance rail journey in summer and also cold and cough, breathing problems and fever in winter. There are high risks of attacks of infectious diseases (e.g. conjunctivitis, eye infection, skin rashes etc) from the other travelers during rail travel. Should the passengers carry emergency medicines (e.g. anti-allergic tablets, fever, cold and cough, digestion problem, stomach upset) and pure drinking water as proactive and reactive approaches of healthcare? Should they avoid spicy, oily, rich and fast food during travel? Railway catering services must take care of such issues. The travelers should clean their seats and berths with disinfection germ protection stuff proactively.

10. CONCLUSION

How to manage evolution of technological innovation in RailTech security and safety? The nature of innovation is expected to shift after the emergence of a dominant design. The pace of improvement of RailTech performance should be monitored properly. The evolution of this innovation is influenced by intersecting trajectories of performance as demanded by the drivers and the performance supplied by RailTech system. The diffusion of innovation depends on how the new technology will spread through a population of potential adopters globally. The present work considers only a specific area of RailTech with focus on DAS and real-time fault diagnostics from the perspectives of MIS. It is really an interesting and potential research agenda. It is possible to extend this study in various ways. Is it rational to imagine a train as a block chain? There are other various issues of RailTech safety and security such as consistency in train length, fire hazards, food poisoning, health & hygiene issues, anti-collision devices, modernization of rail signaling system, smart coaches, smart grid, black box, use of CCTV/Wi-Fi/Webcam, unmanned level crossing, passengers crossing railway tracks while talking on mobile phones, derailment of trains due to cracks in tracks or poor maintenance, rushing attacks, non-availability of overbridges, footbridges and skywalks and miscellaneous flaws in mechanical, electrical and civil infrastructure. Is it possible to extend this study to the decision making problems of external and home affairs ministries in corporate governance such as human traffic and refugees control in a country? An intelligent rail budget is expected to address all these issues rationally.

REFERENCES

1. T. Albrecht. 2005. Energy-efficient train control in suburban railways: experiences gained from onboard tests of a driver assistance system. In: 1st International Seminar on Railway Operations Modelling and Analysis, Delft, Netherlands.
2. T. Albrecht. 2009. The influence of anticipating train driving on the dispatching process in railway conflict situations. Netw. Spat. Econ. 9 (1), 85.
3. T. Albrecht. 2013. Human factor challenges in the development of a driver advisory system for regional passenger trains. In: Rail Human Factors: Supporting Reliability, Safety and Cost Reduction, pp. 129–138.
4. S.Dekker. 2007. Conflict detection and human-machine coordination. In: Hindsight, 4, January 2007. EUROCONTROL Directorate of ATM Programme – Security, Safety and Human Factors Business Division (DAP/SSH), pp 7–9.
5. DeltaRail Group. 2008. Advisory speeds for drivers for energy management and regulation. In: RSSB Interim Report Milestone 2, Issue 01 and 02.
7. DeltaRail Group. 2009. Driver advisory information for energy management and regulation. In: Stage 1 Report, RSSB Research Programme, T724.
8. W. Hamilton and T. Clarke. 2005. Driver performance modelling and its practical application to railway safety. Appl. Ergon. 36 (6), 661–670.
9. P.G.Howlett, I.P. Milroy and P.J. Pudney. 1994. Energy-efficient train control. Control Eng. Pract. 2 (2), 193–200.
10. R. Liu AND I.M. Golovitcher. 2003. Energy-efficient operation of rail vehicles. Transp.Res. A 37, 917–932.
11. P. Lukaszewicz. 2008. Methods for energy efficient driving – algorithms. RailEnergy, Document ID NRG-KTH-D-2.3-005.
12. I. Mitchell. 2009. The sustainable railway: use of advisory systems for energy savings. IRSE News, No.151, pp. 2–7.
13. Rail Safety and Standards Board, 2008. The Rule Book. GE/RT8000, Issue 7.
14. Rail Safety and Standards Board, 2008. Good Practice Guide To Train Driver Training. RS/221,Issue 1.
15. Rail Safety and Standards Board, 2008. Train Movement – Staff Suitability and Fitness Requirements, GO/RT3451, Issue 01.
16. S. Tschirner, S., A.W.Andersson and B. Sandblad. 2013. Designing train driver advisory systems for situation awareness. In: Rail Human Factors: Supporting Reliability,Safety and Cost Reduction. pp.150–159.
17. J. Wardale. 2008. Advice on energy efficient driving. Presentation to drivers, CrossCountry Rail.

18. C.Conte and A. Schöbel. 2007. Identifying dependencies among delays. In: Proceedings of 2nd International Seminar on Railway Operations Research (RailHannover 2007), Hannover.
19. W.Daamen, T. Houben, R.M.P. Goverde, I.A. Hansen, V.A. Weeda. 2006. Monitoring system for reliability of rail transport chains. In: Proceedings of the 7th World Congress on Railway Research (WCRR 2006), Montreal.
20. S. De Fabris, G.Longo and G. Medeossi. 2008. Automated analysis of train event recorder data to improve micro-simulation models. In: J. Allan, E. Arias, C.A. Brebbia, C. Goodman, A.F. Rumsey, G. Sciutto, G. and A. Tomii (Eds.), Computers in Railways XI. WIT Press, Southampton, 575–583.
21. A. Exer. 1995. Rail traffic management. In: Bailey, C. (Ed.), European Railway Signalling. IRSE, A&C Black, London, 311–342.
22. H. Flier, R. Gelashvili, R., T. Graffagnino and M. Nunkesser. 2009. Mining railway delay dependencies in large-scale real-world delay data. In: Ahuja, R.K., Möhring, R.H., Zaroliagis, C.D. (Eds.), Robust and Online Large-Scale Optimization: Models and Techniques for Transportation Systems, LNCS 5868. Springer, Berlin, 354–368.
23. R.M.P. Goverde. 2005. Punctuality of railway operations and timetable stability analysis. PhD thesis, Delft University of Technology.
24. R.M.P.Goverde. 2011. A delay propagation algorithm for large-scale railway traffic networks. Transportation Research, Part C 18 (3), 269–287.
25. R.M.P.Goverde, W. Daamen, I.A. Hansen, I.A. 2008. Automatic identification of route conflict occurrences and their consequences. In: Allan, J., Arias, E., Brebbia, C.A.,Goodman, C., Rumsey, A.F., Sciutto, G., Tomii, A. (Eds.), Computers in Railways XI. WIT Press, Southampton, pp. 473–482.
26. P.Konstantinos, P. Tzieropoulos and D. Emery. 2014. Railway driver advice systems: Evaluation of methods, tools and systems. Journal of Rail Transport Planning & Management.
27. M.Ullius. 2004. Verwendung von Eisenbahnbetriebsdaten für die Schwachstellenund Risikoanalyse zur Verbesserung der Angebots- und Betriebsqualität. PhD thesis, Swiss Federal Institute of Technology, Zurich.
28. N.Van Oort. 2011. Service reliability and urban public transport design. PhD thesis, Delft University of Technology.
29. Fault Tree Analysis, CEI/IEC 61025:2006.
30. S. Padalkar, J. Sztipanovits, G. Karsai, N. Miyasaka and K. C. Okuda. 1991. Real-time fault diagnostics. IEEE Expert, vol. 6, no. 3, pp. 75–85.
31. A.Misra, J.Sztipanovits, A. Underbrink, R. Carnes and B. Purves. 1992. Diagnosability of dynamical systems. In 3rd International Workshop on Principles of Diagnosis.
32. A.Misra. 1994. Senor-based diagnosis of dynamical systems. Ph.D. Dissertation, Vanderbilt University.
33. S.C.Ofsthun and S. Abdelwahed. 2007. Practical applications of timed failure propagation graphs for vehicle diagnosis. In Autotestcon, 2007 IEEE, 250–259.
34. S. Abdelwahed, G. Karsai and G. Biswas.2006. Notions of Diagnosability for Timed Failure Propagation Graphs. In IEEE Systems Readiness Technology Conference, AUTOTESTCON'06, CA.
35. R.Alur, and T.A. Henzinger. 1993. Real-time logics: complexity and expressiveness. Information and Computation 104(1):35–77.
36. B.Bittner, M.Bozzano, A. Cimatti, M.Gario and A.Griggio. 2014. Towards pareto-optimal parameter synthesis for monotonic cost functions. In Proceedings of the 14th Conference on Formal Methods in Computer-Aided Design, 23–30.
37. B. Bittner, M. Bozzano, R.Cavada, A. Cimatti, M.Gario, A. Griggio, C. Mattarei, A. Micheli, and G. Zampedri. 2015. The xSAP safety analysis platform. arXiv preprint arXiv:1504.07513.
38. M. Bozzano, A. Cimatti, A. Pires, D. Jones, G. Kimberly, T. Petri, R. Robinson, and S. Tonetta. 2015. Formal Design and Safety Analysis of AIR6110 Wheel Brake System. In Proc. CAV 2015, 518–535.
39. M. Bozzano, A. Cimatti, M. Gario and A.Micheli. 2015. Smt-based validation of timed failure propagation graphs. In 29th AAAI Conference on Artificial Intelligence.
40. M.Bozzano, A. Cimatti and f. Tapparo. 2007. Symbolic fault tree analysis for reactive systems. In Automated Technology for Verification and Analysis, Springer, 162–176.
41. R. Cavada, A. Cimatti, M. Dorigatti, A. Griggio, A. Mariotti, A. Micheli, S. Mover, M. Roveri and S. Tonetta. 2014. The nuxmv symbolic model checker. In Computer Aided Verification.334–342. Springer.
42. C. Roberts and R.M.Goodall. 2009. Strategies and techniques for safety and performance monitoring on railways. Proceedings of the 7th IFAC Symposium on, Fault Detection, Supervision and Safety of Technical Processes, Spain.

Exercise

1. **Explain the technology of Railtech Security and Safety? Justify it as a technology for humanity. What is the scope of this technology?**
2. **What is the dominant design of the technology?**
3. **What are the basic elements of the system architecture?**
4. **What do you mean by technology security? How to verify the security intelligence?**
5. **What are the strategic moves of technology innovation, adoption and diffusion for Railtech Security and Safety'? What is the outcome of technology life-cycle analysis?**
6. **How to manage resources for this innovation project?**
7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
9. **Design an optimal DAS architecture through SWOT analysis.**
10. **Design Real-time Fault Diagnostics which can be integrated with DAS.**

CHAPTER 5: EMERGING DIGITAL TECHNOLOGIES: INNOVATION, ADOPTION and DIFFUSION

Abstract: With the significant advancement of information and communication technology, computing is perceived to be used as the next utility after water, electricity, gas and telecommunication. This chapter explores the scope of emerging digital technology in terms of communication and information technology. The scope of emerging communication technology is explored in terms of cloud computing, cloud streaming, cloud analytics, Internet of Things (IoT), Industrial IoT, Edge computing, next generation wireless and mobile communication, broadcast and satellite communication, RFID and sensor networks. The scope of information technology is explored in terms of ISI analytics, adaptive security, dynamic data protection, cyber security, crash proof code; applied AI and machine learning, soft computing, deep learning, robotics; deep analytics, predictive analytics, collaborative analytics, virtual and augmented reality, digital twins, solar computing, pervasive computing, wearable computing, quantum computing and ray tracing. This work also evaluates emerging digital technology in terms of system, structure, security, strategy, staff-resources and skill-style-support. Specifically, the technologies of adaptive security, dynamic data protection and solar computing have been evaluated in depth in chapters 5,6 and 7. The scope of deep analytics and deep learning have been outlined in chapter 1 and 8 respectively.

Keywords : Information technology, Communication technology, Applied AI, Green IS, Smart Grid, Machine learning, Virtual reality, Cloud streaming, Adaptive security, Dynamic data protection, Big data analytics, IoT, Cyber security, Pervasive computing, Edge computing, RFID, Sensors, 3G,4G,5G

1. SCOPE

Figure 5.1 : Scope analytics on emerging digital technology

It is possible to explore the scope of digital technology through Business Process Reengineering (BPR) approach (analyze as-is process and related IS, identify gaps and risks of as-is processes and IS and design to-be processes and system); top-down approach, critical success factor (CSF) analysis based on business objectives, constraints and requirements engineering, value chain analysis, bottom-up approach and inside-outside approach. One of the contributions of this chapter is scope analytics of emerging technology in figure 1. The scope analytics shows a set of information and communication technologies; among which the concept of deep analytics, solar computing and information security intelligence (ISI) analytics are unique and have been explored in details in chapters 1,6 and (5,7) respectively.

1.1 Communication Technology

The scope of emerging communication technology may be explored in terms of cloud computing, cloud streaming, cloud analytics, Internet of Things (IoT), Industrial IoT and Edge computing next generation wireless and mobile communication, broadcast communication, satellite communication, RFID and sensor networks. The wireless technology is going through an evolution of a set of generations (1G->2G->3G->4G->5G). This chapter analyzes the technology of cloud computing, streaming and analytics and edge computing. Chapter 7 is focused on IoT.

1.1.1 Cloud Computing, Cloud Streaming & Cloud Analytics

With the significant advancement of information and communication technology, computing is perceived to be used as the next utility after water, electricity, gas and telecommunication. The concept can be extended to cloud computing and grid computing for a market oriented grid. Utility computing is associated with a parallel and distributed system that enables the sharing, selection and aggregation of geographically distributed autonomous computational resources dynamically at runtime depending on their availability, capability, performance, cost and quality through web service. The computational resources include different types of sophisticated software applications such as data mining, scientific computing and image processing, data, CPU or processing power, servers, storage devices, scanners, UPS and network interfaces which can be shared through web service. The objective of utility computing is to provide computing power and storage capacity that can be used and reallocated for any application and billed on a pay-per-use basis. Utility computing consists of a virtualized pool of information systems and other IT resources that can be continually reallocated to meet changing business and service needs of the consumers. These resources can be located anywhere and managed internally or externally. The service provider tracks the usage of computational resources of the consumers and makes invoice based on predefined price setting and usage data. An efficient resource management system coordinates and monitors the complex operation. Utility computing supports virtualization. Cloud computing is basically a distributed computing where dynamically scalable and virtualized resources are provided as a service over the internet to achieve cost saving, easy scalability and high availability. The services offered through cloud computing usually include Software-as-a-Service (SaaS), Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), data-Storage-as-a-Service (dSaaS) and database-as-a-service (DaaS). SaaS allows users to run applications remotely from the cloud. IaaS provides a set of computing resources as a service which includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access. PaaS includes operating systems and required services for particular applications along with data security, backup and recovery, application hosting and scalable architecture. dSaaS provides data storage, data warehousing and data mining facilities. This is a cost effective, innovative IT infrastructure from which the consumers are able to access desired computational resources and from anywhere in the world on demand.
The key technologies that enable cloud computing are virtualization, web service, service oriented architecture, service flows and work flows. The trading in cloud computing depends on several technological issues such as high availability of service, business continuity, data lock-in, security and privacy of data, efficient data transfer, performance predictability, scalable storage, efficient bugs management in large distributed system, adaptive scaling of operation, innovative software licensing and reputation mechanisms. Strategic pricing considers all these QoS factors to define optimal price setting for

cloud computing. In fact, an intelligent, innovative competitive pricing mechanism and secured high QoS can make cloud computing an attractive IT business model as compared to traditional corporate computing model based on direct IT investment. Nowadays, pay-for-use or pay-as-you-go licensing are becoming popular in cloud computing market. Thus, the computing world is rapidly transforming towards developing information systems to be consumed as a service. Various service providers have started to build scalable data centers at various locations for hosting cloud computing.

The key players of the market of cloud computing are a set of service providers, service consumers and resource brokers. There are several challenges of trading in cloud computing : fair resource allocation protocols, optimal task scheduling, tendering, contract net protocols, auction, market clearing and negotiation mechanisms and pricing algorithms. The major threats are reduced contract duration, uncertainty, risk and variable duration of a portfolio of contracts, reduced switching costs and customer lock-in, uncertain customer demand, short life-cycle and high sunk cost. Cloud computing may require high development cost for instrumentation, provisioning and monitoring and start up costs in the face of uncertain demand.

*Cloud streaming***:** Cloud based mobile video streaming techniques are used in online gaming, videoconferencing, augmented reality and watching videos (e.g. movies, music) through smart phones (e.g. mobile visual search smart phones, Tablets). The scope of cloud streaming may be explored through a set of technologies such as mobile multimedia, wireless network, cloud computing, video streaming and video sharing technologies. In mobile communication network, video sharing is done through wireless link (e.g. 3G, 4G, Wi-Fi); on-demand, dynamic and easily accessible video data are provided through streaming protocols in cloud environment. Mobile devices have various constraints such as computation, memory and energy capacity. Mobile cloud computing paradigm is used in transmission of real-time data (e.g. audio, video, text, GPS) transmission; it is bridging the gap between the demand of the service consumers and capability of various mobile devices in terms of data storage and processing of video and audio data.

1.1.2 Edge Computing

Edge computing is a distributed computing paradigm which enables computation and data storage closer to the location where it is needed; improves response times and saves bandwidth. It supports data processing at or near the source of data generation. IoT connected devices interact with remote sensors and may generate data. Edge computing is a perfect fit for IoT - data is processed near the point of origin, the latency between devices and data processing layer is reduced and enable faster response and correctness in decision making. The increase of IoT devices at the edge of the communication network may generate massive amount of data to be computed to data centers and may result the constraints of network bandwidth. Data centers may not guarantee acceptable transfer rates and response times. The devices at the edge constantly consume data from the cloud and demand the development of content delivery networks to decentralize data and service provisioning.

The basic objective of edge computing is to move the computation away from data centers towards the edge of the network through a set of smart objects, smart phones and network gateways to perform various tasks such as service delivery, storage and IoT management and ensure improved response time and transfer rate. But there are various news issues in distributed computation such as security and privacy of data, scalability, resiliency, reliability and consistency of system performance. The data should be encrypted for the protection from hacking but it may result increased cost of computation and communication. Scalability in a distributed network should consider different constraints of system performance, energy constraints, dynamic data management and heterogeneity of IoT devices. The system should be protected in terms of liveness, fast fault detection and recovery and stability of the topology of entire distributed system. It is interesting to explore the applications of edge computing in cloud streaming, smart cities and villages and home automation systems.

1.1.2 Internet of Things (IoT), IIoT, RFID, Sensors

Internet of Things (IoT) is a system of interrelated computing devices, mechanical, electrical, electronics and biomedical machines, objects, animals and people with unique identifiers (UIDs) with the ability to transfer data over a network without human-to-human or human-to-computer interaction. IoT has been evolving due to the convergence of multiple technologies such as real-time analytics, machine learning,

sensors, embedded systems, wireless sensor networks, control systems, automation (home and building automation), smart home (e.g. lighting fixtures, thermostats, home security systems, cameras), smart phones and smart speakers. But, there are constraints of information security and privacy. The technology has been evolving through various phases of RFID, sensor networks and Industrial IoT (IIoT).

1.2 Information technology

1.2.1 Analytics

Analytics is one of the most promising digital technologies today. The technology is going through an evolution of various phases such as shallow, predictive, collaborative, big and deep analytics. Deep analytics is an intelligent, complex, hybrid, multi-phased and multi-dimensional data analysis system. The basic steps of computation are data sourcing, data filtering / preprocessing, data ensembling, data analysis and knowledge discovery from data. The authorized data analysts select an optimal set of input variables, features and dimensions (e.g. scope, system, structure, security, strategy, staff-resources, skill-style-support) correctly being free from malicious attacks (e.g. false data injection, shilling); input data is sourced through authenticated channels accordingly. The sourced data is filtered, preprocessed (e.g. bagging, boosting, cross validation) and ensembled. It is rational to adopt an optimal mix of quantitative (e.g. regression, prediction, sequence, association, classification and clustering algorithms) and qualitative (e.g. case based reasoning, perception, process mapping, SWOT, CSF and value chain analysis) methods for multi-dimensional analysis. The analysts define intelligent training and testing strategies in terms of selection of correct soft computing tools, network architecture – no. of layers and, nodes; training algorithm, learning rate, no. of training rounds and stopping criteria;. The hidden knowledge is discovered from data in terms of collective, collaborative, machine, security and business intelligence. The analysts audit fairness and correctness of computation and also reliability, consistency, rationality, transparency and accountability of the analytics.

Deep analysis (e.g. in memory analytics) can process precisely targeted, complex and fast queries on large (e.g. petabytes and exabytes) data sets of real-time and near real-time systems. For example, deep learning is an advanced machine learning technique where artificial neural networks (e.g. CNN) can learn effectively from large amount of data like human brain learn from experience by performing a task repeatedly and gradually improves the outcome of learning. Deep analytics follows a systematic, streamlined and structured process that can extract, organize and analyze large amounts of data in a form being acceptable, useful and beneficial for an entity (e.g. individual human agent, organization or BI information system). It is basically a specific type of distributed computing across a number of server or nodes to speed up the analysis process. Generally, shallow analysis use the concept of means, standard deviation, variance, probability, proportions, pie charts, bar charts and tabs to analyze small data set. Deep analytics analyze large data sets based on the concepts of data visualization, descriptive and prescriptive statistics, predictive modeling, machine learning, multilevel modeling, data reduction, multivariate analysis, regression analysis, logistic regression analysis, text analysis and data wrangling. Deep analytics is often coupled with business intelligence applications which perform query based search on large data, analyze, extract information from data sets hosted on a complex and distributed architecture and convert that information into specialized data visualization outcome such as reports, charts and graphs.

Collaborative analytics is a set of analytic processes where the data analysts work jointly and cooperatively to achieve shared goals through data sharing as per revelation principle, privacy and information disclosure policy, collective analysis and coordinated decisions and actions. Collaborative analytics allows sharing of strategic information among various phases of data analysis such as demand planning of data, data sourcing, organizing data, exception management, data warehousing, execution of data analysis, reporting conclusions and determining actions. The data loop promotes data sharing to avoid redundancy. Communication and sharing improves reliability and consistency of data analysis across an organization. The analysis loop explores insights in terms of multi-dimensional analysis through a recursive process of developing and validating hypotheses for robust and complete conclusions. The action loop focuses on coordination of complete and connected set of actions across an organization through better understanding and in-depth analytical skills. Conventional analytics explore hidden intelligence of data to make rational decisions. Collaborative analytics is focused on increased coordination, cooperation and integration among various units to improve alignment of decisions and actions across entire business unit.

1.2.2 Information Security Intelligence (ISI) Analytics

ISI analytics is an emerging digital technology; its scope may be analyzed in terms of adaptive security, dynamic data protection, self-healing mechanism and crash proof codes. An enterprise information system may face various threats of malicious attacks from external and internal environments; it is essential to protect the system through ISI analytics. ISI analytics monitors enterprise information system in real-time to detect any anomalies and vulnerabilities. If a threat is detected, ISI analytics should be able to mitigate the risks through a set of measures. Let us consider the technology of crash proof codes which verify the reliability of an operating system through formal verification methods. The concept is applicable to the operating system designed for processors embedded in smart phones, vehicles, aircrafts, drones and medical devices where software bugs can be disastrous and unnecessarily risky programs may put lives in danger. Is it possible to mitigate the risks by making kernel i.e. the core component of an operating system in such a way that it will never crash? Section 4 outlines the concept of adaptive analytics and dynamic data protection. Chapter 6 highlights self-healing mechanism of a smart grid.

1.2.3 Applied AI, Deep learning & Robotics

AI simulates human intelligence and develops algorithms that learn and perform intelligent behavior with minimal human intervention, high precision, accuracy and speed. Robotics is an interdisciplinary branch of mechanical, electrical and electronics engineering and computer science. The basic objectives of Robotics are design, construction, operation and use of robots and related information system for control, sensory feedback, and information processing; human robot interface, mobility, manipulation, programming and sensors development. Various domains of artificial intelligence (AI) are being used in Robotics such as computer vision, NLP, Edge computing, deep, transfer and reinforcement machine learning. A robot is a programmed machine designed to execute one or more tasks automatically and repeatedly with speed and precision. There are as many different types of robots as there are tasks for them to perform. Engelberger and George Devol developed first industrial robot; there are different types of industrial robots such as cartesian, SCARA, cylindrical, delta, polar and vertically articulated. The main components of a robot are controller or brain run by a computer program; Robotic operating system; electrical parts such as motors, sensors for sensing and touch, power sources: solar power, pneumatics, flywheel, hydraulic; mechanical parts such as actuators, effectors, grippers, manipulators, air muscles, muscle wire, pistons, grippers, wheels, and gears that make the robot move, grab, turn and lift, locomotion : walking, hopping, dynamic balancing, flying, snaking, skating, climbing, swimming and sailing. Robotics is extensively used in automotive industry in various types of applications such as collaborative robots, painting, welding, assembly, material removal, parts transfer and machine tending. Medical robots are used for delicate surgical operation in healthcare. Robots can substitute for humans and replicate human actions in dangerous environments (e.g. bomb detection and deactivation, toxic manufacturing environment or where humans cannot survive such as space, under water, high heat, hazardous materials and radiation) and other various types of interesting application (e.g. Cobots, Nano robots, autonomous drones in defense and bio-inspired robots). The advantages of robotics include the execution of heavy duty jobs with precision, repeatability, reliability and consistency. Is it possible to develop robots with intelligent human skills such as innovation, creativity, decision making, flexibility and adaptability, speech and voice recognition, gestures, facial expression, artificial emotions, personality and social intelligence?

1.2.4 Miscellaneous

1.2.4.1 Solar Computing: Solar computing is an emerging technology which should be able to interact with the consumers of energy on various issues such as demand response schemes, current energy sources, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing is associated with various types of emerging applications such as internet of energy, smart homes and autonomous micro-grids to manage and

monitor the use, storage and production of electrical energy though a network of automated modules. It is essential to explore the scope of solar computing from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; threats of climate change; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms. The scope of solar computing spans over several factors such as demand and supply management, electrical and hybrid vehicles, virtual power plants, prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy. The ultimate objective is to match demand with supply. A smart grid may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers. The other important objectives of solar computing are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. Solar power is an interesting option for running computers in rural area and remote zone (e.g. forest, hills, desert, sea coast). Is it possible to explore a highly energy efficient, low cost (e.g. operation, transport and service), lightweight, rugged and reliable system that can run from direct current generated by solar panels and smart batteries in a hot and dusty hazardous environment?

1.2.4.2 Virtual and augmented reality : VR and AR are sophisticated, creative and powerful tools to offer digital experience by integrating AI, computer vision, graphics and automation in various applications such as manufacturing, retail, healthcare and entertainment. These reality technologies can effectively support direct-to-consumer e-commerce models through vertical integration bypassing tiers of supply chain at reduced costs and enhanced profit margin. Virtual reality technology provides immersive and interactive experiences to the human agents through computer graphics or visual elements and support V-Commerce business models through an alternate technology platform. Voice activated commerce (e.g. voice logistics) uses natural language processing, speech and voice recognition technologies for the interaction between the users and commercial platforms and applications.

.

1.2.4.3 Digital twins : How is it possible to represent the structure of a system associated with a technology innovation correctly and transparently? Digital twins may be an interesting solution; it integrates the concept of industrial IoT, AI, machine learning and software analytics to optimize the operation and maintenance of physical assets, systems and manufacturing processes. A digital twin is the digital replica of a living or non-living physical entity (e.g. physical asset, process, agent, place, system, device); it is expected to bridge and support data sharing between the physical and virtual entities. Digital twins can learn from multiple sources such as itself through sensors, historical time series data, experts and other nodes of the networking schema of the system and get updated continuously to represent real-time status, working conditions or positions.

The concept of digital twins are expected to be useful for manufacturing, energy (e.g. HVAC control systems), utilities, healthcare and automotive industries in terms of connectivity, digital traces and product life-cycle management. The concept can be used for 3D modeling to create digital companions of the physical objects i.e. an up-to-date and accurate copy of the properties and states of the objects (e.g. shape, position, gesture, status, motion) based on the data collected by the sensors attached to the system. It may be useful for the maintenance of power generation equipment such as turbines, jet engines and locomotives; monitoring, diagnostics and prognostics to optimize asset performance and utilization through root cause analysis and to overcome the challenges in system development, testing, verification and validation for automotive applications. The physical objects are virtualized and can be represented as digital twin models seamlessly and closely integrated in both physical and cyber spaces. Digital twins should represent the structure of a product innovation intelligently through various phases of the product life-cycle.

1.2.4.4 Ray Tracing : In computer graphics, ray tracing is a rendering technique to generate an image by tracing the path of light as pixels in an image plane and simulate the effects with virtual objects. The technique can create a very high degree of visual effects at high cost of computation. This concept is useful for film, TV and video games applications. Ray tracing can simulate various optical effects like reflection, refraction, scattering, and dispersion.

1.2.4.5 Quantum computing: Quantum computing is a promising technology to solve computation problems significantly faster as compared to classical computers. This technology is based on the concepts of quantum mechanical phenomena such as superposition and entanglement to process data efficiently. Quantum theory analyzes the nature of energy and matter on the atomic and subatomic level. Quantum computing is a branch of quantum information science (e.g. quantum cryptography, quantum communication). In a classical computer, the Boolean logic is represented through a set of bits where each bit is either 1 or 0. Quantum computers are not limited to two states and encode information as quantum bits. Qubits are the basic building blocks of quantum computing. Qubits can be in a 1 or 0 quantum state; can also be in a superposition of 1 and 0 states. When qubits are measured, the result is always either 0 or 1; the probabilities of the two outcomes depend on the quantum state of the qubits. Qubits represent atoms, ions, photons or electrons that work together to act as computer memory and a processor.

2. SYSTEM

The basic objectives of digital technology is intelligent decision making in complex and rapidly changing business environment, fast decision making in adaptive situation, improved accuracy in decision making, discovery of hidden intelligence from large pool of data, fast and correct transaction processing; support creation, storage, transfer and application of knowledge in an enterprise, support office automation and efficient management of resources (e.g. man, machine, materials, method and money) of an enterprise. An information system associated with digital technology can be classified into different categories such as transaction processing, decision support, group decision support, knowledge management, knowledge based, office automation and business intelligence system. It is possible to analyze digital technology in terms of computing (e.g. centralized, distributed, local, global), data, networking (e.g. wired, wireless, Internet), application (e.g. features, modules, functions, application integration) and security schema.

dSaaS / DaaS : The basic objective of DaaS is to avoid the complexity and cost of running a database with improved availability, performance, price and flexibility. It gives the access to various types business intelligence solutions (through web) which include distributed database, data warehousing, data mining, business and web analytics, data visualization and business performance measurement applications. The pricing of dSaaS is based on the cost of hardware (e.g. data warehouse, servers), the cost of software (e.g. business intelligence solutions) and system administration cost (e.g. data centre administration, data base security, backup, recovery and maintenance). A consumer can lease a data storage space where it is required to measure different system parameters such as stored data (GB/month) and number of processed queries (per 10k requests / month) to compute the price of dSaaS / DaaS. The provider can offer quantity discount in case of group buying of storage space. The prices of DaaS / dSaaS are also determined by various QoS parameters such as connection speed, data store delete time, data store read time, deployment latency (i.e. the amount of latency between when an application is posted and ready to use) and lag time (how slow the system is). The pricing of dSaaS is also governed by the security and privacy of data. Some applications (e.g. education sector) require low level of privacy of data. Some applications (e.g. financial service, healthcare etc.) need high level of security and privacy in data outsourcing and this involves high cost of computation and communication from the perspectives of statistical disclosure control, private data analysis, privacy preserving data mining, intelligent access control and query processing on encrypted data. The service provider should define a discriminatory pricing mechanism for dSaaS: high level of security and privacy of data demands high price and low level of security asks low price.

The price of dSaaS is a function of miscellaneous cost elements of a data center. A *data centre* or data bank is the collection of servers where the applications and data are stored. Data center consists of a set of servers and network architecture. The servers store the data from different organizations and network architecture facilitates the services to use, store, and update the data of the servers. The cost of administration of data centre includes several factors: initial development cost, operating cost, maintenance cost and cost associated with disaster recovery plan. The development cost includes the cost that requires making master plan, building infrastructure, buying hardware and software, making database and security schema. Operating cost includes the cost of energy, cooling system, system administrators, software license and network cost. Maintenance cost is the cost of maintaining the system which includes upgradation of hardware and software. One of the most challenging issues of data center management is the resource allocation strategy: how it is possible to cater the demand of the service consumers using minimum number

of servers. It has an impact on the size, complexity and cost of data center. The data centre administrator can follow dedicated or shared server allocation strategy.

The price of dSaaS is also a function of energy consumption of cloud computing system in a data center. There are many open challenges of energy efficient design of computing systems and green IT covering the hardware, operating system, virtualization and data center levels. The basic objective of the cloud computing system design has been shifted to power and energy efficiency to improve the profit of the service provider. Energy consumption is not only determined by hardware efficiency, but it is also dependent on the resource management system deployed on the infrastructure and the efficiency of applications running in the system. Solar power electronics is an interesting option of green IT. Higher power consumption results not only high energy cost but also increases the cost of cooling system and power delivery infrastructure including UPS and power distribution units / panels. The consolidation of IT infrastructure should be done intelligently to reduce both energy consumption and performance degradation through improved power management. Energy consumption can be reduced by increasing the resource utilization and use of energy efficient cloud computing system.

Software-as-a-Service (SaaS): SaaS is an application hosted on a remote server and accessed through web; it can be business service or customer oriented service. The basic objective is to reduce software licensing cost and improve productivity by using sophisticated applications. The pricing strategy of SaaS is based on pay-as-you-go basis; not dependent on number of licensing period and licensing users as in case of direct software procurement. Another concept is *software plus service* where an enterprise uses a locally hosted software application and additionally uses SaaS through cloud for a specific type of application. Using the existing software paradigm, the consumer purchases a software package and license by paying a one-time fee. The software then becomes the property of the consumer. Support and updates are provided by the vendor under the terms of the license agreement. This can be costly if the user is installing a new application on hundreds or thousands of computers. SaaS, on the other hand, has no licensing. Rather than buying the application, the consumer pay for it through the use of a subscription based on number of concurrent users and only pay for what is used.

The computation of subscription fee can be *stochastic* pricing or simple *cost* based pricing. The price of SaaS depends on the specific business model of the service provider. Suppose, a service provider develops in-house software products. Another service provider buys COTS from third-party vendor based on number of licensed users and licensing period and provides SaaS to the consumers. There may be restriction of number of concurrent users and different subscription rate of SaaS in second case.

This pricing strategy should also consider cost of upgrading software application; the provider may offer incentive for upgrading applications. In case of security software pricing, there may be different alternative strategies to manage network security: (i) consumer self-patching where no external incentives are provided for patching or purchasing, (ii) mandatory patching, (ii) patching rebate and (iv) usage tax. For proprietary software, when the software security risk and the patching costs are high, a patching rebate dominates the other strategies. When the patching cost or the security risk is low, self-patching is the best option.

Stochastic risk based pricing mechanism considers several risk factors and optimizes the expected net present value of revenue subject to maximum acceptable risk of the provider. In this case, the service provider does not give much focus on cost accounting model or profit margin but tests the price sensitivity of the customers experimentally or through trial and error method. The provider does not have any precise perception about the demand of the new software products. But, it follows dynamic risk based pricing based on assessed risks and competitive intelligence. For in-house software development, software cost is a function of efforts on feasibility study, requirement analysis, system design, program design, coding, testing and modification following waterfall / v-process / spiral / proto-typing / incremental delivery model. The service provider estimates effort for a specific SDLC model and then selects an optimal profit margin.

Infrastructure-as-a-Service (IaaS): A cloud computing infrastructure consists of different types of elements: clients (e.g. mobile, PDA, laptop, thin and thick), the data center and distributed servers. *Thin clients* are less costly than thick clients. A growing trend in the cloud computing is *virtualization* of servers. In a virtualized environment, applications run on a server and are displayed on the client. The server can be local or on the other side of the cloud. Software can be installed allowing multiple instances of virtual servers which run on a physical server. Full *virtualization* is a technique in which a complete installation of one machine is run on another. It allows the running of different and unique operating systems. *Hardware-as-a-Service (HaaS)* simply offers the hardware required by a consumer. Cloud computing is a business model of delivering IT resources and applications as services accessible remotely over the Internet rather than locally. IaaS supports remote access of computer infrastructure as a service.

Cloud computing supports elastically scaling computation to match time varying demand. But, the uncertainty of variable loads necessitate the use of margins i.e. the servers that must be kept active to absorb unpredictable potential load surges which can be a significant fraction of overall cost. [23] addresses the challenges of minimizing margin costs and true costs for IaaS. The provider should not adopt a fixed margin strategy; the margin should be load dependent. The margin required at low loads may be higher than the margin required at high loads. Secondly, the tolerance i.e. the fraction of time when the response time target may be violated need not be uniform across all load levels. It is really challenging to achieve optimal margin cost while guarantying desired response time for IaaS.

The pricing strategy of IaaS is based on the cost of servers, storage space, network equipment and system software like operating systems and database systems. The price of IaaS is basically a subscription fee for a specific timeline. Now the question is how to compute this subscription fee. The rate should be fixed based on the cost of hardware and software, target revenue and profit margin. The service provider may adopt a profit maximizing pricing strategy or revenue maximizing pricing strategy within reasonable, stable target profit margin. The profit margin is a dynamic variable; it should be set intelligently according to competitive intelligence and quality of service. The quality of service is measured in terms of computing time. For small firm or individual service consumer, the provider can set a fixed price per unit time; there may be SLA but there is no scope of negotiation of price. Large PSU can negotiate with the service provider to set a rational price for fixed timeline.

Incentive compatibility plays a significant role in IaaS pricing, it is important to analyze the significance of incentives for network infrastructure investment under different pricing strategies: *congestion based negative externality pricing* and the flat *rate pricing* [33]. A lack of proper infrastructure investment incentive may lead to an environment where network growth may not keep pace with the service requirements. It is really complex to compute maximum capacity that IaaS provider will be willing to invest under different pricing schemes. Optimal capacity of IaaS is determined by different factors: per unit cost of capacity of network resources, average value of the user's requests, average value of the user's tolerance for delay and the level of exogeneous demand for the services on the network. It is hard to determine whether time based pricing is more profitable than flat rate pricing. IaaS consumers always try to identify whether average stream of the net benefits realized under congestion based pricing is higher than the average net benefits under flat rate pricing. IaaS provider may adopt different types of pricing strategies at different points of time but the service consumers may control their demand of IaaS service adaptively to avoid the increase in cost.

Platform-as-a-Service (PaaS) : PaaS supplies all the resources required to build applications and services completely from the web without any download or installation of any software in the clients. The price of PaaS can be negotiated for a specific project. There can be different types of project environments such as application-delivery-only-environment (e.g. security and on demand scalability), standalone environment and add-on-developmental-environment (e.g. subscriptions of add-on SaaS application are bought). The price of system software can be charged as a subscription fee based on number of concurrent users and usage period. The pricing of PaaS is also governed by the complexity of platform services which may include application design, development, testing, deployment, hosting, geographically dispersed team collaboration, web service integration, database integration, security, scalability, storage, state management and versioning. The developers, project managers, and testers can access the development and testing softwares of the service provider through web; but, lack of interoperability and portability may be a critical issue in PaaS. The price of PaaS is determined by the complexity of interoperability between the systems of the service provider and service consumer.

Virtual and Augmented Reality : There are three types of reality technologies : virtual reality (VR), mixed reality (MR) and augmented reality (AR). These reality technologies are sophisticated, creative and powerful tools to offer a complete computerized digital experience through artificial intelligence, computer vision, computer graphics and automation. A virtual entity may not exist physically but created by software in a digital environment. Augmented reality an enhanced version of the real-world by overlaying our existing reality with an additional layer of digital information, which can be viewed through smartphones or smart glasses (ARSGs). Mixed reality facilitates the merger of, and real-time interaction with and between, digitally rendered and real-world data and objects through MR headset. Virtual reality is characterized by generating real-time, immersive and interactive multi-sensory experiences situated in, and artificially induced by, a responsive three-dimensional computer-generated virtual environment - usually paired with advanced input and output devices.

3. STRUCTURE

IIoT: IoT is the network of physical objects embedded with sensors, software and network connectivity that enables the objects to monitor, collect, exchange and analyze data. Industrial Internet of Things (IIoT) is a set of hardware and software components (e.g. smart sensors and actuators) enabled by IoT to support manufacturing and industrial processes. IIoT leverages the power of smart machines and real-time analytics across several industries such as manufacturing (Industry 4.0), logistics, oil, gas, transportation, energy, utilities, mining, metals and aviation. The benefits of IIoT may include better connectivity, scalability, cost savings, improved productivity and better analytics for predictive maintenance.

Pervasive & wearable computing : One of the most promising emerging digital technology is health monitoring smart wearable systems (SWS) through advances of microelectromechanical systems, electrical simulation, mechatronics, sensors, actuators, biomedical instrumentation and nanotechnology. SWS is an interesting cost-effective solution which can monitor a patient's health status in real-time and support complex healthcare applications for disease prevention, symptom detection and medical diagnosis. Let us consider the structure of smart wearable system (SWS). The system may have various types of digital and mechatronics components such as sensors, actuators, power supplies, wireless communication units, processing units, algorithms, software, user interfaces and smart fabrics to capture and process data and make intelligent decisions based on the measurement of various parameters of human body such as temperature, blood pressure, heart rate, respiration rate, blood oxygen saturation and ECG. The measured data are sent to a central node (e.g. PDA, medical centre) through wireless communication system. SWS is expected to monitor the state of the health of human agents (e.g. patients, athletes, issue alerts and send feedback to the medical staff in real-time. The healthcare experts and consultants can take rational decisions on patientcare accordingly. There are various issues and challenges in telecare, telehealth and telemedicine through new models, prototypes, test beds and industrial products to enhance the performance of healthcare system and minimize the risk of illness, injury, inconvenience and rehabilitation. But, there are various constraints such as high cost, size, weight, energy consumption, complexity of sensor implementation and connectivity, ethics, laws, information security and privacy, freedom, autonomy, reliability, consistency, safety and service issues.

Edge computing needs the support of a distributed and open IT architecture having decentralized processing power, mobile computing and IoT technologies. Data is processed by the device itself or by a local computer or server, rather than being transmitted to a data center. Edge structure consists of servers, applications, content distribution network and small clouds at the edge. An edge gateway is a virtual router in either a compact or a full configuration. Edge devices are used by enterprises and service providers through cloud computing and IoT technologies for more intelligence, computing power and advanced services at the network edge. Edge structure uses cloud infrastructure but keeps assets at the edge of the network. A version of the client's apps may run locally to allow ready use without latency, with another versions residing in the regional and central data centers for data warehousing and mining.

4. SECURITY

ISI Analytics, adaptive security and dynamic data protection: An information system (IS) may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. Emerging digital technologies demand the support of adaptive security architecture so that the associated information systems can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of an emerging digital technology that monitors IS in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, IS should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of an information system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks.

The basic objective of emerging adaptive security architecture and dynamic data protection mechanism is to assess and mitigate the risks of enterprise information system rationally and intelligently. What constitutes an effective strategy of IS security schema? It is debatable whether the proactive approach to IS security is superior to reactive approach. It is possible to recommend an interesting strategy: reactive security may be competitive with proactive security as long as the reactive approach learns from past attacks instead of overreacting to the last attack on the information system. It is not a trivial problem and needs the support of an efficient security protocol from intelligent threat analytics and adaptive security architecture. The following section presents the construction of an adaptive security algorithm to ensure the security of an information system based on proactive and reactive approaches. The basic building blocks of the algorithm are intelligent threat analytics, cryptographic solutions and dynamic data protection. It is basically an attempt of the cross fertilization of algorithmic game theory and cryptography.

Adaptive Security Algorithm [ASA]

Agents: Defender (e.g. system administrator), Attacker (e.g. malicious agent or adversary);
System : Enterprise information system;
Objectives: optimize enterprise IS security investment;
Constraints: budget, resources, time;
Input: Enterprise information system performance parameters and architecture;
Strategic moves:

- Adaptive security
- Dynamic data protection
- Self healing mechanism
- Crash proof code
- Adoption of hybrid strategy i.e. an optimal mix of proactive and reactive approaches.

Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defender does not disclose the proactive and reactive approach of information security to the adversaries.
- **Attacker :** The adversaries preserve the privacy of the plan of malicious attack, information of targets and weak links.

Security intelligence verification:

- **Proactive approach**:
  - **Threat modeling**
    - Call threat analytics function (f_a);
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate security requirements in terms of demand plan (P_d);
    - Develop risk mitigation plan (P_m) : accept / transfer / remove / mitigate risks.
  - **Identify targets** : computing, data, networking and application schema;
  - Verify **security intelligence** of information system in real-time.
    - **Data schema** :
      - **Dynamic data protection** :
        - check data integrity;
        - assess the risks of false data injection and shilling attacks by the intruders;
        - verify access control efficiency in terms of authentication, authorization, correct identification, privacy, audit, confidentiality and nonrepudiation;
    - **Computing schema**: verify fairness, correctness, accountability, transparency, rationality, trust and commitment in multi-party computation;
    - **Networking schema :**

- Verify system performance in terms of reliability, consistency, stability, liveness, deadlock-freeness, reachability, safety, resiliency;
- assess the risks of intrusion, denial of service (DoS), coremelt, Sybil, node replication and wormhole attacks;

♦ **Application schema**

- do penetration testing;
- audit user acceptance, system performance and quality of application integration.

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the information system; analyze performance, sensitivity, trends, exception and alerts.
    - what is **corrupted** or compromised?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
- Adjust P_d and P_m.

Payment function:

- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements.
- Trade-off proactive vs. reactive security: assign weights to each risk profile.
- Do portfolio rationalization of the security schema.
- Select dominant strategy of IS investment from the options of process re-engineering, transformational, renewal, experiment and reinforcement on the weakest link.

Output: Optimal security investment plan

4.1 Analysis of Adaptive Security Algorithm (ASA)

Recently, there is a trend of cross fertilization between two disciplines: game theory and cryptography. Cryptography focuses on secure multi-party computation preserving privacy, fairness and correctness against the threats of malicious agents. Game theory tries to understand the behavior of rational agents with well defined goals in a given situation and designs the rules of interaction. There are differences between the two disciplines based on specific issues such as players, solution drives, incentives, privacy, trust, early stopping, deviation and collusion. Cryptography assumes honest or malicious players; game theory assumes rational players; the solution drivers are secure protocol and equilibrium respectively. Both disciplines study collaborative interactions among the agents with conflicting interests. It is possible to solve traditional game theoretic problems and design of efficient mechanisms using the concept of cryptographic solutions and secure multi-party computation. It is also an interesting research agenda to explore new cryptographic concerns using game theoretic concepts such as secure and fair computation and rational secret sharing. Traditionally, cryptographic solutions are focused on the privacy, fairness and correctness to ensure information security. The domain needs a broad outlook for improved efficiency in new applications.

ASA is associated with the problem of information security investment decisions based on the concept of computer science, economics, management science and related disciplines. It is a complex decision making problem. The existing woks attempt to derive and compare optimal investment strategy exploring the delicate balance between proactive and reactive approaches. The current work is an attempt to extend the existing research. It presents the construction of a deep learning based algorithmic mechanism to ensure the security of an information system based on proactive and reactive approaches. The basic building blocks of the mechanism are threat analytics, cryptographic solutions and adaptive secure multiparty computation.

ASA is associated with a security game. Game theory is concerned with a complex decision making process in which two or more players interact. Each of these players tries to optimize its own objective function. A game can be classified as cooperative game or a non-cooperative game. In a cooperative game,

the players make agreements in order to minimize their common cost or to maximize their common payments. This is not possible in a non-cooperative game. A cooperative game is a game where a group of players enforce a cooperative behavior. The game is defined by (N,u) where N denotes a group of agents and u is a real valued characteristic function. The ASA is defined by various types of elements: a group of agents or players, model, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payments, a strategy profile, a dominant strategy which maximizes the utility of an agent for all possible strategies of other agents involved in the mechanism, security intelligence and revelation principle. There are two agents in the security game: a defender (D) and the attacker (A). Each agent adopts and executes a or a set of strategies. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy. The best strategy may depend on the knowledge of the defender about prospective attacks and the sunk costs incurred when upgrading information security schema reactively. The payment function of the mechanism estimates an optimal investment plan for the security of information system. One of the most critical issues of ASA is revelation principle and verification of security intelligence of the information system schema. The agents preserve the privacy of strategic data. The defender does not disclose the proactive and reactive approach of information security to the adversaries. The adversaries preserve the privacy of the plan of malicious attack. The basic building block of ASA is adaptive security and DDP.

Let us explain the objectives of adaptive security architecture in depth. New threats are getting originated as an outcome of digital technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The systems demand continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

For example, prevention and detection are traditional approaches to the security of an information system. In today's world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt cloud based solutions and open application programming interfaces also. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture.

Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema: real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging digital technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

Adaptability is about responding to change effectively and decisively through reactive approach: the ability to identify the change in search space for the adversaries, understanding the probable impacts of the hit by the adversaries, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The defender tries to define the requirements of the security schema of an information system in terms of aspiration point, reservation point and adjustment of various preferential thresholds (e.g. indifference, strong preference, weak preference, veto) and preferred solutions. The value of the objective function which is desirable or satisfactory to the decision maker or defender is defined as aspiration point. The value of the objective function that the defender wants to avoid is reservation point. The defender can use various preference thresholds in order to compare alternatives and to define outranking relations. There

is an interval of preference wherein it is not possible for the defender to distinguish between different alternatives and this is defined as indifference threshold. Strict preference threshold is defined as minimal increase or decrease of any objective that makes the new alternative strictly preferred with respect to this objective. There exists an intermediate region between indifference and strict preference threshold where the defender may hesitate to compare alternatives. It is defined as weak preference threshold. Veto threshold indicates what is the minimal increase or decrease of any objective that makes the new alternative unacceptable regardless of the value of other objectives.

The adaptive security algorithm evaluates the security intelligence of an information system based on proactive and reactive approaches. Real-time security management involves high cost of computation and communication. The vulnerability of the system to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The defender must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in the operation of the system? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map has four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences. The system may face a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in the vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.

The computational cost of adaptive security algorithm depends on the complexity of threat analytics function (f_a) and payment function (f_p) in terms of investment allocation heuristics.

The cost of computation is a function of the complexity of threat analytics. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? assess probability of occurrence (p) and impact or sunk cost (c). The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen? The threat analytics also evaluates the vulnerability of the information system to a disruptive event in terms of likelihood of a disruption and its potential severity. The computational burden is also associated with the identification of a set of feasible risk metrics for each type of threat on the information system, assessment of the probability of each risk metric, computation of severity or sunk cost of each risk metric and plotting each risk metric in the vulnerability map.

Another major computational burden of ASA is the complexity of verification or model checking algorithms. The verification system requires both automated and semi-automated verification options. The verification system calls threat analytics and a set of model checking algorithms for various phases: exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

The cost of computation also depends on the complexity of payment function. The payment function estimates aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements; makes trade-off proactive vs. reactive security: assign weights to each threat; exercises portfolio rationalization of the security schema and allocates fund based on the selection of invest options. There are various objectives of investment of information security schema such as process re-engineering,

transformational, renewal, experiment and reinforcement on the weakest link. The payment function selects appropriate heuristics of fund allocation such as selective based on ranks, linear and proportional allocation. When the budget of the defender is more than the total projected demand, the agent would like to satisfy all the portfolios of IS security schema using the resource allocation function. However, when the budget is less than total demand, the agent should find the investment plan based on various types of allocation heuristics, objectives and constraints [18].

Linear allocation is an equal sharing of the pain or shortage of capacity among various components of IS security schema. The threat T_i is allocated fund $q_i = d_i - (1/n) \max (0, \sum_{i=1}^{n} d^*_i - C)$ where n is the number of threats and C is the budget capacity of the defender. In case of *proportional allocation*, the threat T_i is allocated fund $q_i = \min \{d^*_i, C.d^*_i/(\sum_{i=1}^{n} d^*_i)\}$. Reactive approach may consider reinforcement learning strategy and allocates more budget to easier-to-defend edges of the attack graph. When new edges are revealed, the budget is reallocated uniformly from the already revealed edges to the newly revealed edges. Myopic bug chasing is most likely an ineffective reactive approach. But, the strategy of gradually reinforcing attacked edges by shifting budget from unattacked edges of the attack graph may be cost effective. Another fund allocation strategy is *selective allocation* based on the computation of the rank of the threats which is computed based on probability of occurrence (*p*) and impact or sunk cost (c).

The security intelligence of ASA is associated with the computing, data, application and networking schema of an information system and is verified through the properties of adaptive secure multi-party computation.

ASA evaluates the security of an enterprise information system in breadth and depth from the perspective of collective intelligence. The targets of the defender are computing, data, networking and application schema of an information system. It is basically a holistic approach which is focused on both proactive and reactive security. *Let us first consider proactive approach*. The verification algorithms check fairness, correctness, accountability, transparency, rationality, trust and commitment of the computing schema. It is essential to verify authentication, authorization, correct identification, privacy and audit of data schema. The health of networking schema is verified in terms of safety, reliability, consistency, liveness, deadlock-freeness, reachability and resiliency. The security of application schema is evaluated through penetration testing in terms of user acceptance, system performance and quality of application integration. In case of machine learning with adversarial setting, the ASA also audits the security of data schema and monitors the risk of false data injection attack, noise, missing data and incomplete features and assesses the risk of Sybil attack. The security of application schema is verified in terms of flaws in training and testing strategy (no. of training and testing samples, learning rate), the efficiency of data mining algorithms and knowledge extraction procedure through penetration testing. Penetration testing searches for potential vulnerabilities and it can be modeled to reduce uncertainty in a security game. It is an information gathering option prior to investing into protection against a threat.

Next let us consider *reactive approach* which adopts sense-and-respond strategy. The basic objective of adaptive secure multi-party computation is to identify the hit of adversaries on computing schema that may choose the corrupted parties during the course of computation. The verification algorithms check the scope of information leakage or violation of privacy in various steps of secure multi-party computation algorithm : adding random noise to data, splitting a message into multiple parts randomly and sending each part to a decision making agent through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. *Adaptability* is basically responding to change(s) effectively and decisively: the ability to identify the occurrence of uncommon threats which are not considered in proactive approach; change in system performance, understanding the probable cost of malicious attacks, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time. The defender adjusts the requirements of the security schema of an information system adaptively in terms of aspiration and reservation point and various preferential thresholds. Adaptive secure multi-party

computation identifies what is corrupted or compromised; what has occurred or what is occurring; performs cause-effect analysis for more transparency and insights; decides what the next best action is and also predicts what is the best or worst that can happen.

5. STRATEGY

The technological innovation on digital technology is associated with a set of intelligent strategic moves such as scope analysis, requirements engineering, system design, talent management, team management and coordination, resources planning, concept development, concept evaluation, system architecture design, system development plan, roll out, process design, prototyping and testing. Efficient change management ensures that an organization and its workforce are ready, willing and able to embrace the new processes and information systems. The change management is a complex process. The change should occur at various levels such as system, process, people and organization. Communication is the oil that ensures that everything works properly. It is essential to communicate the scope of digital technology to the policy makers, state and central governments, corporate executives, academic and research community.
Strategy can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that the technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. The emerging digital technologies are now passing through the growth phase of S-curve [figure 5.2]. Initially, it may be difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the customer, supply and design chain in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory of digital technology

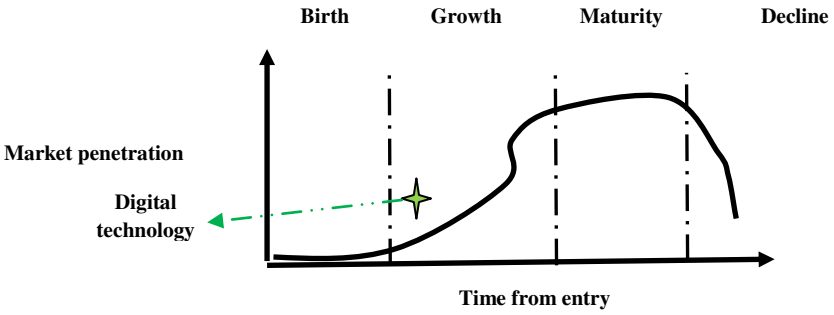


Figure 5.2 : Technology life–cycle analysis

6. STAFF-RESOURCES

Emerging digital technologies demand efficient staff-resources which should be analyzed in terms of sources of innovation and roles of academic institutes, computer science and information technology engineers, government and collaborative networks and optimal utilization of critical resources. The innovation demands the commitment of creative experts in IT and computer science who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab and academic institutions of state and central government. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision in various domains such as requirements engineering, system design, coding, and testing and

performance optimization. The critical resources are intelligent hardware, software, security and networking solutions.
Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment. Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers or clients or private nonprofit organizations may innovate new products or services based on their own needs. Many firms set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities define sound research mission and vision and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators). A complex technological innovation often needs collaborative intelligence to manage the gap between demand and supply of a specific set of capabilities, skills and resources. It is possible to control cost, speed and competencies of technological innovations through efficient sharing mechanisms. It is rational to share the cost and risks of new innovations through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem.

7. SKILL-STYLE-SUPPORT

The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (Computer science, Information technology, MIS), research and development, knowledge management, system design and project management. It is essential to teach the aforesaid technologies in various programmes of computer science, BCA, MCA, Electrical and Electronics engineering, information and communication technology as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented. The emerging digital technologies also demand efficient leadership style in terms of optimal resource allocation and utilization, collaboration, coordination and communication.
Next, let us focus on support. The aforesaid digital technologies should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated HR workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for the diffusion of the new technology. New skill should be developed in digital, information and communication technologies. The business model requires the support of a good human resource management system for talent acquisition, talent retention, skill development, training, career growth planning, incentive, reward, recognition and payment function. The workforce should develop different types of skills such as research and development, system design, project management, testing, commissioning and system maintenance. The system administrators must have leadership skill in terms of smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes**.**
What should be the innovation model for emerging digital technology? Is it possible to adopt K-A-B-C-D-E-T-F model? Knowledge managers should arrange various types of events such as workshops, seminars and conferences so that the innovators can acquire the basic and fundamental concept. The activators should initiate the innovation process by identifying a set of good research problems through scope analysis. Random selection of research problem should be avoided by evaluating the strength, experience and skill of the innovators. The research problem should have potential business intelligence and social benefits. The browsers should search for information; investigate throughout the process and find relevant data or information to start innovation. The creators should analyze the gap and think of to-be system; generate new ideas, concepts and possibilities and search for new solutions. The developers should

transform the ideas of the creation phase into good solutions; turn the ideas into deliverables, products and services. They should collaborate with different research forums, industries and experts during this phase. The executors should implement and execute the roadmap of the innovation. The testers should do various types of experiments and laboratory works; verify system dynamics and monitor the performance of the deliverables. Advanced research laboratories are required for complicated testing and experiments. The facilitators should define project plan, corporate governance policy, marketing plan, production plan, investment plan and cost-benefit analysis. They should be able to identify the revenue and profit making stream and fair, rational business intelligence. The government should provide financial assistance to the innovators in patent registration.

8. CONCLUSION

Some people may argue whether the aforesaid digital technologies are really technologies for humanity. However, these technologies support path breaking technologies for humanity directly and indirectly. ASA shows the importance of an efficient algorithmic mechanism for proper evaluation of the security schema of an information system. It is basically a hybrid approach which recognizes the role of both proactive and reactive approaches in making decisions on investment of IS security schema rationally. The reactive approach may outperform proactive one against the threats that never occur actually. Sometimes, reactive approach may be cost effective as compared to proactive approach. The basic building blocks of the ASA are threat analytics, cryptographic solutions and adaptive security architecture. The threat analytics monitor the system performance based on time series data, detects and analyzes different types of vulnerabilities on enterprise information system. This work finds a set of interesting research agenda for future work: (a) explore new cryptographic concerns using game theoretic concepts and intelligent reasoning; (b) how to design an intelligent threat analytics; (c) how to design automated verification algorithms; (d) how to rationalize adaptive secure multi-party computation protocols and (e) how to quantify and code miscellaneous security intelligence parameters?

References

[1] Armburst, M. et al. (2010). A view of cloud computing, Communications of the ACM, 53(4), 50-58.
[2] Buyya, R., Yeo, C.S., Venugopal, S., Broberg,J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. Future generation computer systems.
[3] Chakraborty, S. (2007). A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Fellow programme dissertation, Indian Institute of Management Calcutta.
[4] Forouzan, B.A. (2007). Cryptography & network security. McGraw Hill.
[5] Furht,B. and Escalante, A. (2010). Handbook of Cloud Computing. Springer.
[6] Goldreich, O. (2004). Foundations of Cryptography, Basic Applications. Volume 2. Cambridge University Press.
[7] Reports of Gartner and Forrester; 2017,2018,2019.
[8] Beloglazov, A., Buyya, R., Lee, Y.C and Zomaya, A. (2011). A taxonomy and survey of energy efficient data centers and cloud computing systems. Advances in computers, volume 82.

Exercise

1. **Explore the scope of digital technologies for the future. Justify the same as technologies for humanity.**
2. **Identify dominant design schema of various emerging digital technologies.**
3. **What are the basic elements of the system architecture associated with digital technologies?**
4. **What do you mean by digital technology security? How to verify the security intelligence? Design adaptive security algorithms and dynamic data protection mechanisms.**
5. **What are the strategic moves of innovation, adoption and diffusion of digital technologies? What is the outcome of technology life-cycle analysis?**
6. **How can you manage resources for digital technology innovation projects?**

7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by digital technology innovation?**
8. **How can You manage digital technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**

CHAPTER 6 : SOLAR COMPUTING - SELF-HEALING MECHANISM for a SMART GRID

Abstract : Solar computing is an emerging technology which should be able to interact with the service consumers on various issues such as solar and grid energy sources, demand response schemes, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing is associated with various types of emerging applications such as internet of energy, smart homes and autonomous microgrids to manage and monitor the use, storage and production of electrical energy though a network of automated modules. It is essential to explore the scope of solar computing from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; threats of climate change; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms. The scope of solar computing spans over several factors such as demand and supply management, electrical and hybrid vehicles, virtual power plants, prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy. The ultimate objective is to match demand with supply. A smart grid may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers. The other important objectives of solar computing are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. Solar power is an interesting option for running computers in rural area and remote zone (e.g. forest, hills, desert, sea coast) and maximum power point tracking (MPPT) is a critical function of solar computing. Is it possible to explore a highly energy efficient, low cost (e.g. operation, transport and service), lightweight, rugged and reliable system that can run from direct current generated by solar panels and smart batteries in a hot and dusty hazardous environment?
This chapter shows the application of deep analytics [7-S], SWOT analysis and technology life-cycle analysis on the technological innovation of a self-healing smart power grid from the perspective of solar computing. We have done the scope analysis of the technological innovation on a smart power grid in terms of self-healing mechanism, solar computing, demand supply management, virtual power plants, electrical and hybrid vehicles and energy prosumers. This work also shows the analysis on adaptive security and dynamic data protection, strategy, staff-resources and skill-style-support for the innovation, adoption and diffusion of solar computing. It is essential to verify the security intelligence of the power grid at multiple levels and assess the risks of various types of threats from the perspectives of over current, earth fault, short-circuit, voltage, reactive power and distance protection. Finally, this work outlines a self-healing mechanism [SHM] based on case study and review of relevant works on security of smart grid.
Keywords : Solar computing, Smart power grid, Self-healing mechanism, Adaptive security, Dynamic data protection,, Maximum power point tracking, AI, Threat analytics, Digital relay protection

1. INTRODUCTION

What is a smart grid in the context of solar computing? What is the problem of technology innovation of solar computing and a smart power grid? A smart grid is a fully automated power delivery network that monitors and controls a set of nodes, supports a bidirectional flow of electricity and information between the power plants, loads and all intermittent points. Today's smart grid needs the support of distributed intelligence, broadband communication and automated control system for real -time market transactions and seamless interfaces among people, building, industrial plants, power generation, transmission and distribution networks. There are various types of challenges, complexities, constraints, security and privacy issues in power system engineering, telecommunication, cyber security, distributed intelligence, automation and information exchange among various system components of a smart grid. This chapter explores the technological innovation of a smart grid. Sections 2-8 present the analysis on scope, system, structure,

security, strategy, staff-resources and skill-style-support on smart grid technology. Section 9 analyzes a case on self-healing mechanism [SHM] for smart grid. Section 10 concludes the work.

2.SCOPE

It is essential to explore the scope of a smart power grid from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; strength, weakness, opportunities, threats of climate change, natural disasters and acts of terrorism; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms (e.g. dynamic pricing, swing option, trading agent competition); emerging applications such as electrical and hybrid vehicles; supply chain planning, collaboration, execution and resource management; various scopes of energy informatics and green information system; computing methodologies (e.g. AI, machine learning), data, networking and security schema, application integration and intelligent analytics [33-43].
Typically, the scope of a smart grid spans over several factors such as demand and supply management, electrical vehicles, virtual power plants (VPP), prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy [1-15]. The ultimate objective is to match demand with supply. A VPP may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers (both consume and produce power). The other important objectives are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. It is essential to develop a set of coordination mechanisms for a decentralized, autonomous and intelligent smart power grid.
Let us explore the scope of Artificial intelligence (AI) for a smart power grid. AI is basically the simulation of human intelligence. It represents and executes a processes through machines. The objective of AI is how to make computers do things at which, at the moment, the people are better. A smart grid system is expected to be an intelligent knowledge based system having a set of features from the perspectives of AI: ability of learning and understanding from experience, rational reasoning, making sense out of fuzzy data or approximate reasoning, adaptive system performance i.e. sense and respond, analytical, logical and case base reasoning in solving problems and ability in dealing with complex situations. Is it possible to develop a smart grid that can mimic human intelligence? Another critical issue is heuristics search; heuristics are intuitive knowledge or rules of thumbs learnt from experience; it can reduce the complexity of problem solving. It is not required to rethink completely to solve a problem of a smart grid if it occurs repeatedly.

3.SYSTEM

Let us first do the system analysis on a smart grid in terms of self-healing network. The basic building blocks of a self healing network are computationally efficient state estimation algorithms that can predict voltage and phase at different nodes of a smart grid in real-time given the current and predicted energy demand and supply of the prosumers. Distributed coordination is important for automated voltage regulators, voltage control and balancing demand and supply during recovery of faults. It is really challenging to develop automated and distributed active network management strategies given the uncertainty of demand and supply at different levels in the smart grid, fault correction mechanisms, self healing strategies, cause-effect analysis on various types of faults (e.g. overload, over current, earth fault, short circuit, over voltage, under voltage, over frequency, under frequency, automatic voltage regulation). An active network configures the topology automatically, sends control signals to individual customers to adjust generation and also load control, automatically correct faults and self-heals the smart grid.
A self healing mechanism should maintain the stability of a distribution network, perform accurate and timely monitoring and control of the prosumers; big data analysis for multiple actors and sensors, micro-level measurement and predict the future state of smart grid. It can adopt a set of active network management techniques based on distributed intelligence in the self healing network for fast recovery from faults. In case of voltage drift, automatic action is necessary on the transformer to reestablish correct voltage levels. It is essential to balance the mismatch between supply and demand to avoid blackout

situation. Essential need of a self healing mechanism is that various components of a smart grid should be able to communicate for voltage regulation and control of generation capacity and load demand.
Artificial intelligence can be applied to a smart grid in various ways such as knowledge based expert system for knowledge acquisition, inference engine, knowledge base, applications, fault diagnosis; real time alarm handling and fault analysis (AHFA); voltage control such as voltage collapse monitor (VCM), reactive power management (RPM), combined active and reactive dispatch (CARD), power system protection for protective relay setting, phase selection, static security assessment, condition monitoring, scheduling and maintenance of electrical transmission networks and intelligent system for demand forecasting. It is interesting to apply various types of soft computing tools for smart grid system performance analysis. Adaptive fuzzy system is used for fuzzy reasoning, defuzzification and function approximation on imprecise and uncertain data. Artificial neural network can be useful for intelligent data mining, neuro-fuzzy control, neuro expert power system and evolutionary computing (e.g. neuro GA).
Let us do technical analysis on evolution of AI in a smart grid system. A knowledge based expert system captures the knowledge of human expert in a specific domain. It uses the knowledge for decision making and appropriate reasoning of complex problems. The expert system needs a knowledge structure in the form of production rules, frames and rules. A knowledge base is a form of database containing both facts and rules. Let us present here examples of few rules.
Rule 1 : If X = True, Then Y= True.
Rule 2 : If X= True and Y= True then Z= True.
Rule 3 : IF I is An isolator AND current through I is 0 AND I = closed
THEN open I.
Rule 4: AND Rule - A.B = X.
Rule 5 : NAND Rule - NOT (A.B) = NOT (X).
Rule 6: OR rule - A+B = Y.
Rule 7 : NOR rule - NOT (A + B) = NOT (Y).
Rule 8 : XOR rule - $A \oplus B = Z$ /* NOT (A). B + A. NOT (B) = Z*/
An expert system (ES) can function based on knowledge of power system operation which may or may not be complete. An ES performs several functions such as knowledge acquisition and inference engine [16]. Data mining algorithms analyze SCADA data. This component acquires new facts or rules. Inference engine performs several functions such as verification, validation, cause-effect analysis, sequence control for rule firing, data processing, meta knowledge management, forward and backward chaining. But, ES may have some limitations from the perspectives of inappropriate representation of knowledge structure. Expert systems can be used in power system analysis

- Planning : AC/DC network design, power plant management, capacity planning;
- Operation: alarm processing, fault diagnosis, forecasting. Maintenance scheduling, demand side management, reactive voltage control;
- Analysis : Control system design, power system protection and coordination;
- AC load flow analysis : Input data includes network parameters, connections, loads, maximum active and reactive power output. It minimizes a set of objective functions subject to a set of constraints such as network laws, plant loading limits, busbar voltage limits, line loading constraints and security.

4. STRUCTURE

The next element of deep analytics is structure, which analyzes a smart grid in terms of various system components such as power generation, transmission and distribution system, generators, transformers, transmission lines, loads, switchyards, microgrids comprising of AC/DC sources and loads, renewable energy sources and energy storage system. Figure 6.1 shows the layered structure of a smart power grid having two core layers: (a) physical and (b) information [33,38,41,43] . The physical layer consists of bottom three layers. The first layer connects various components of a power system such as power generation, transmission, distribution and loads. The next layer is system control which consists of smart meters, voltage, frequency and power factor controllers, sensors and monitoring instruments. Smart meters are able to support exchange of real-time information on demand and supply of electrical power from a smart grid. The meter reading may be communicated to the consumers through SMS and e-mail. The third layer protects the smart grid through various types of relays, circuit breakers, switchgears, fuses and isolators.

Application schema	ERP : MM, HR, FICO, CRM, SCM	Demand response	Predictive analytics	Business analytics
Data schema	Demand Supply	Tariff price	Grid status	Environmental analysis
Security schema	Stability analysis	Reliability consistency	Access control	Attacks DoS
Networking schema	Internet	Mobile communication	LAN	Satellite GPS
Computing schema	AI : Expert system	Soft computing	Billing & payment fn.	Service oriented computing
System protection	Relay	Circuit breaker	Switchgear fuse isolators	Measurement instrumentation
System control	Smart meters	Voltage control	Frequency & PF control	Sensors & monitoring
Power system	Power generation	Power transmission	Power distribution	Load Smart homes

Figure 6.1 : Information System Structure for Solar Computing

The next layer of the smart grid structure is information layer which is associated with computing, networking, security, data and application schema. This layer aggregates information from the physical layer and analyzes data intelligently. The computing schema uses knowledge based expert system and various soft computing tools for automated system control of the smart grid. It is also necessary to compute bills or invoices for the consumers based on consumption of energy; The basic building blocks of networking schema are internet and mobile communication systems. The data schema manages data on demand and supply, tariff and pricing plans. The application schema has various components such as ERP, SCM, CRM, DSS and business analytics; the ERP system may have materials management, finance and cost control, HR and maintenance modules.

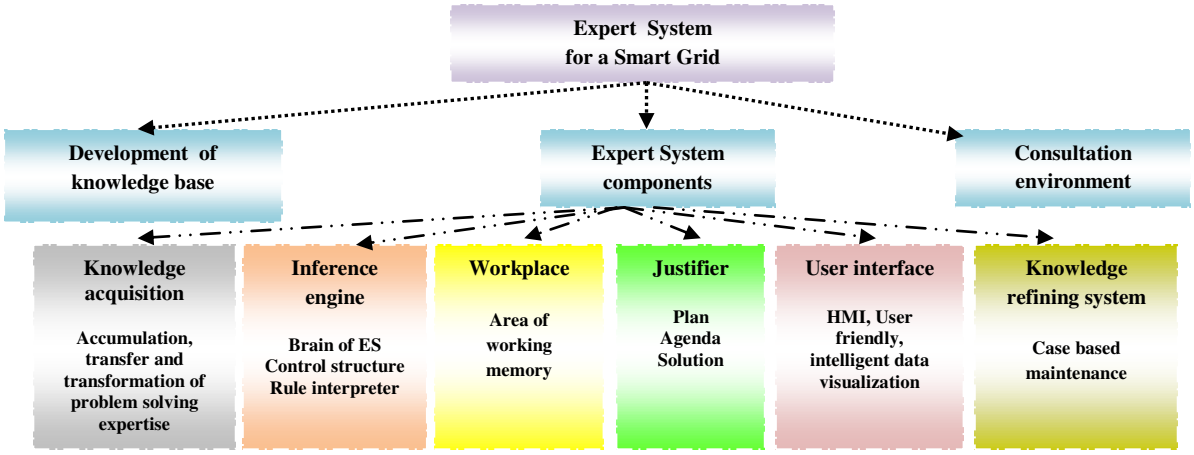


Figure 6.2 : Expert System for a Smart Grid

The solar computing system should be able to interact with the consumers on various issues such as demand response schemes, current energy sources, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles [36, 42]. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing considers the scope of various types of emerging applications such as internet of energy, smart homes and autonomous micro-grids to manage and monitor the use, storage and production of electrical energy though a network of automated modules.

Expert systems are computer based information systems that use expert knowledge to attain high level decisions performance in a specific problem domain [16,17]. The basic principles of ES include how to determine who experts are, the definition of expertise, how expertise can be transferred from an agent to a computer, how the system works. An expert is an agent who has special knowledge, judgement, experience and methods to give advice and solve problems. The knowledge is basically a set of facts and rules. An ES is expected to recognize and formulate a problem, solve a problem quickly and correctly, explain a solution, learn from experience, restructure knowledge, breaking rules if necessary, determining relevance and degrading gracefully. Expertise is extensive task specific knowledge that use expert process. The level of expertise determines the performance of a decision. Expertise is obtained in various ways ; implicit knowledge is gained from experience; explicit knowledge is gained through supervised learning. Expertise is associated with high degree of intelligence, learning from past success and mistakes, well stored, organized and quickly retrievable knowledge from an expert who has excellent recall of patterns from previous experience. The knowledge is related to a specific problem domain, rules and procedures, heuristics about what to do in a given problem situation, global strategies for solving a problem, meta knowledge (knowledge about knowledge) and facts about problem areas.

5. SECURITY

It is essential to verify the security intelligence of a smart grid at various levels : L_1, L_2, L_3, L_4 and L_5 [26-32, 45-50] Please refer to section 9 wherein we have analyzed the case of a self-healing smart grid in details to evaluate the security of the technological innovation. At level L_1, the system performance of the grid is verified in terms of reliability, consistency, stability, robustness, safety, liveness and resiliency. Resiliency measures how fast a system can return to the normal operation following a disruption. The other critical factors are deadlock-freeness and synchronization. The next level is L_2 wherein it is required to audit the access control policy of the grid in terms of authentication, authorization, correct identification, privacy, confidentiality, commitment and trust of the users and the system administrator. At level L_3, the security schema is verified in terms of fairness and correctness (e.g. accuracy of measurement of data in meter reading). At level L_5, it is crucial to assess the risks of various types of malicious attacks on a smart grid such as denial of service (DoS), Sybil and false data injection attack.

At level L_4. it is essential to verify the efficiency of digital relay protection of the transmission lines, generators and motors connected to the power grid such as overcurrent, earth fault, short circuit, voltage and reactive power control and distance protection. Digital relays protect the power system from the adverse effects of a fault which occurs as a random event. The fault current is always greater than the normal load current. If the faulty power system component is not isolated from the grid in time, it may lead to instability. A protection system may consist of CT / PT, CVT, battery, circuit breaker, transducers and protection relays. Overcurrent relays can be used to protect transmission lines, transformers, generators and motors. Reliability and consistency are expected in power system protection. A relay must be dependable and secure; it should operate for specific operating conditions; it should not operate for any other power system disturbance. The responsibility and accountability is defined by a zone of protection. A protection system is responsible for all types of faults occurring within the zone of protection.

Let us present the SWOT analysis on digital power system protection. Smart power grid protection is going through a diffusion of technology from electromagnetic and static relays towards computer enabled digital relays; digital computers have been replacing traditional tools used for short circuit, load flow and stability analysis. Power system protection relays are the next promising scope of computerization based on improved computer hardware, efficient algorithms and programming codes. Digital relays offer the best economic and technical solutions for real-time monitoring and control of power systems today.

Digital relay protection provides several benefits in terms of cost, self-checking reliability, consistency, system integration, adaptive relaying and functional flexibility. The cost of a relay is the main consideration in its acceptability. The cost of digital relays has been declining steadily; the cost of conventional electromagnetic and static relays has been increasing due to change in design, inflation and declining sales and production. A digital relay can be programmed to monitor its hardware and software schema continuously and can detect any malfunctions. It fails in a safe mode and sends a service request alarm to the system center. Digital computers and digital technology have become the basis of measurements, communication, and control of a smart grid. Digital relays can accept digital signals from transducers and fiber optic channels and can be integrated with the control and monitoring system efficiently. Digital computer can be programmed to perform several functions such as measuring and monitoring flows and voltages in transformers and transmission lines, controlling the opening and closing of circuit breakers and switches and providing necessary backup. The relaying function calls for intensive computational activity at no extra cost when a fault occurs on the system. It is an interesting innovation agenda how AI algorithms, heuristics and computing techniques can be applied in various roles of digital power system protection: (Level A) relaying, switch yard protection, measurements, control, diagnostics, communication with levels B and C; (Level B) man machine interface, data acquisition and storage, sequence of events analyses, coordination, back-up protection, communication with level A and B and (Level C) system control, event analyses, communication with levels A & B, adaptive relaying and system performance analysis.

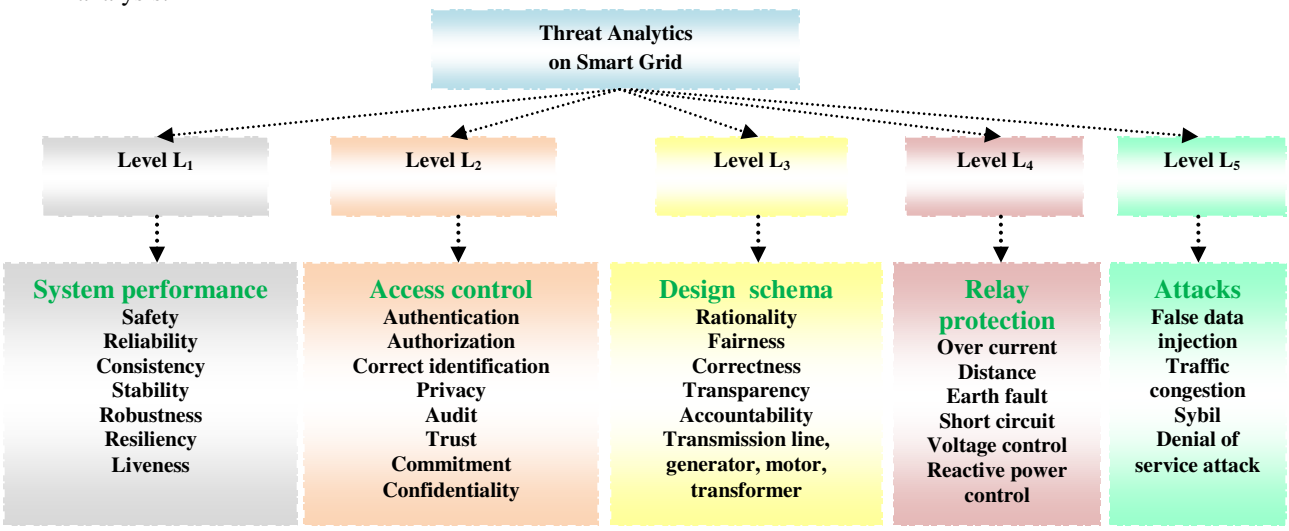


Figure 6.3 : Threat Analytics of a Smart Grid

5.1 ADAPTIVE SECURITY & DYNAMIC DATA PROTECTION

Let us consider the technology associated with adaptive security and dynamic data protection of a smart grid operated through solar computing. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for solar computing. A smart grid demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. Adaptive security is an essential part of solar computing. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

For example, prevention and detection are traditional approaches to the security of a smart grid. In today's digital world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. User Entity Behavior Analytics detect anomalous patterns by comparing with the normal profile and the activities of the users and trigger alarms by sensing single or multiple attacks on solar computing system. The security must overcome the interorganizational

barriers among security, application development and operations teams and be integrated deeply into solar computing architecture.

Dynamic data protection is an effective way to move towards adaptive security architecture. DDP surfaces anomalies and adjusts individualized data security controls proactively in near real-time to protect the critical data of an enterprise. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of organization and networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of solar computing system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of information security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. Adaptive security monitors a solar computing system in real time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventative capabilities allow enterprises to create products, processes, and policies that counter-attack malicious attack (e.g. web security) on the solar computing system. The detective capabilities should identify those attacks in time at minimum impact and not detected by preventative capabilties. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.

6.STRATEGY

The technological innovation on a smart grid is associated with a set of intelligent strategic moves such as scope analysis, requirements engineering, quality control, system design, concurrent engineering, talent management, team management and coordination, resources planning, concept development, concept evaluation, system architecture design, system development plan, roll out, process design, prototyping and testing. Efficient change management ensures that an organization and its workforce are ready, willing and able to embrace the new processes and systems associated with a smart grid. The change management is a complex process. The change should occur at various levels such as system, process, people and organization. Communication is the oil that ensures that everything works properly. It is essential to communicate the scope of AI enabled smart grid to the public policy makers, state and central governments, corporate executives, academic and research community.

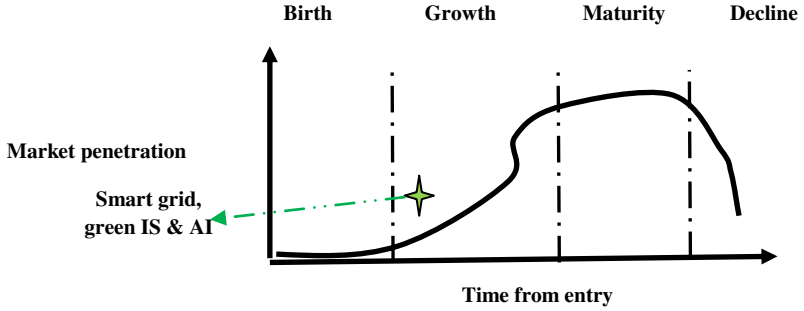


Figure 6.4 : Technology life–cycle analysis

The fifth element of the deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that the technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. This technology is now passing through the growth phase of S-curve [figure 3.4]. Initially, it may be difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the customer, supply and design chain in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory of modern smart grid technology.

7. STAFF-RESOURCES

The sixth element of deep analytics is staff-resources which should be analyzed in terms of sources of innovation and roles of electrical and electronics engineering, information technology, SCADA, power grid, government and collaborative networks and optimal utilization of resources. The innovation demands the commitment of creative experts who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab, academic institutions, power grids of state and central government, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

Traditional scope and approaches of smart grid operations focus on long-term planning and stability to mitigate various types of risks. But, complex operation management requires a mix of traditional and agile approaches to cope with uncertainties. The intension driven role develops collaboration. The event driven role integrates planning and review with learning. The other important roles of the system administrators are to prevent major disruptions and maintaining forward momentum continuously. They must acknowledge the emergence of a problem and then try to minimize the frequency and negative impact of unexpected events in a dynamic environment. They must be people oriented, information oriented and action oriented.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. smart grid, solar computing), research and development, knowledge management, system design and project management. It is essential to teach smart grid technology in various programmes of Electrical and Electronics engineering and information and communication technology as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented. Smart grid technology demands efficient leadership style in terms of optimal resource allocation and utilization, collaboration, coordination and communication.

It is essential to focus on cause-effects analysis of various unwanted occurrences which may affect individuals, system, organization, critical infrastructure, services, environment or the society. It may be possible that the design of old power grid had not considered the issues of information and cyber security and secure and robust protocols correctly due to specialized hardware and technical skill, proprietary code, protocol standards and operation in closed environment. But, today, the system may be connected to the internet directly or indirectly and controlled by human machine interface. There are other organizational

factors such as lack of understanding of the cyber security at the levels of executives and chief information security officers, accountability, lack of proper training and ICT security standards and cultural difference between IT and power grid departments. The primary focus of the power grid department may be efficiency and safety of operation and process control and less focus on IT and cyber security. Further, there are threats from the perspectives of system architecture, old technology, system design, operation and maintenance and inefficient protocols.

Next, let us focus on support. The system is expected to be resilient. The resiliency measures the ability to and the speed at which it can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of the power grid to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The system administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in grid operation? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs?

The smart grid should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated HR workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for the diffusion of the new technology related to smart grid. New skill should be developed in erection, testing, commissioning, operations, maintenance and trading of smart power grid. The business model requires the support of a good human resource management system for talent acquisition, talent retention, skill development, training, career growth planning, incentive, reward, recognition and payment function. The workforce should develop different types of skills such as research and development, system design, project management, erection, testing, commissioning and service maintenance. The system administrators must have leadership skill in terms of smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes.

9. CASE ANALYSIS – SELF-HEALING SMART GRID

North American power grid, one of the greatest engineering innovations of 20th century is now 50 years old and needs a smart self healing grid to incorporate renewable energy sources, reduced number of power outages and reduced carbon emissions [44]. North America has already experienced a number of power outages. In 2012, the occurrence of hurricane Sandy caused power outages in twenty four state of USA and shut down of schools and offices. In 2003 a blackout occurred for two days throughout North-eastern and Midwestern parts of USA and United States and the Canadian province of Ontario. The cause of the blackout was a software bug in the alarm system at a control room of the First Energy Corporation in Ohio. In 2011, New England experienced a Halloween snowstorm that put millions of people in the dark for several days. The following section presents a self healing mechanism [SHM] for the smart power grid.

Self Healing Mechanism [SHM]

++

Agents : Service consumers (B)[e.g. smart home, smart building, industrial load, solar pump for agriculture, microgrid], Service provider (S);

Structure

- Smart power grid comprising of power generation, transmission and distribution system, generators, transformers, transmission lines, loads, switchyards, microgrids comprising of AC / DC sources and loads, renewable energy sources (e.g. PV panels) and energy storage system;
- fully automated power delivery network that monitors and controls a set of nodes, supports a bidirectional flow of electrical power and information among the power plants, loads and all intermittent points;

Scope

- ensure stability, reliability, consistency and improved efficiency during normal operating conditions;
- self-recovery during human error or natural disaster;
- enable better integration between conventional grid and renewable energy sources;

- mitigate the impact of power outages;
- ensure fewer blackouts for shorter periods;
    - maintain the stability of the smart grid;
    - perform accurate and timely monitoring and control of the prosumers;
    - big data analysis for multiple actors and sensors through micro-level measurement;
    - predict the future state of smart grid;
    - fast recovery from faults;
    - automatic action on the transformer to reestablish correct voltage levels in case of voltage drift
    - balance the mismatch between supply and demand to avoid blackout situation
    - various components of a smart grid should be able to communicate for voltage regulation and control of generation capacity and load demand;
- **Constraints :** time, cost, technology;

Strategy: Select a set of intelligent strategic moves rationally.

- Call deep analytics : '7-S' model
- Automated model checking and system verification
- Real-time smart grid monitoring; adaptive and resilient approach in fault analysis and fault clearing
- Adoption of self-stabilizing and self-organizing distributed network management strategy
- Digital power system protection system for giving alarm / alert in time, voltage and reactive power control
- SWOT analysis **:** AI enabled smart grid has more benefits in terms of cost, flexibility and
- TLC analysis **/*** AI enabled smart grid is at growth phase of S-curve today */.

System : AI enabled expert system

- **Input :** Demand plan of B, Supply plan of S;
- **Output :** Energy contract;
- **Protocol:**
    - define and configure expert system in the form of knowledge base, knowledge acquisition system, inference engine, workplace or memory, justifier, user interface, knowledge refining system and consulting environment;
    - develop self-stabilizing and self-organizing distributed network management algorithms;
    - call computationally efficient state estimation algorithms that can predict voltage and phase at different nodes of a smart grid in real-time given the current and predicted energy demand and supply of the prosumers;
    - distributed coordination for automated voltage regulators, voltage control and balancing demand and supply during recovery of faults;
    - automated and distributed active network management strategies given the uncertainty of demand and supply at different levels in the smart grid, fault correction mechanisms, self healing strategies, cause-effect analysis on various types of faults;
    - Configuration of the network automatically, sends control signals to individual customers to adjust generation and also load control, automatically correct faults and self-heals the smart grid.

Security

- verify *security intelligence* through automated or semi-automated system verification**.**
    - **Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities**.
    - call threat analytics and assess risks on smart grid; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised: agents, communication schema, data schema, application schema and computing schema ?

- time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.
- insights : how and why did it occur? do cause-effect analysis.
- recommend : what is the next best action?
- predict : what is the best or worst that can happen?

- Verify a smart grid in terms of security intelligence at various levels such as L_1, L_2, L_3, L_4 and L_5.
- Level L_1 verifies system performance in terms of safety, liveness, reliability, consistency, stability, robustness, resiliency, deadlock-freeness and synchronization.
- Level L_2 verifies access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, trust and commitment of the users and system administrator.
- Level L_3 verifies computing schema in terms of fairness, correctness, transparency, accountability and accuracy of measurement of data.
- Level L_4 verifies the efficiency of digital relay protection such as overload, over current, earth fault, short circuit, over voltage, under voltage, over frequency, under frequency, automatic voltage regulation, reactive power control and distance protection;
- Level L_5 assesses the risks of various types of malicious attacks on a smart grid such as denial of service (DoS), sybil attack, false data injection attack and coremelt attack.
- Revelation principle : B and S preserve privacy of energy contract as per revelation principle;

Staff-Resources : system administration, technical, management, operation, maintenance;
Skill-Style-Support :

- intelligent coordination and integration among 7-S elements;
- Proactive and preventive support
- Reactive support

Payment function:

- The agents settle single or multiple intelligent service contracts.
  - Collaborative planning, forecasting and replenishment (CPFR)
  - Swing option
  - verify business intelligence of service contracts in terms of (pay per use, payment mode, payment terms).

++

A smart self-healing grid is a sophisticated electrical platform that is expected to ensure stability, reliability, consistency and improved efficiency during normal operating conditions; self-recover during human error or natural disaster and enable better integration of renewable energy sources. A self-healing grid should be able to mitigate the impact of power outages during polar vortex, flood, cyclone or snow storm and must ensure fewer blackouts for shorter periods. Self-stabilization and self-organization are two important properties of a self-healing smart grid. Availability, robustness and the possibility for on-demand reconfiguration of distributed complex systems are important in various types of applications such as self-healing smart grid, dynamic sensor network and communication network. A smart grid is expected to be a self-stabilizing system that reaches an arbitrary inconsistent state due to the occurrence of transient faults but can recover automatically from such faults and converge to a desired state. It is not only applicable to a large, distributed and heterogeneous smart grid but also to routing algorithms in communication networks.

Is it possible to adopt collaborative planning, forecasting and replenishment (CPFR) as a strategic tool for comprehensive value chain management of a group of trading agents associated with the smart grid? It may be an interesting initiative among all the stakeholders of the smart grid in order to improve their relationship through jointly managed planning, process and shared information. The interplay between trust and technology encourages the commitment of collaboration among the trading agents.

Let us consider a specific scenario of multi-party negotiation in trading of smart grid. Swing option is a specific type of supply contract. It gives the owner of the swing option the right to change the required delivery of a resource through short time notice. It gives the owner of the swing option multiple exercise

rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, $i \in [1,2,..,n]$, $1 \leq t_1 \leq t_2 \ldots \leq t_n \leq T$ at which a fixed number of d_0 units of a resource may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where $g \leq n$ is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0.

There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function for violating local or global constraints. In this contract, the primary negotiation issue may be a discriminatory pricing plan which depends on the negotiation of a set of secondary issues such as up-swing limit, down-swing limit, maximum total demand, minimum total demand, penalty function and number of swings for a specific period.

Self-stabilization is well defined but self-organization property is not. Self-organization satisfies locality and dynamicity [18, 22]. A smart grid is self-organizing if the distributed algorithm associated with it converges or stabilizes in sub-linear time with regards to the number of nodes and reacts fast to the changes of the topology of the distributed network [19,20,21]. The addition and removal of nodes influences a small number of states of other nodes of the distributed network. If s(n) is upper bound on the convergence time and d(n) is upper bound on the convergence time following a change in topology, then $s(n) \in o(n)$ and $d(n) \in o(s(n))$. The algorithm converges in O(log n) expected number of rounds, responds to dynamic changes locally and is therefore self-organizing.

In a distributed smart grid, it is hard to predict in advance the exact combination of failures and the systems require intelligent and complex coordination mechanisms among the processors, computers and communication networks. A distributed system can be modeled by a set of n state machines or processors ($P_{i,i=1,\ldots,n}$) which communicate with other neighbors [23,24,25]. A distributed smart grid can be represented by a graph G = (V,E) in which each processor is known as node and each two neighboring nodes are connected by a link of the graph. Each node runs a program and changes state with execution of each executable program statement.

10. CONCLUSION

Is it possible to imagine the smart grid as a complex graph in solar computing system? Let us consider a unidirected graph G = (V,E) to represent the system associated with the smart grid, each processor p_i is represented by a vertex $v_i \in V$ and each communication link used for transferring data from p_i to p_j is an edge $(i, j) \in E$; opposite directed edge $(j, i) \in E$; the number of edges linked to a node is bounded by a constant. The distance between two processors p and q is dist(p, q), the shortest path between p and q in the graph. Overlay edge denotes a path of edges that connects two processors in the system. When the path is predefined and fixed, it acts as a virtual link where a processing time is required by intermediate processors to forward the data from source to destination. We regard the time it takes a message to traverse such an overlay link as the time for traversing a link that directly connects two neighboring processors.

A configuration c of the system is a tuple c = (S,L); S is a vector of states, $s_1, s_2, \cdots s_{ni}$, where the state s_i is a state of processor p_i; L is a vector of *link states.* A processor changes its state according to its transition function. A transition of processor p_i from a state s_j to state s_k is called a *step* and is denoted by a. A step a consists of local computation and of either a single send or a single receive operation. An *execution* is a sequence of global configurations and *steps*, $E = \{c_0, a_0, c_1, a_1, \ldots\}$, so that the configuration c_i is reached from c_{i-1} by a step a_i of one processor p_j. The states changed in c_i, due to a_i, are the one of p_j and possibly that of a link attached to p_j . The content of a link state is changed when p_j sends or receives data during a_i. An execution E is *fair* if every processor executes a step infinitely often in E and each link respects the bounded capacity loss pattern. In the scope of self-stabilization, we should consider executions that are started in an arbitrary initial configuration. A *task* is defined by a set of executions called *legal executions* and denoted LE. A configuration c is a *safe configuration* for a system and a task LE if every fair execution that starts in c is in LE. A system is self-stabilizing for a task LE if every infinite execution reaches a safe configuration with relation to LE. The algorithm stabilizes if it has reached a safe configuration with regards to the legal execution of the corresponding task.

A solar computing system must ensure real-time secure monitoring and sense-and-respond modeling; the system should be able to tune itself automatically to an optimal state adaptively. It should be able to anticipate various types of threats automatically that could disturb the stability of the system. Another important task is to isolate the healthy part from the faulty one. A smart power grid is vulnerable to both natural disasters and intentional attacks, physical and cyber challenges and threats of deception. The size and complexity of the grid structure and related cost of erection, testing, commissioning and maintenance are the major constraints to protect the entire infrastructure physically. There are also threats of act of terrorism on the disruption of smart grid and related adverse effects on national security, economy and the quality of life of the common people. Energy security demands fundamental rethinking and radical redesign of the existing power grids globally.

REFERENCES

[1] G.Chalkiadakis, V. Robu, R.Kota, A. Rogers and N.R. Jennings. 2011. Cooperatives of distributed energy resources for efficient virtual power plants. In Proc. of 10th Intl. Conf. on Autonomous Agents and Multiagent Systems, May, 787–794.

[2] S.Chowdhury, S. Chowdhury and P. Crossley. 2009. Microgrids and Active Distribution Networks. Institution of Engineering and Technology (IET).

[3] E. Davidson, S. McArthur, C.Yuen and M.A. Larsson. 2008. Towards the delivery of smarter distribution networks through the application of multiagent systems technology. IEEE Power and Energy Society General Meeting, 1– 6.

[4] M.Deindl, C. Block, R. Vahidov and D.Neumann. 2008. Load shifting agents for automated demand side management in micro energy grids. In Proc. of 2nd IIEEE Intl. Conf. on Self-Adaptive and Self-Organizing Systems, 487–488.

[5] A. Dimeas and N.Hatziargyriou. 2007. Agent based control of virtual power plants. In Proc. of the Intl. Conf. on Intelligent Systems Applications to Power Systems, 1– 6.

[6] J. McDonald. 2008. Adaptive intelligent power systems: Active distribution networks. Energy Policy 36, 12, Foresight Sustainable Energy Management and the Built Environment Project, 4346–4351.

[7] S. Ramchurn, P. Vytelingum, A. Rogers and N.R. Jennings. 2011. Agent-based homeostatic control for green energy in the smart grid. ACM Transactions on Intelligent Systems and Technology, 2, May.

[8] S.D. Ramchurn, P. Vytelingum, A. Rogers and N.R. Jennings. 2011. Agent-based control for decentralized demand side management in the smart grid. In Proc. of the 10th Intl. Conf. on Autonomous Agents and Multiagent Systems. May, 5–12.

[9] P. Ribeiro, B. Johnson, M.Crow, A. Arsoy and Y. Liu. 2001. Energy storage systems for advanced power applications. In Proc. of IEEE 89, 12, 1744 –1756.

[10] G. Strbac. 2008. Demand side management: Benefits and challenges. Energy Policy 36, 12, 4419–4426.

[11] V. Sundramoorthy, G.Cooper, N. Linge and Q. Liu. 2011. Domesticating energy-monitoring systems: Challenges and design concerns. IEEE Pervasive Computing, 10, 20–27.

[12] P. Vovos, A. Kiprakis, A. Wallace, A. and G. Harrison. 2007. Centralized and distributed voltage control: Impact on distributed generation penetration. Power Systems, IEEE Transactions, 22, 1, 476– 483.

[13] P.Vytelingum, T.D.Voice, S.D., Ramchurn, A. Rogers and N.R.Jennings. 2010. Agent-based micro-storage management for the smart grid. In Proc. of 9th Intl. Conf. on Autonomous Agents and MultiAgent Systems, May, 39–46.

[14] EU SmartGrid Technology Platform. Vision and strategy for Europe's electricity networks of the future. Tech. Report, European Union, 2006.

[15] J. Froehlich, L. Findlater and J. Landay. 2010. The design of eco-feedback technology. In Proc. of 28th Intl. Conf. on Human Factors in Computing Systems. ACM, NY, 1999–2008.

[16] E.Rich and K. Night. 1991. Artificial intelligence. 2nd edition. Mcgraw-Hill, New York.

[17] H. Eriksson 1996. Expert system in knowledge servers. IEEE Expert.

[18] Y. Afek and S. Dolev. 2002. Local Stabilizer. Journal of Parallel and Distributed Computing, special issue on self-stabilizing distributed systems, Vol. 62, No. 5, pp. 745-765, May.

[19] E. Anceaume, X. Defago, X., M. Gradinariu and M.Roy. 2005. Towards a theory of self-organization. 9th International Conference on Principels of Distributed Systems, OPODIS, pp. 146-156.

[20] M.Chandy and L.Lamport. 1985. Distributed snapshots: determining global states of distributed systems. ACM Transactions on Computing Systems, 3(1):63-75.
[21] E.W. Dijkstra. 1974. Self-stabilizing systems in spite of distributed control. Communications of the ACM, 17(11):643-644.
[22] S. Dolev and T.Herman. 1995. Super Stabilizing Protocols for Dynamic Distributed Systems. Proc. of the 2nd Workshop on Self-Stabilizing Systems, May.
[23] S.Ghosh, A.Gupta, T.Herman and S. Pemmaraju. 1996. Fault-Containing Self-Stabilizing Algorithms. *PODC* 1996, pages 45–54.
[24] G. Varghese. 2000. Self-stabilization by counter flushing. SIAM Journal on Computing, 30(2):486-510.
[25] H. Zhang and A. Arora. 2002. GS3: Scalable Self-configuration and Self-healing in Wireless Networks. Symposium on Principles of Distributed Computing, pages 58-67.
[26]. Clemente. 2009. The security vulnerabilities of smart grid. J. Energy Security, June.
[27] G. N. Ericsson. 2009. Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment and technology. IEEE Trans. Power Delivery, vol. 24, no. 3, pp. 1174–1181, July.
[28] P. McDaniel and S. McLaughlin. 2009. Security and privacy challenges in the smart grid. IEEE Security Privacy, vol. 7, no. 3, pp.75–77, May/June.
[29] NIST. 2010. Guidelines for smart grid cyber security. The Smart Grid Interoperability Panel - Cyber Security Working Group, NISTIR 7628, Gaithersburg, MD, August.
[30] S. M. Amin. 2010. Securing the electricity grid. Bridge, vol. 40, no. 1, pp. 13–20, Spring.
[31] S. M. Amin. 2005. Energy infrastructure defense systems. Proc. IEEE, vol. 93, no. 5, pp. 861–875, May.
[32] S. M. Amin. 2004. Balancing market priorities with security issues: Interconnected system operations and control under the restructured electricity enterprise. IEEE Power Energy Mag., vol. 2, no. 4, pp. 30–38, Jul./Aug.
[33] J.Brocke, R. T. Watson, C. Dwyer, S. Elliot, and N. Melville. 2013. Green Information Systems: Directives for the IS Discipline. Communications of the Association for Information Systems 33 (1): 509--520.
[34] C. A. Santos, S. C. Romero, C. P. Molina, and M. Castro-Gil. 2012. Profitability Analysis of Grid-Connected Photovoltaic Facilities for Household Electricity Self-Sufficiency. Energy Policy 51 (December): 749–64.
[35] P. Cramton. 2017. Electricity Market Design. Oxford Review of Economic Policy 33 (4): 589–612.
[36] G. Christoph, H. Jacobsen, V. Razo, C. Doblander, J. Rivera, J. Ilg, C. Flath. 2014. Energy Informatics. Business & Information Systems Engineering 6 (1): 25–31.
[37] C.Loock, T. Staake and F. Thiesse. 2013. Motivating Energy-Efficient Behavior with Green IS: An Investigation of Goal Setting and the Role of Defaults. MIS Q. 37 (4): 1313–1332.
[38] N.P.Melville. 2010. Information Systems Innovation for Environmental Sustainability.MIS Quarterly, 34 (1): 1--21.
[39] M. Paschmann and S. Paulus. 2017. The Impact of Advanced Metering Infrastructure on Residential Electricity Consumption - Evidence from California. Working Paper WP 17/08. University of Cologne.
[40] P. Markus, W. Ketter, M. Saar-Tsechansky, and J. Collins. 2013. A Reinforcement Learning Approach to Autonomous Decision-Making in Smart Electricity Markets. Machine Learning, 92 (1): 5–39.
[41] S. Stefan, J. Recker, and J. Brocke. 2013. Sensemaking and Sustainable Practicing: Functional Affordances of Information Systems in Green Transformations. MIS Quarterly, 37 (4): 1275-A10.
[42] S. M. Godoy, R. Roche, E. Kyriakides, A. Miraoui, B. Blunier, K. McBee, S. Suryanarayanan, P. Nguyen, and P. Ribeiro. 2011. Smart-Grid Technologies and Progress in Europe and the USA. In Energy Conversion Congress and Exposition (ECCE), IEEE, 383–90.
[43] R.T. Watson, M. Boudreau, and A. J. Chen. 2010. Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. Management Information Systems Quarterly 34 (1): 4.
[44]https://www.power-technology.com/features/feature-upgrading-us-grid-smart-self-healing-reality accessed on 1.2.2019
[45] A. Aggarwal, S.Kunta and P.K.Verma. 2010. A proposed communications infrastructure for the smart grid. Innovative Smart Grid Technologies, January,Gaithersburg, MD, pp.1–5.

[46] H. Khurana, M. Hadley, N. Lu and D.A. Frincke. 2010. Smart-grid security issues', Security Privacy. *IEEE*, Vol. 8,No. 1, pp.81 –85.
[47] Y. Liu, M.K.Reiter and P.Ning. 2009. False data injection attacks against state estimation in electric power grids. Proceedings of the 16th ACM Conference on Computer and Communications Security, *CCS '09*, ACM, NY, USA, pp.21–32.
[48] J.Lu, D. Xie and Q. Ai. 2009. Research on smart grid in China. Transmission Distribution Conference Exposition: Asia and Pacific, October, Seoul, Korea, pp.1–4.
[49] S.M. Amin and B.F. Wallenberg. 2005. Toward a smart grid: power delivery for the 21st century. Power and Energy Magazine*, IEEE*, Vol. 3, No. 5, pp.34–41.
[50] P. McDaniel and S. McLaughlin. 2009. Security and privacy challenges in the smart grid. Security Privacy, IEEE, Vol. 7, No. 3, pp.75 –77.

Exercise

1. **Define solar computing. What is the scope of solar computing innovation?**
2. **What is the dominant design of solar computing innovation?**
3. **What are the basic elements of the system architecture associated with solar computing innovation? How to represent the structure correctly?**
4. **What do you mean by technology security for solar computing ? How to verify the security intelligence? What is the role of adaptive security and dynamic data protection in solar computing? Design an adaptive security architecture. Develop a self-healing mechanism.**
5. **What are the strategic moves of technology innovation, adoption and diffusion of solar computing? What is the outcome of technology life-cycle analysis?**
6. **How to manage resources in solar computing innovation project? What should be the talent management strategy?**
7. **What are the skills, leadership style and support demanded by the technological innovation in solar computing ?**
8. **How to manage technology innovation project in solar computing efficiently?**
9. **What should be the shared vision, common goals and communication protocols?**
10. **How can you ensure a perfect fit among '7-S' elements?**

CHAPTER 7: ADAPTIVE SECURITY & DYNAMIC DATA PROTECTION for IIoT ENABLED SCADA: ISI ANALYTICS

Abstract : Information Security Intelligence (ISI) analytics is an emerging digital technology; its scope may be analyzed in terms of adaptive security and dynamic data protection. SCADA / ICS may face various threats of malicious attacks from external and internal environments; it is essential to protect the system through (ISI) analytics. ISI analytics can monitor SCADA / ICS in real-time to detect any anomalies and vulnerabilities. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities. This chapter is focused on digital defense of Industrial Internet of Things (IIoT) enabled SCADA and Industrial Control Systems (ICS), an emerging technology in energy, utility, defense, transportation and financial sectors. The technology is analyzed through deep analytics along seven 'S' dimensions: scope, system, structure, strategy, security, staff-resources and skill-style-support. It highlights technology life-cycle analysis on S-Curve; the technology is passing through growth phase at present. The technology has been analyzed based on related literature review on IIoT, SCADA and ICS and also reasoning of three cases: (a) SCADA for a smart power grid, (b) adaptive industrial control system (ICS) and (c) defense – border security surveillance. We have also outlined security intelligence verification mechanism (SIVM) of IIoT enabled SCADA and ICS based on an adversary model and intelligent threat analytics.

Keywords: ISI analytics, Adaptive security, Dynamic data protection, Industrial Internet of Things, SCADA, Industrial Control System, Deep analytics, Threat analytics, Adversary model, Security intelligence verification algorithm, Defense, Smart power grid, Fuzzy control of industrial plant.

1.INTRODUCTION

The basic objective of the technological innovation of ISI analytics is to verify the security intelligence of SCADA and industrial control system so that the assets of information and communication technology of an enterprise are protected from various types of malicious attacks. ICS / SCADA performs key functions to provide essential services such as defense, energy (e.g. smart power grid), utilities, transportation and communication system of a country. It is a part of a nation's critical infrastructure and operates with the support of industrial control systems, supervisory control and data acquisition (SCADA), sensor networks, information and communication technologies. ICS / SCADA systems are potentially vulnerable to various types of malicious attacks which may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss.

Any comprehensive and complete solutions are missing in the existing works for the verification of security intelligence of SCADA / ICS. The present work evaluates the technology associated with IIoT enabled SCADA / ICS and also outlines security intelligence verification algorithm (SIVM) in terms of system, input, output, objectives, constraints, moves, revelation principle, payment function, security intelligence and proactive and reactive risk mitigation approaches. The security intelligence of ICS / SCADA is explored in association with the computing, data, networking, application and security schema at five levels : L1, L2, L3, L4 and L5 in terms of intrusion and access control, secure multi-party computation, system performance, malicious attacks and multi-party corruption respectively through an intelligent threat analytics. The present work assesses the risk of different types of threats on ICS / SCADA and presents a set of intelligent verification mechanisms which can protect the system from potential malicious attacks. The verification mechanisms are based on cryptography and distributed secure multi-party computation. An efficient system is expected to be resilient. Resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption. The vulnerability of the system to a disruptive event can be viewed as a combination of likelihood of a disruption and its potential severity.

Let us first present a deep analytics for IIoT enabled ICS and SCADA. It is basically an integrated framework which is a perfect combination or fit of seven factors. A complex operation of ICS and SCADA may fail due to the inability of the system administrator to recognize the importance of the fit and the tendency to concentrate only on a few of these factors and ignore the others. These factors must be integrated, coordinated and synchronized for effective SCADA operation. This work is organized as

follows. Section 1 defines the technology of IIoT enabled SCADA and ICS. Sections 2-8 have analyzed the technology through scope, system, structure, strategy, security, staff-resources and skill-style-support respectively. Section 5 outlines security intelligence verification mechanism (SIVM). Section 9 analyzes three test cases: (a) SCADA for a smart power grid, (b) industrial control system and (c) defense – border security surveillance. Section 10 concludes the work showing the future scope of the technology.

2. SCOPE

Supervisory control and data acquisition (SCADA) networks perform key functions to provide essential services for energy and utilities (e.g. electricity, oil, gas, water), defense and communication sectors. SCADA is a part of a nation's critical infrastructure and operates with the support of industrial control systems, sensor networks and information and communication technologies. SCADA networks are potentially vulnerable to various types of malicious attacks that result disruption of critical security services in terms of confidentiality, integrity, availability, authentication, non-repudiation, access and inference control, intrusion, process redirection or manipulation of operational data. These attacks may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss. Therefore, the protection of SCADA networks should be a national priority.

Industrial control systems for critical infrastructure like national power grid make increasingly use open technologies and Internet protocols. A smart energy grid often faces the challenge of malicious attacks (e.g. cyber attack) from power play and politics, industrial espionage and terrorists and also compromises of information infrastructure due to user errors, equipment failures and natural disasters. A malicious agent may be able to penetrate an energy grid, gain access to control software and hardware and alter load conditions to destabilize the grid in an unpredicted way [17].

Let us analyze the scope of IIoT technology. Internet of Things (IoT) is a networked smart devices equipped with sensors and RFID tags, connected to the Internet, all sharing information with each other without human intervention, dynamic global network infrastructure with self configuring capabilities, standard interoperable communication protocols, intelligent interfaces and are seamlessly integrated with information network [41-44]. The fast development of networked smart devices with Internet, sensors and radio-frequency identification devices (RFID) is enabling the emergence of many new applications in remote access control, effective monitoring and supervision, better performance, real-time decision making, system integration and access to cloud based resources. IIoT is used for various types of industrial applications such as aerospace and aviation, airports, automotive, environment monitoring, food technology, smart cities, intelligent buildings, intelligent transportation infrastructures, healthcare, operation in hazardous environment, retail, logistics, supply chain management and monitoring of safety and security of smart grid (e.g. advanced metering, energy management, interaction with smart appliances).

Next, let us explain the scope of digital defense: how to protect information and communication technology (ICT) assets of an enterprise from various types of malicious attacks. Why should a business model address information security in an effective and comprehensive way? It is basically a problem of risk management; attacks on ICT technology schema and the theft or misuse of critical data should be assessed and mitigated appropriately for digital transformation. Digital defense is associated with a complex process which includes identification of information assets, assessment of critical vulnerabilities, selection of appropriate security solution for the protection of ICT schema, trusted computing environment development, preserving the authenticity, authorization, correct identification, privacy and audit of electronic transactions, access control and defining security policy, process and maintenance intelligently [1]. This work talks about traditional issues of user permission control, confidentiality by encryption, authorization through passwords, tokens, digital certificates, role based access control, audit trails and digital signature for the protection of general information assets such as data on sales, customers, vendors and human resources.

The existing works have been reviewed on system architecture, computational intelligence of verification mechanisms, potential threats and vulnerabilities, security concerns and risk analysis of various types of industrial control systems and SCADA [1,2,3,4,5,6,7,14,15,16,17,18,19,20,26,37]. The review of existing literature could not find out an efficient mechanism for SCADA / ICS. The existing works have several gaps. The security intelligence is expected to be defined strongly with robustness, completely and precisely. The protocols should have intelligent model checking or system verification strategies based on rational threat analytics. The present work has identified three critical issues to be associated with digital defense of

information and communication technology assets of ICS and SCADA: threats analytics, verification mechanisms of security intelligence and the relevant computational challenges. Case based reasoning approach is adopted also for experimenting three test cases on smart power grid, industrial plant and defense SCADA.

This work assesses the risk of different types of threats on ICS/ SCADA and presents a set of intelligent verification mechanisms which can protect ICS / SCADA from potential malicious attacks. The mechanisms are based on cryptography and distributed secure multi-party computation and check the security intelligence of a resilient ICS from the perspectives of intrusion detection, secure communication, service oriented computing, credential based biometric access control, privacy and inference control. The research methodology adopted in the present work includes case analysis and review of relevant literature. The logic of the verification mechanisms has been explored through analysis of three cases in section 9.

3. SYSTEM

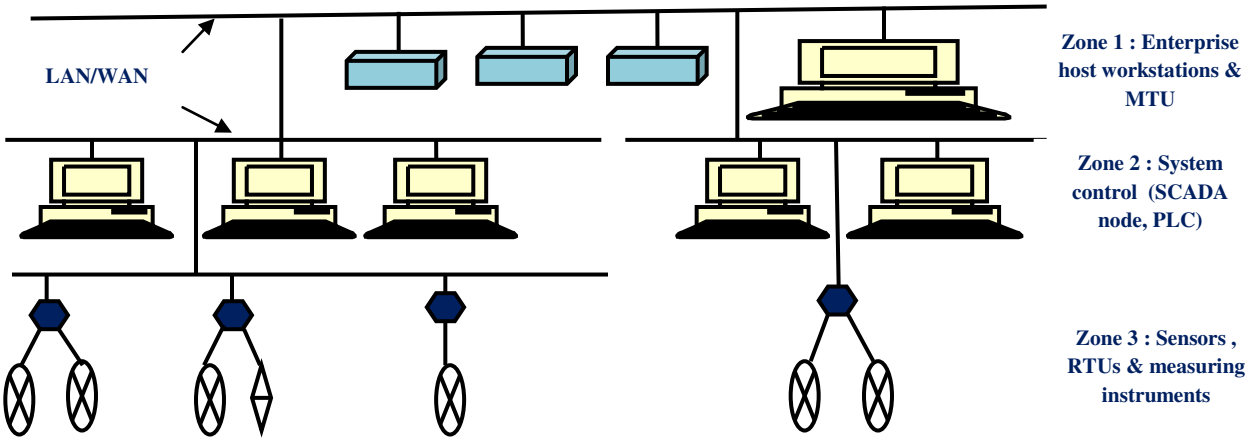


Figure 7.1 : ICS / SCADA Architecture

In this chapter, We have considered the technology of IIoT enabled Industrial Control System (ICS) and SCADA configured with computers, electrical, electronics and mechanical equipments; operated in automated or semi-automated operation mode and used in manufacturing and chemical plants, power plants, energy and utilities distribution, communication and transportation systems. ICS interact with the physical environment and is associated with a complex information system. ICS integrates computing, networking, data, application and security schema, sensors and actuators. ICS may be threatened by cyber and other various types of malicious attacks; safety, reliability, consistency and fault tolerance are critical issues.

In general, ICSs can be simple, medium and very complex systems which may include thousands of different components distributed over different zones and controlling real-time complex processes. ICS systems can be broadly segmented into three different zones such as Enterprise, Control and Field zone (as per IEC TS 62443-1-1 2009) [26, Figure 7.1]. The enterprise zone includes business networks and enterprise systems; the control zone includes various control elements; the field zone includes the devices (e.g. PLC) and networks used for automation. A smart grid may have different segments such as power generation, transmission, and distribution and metering. Next, let us focus on networking schema of ICS/ SCADA architecture. Typically, several wireless technologies can be used for ICS / SCADA such as Wireless Local Area Network (WLAN) and Bluetooth (as per open IEEE 802.15.1 standard; operates in 2.4 GHz ISM band). Various components of an ICS / SCADA can communicate with each other through a set of protocols such as IEEE 802.11x, Bluetooth, cellular, Wireless HART, ISA 100.11a, Z-Wave, Zigbee, Microwave and satellite technologies.

Let us discuss IoT enabled SCDA / ICS. Due to recent innovation of internet connectivity, digital and smart manufacturing technologies, IoT has become a revolutionary technology. The applied domains include supply chain management, transport, utilities, industrial automation, healthcare, building and home automation. IoT is an emerging technology that connects physical objects, internet and communicate with one another (similar to HCI). IoT connects systems, sensors and actuators to the internet. Physical objects +

Sensors, actuators and controllers + Internet = IoT (Connect, communicate and data exchange). Another emerging trend of SCADA / ICS is IIoT; this includes real-time monitoring and process control like real-time optimization of production and supply chain networks in manufacturing industry; deployment of smart machines, sensors and controllers with proprietary communication and internet technologies, automated process control using digital controllers to achieve enhanced productivity and safe distribution system; maximizing safety, sensitivity, security and reliability through high precision automation and control. What are the scopes of IoT for electric power system? It includes smart metering, AMI (Advanced Metering Infrastructure), connected public lighting, smart inverters, smart grid, SCADA, remote control operation of energy consuming devices, home entertainment (audio, video, projectors), smart lighting adapting ambient conditions based switching, wireless internet connected lights, smoke and gas detection, smart appliances, management and control, intrusion detection and surveillance system.

4. STRUCTURE

Let us exercise the complexity analysis on the structure of IIoT enabled ICS and SCADA technology in terms of various components such as PLC, RTU, field devices, intelligent electrical and electronic devices, workstations, human machine interface, communication gateways, data historians, controllers and software applications; their functions, topology, connectivity and communication protocols. The configuration and scope of an ICS may be simple, medium or highly complex; may be fully or semi-automated. There are various types of ICS like SCADA, process control system (PCS), distributed control system (DCS), safety (SIS), building automation system (BAS), energy management system (EMS) and embedded system (ES).
A Process Control System (PCS) controls an automation process in an industrial plant (e.g. steel, chemical, life-science). SIS monitors an automation process and prevents an unsafe plant operation through a set of sensors and controllers. DCS controls multiple automation processes at a plant (e.g. oil refineries, water treatment plant). BAS monitors and controls a building's infrastructure services such as heating, ventilation, air conditioning, cooling, lighting, elevators, fire protection, energy management etc. through intelligent Internet Protocol (IP). EMS monitors and controls a smart power grid.
SCADA is a type of ICS which collects data and monitors an automated power plant. SCADA control center monitors and manages RTUs and IEDs; the human operators or supervisors use HMI or a supervisory control software to control the power plant by changing set points. A SCADA system may supervise one or more DCSs or PCSs at distant locations, through intelligent communication protocols wherein bandwidth, reliability, latency and jitter are critical success factors. A SCADA system is a process automation system; it is used to gather data from the sensors and the instruments distributed at remote sites and to transmit the data into a central system for controlling or monitoring the basic mechanism. The system controller can view the data collected from the sensors on SCADA host computers located at master site. Automated or operator driven supervisory commands are transmitted to the control system based on the data received from the remote sensors.
Generally, a SCADA system is composed of five basic components [1]: (i) a sensor network that senses process variables at remote site, (ii) a set of operating instruments connected to the sensors, (iii) a set of local processors that collect data and communicate with programmable logic controllers (PLC), RTU, intelligent electronic devices (IED), transducers, relays and process controllers; (iv) SCADA servers / host computers / master terminal units (MTU) as central point of process control, performance monitoring, data warehousing and data mining and (v) wired / wireless communication channels between local processors and host computers.
Let us do the technical analysis on various components of an industrial control system / SCADA. A PLC is a microprocessor controlled electronic device that reads input data from sensors, executes programmed instructions based on input and supervisory control, generate output signals for change of switch settings or actuators. A PLC has CPU, communication interface, input/output modules and power supply and executes various types of programming languages such as ladder diagram, block diagram, structured text, instruction list and sequential function chart. A RTU is a microprocessor controlled electronic device and of two types such as station and field RTUs. Intelligent Electronic Devices (IED) may have one or more processors and can interact with various external entities like digital relays and meters.
A workstation is typically a computer or server running a standard operating system; hosts the programming software for making changes in the logic of the controllers and other applications. HMI is a software application which provides alarms, process status and data trends of an automated processes to a plant supervisor. An HMI can operate on various platforms such as desktop computers, tablets, smart

phones or SCADA panel screens. A Data Historian is a software application for time series analysis of real-time data. A Communication Gateway enables two devices to communicate with each other. A Front End Processor is a dedicated communications processor. There may be various types of field devices like sensors, transducers and actuators which directly interface with a controller through digital or analog I/O module or industrial protocol (e.g. Modbus). The typical architecture of SCADA supports TCP, IP, UDP and wireless communication protocols as well as Modbus TCP, private radio, cellular or satellite networks [6]. The selection of appropriate communication schema depends on various factors such as data rate, polling frequency, distance, area, budget and future needs. A SCADA system can monitor and control thousands of input / output (I/O) points. This is a complex integrated system: a SCADA network may be integrated with other different types of information and communication systems such as web enabled enterprise applications and business intelligence solutions [3,4]. This architecture provides a real-time, fault-tolerant and intelligent distributed computing platform.

Let us do system audit analysis on digital transformation of ICS / SCADA [Figure 7.2]. In many plants, ICS and SCADA were installed a long time back. It is possible to improve the system performance and productivity of various old plants through system audit grid analysis : divest the dead, old and obsolete technologies (e.g. electromagnetic relays, PLCs) and invest on emerging technologies (e.g. digital relay protection, sensor networks, Internet communication protocols, self healing system, AI based smart grid) for digital transformation.

What are the benefits of deploying wireless communication schema in ICS and SCADA? It is a costly strategic option; it requires high capital allocation and technological skill for the replacement of wired networking schema with wireless schema and extensive upgrading efforts. This initiative of digital transformation also requires the replacement of critical electrical and electronic equipments such as digital relays, digital smart meters and sensors which should be fit for operation in wireless environment. It is also important to look into security and privacy of critical data in wireless environment against malicious cyber and physical attacks. It is really challenging to select appropriate wireless technologies for multi-tiered ICS / SCADA architectures. A typical wired ICS infrastructure may be damaged due to natural disaster or act of terrorism. However, there are several benefits of wireless schema in terms of network bandwidth, high speed, reliability, adaptability, availability, safety, scalability, reduced cost of cabling and installation, flexible installation, ad-hoc on-demand deployment, providing redundancy and efficient integration among different components of smart grid.

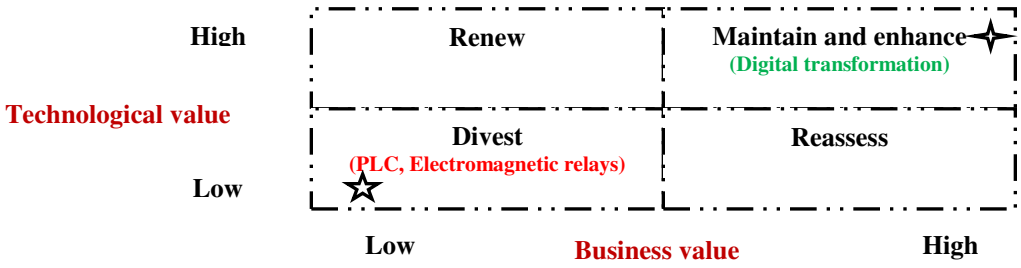


Figure 7.2: System Audit Grid for IIoT enabled SCADA / ICS

5. SECURITY

The next element of the deep analytics is security.. The basic building block of security of IIoT enabled ICS and SCADA technology is an intelligent threat analytics. The threats to a smart grid may be method, target, protocol and identity specific. Insider attacks are more malicious than outsider attacks as the adversaries may have more knowledge about the internal architecture of SCADA / ICS. Method specific threats define how active or passive threats are executed. The method specific threats can be either passive or active. In passive attack, the adversary monitors and analyzes the data captured from SCADA / ICS. In active method, the adversary may send false data to the components of SCDA system.. Target-specific threats attack specific component of SCADA network such as PLC, relay and smart meters. The adversaries may try to exploit the vulnerabilities associated with the networking protocols (e.g. DNP3, Modbus).

Please refer to section 9 which outlines security intelligence verification algorithm (SIVM) and also shows its application in three different cases: (a) SCADA for a smart power grid, (b) adaptive industrial control system and (c) defense – border security surveillance. SIVM is the backbone of the security of IIoT enabled SCADA and ICS technology. Table 1 summarizes the major findings of an intelligent threat analytics for the protection of SCADA / ICS in terms of target, risks assessment and mitigation strategies and verification mechanisms. A verification mechanism is expected to provide one or more services by detecting, preventing or recovering from one or more security attacks. We have found that no single verification algorithm can provide adequate security to ICS / SCADA.

Target	Security Threats on SCADA / ICS	Verification mechanisms	Risk mitigation strategies
Networking schema	**Intrusion: sybil, cloning or node replication, wormhole, DoS, node capture**	**Intrusion Verification Mechanism (IVM)**	**Bio-inspired AI: self / non-self classification for negative selection, danger signal detection; identity control**
Networking schema	**Secure communication : Device attestation, false data injection attack, coremelt attack, multicast attack: rushing, blackhole, neighbor, jellyfish**	**Private communication verification mechanism (PCVM)**	**Challenge response protocol, bad data measurement, SCADA network traffic congestion analysis; Key management protocol to preserve group, forward and backward privacy.**
Cyber application schema	**Web service security**	**Web security verification mechanism (WSVM)**	**Trusted service oriented computing**
Computing and application schema	**Biometric access control**	**Access Control Verification Mechanism (ACVM)**	**Biometric enrollment and recognition; credential based access control**
Data schema	**Privacy : inference control**	**Privacy Verification Mechanism (PVM)**	**Statistical disclosure control preserving confidentiality and privacy: randomization, suppression, generalization, sampling, summarization, aggregation.**

Table 1: Threat Analytics

An intelligent threat analytics should perform various type of vulnerabilities analysis as follows :
Vulnerability analysis 1: Domain (configuration, design specification, implememtation) vs. weakness (account mgmt, poor coding practice, poor authentication, interface programmimg, malfunctioning devices, poor logging, inefficient monitoring);
Vulnerability analysis 2 : Risk elements (purpose of attacks [information capture, sabotage], lateral movement [automatic], location command and control server [Insider and outsider attack], initial attack vector [Automatic]) vs. types of attacks (e.g. capture information from target through industrial espionage, identity theft, IP theft, spearphishing, drive-by-download attack)
Vulnerability analysis 3 : Classification of vulnerabilities (buffer outflow, forced browsing, code injection, access control, input validation, resource exhaustion, authentication attack, path traversal, resource allocation, weak password, DLL hijacking, SQL injection, cryptographic failure, CSRF, weak encryption) vs. history of occurence;
Vulnerability analysis 4 : metrics (physical, information, cognitive, social) vs. risk mitigation practice (plan, absorb, recover, adapt);

It is essential to define an optimal set of security metrics in terms of risk and resilience. The metrics are the measurable properties of ICS that quantify the degree to which objectives have been achieved and provide vital information of system performance. Security metrics are associated with critical business functions such as incident, vulnerability, patch, configuration, security and change management. The metrics should be linked to a strategy, can be quantified, comprehensive, and measurable and indicates the right behavior of a system. Relevant Metrics are directly linked to decision making goals, objectives and relevant attributes of a system.

5.1 ADAPTIVE SECURITY & DYNAMIC DATA PROTECTION

Let us consider the technology associated with adaptive security and dynamic data protection of ISI analytics. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for SCADA / ICS which demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. Adaptive security is an essential part of ISI analytics. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

For example, prevention and detection are traditional approaches to the security of SCADA / ICS. In today's digital world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. User Entity Behavior Analytics detect anomalous patterns by comparing with the normal profile and the activities of the users and trigger alarms by sensing single or multiple attacks on SCADA / ICS. The security must overcome the inter-organizational barriers among security, application development and operations teams and be integrated deeply into ISI analytics architecture.

Dynamic data protection is an effective way to move towards adaptive security architecture. DDP surfaces anomalies and adjusts individualized data security controls proactively in near real-time to protect the critical data of an enterprise. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of organization and networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of ISI analytics irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of information security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. Adaptive security feature of ISI analytics monitors SCADA / ICS in real time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventative capabilities allow enterprises to create products, processes, and policies that counter-attack malicious attack (e.g. web security) on SCADA / ICS. The detective capabilities should identify those attacks in time at minimum impact and not detected by preventative capabilties. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.

6. STRATEGY

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that IIoT enabled ICS and SCADA technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. This technology is now passing through the growth phase of S-curve [Figure 7.3]. Initially, it is difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the customer, supply and design chain in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory IIOT enabled SCADA and ICS technology.

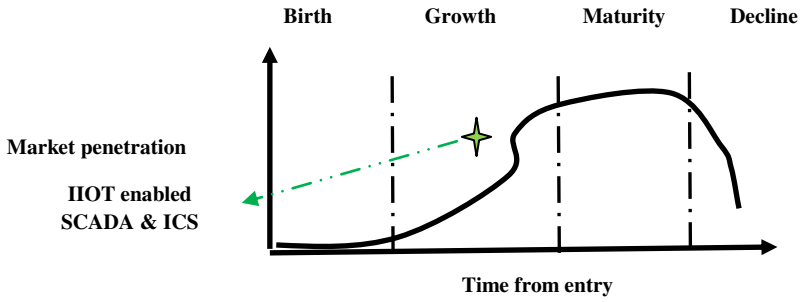


Figure 7.3 : Technology life–cycle analysis

Strategy 1 : SIVM verifies innate and adaptive system immunity in terms of collective, machine, security, collaborative and business intelligence through multi-dimensional view on intelligent reasoning.

SIVM is defined by a set of elements : system, a group of agents, a finite set of inputs, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payment function, an optimal set of moves, revelation principle and model checking or system verification protocol. The proposed mechanism evaluates the innate and adaptive immunity of a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations.

The mechanism follows a set of strategic moves. The basic building block of the mechanism is an analytics having multidimensional view of intelligent reasoning. Reasoning has multiple dimensions like common sense, automated theorem proving, planning, understanding, hypothetical, simulation dynamics and envisioning i.e. imagination or anticipation of alternatives. The inference engine selects appropriate reasoning techniques from a list of options such as logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception based reasoning depending on the demand of an application. Another important move is the collection of evidence through private search which may require a balance between breadth and depth optimally.

The critical challenge is how to detect the danger signal from a system? The mechanism evaluates system immunity (i) combinatorially in terms of collective, machine intelligence, security, collaborative and business intelligence. The *collective intelligence* (a) is defined in terms of scope, input, output, process, agents and system dynamics. For a complex application, it verifies coordination and integration among system, strategy, structure, staff, style, skill and shared vision. What is being done by the various components of a system? Who is doing? Why? How? Where? When? The *machine intelligence* (b) checks the system in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For example, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion,

time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states and state transition plans of the information system associated with ICS/SCADA.
The *security intelligence* (c) verifies the system in terms of authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, commitment, reliability and consistency. The *collaborative intelligence* (d) evaluates the feasibility and effectiveness of human-computer interaction to achieve single or multiple set of goals, information sharing principle and negotiation protocol. The *business intelligence* (e) is associated with business rules such as HR policy, payment function, cost sharing, bonus, contractual clauses, quality, performance, productivity, incentive policy and competitive intelligence.
The mechanism verifies system immunity through a set of verification algorithms. It is possible to follow various strategies like model checking, simulation, testing and deductive reasoning for automated verification. Simulation is done on the model while testing is performed on the actual product. It checks the correctness of output for a given input. Deductive reasoning tries to check the correctness of a system using axioms and proof rules. There is risk of state space explosion problem in case of a complex system with many components interacting with one another; it may be hard to evaluate the efficiency of coordination and integration appropriately. Some applications also demand semi-automated and natural verification protocol. The mechanism calls threat analytics and assesses risks of single or multiple attacks on the system under consideration: analyze performance, sensitivity, trends, exception and alerts; checks what is corrupted or compromised: agents, protocol, communication, data, application and computing schema? Performs time series analysis: what occurred? what is occuring? what will occur? assess probability of occurrence and impact; explores insights : how and why did it occur? do cause-effect analysis; recommends : what is the next best action? predicts: what is the best or worst that can happen?

Strategy 2 : SIVM verifies security intelligence collectively through a rational threat analytics.

Model checking is an automated technique for verifying a finite state concurrent system such as a hardware or software system. Model checking has three steps: represent a system by automata, represent the property of a system by logic and design model checking algorithm. The security intelligence of SCADA is a multi-dimensional parameter which is defined at five different levels L1,L2,L3,L4 and L5. At level L1, it is essential to verify the security of data schema in terms of authentication, authorization, correct identification, privacy and audit of access control mechanism offered by the system. In this case, the system should ask the identity and authentication of one or more agents involved in SCADA operation and system administration. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After correct identification and authentication, SIVM should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The privacy of data may be preserved in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to an agent through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. The agents must commit the confidentiality of data exchange associated with private communication.
At level L2, it is essential to verify the computing schema in terms of fairness, correctness, transparency, accountability and trust. A protocol ensures correctness if the sending agent broadcasts correct data free from any false data injection attack and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with proper resource allocation, trust, commitment, honesty and rational reasoning of the agents involved in SCADA system administration. Fairness ensures that something will or will not occur infinitely often under certain conditions. The mechanism must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. The transparency of SCADA system administration is associated with communication protocols and revelation principle.

At level L3, it is essential to verify the application schema in terms of system performance. The performance of the system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. SCADA is expected to be a resilient system. The resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption.
At level L4, SIVM verifies networking schema and assesses the threats of internal and external malicious attacks on SCADA / ICS such as cyber attack, rubber hose, sybil, node replication, wormhole, coremelt, forward, blackhole, neighbor, jellyfish and crypto jacking attack. At level L_5, SIVM verifies security schema and assesses the risk of multi-party corruption (e.g. sender, receiver, data, communication channel, mechanism and protocol) and business intelligence of payment function.

Strategy 3 : The security intelligence of an industrial control system is verified comprehensively in terms of correctness of computing schema, stability and robustness in system performance of the plant, data, networking, security and application schema.

Please refer to second test case in the appendix where SIVM is applied for a plant having supervisory adaptive fuzzy control. Let us first explain various types of circuits for intelligent process control of the plant. Next, it is essential to call threat analytics and verify the security intelligence of data, computing, application, networking and security schema at levels 1,2,3,4 and 5. At **level L1**, it is crucial to verify the **data schema** in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, integrity, non-repudiation, locking of passwords, false data injection attack and intrusion for proper access control of the plant. Any flaws in access control may affect the stable performance of the plant negatively. A malicious agent can take over the control of the plant completely or partially by hacking system control passwords or compromising system administration.
Next, let us consider **level L2** to verify the **computing schema**. Fuzzy logic is a multi-valued logic used for approximate reasoning. Fuzzy logic based algorithms are used for the control of complex plants through fuzzy controllers. The fuzzy controllers (FC) operate based on IF-THEN fuzzy rules. Industrial process control systems use various types of controllers such as P/PI/PID through adaptive gain scheduling, supervisory control architectures and algorithms. The fuzzy controllers use IF-THEN rules, can learn universal approximation property and can deal with fuzzy values. If there are flaws in design of these basic features of fuzzy controllers, a plant may face various types of problems in terms of system performance, stability and robustness.
A plant's behavior can be defined by a set of IF-THEN fuzzy rules based on knowledge acquisition from knowledge based expert system, ANN and GA based algorithms. ANN and GA are used to learn fuzzy rules through structural identification which requires structural apriori knowledge such as linear or nonlinear control of a system. Another approach is parameter identification, scaling and normalization of physical signals. Another important feature is universal approximation: a fuzzy system with IF-THEN rules firing, defuzzification and membership function can approximate any real continuous function with certain approximation error due to the overlap of membership function from IF parts of a set of fuzzy rules. The inputs to the fuzzy controller are fuzzy values; they are quantitative numbers being obtained from different sources. For example, the intensity of a signal with respect to time interval is expressed by a membership function. FCs are able to deal with fuzzy value through heuristics or model based approaches.
The objective of fuzzy control is to design a feedback control law in the form of a set of fuzzy rules such that the closed loop system exhibits the desired behavior of a given model of the system and its desired behavior. The quality of nonlinear control is measured in terms of system performance, stability, robustness, accuracy and response speed In case of stabilization, the state vector of a closed loop system should be stabilized around a set point of the state space. Here, the challenge is to define a set of fuzzy rules based control law. In case of tracking, a FC is to be designed so that the output of closed loop system follows a time varying trajectory. The basic objective is to find a control law in terms of a set of fuzzy rules such that the tracking error $[x(t) - x^d(t)]$ tends to zero. In fact, stabilization is a special type of tracking where the desired trajectory is constant.
Next, let us consider system performance of a plant in terms of computing and application schema at level L3. In case of linear control, the behavior of a closed loop system can be specified in exact quantitative

terms such as rise time, setting time, overshoot and undershoot. The desired behavior of a non-linear closed system can be specified in qualitative terms such as stability, accuracy, response speed and robustness. In case of linear control, stability implies the ability to withstand bounded disturbances in linear range of operation of the system. In case of nonlinear control, the behavior of the system is analyzed in terms of effects of positive disturbances and robustness. Robustness is the sensitivity of the closed loop system to various types of effects such as measurement noise, disturbances and unmodelled dynamics. The closed loop system must be insensitive to these effects. Accuracy and response speed must be considered for desired trajectories in the region of operation. Moreover, it is important to verify the plant's performance in terms of reliability, consistency, resiliency, liveness, denial of service (DoS) attack, deadlock freeness, synchronization and application integration. It is expected to minimize human error in plant's operation from the perspectives of correct decision making and adjustment of the setting of plant's parameters.

The verification of correctness of computing schema of a fuzzy controller is a critical issue. A fuzzy logic controller defines a control law in terms of a transfer element due to non-linear nature of computation. The fuzzy control law is expressed by a set of 'IF THEN' fuzzy rules. 'IF' part of a fuzzy rule describes a fuzzy region in the state space. 'THEN' part specifies a control law applicable within fuzzy region from IF part of the same rule. FC yields a smooth non-linear control law through the operation of aggregation and defuzzification. The correctness of computing schema is associated with a set of computational steps such as input scaling or normalization, fuzzification of controller input variables, inference rule firing, defuzzification of controller output variables and output scaling or denormalization.

In case of supervisory control, one or more controllers are supervised by a control law on a higher level. The low level controllers perform a specific task under certain conditions keeping a predefined error between desired state and current state, performing a specific control task and being at a specific location of the state space. Supervision is required only if some of the predefined conditions fail : change the set of control parameters or switches from one control strategy to another. Supervisory algorithms are formulated in terms of IF-THEN rules. Fuzzy IF-THEN rules support soft supervision and avoid hard switching between set of parameters or between control structures.

In case of adaptive control, a dynamic system may have a known structure, but uncertain or slowly varying non-linear parameters. Direct adaptive approaches start with sufficient knowledge about the system structure and its parameters. Direct change of controller parameters optimize the system's behavior with respect to a given criterion. Indirect adaptive control methods estimate the uncertain parameters of the system under control on-line and use the estimated parameters in the computation of the control law. Adaptive control audits system performance in terms of stability, robustness, tracking convergence, tuning and optimization of various parameters like scaling factors for input and output signals, input and output membership functions and fuzzy IF-THEN rules.

It is also essential to audit security intelligence of the networking schema of the plant at level L_4: detect threats of internal and external attacks such as cyber, rubber hose attack, sybil, node replication, wormhole, coremelt, forward, blackhole, neighbor, jellyfish and Crypto jacking attack. A real-time monitoring system must audit multi-party corruption at level L_5[e.g. sender, receiver, data, communication channel, mechanism, protocol, process, procedure]. The system administrator should mitigate the risks of various threats through proactive, reactive approaches and sense-and-response against bad luck like the occurrence of natural disaster.

Strategy 4 : SCADA / ICS requires both automated and semi-automated verification mechanisms for intrusion detection.

SCADA / ICS calls threat analytics and a set of model checking algorithms for various phases : exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

There are two different phases : explanatory phase to locate errors and fault finding phase to look for short error trails. Model checking is an efficient verification technique for communication protocol validation, embedded system, software programmers', workflow analysis and schedule check. The basic objective of

the model checking algorithm is to locate errors in a system efficiently. If an error is found, the model checker produces a counter example how the errors occur for debugging of the system. A counter example may be the execution of the system i.e. a path or tree. A model checker is expected to find out error states efficiently and produce a simple counterexample. There are two primary approaches of model checking: symbolic and explicit state. Symbolic model checking applies a symbolic representation of the state set for property validation. Explicit state approach searches the global state of a system by a transition function. The efficiency of model checking algorithms is measured in terms of automation and error reporting capabilities. The computational intelligence is also associated with the complexity of threat analytics equipped with the features of data visualization and performance measurement.

The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? Assess probability of occurrence and impact. The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen?

How can you assess the immunity of ICS against intrusion in the form of sybil, cloning, wormhole or node capture attacks? Traditional intrusion detection techniques may not be able to sense danger signal or perform negative or clonal selection due to non-availability of intelligent threat analytics and ill-defined system immunity. The verification algorithm is expected to detect, assess and mitigate the risks of intrusion attacks more efficiently as compared to traditional approaches since it has a broad vision and adopts a set of AI moves including multi-dimensional view of intelligent reasoning, private search for evidence by balancing breadth and depth optimally and exploring system immunity combinatorially. Another interesting strategy is the use of a rational threat analytics.

Possible functionalities, constraints like computational and communication complexities and systematic features influence the perception of security and trust of a distributed network. For example, the computational power, memory capacity and energy limitations enforce slightly different approaches to the problems of security and privacy in sensor networks. In an open environment, sensor nodes operate without any supervision; a malicious attacker can capture a node for reconfiguration or extract the private data stored in the node through cryptanalysis. An attacker may be able to deploy multiple physical nodes with same identity through cloning or node replication attack. An adversary may be able to deploy multiple identities of a node to affect the trust and reputation of the system through Sybil attack. The attacker may be able to build an additional communication channel to capture private communication through wormhole attack. A key can be compromised either by physical extraction from a captured node or by breach in SMC protocol. The denial of service attack renders a node by overloading it with unnecessary operations and communication and may be able to make the whole network inoperable. Coremelt attacks can target communication links blocking the exchange of useful information. Replay attacks allows an attacker to record messages at one instance and replay it later at different locations.

There are possibilities of blackhole, jellyfish, neighbor and rushing attacks. A blackhole attacking agent tries to intercept data packets of the multicast session and then drops some or all data packets it receives instead of forwarding the same to the next node of the routing path and results very low packet delivery ratio. A jellyfish attacker intrudes into the multicast forwarding group and delays data packets unnecessarily and results high end-to-end delay and degrades the performance of real-time application. A neighborhood attacking agent forwards a packet without recording its ID in the packet resulting a disrupted route where two nodes believe that they are neighbors though actually they are not. Rushing attack exploits duplicate suppression mechanisms by forwarding route discovery packets very fast.

The proposed algorithm explores the concept of next generation Intrusion Detection System (IDS) based on bio-inspired artificial intelligence and immunological theories. The critical challenge of information security is to determine the difference between normal and malicious activities. Traditionally, a distributed system is protected by access control policy that blocks malicious events. Actually, it should be protected by artificial immune systems through automated and adaptive verification mechanisms based on negative selection i.e. self / non-self discrimination, clonal selection and danger signal detection. Different strategic moves are useful for different situations.

A distributed network consists of a set of entities, a broadcast communication cloud and a set of pipes connecting the entities to the communication cloud. The entities can be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities of the distributed system.

Each faulty entity presents one legitimate identity and one or more counterfeit identities to the other entities. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate with each other through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy. This is known as sybil attack [21]. Sybil attacks may affect fair resource allocation, routing mechanisms, voting, aggregation and storage of distributed data by injecting false data or suppressing critical data. A large-scale distributed system is highly vulnerable to Sybil attack; it includes sensor and mobile ad hoc networks, p2p applications and SCADA network.

The basic objective of intrusion detection mechanism is to monitor the actions of the users on distributed network and detect the occurrence of any intrusion. Here the challenge is how to perform negative selection, clonal selection and danger signal detection. Auditing is primarily required to validate the security policies and to review the observed behaviors of distributed applications, users and database. User profiling monitors and analyzes the activities of the users. Data profiling analyzes the managed data. In case of anomaly detection, the data of repetitive and usual behavior of the users is collected and suitably represented as normal profiles. The profile and the activities of the current user is compared with the normal profile. If there is significant mismatch, it indicates an intrusion in the network. It is useful for unknown attack. Misuse detection is useful for known attack. SIVM follows a set of AI moves to detect the risk of intrusion:

(a) *multi-dimensional view of intelligent reasoning* {logical, analytical, case based, forward and backward chaining, probabilistic, predictive, perception based approximation reasoning} for system monitoring;

(b) define system immunity (i) combinatorially. $i = f(a_i,b_i,c_i,d_i,e_i)$; a_i: collective intelligence, b_i: machine intelligence; c_i: security intelligence; d_i: collaborative intelligence; e_i: business intelligence;

(c) *assess system immunity* (S_i) through a hybrid approach in terms of negative selection, danger signal detection, clonal selection and suppression*;*

(d) *verify collective intelligence* in terms of policy, scope, input, output, process, agents, location and system dynamics;

(e) *define collaborative intelligence* (revelation principle);

(f) *evaluate business intelligence in terms of* payment function and incentive;

(g) *monitor machine intelligence* in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For an information system, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states, state transition plans*;*

(h) *check security intelligence in terms of* safety, authentication, authorization, correct identification, non-repudiation, integrity, audit and group, forward and backward privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment).

- Recognise pattern of intrusion attack like sybil, cloning or node replication, wormhole and node capture;
- Sense possibilities and impact of secondary threats such as coremelt, blackhole, jellyfish, rushing, neighbor, replay and shilling attacks;
- Select single or multiple approaches from trusted explicit and implicit certification, robust authentication checking of e-passport, resource testing, auction and incentive based sybil detection game;
- Verify efficiency of cryptographic signcryption algorithms for private communication.

There are various approaches of sybil detection: trusted explicit and implicit certification, robust authentication protocol, resource testing, auction and incentive based sybil detection game [22]. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority can verify computing, storage and bandwidth capability of the entities on periodic basis. A local identity (l) accepts the identity (i) of an entity (e) if e presents i successfully to l. An entity may validate the identity of another identity through a trusted agency or other entities or by itself directly. In the absence of a trusted authority, an entity may directly validate the identities of other entities or it may accept identities vouched by other accepted entities. The system must ensure that distinct identities refer to distinct entities. An entity can validate the identity of other entities directly through the verification of communication, storage and computation capabilities. In case of indirect identity validation, an entity may validate a set of identities which have been verified by a sufficient count of other identities that it has already accepted. But, a group of faulty entities can vouch for Sybil identities.

A *wormhole* attacker records packets at one point in adhoc wireless communication network, tunnels the packets possibly selectively to another point and retransmits them there into the network. The attacker may not compromise any hosts and even if all communication protocols provide authenticity and confidentiality correctly. *Packet leashes* may be used for detecting and defending against wormhole attacks. A leash is any information that is attached with a packet to restrict its maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sending agent. A temporal leash ensures that the packet has an upper bound on its lifetime which restricts the maximum travel distance.

Sensor node attestation verification is an intelligent move to detect intrusion : check if a sensor node is tampered by an adversary; check the configuration and correct setting of each sensor node; detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code. Each node should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each node. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each node. A challenge response protocol is employed between a trusted external verifier and a sensor node.

Each sensor node should be is provided with an 'e-passport' which should have unique identification features like biometric traits. It is an open issue of research: can a sensor node be equipped with traits like unique biometric features of a human being (e.g. voice, fingerprints, retina, vein patterns and facial dimensions)? An e-passport should have unique passport identification number, time stamp (or date of birth), erection testing and commissioning history, location, digital signature of issuing authority and neighborhood data. It is essential to check the authenticity of e-passport data of each sensor node periodically or for specific suspicious cases to detect intrusion. A single move may not be sufficient to detect intrusion.

7. STAFF –RESOURCES

The sixth element of deep analytics is staff-resources which can be analyzed in terms of sources of innovation and roles of electrical and electronics engineering, information technology, IIOT, SCADA, industrial control system, government and collaborative networks and optimal utilization of resources. The innovation demands the commitment of creative experts who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab, academic institutions, service providers of state and central government, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

Traditional scope and approaches of ICS and SCADA operations focus on long-term planning and stability to mitigate various risks. But, complex operation management requires a mix of traditional and agile approaches to cope with uncertainties. The intension driven role develops collaboration. The event driven role integrates planning and review with learning. The other important roles of the system administrators are to prevent major disruptions and maintaining forward momentum continuously. They must acknowledge the emergence of a problem and then try to minimize the frequency and negative impact of unexpected events in a dynamic environment. They must be people oriented, information oriented and action oriented.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. IIOT, SCADA, ICS), research and development, knowledge management, system design and project management. It is essential to teach IIOT, SCADA and ICS in various programmes of Electrical and Electronics engineering and information and communication technology as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep

analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented.

ICS / SCADA operation demands efficient leadership style in terms of optimal resource (5M : man, machine, materials, method, money) allocation and utilization, collaboration and coordination, communication, project management and predictive analytics for analytical and logical reasoning; a set of specific skill set in system administration, technology management, operations management, ERP, SCM, strategic and financial management. It is essential to consider various organizational and human factors such as user awareness of IT and cyber security and overall ICS / SCADA security, transparency in operation and maintenance policies and procedures, threats from disgruntled employees and hackers, weak password protection (e.g. password strength and expiration time), malware protection and external threats in ICS environment (e.g. unauthorized access of ICS / SCADA components).

It is essential to focus on cause-effects analysis of various unwanted occurrences which may affect individuals, system, organization, critical infrastructure, services, environment or the society. It may be possible that the design of old ICS / SCADA technology had not considered the issues of information and cyber security and secure and robust ICS protocols correctly due to specialized hardware and technical skill, proprietary code, protocol standards and operation in closed environment. But, today the system may be connected to the internet directly or indirectly and controlled by HMI interface. There are other organizational factors such as lack of understanding of the cyber security at the levels of executives and chief information security officers, accountability, lack of proper training and ICT security standards and cultural difference between IT and ICS departments. The primary focus of ICS department may be efficiency and safety of operation and process control and less focus on IT and cyber security. Further, there are threats from the perspectives of system architecture, old technology, system design, operation and maintenance and inefficient protocols.

Next, let us focus on support. The system is expected to be *resilient*. The resiliency measures the ability to and the speed at which it can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of ICS to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The system administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in ICS operation? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A system vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map may have four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences.

The system administrator faces a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in system vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.

SCADA is a good solution of resilient, smart and intelligent energy grid. An operationally secure power system is one with low probability of system black out or collapse. If the process of cascading failures continues, the system as a whole or its major parts may completely collapse. It is known as system blackout. This problem can be solved through security constrained power system optimization: system monitoring, contingency analysis and corrective action analysis. The contingency analysis is basically computerized simulation technique: it checks line flow limit violation and bus voltage limit violation by simulating each unit and line outage of the power system model. If it finds any violation, it gives alarm. The blackout problem is related to transient stability; it can be solved by fast short circuit clearing, powerful excitation systems and stability control techniques. Voltage stability is another reason of power system collapse. It is concerned with the ability of a power system to maintain acceptable voltages at all buses in the system under normal conditions and after being subjected to a disturbance. Inadequate reactive

power support from generators and transmission lines leads to voltage instability or voltage collapse. Voltage collapse leads to unacceptable voltage instability in a specific zone. This risk can be mitigated by raising generator voltage, generator transformer tap value, reactive compensation by using shunt capacitors, static VAR system and synchronous condensers, OLTC adjustment and strategic load shedding.

Disaster management plan for a resilient SCADA system is concerned with miscellaneous issues - a set of coordination mechanisms and intelligent priority based resource allocation strategies, organizing disaster management task force during disruption, assessing the expected vulnerabilities approximately, reducing the likelihood of disruptions, collaborative planning for security, building in redundancies i.e. alternative stand-by or back-up system, designing a resilient system and rational investment in training and corporate culture. The SCADA system administrator should develop a business continuity plan for resilience. Collaboration is a strategic tool for developing comprehensive standards of security and safety measures for SCADA system. This is an initiative among all the stakeholders of SCADA system in order to improve the security standards through jointly managed planning, process and shared information.

A special well-trained taskforce should be ready for disaster management during disruption of SCADA system. The first challenge is to detect the root cause of disruption quickly and recognize. The system administrator should isolate the abnormal process or system components from the normal one. Security and safety measures should be layered. Properly layered security measures woven together can reduce the probability of disruption of a complex system where a single security move may not be adequate to provide adequate security. During disruption, a SCADA system may be isolated from the power grid through a set of protection relays. In fact, a system requires preventive maintenance on periodic basis. The maintenance plan and shut down schedule should be published to the public in advance. In case of transient disaster, the public should be alerted in time to avoid the sudden uncertainties. In manufacturing domain, a steel / cement / automotive plant should be shut down for periodic maintenance or production capacity control adaptively; soft start is essential for intentional disruption of continuous production system.

The SCADA system administrator should identify all connections to SCADA network; disconnect unnecessary connections; evaluate and strengthen the security of any remaining connections to the SCADA network; avoid unnecessary services; should not only rely on traditional security protocols; select appropriate vendors and consultants and implement the optimal set of security features; establish strong controls over any medium that is used as a backdoor into the SCADA network; implement intruder detection system; perform technical audits of SCADA network and the associated applications and should conduct physical surveys of all the remote sites connected with SCADA network regularly. The system administrator should identify and evaluate possible attack scenarios; define the role of security and disaster management workforce clearly; document the IT architecture of the security system of SCADA network; define a risk assessment and risk mitigation strategy; determine the basic security requirement of SCADA system; establish effective configuration management process; conduct self-assessments and establish system back-up and disaster recovery plan. Security workforce plays an important role to control various types of chaotic situation near SCADA system. Finally, the security reengineering team of SCADA system requires the commitment and support of the leaders and senior management for proper communication of the security policy (e.g. access control, information disclosure), user training and implementation of SCADA security system. Much of the current SCADA system is outdated, unreliable and insecure having high maintenance cost. New capabilities can enhance efficiency and reliability but also create various types of vulnerabilities. The reengineering of SCADA system should focus on distributed computational intelligence, broadband communication capabilities and robust security infrastructure.

9. CASE ANALYSIS

This section has analyzed three test cases to develop Security Intelligence Verification Mechanism [SIVM] for IIoT enabled SCADA and ICS technology : (a) SCADA for a smart power grid [section 9.1], (b) industrial control system [section 9.2] and (c) defense - border security surveillance [section 9.3].The basic building blocks of SIVM are a set of security protocols [section 9.4] : intrusion verification [section 9.4.1], private communication [section 9.4.2], web security verification [section 9.4.3], biometric access control verification [section 9.4.4]and privacy verification [section 9.4.5]. SIVM is useful to analyze the security element of the deep analytics.

9.1 Test Case 1 : SCADA for a Smart Power Grid

Security Intelligence Verification Mechanism [$SIVM_{PG}$]

System: Intelligent System [Knowledge based system (KBS), DSS/ GDSS, BI]
Input : Sensors data;
Move : Call deep analytics → assess threats on 7-'S' elements;

- **Scope :** SCADA for smart power grid,
- **System :** Information system having computing, networking, data, application and security schema;
- **Structure :** Sensors, central server, connecting link or communication channel;
- **Strategy :**
    - Governance :
        - proactive approach
        - reactive approach
    - Automated system verification and model checking
    - Goal setting : call deep threat analytics
    - Shared vision
    - Intelligent Communication protocol for collaborative and collective intelligence
- **Security** at multiple levels (L1, L2,L3,L4 and L5)
- **Staff:** System administration, technical and maintenance staff, operation team, management consultants;
- **Skill :** technical, management;
- **Style :** Adaptive, resilient leadership style, system coordination, intelligent coordination;
- **Support:** Preventive and breakdown maintenance;

Revelation principle: Audit privacy and confidentiality of critical data based on information disclosure policy.
Payment function: Audit business intelligence of contracts with the service providers.
Verification algorithms [refer section 9.4]**:**

1. Call threat analytics.
2. Do *automated verification* of the security intelligence of data, computing, application, networking and security schema at levels 1,2,3,4 and 5.
3. **Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities**.

Level 1 (data schema):

- Flaws in access control: Authentication, Authorization, Correct identification, Privacy, Audit, Confidentiality, Integrity, Non-repudiation, locking of passwords, false data injection attack;
- Intrusion detection;
- Data warehousing, data mining, data visualization and performance measurement strategy;

Level 2 (computing schema):

- Correctness of computation, system configuration and mechanism
    - KBS :
        - knowledge base, inference engine, user interface, knowledge acquisition and refining subsystem, justifier, workplace;
        - case based reasoning through case base maintenance, case retrieval, case adaptation and learning;
    - **DSS/GDSS :**
        - Intelligence in search of right conditions;
        - Design of possible alternatives;
        - Choice of appropriate action or solution;
        - Implementation in problem solving or exploiting opportunities;
        - Structured / semi-structured / unstructured decision making for operational control / managerial control / strategic planning;
    - **BIS**
        - Detection of incomplete, imprecise, noisy or missing data
        - Inefficient data mining algorithms with flaws in training and testing strategy
        - Flaws in knowledge discovery from data (KDD)
- Fairness in resource allocation;

- Transparency of process, procedure and mechanism;
- Accountability of role in system administration, operation and maintenance;

Level 3 (application schema):

- Poor **system performance** : Denial of Service (DoS) attack, reliability, consistency, resiliency, stability, robustness, liveness, deadlock freeness, lack of synchronization, human error in keying of mobile devices or remote operation;
- flaws in **web application design** : logic attack, cross site scripting, injection flaws, malicious file injection, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication, session hijack, insecure cryptographic storage, insecure web communication, failure to restrict URL access, flaws in application integration;

Level 4 (networking schema): Identify types of malicious attack : internal and external; Cyber attacks, Rubber hose attack, Sybil attack, Node replication attack, Wormhole attack, Coremelt attack, Forward, Blackhole, Neighbor, Jellyfish, Crypto jacking on mobile devices;

Level 5 (security schema):

- Assess the risk of multi-party corruption (e.g. sender, receiver, data, communication channel, mechanism and protocol);
- Business intelligence of payment function

Risk mitigation:

- **Proactive approach**
  - Call predictive analytics; analyze probability of occurrence vs. impact;
  - Call challenge response protocol;
  - Preventive maintenance, Technology upgradation, System isolation
- **Reactive approach**
- **Sense-and-response against bad luck**
  - Natural disaster : Heavy rainfall, snowfall, storm, cyclone, flood, earthquake;
  - Industrial / HR unrest / Political strike
  - Accidents
  - Terrorism

3. Adjust device settings automatically.

Output: SCADA performance scorecard; security intelligence.

9.2 Test Case 2: Industrial Control System

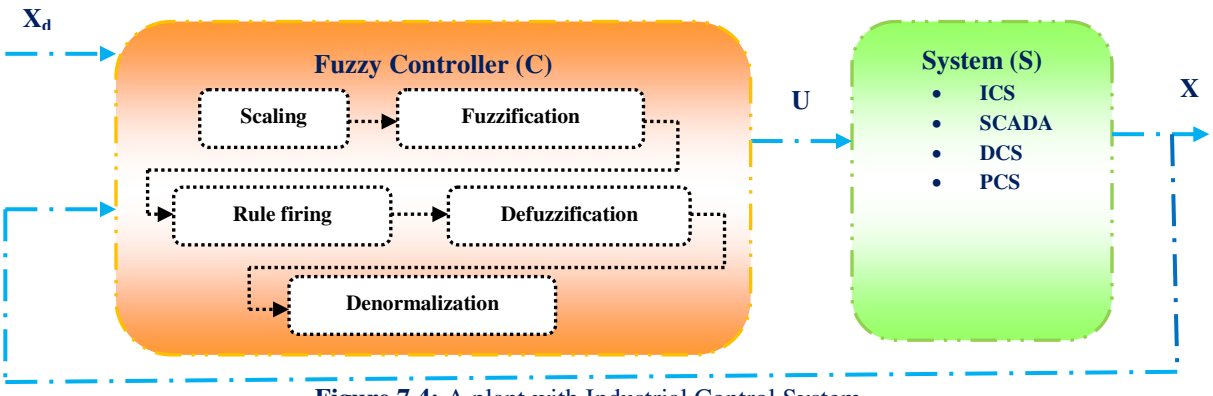


Figure 7.4: A plant with Industrial Control System

Security Intelligence Verification Mechanism [$SIVM_{ICS}$]

System: Industrial Control System;

Input : Sensors data;

Move : Call deep analytics --> assess threats on 7-'S' elements;

- **Scope :** Supervisory, adaptive, fuzzy control of industrial plant
  - Linear model

- Nonlinear model

- **System :** Computing, Networking / Communication, Data, Application and security schema;
- **Structure :** Sensors, central server, connecting link, system, fuzzy controller;
- **Strategy :**
  - Governance : proactive and reactive approach, intelligent secure communication protocol, shared vision, goal setting
  - Automated system verification and model checking
- **Security-sensitivity** at multiple levels
- **Staff:** System administration, technical and maintenance staff, operation team, management consultants;
- **Skill :** technical, management,
- **Style :** Adaptive, resilient leadership style, system coordination, intelligent coordination;
- **Support** : Preventive maintenance, breakdown maintenance.

Revelation principle: Audit privacy and confidentiality of critical data based on information disclosure policy.

Payment function: Audit business intelligence of contracts with the service providers.

Verification algorithms [refer section 9.4];

1. Call threat analytics.
2. Do *automated verification* of the security intelligence of data, computing, application, networking and security schema at levels 1,2,3,4 and 5.

3. Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities.

Level 1 (data schema): Authentication, Authorization, Correct identification, Privacy, Audit, Confidentiality, Integrity, Non-repudiation, locking of passwords, false data injection attack, intrusion detection through access control;

Level 2 (computing schema):

- **Correctness of computation [Reference : Figure 7.4]**
  - **Input scaling i.e. normalization /*** For a MISO, $x_1, x_2,\ldots,x_n$: controller inputs in IF part of fuzzy rules; $u_1,u_2.,,,,u_m$: controller outputs in the THEN part of fuzzy rules ; Input scaling $E_n = N_e.e$; $E = (e_1,e_2,\ldots e_n)^T$; $E_i = x_i\text{-}x_d$; N_e = normalization of factors ***/**
  - **Fuzzification of controller input variables /*** During fuzzification, a crisp controller input x* is assigned a degree of membership to the fuzzy region from IF part of a fuzzy rule***/** $\mathbf{E^* = e_1^*, e_2^*,\ldots e_n^*; e^*}$ **:** a normalized crisp controller input. $LE^j = LE^j_{11},\ldots,LE^j_n)^T$ LE^j_n : Fuzzy values taken by the controller inputs
  - **Inference i.e. rule firing /*** For a MISO FC, i^{th} fuzzy rule - R^j_c: IF e = LE^j THEN u = LU^j***/**
  - **Defuzzification of controller output variables /*** Obtain a scalar value u from membership function CU(u) where U : defuzzified controller output ***/**
  - **Output scaling i.e. denormalization : $U_N = N_u.u$; /*** The defuzzified normalized controller output U_N is denormalized with the help of an off-line predetermined scalar denoralization factor N_u^{-1} ***/**
- Fairness in system performance,
- Transparency of process / procedure / mechanism.,
- Accountability in system administration, operation and maintenance;

Level 3 (application schema)**:**

- Stability in system performance, robustness, accuracy and speed
- Reliability, Consistency, Resiliency, Liveness, Denial of Service (DoS) attack, Deadlock freeness, Lack of synchronization,
- Human error in keying of mobile devices or remote operation;
- Flaws in application integration;

Level 4 (networking schema): Identify types of attack : internal and external; Cyber attacks, Rubber hose attack, Sybil attack, Node replication attack, Wormhole attack, Coremelt attack, Forward, Blackhole, Neighbor, Jellyfish, Crypto jacking on mobile devices;

Level 5 (security schema) : multi-party corruption [e.g. sender, receiver, data, communication channel, business intelligence in terms of payment function, mechanism, protocol, process, procedure];.

Risk mitigation:

- **Proactive approach**
  - Call predictive analytics; analyze probability of occurrence vs. impact ;
  - Call challenge response protocol;
  - Preventive maintenance, technology upgradation, system isolation
- **Reactive approach**
- **Sense-and-respond against bad luck such as** natural disaster, accidents and terrorism

3. Adjust device settings automatically.

Output: SCADA performance scorecard; security intelligence.

9.3 Test Case 3 : Defense – Border Security Surveillance

This is a great challenge to the SCADA system administrator, power system planners, analysts, researchers and operators to sustain security and safety of a smart, intelligent energy grid. The proposed verification mechanisms and resilient SCADA are also applicable in sensor networks for defense application, automated continuous production plants, refineries, oil and gas pipelines. For instance, the defense security system of a country I tries to monitor the activities and the movement of the security force, tanks, war ships and weapons manufacturing plant of a neighboring country C by deploying a SCADA network [Figure 7.5]. A base station is built at a strategic location to control the SCADA network; the sensors relay critical data to the base station. The adversary i.e. the defense security system of country C may be able to launch different types of attacks such as sybil attack, physical destruction of sensor nodes, resource consumption attack to deplete the limited energy of the sensors and the attack on routing and data link protocols associated with the defense information and communication system of country I.

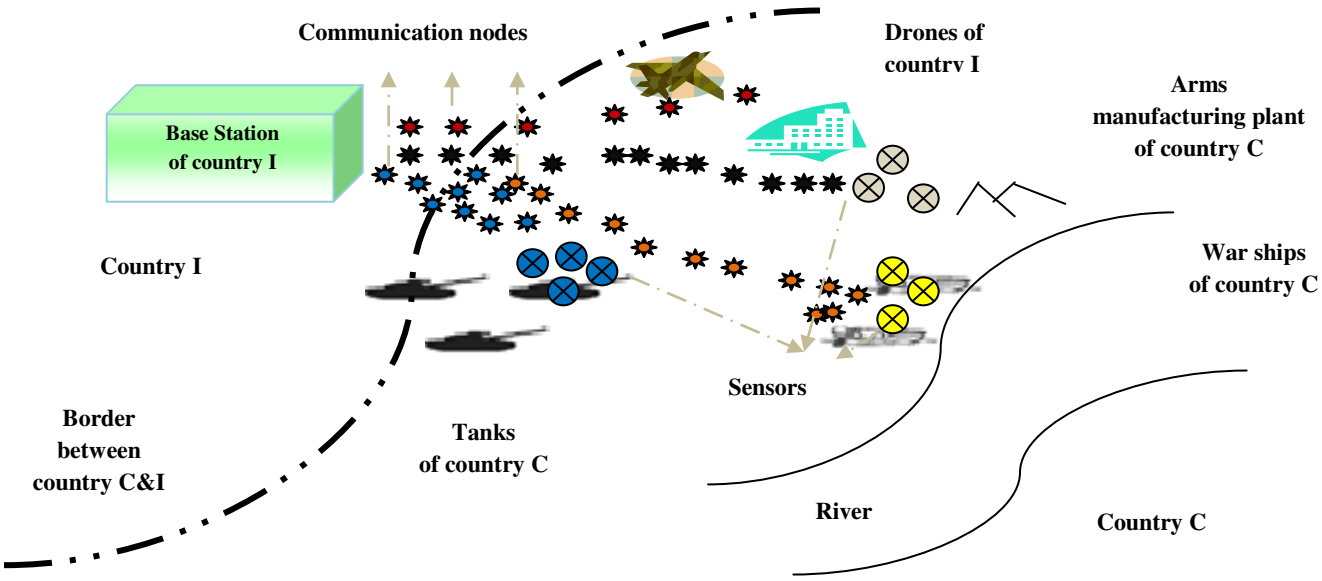


Figure 7.5 : Border security surveillance

The defense system of country I may face the threat of foreign computer hackers who can dismantle the power grid, transportation system, financial networks and e-governance system. The adversaries may try to gain control of critical switches; may derail passenger trains, contaminate the water supply in major cities or shut down the power grid. Actually, country I requires new standards for critical public and private infrastructure facilities like power plants, water treatment plants and gas pipelines where a breach of security could cause significant economic damage. The recent wave of cyber attacks on various financial institutions and oil companies globally should be recalled in this context. A smart, resilient SCADA system can protect the critical infrastructure of a country through a set of efficient verification mechanisms. There is scope of future works on miscellaneous web security issues [25].

Security Intelligence Verification Mechanism [$SIVM_D$]

System: Defense SCADA;
Input : Sensor data;
Move : Call deep analytics → assess threats on 7-'S' elements;

- **Scope :** Private defense communication;
- **System :** Information system associated with SCADA such as computing, networking, data, application and security schema;
- **Structure :** Sensors (e.g. mobile sensors - drones, Unmanned Aerial Vehicle [UAV], static sensors – CCTV camera), base station server, communication channel;
- **Strategy :**
  - Governance :
    - proactive approach
    - reactive approach
  - Automated system verification and model checking
  - Shared vision on privacy and revelation principle
  - Intelligent communication protocol for collaborative and collective intelligence
- **Security :** audit security intelligence at multiple levels $L_{1\text{-}5}$;
- **Staff:** System administration, technical and maintenance staff, operation team;
- **Skill :** technical (e.g. electronics, communication, computer, electrical, mechanical), management information system, system maintenance, military operation;
- **Style :** Dynamic leadership style for efficient system coordination;
- **Support:** preventive and breakdown maintenance.

Revelation principle: Audit privacy and confidentiality of critical data based on information disclosure policy.
Payment function: Audit business intelligence of contracts with the vendors and service providers.
Verification algorithms [refer section 9.4];

1. Call threat analytics → assess threats on private defense communication channel;
2. Adopt risk mitigation strategies to ensure private defense communication :
   - **Proactive approach**
     - Call predictive analytics → analyze probability of occurrence vs. impact;
     - Call challenge-response protocol;
   - **Reactive approach :** interleaved hop-by-hop authentication; **Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities**.
   - **Sense-and-respond against bad luck** such as natural disaster, military revolution, political strike, accidents and terrorism.
3. Verify security intelligence of data, computing, application, networking and security schema of defense SCADA at levels 1,2,3,4 and 5.

Level 1 (data schema):

- Detect flaws in access control : confidentiality, data integrity, non-repudiation; authentication, authorization, correct identification, privacy and audit; false data injection attack;
- Intrusion detection;
- Compromising data warehousing, data mining, data visualization and performance measurement strategy;

Level 2 (computing schema):

- Correctness of computation
- Fairness in resource allocation
- Transparency of process, procedure and mechanism
- Accountability of role in system administration, operation and maintenance

Level 3 (application schema):

- Poor system performance : Denial of Service (DoS) attack, reliability, consistency, resiliency, liveness, deadlock, human error in remote operation of drones;
- Flaws in web application schema (e.g. session hijack, application integration);

Level 4 (networking schema): Assess the risk of coremelt attack causing traffic congestion, delay in communication due to forward, blackhole, neighbor and jellyfish attack, cyber, rubber hose, sybil, node replication and wormhole attack;

Level 5 (security schema):

- Assess the risk of multi-party corruption of one or more entities involved in private defense communication (e.g. sender, receiver, data, communication channel, mechanism and protocol) by adversaries;
- Assess the risks of *insider attack*
    - Ensure privacy of the route and time of travel of the military convoy without any leakage of information.
    - Different time of travel of military and civilian convoy without any mix of the two traffics.
    - A pilot convoy should audit and check the clearance of route through drones.
    - Decomposition of a large convoy into smaller units
    - Intrusion detection through detectives and countermeasures
    - Be alert on false data injection attack.
    - Execute DoS attack on communication services to restrict false data injection attack (if necessary)./*caution : violation of human rights in healthcare and emergency services*/

Output: security intelligence of defense communication network.

9.4 Security Protocols

9.4.1 Intrusion Verification Mechanism

System : *SCADA* states (local, global, initial, goal), state transition relation;
Input : A self-set S $\subseteq$ U, a monitoring set M $\subseteq$ U for a given system parameters;
Output: *f*or each element $m \in M$, either self or non-self, danger or normal;
$D \leftarrow$ set of detectors that do not match any $s \in S$;
for each $m \in M$ do
{
call threat analytics (A) $\rightarrow$ sense danger signal ;
secure function evaluation $\rightarrow$ verify innate and adaptive system immunity (i) = f(a,b,c,d,e);
check e-passport, computing, storage and resource capacity in real-time;
}
sense-challenge-respond to system immunity resiliently;
if m matches any detector $d \in D$ then identify m as non-self;
else identify m as self;
check if non-self suspicious node is benign or malign danger node;
if it is malign then suppress it else give alert.
AI Moves *:*
a. *Multidimensional view of intelligent reasoning* (logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative, perception);
b. *Define system immunity* (i) = f(a,b,c,d,e); a: collective intelligence, b: machine intelligence, c: security intelligence, d: collaborative intelligence, e: business intelligence; f: secure verification function.
c. *Private search for evidence*;

An intrusion is considered as an activity that violates the security policy of a system. Intrusion detection systems are based on the assumption that the behavior of an intruder is different from that of an authorized user and the unauthorized activities can be detected by analyzing user's profile and activities, host based IDs, network based IDs and application based IDs. Auditing is required at different levels of granularity for the detection of misuse and anomaly. An intruder tries to gain access to an unauthorized system to which it has no legitimate access. It occurs by exploiting system vulnerabilities or by simply cracking the user ids and passwords of legitimate users. If a malicious agent is able to access the system, it is considered as an authorized user and is granted the access rights of the user. The basic objective is to effectively detect and

prevent insider misuse. Intrusion may occur in various forms on a distributed network such as sybil, cloning or node replication, wormhole denial of service, key interception and node capture. The following section presents intrusion verification mechanism (IVM).

9.4.2 Private Communication

Defense SCADA System architecture : MTU: Defense base station i.e. master terminal unit; u: Communication nodes of defense network; v: sensor nodes; L: Leader of a cluster of sensor nodes; n: Number of hops between MTU and L; u_i: Upper association node; u_j: lower association node; k_u: Signcryption key of node u shared with MTU; k_{uv}: Pairwise signcryption key shared between nodes u and v; k^t_v: Time-stamped authentication key of node v; M (k,m) : Authenticated message m signcrypted with a key k.

*call challenge response protocol for *device attestation* verification → check whether a sensor node is tampered by a malicious agent;
check the *configuration* and correct setting of each sensor node → detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code;
check state variables and measure bad data against *false data injection* attacks; verify authentication in private communication between sensor nodes and base station or MTU;
do network traffic congestion analysis → assess the risk of *coremelt* attack;
do *multicast* traffic analysis → detect rushing, blackhole, neighbor and jellyfish attacks; check group, forward and backward privacy in secure group communication.

Let us consider test case 3 of private defense communication. It is very important to verify the privacy and security in SCADA communication. A malicious agent can exploit the configuration of a defense network to launch false data injection attack against state estimation and introduce arbitrary errors into certain state variables while bypassing existing techniques for bad measurements detection. Reliable SCADA operation requires system monitoring based on precise measurements of bus voltage, real and reactive power. These measurements are transmitted from the measuring instruments to SCADA. State estimation is used in system monitoring to estimate the best state by analyzing measured data and various system models. The output of the state estimation is used in contingency analysis. A malicious agent can compromise the measuring instruments to inject errors. Here, the real challenge is to detect bad measurements. If the malicious agent knows SCADA configuration, it can systematically generate bad measurements which can bypass the common assumption that the square of difference between observed and estimated data becomes significant during bad measurements. The attacker may try to inject arbitrary errors in certain state variables or aims to find an attack vector as long as it can result a wrong estimation of state variables. Real-time system monitoring is essential to ensure reliable operations of SCADA against false data injection attack. The adoption of communication equipments manufactured by foreign vendors may be a risky option in secure communication, it is an open debatable issue.
Device attestation verification is a critical requirement of a smart SCADA. It securely ensures whether a sensor node or remote terminal unit or any other device associated with SCADA network is tampered by a malicious attack. Each device should be attested with a valid digital test certificate. This certificate indicates the identity of the manufacturers, model number, serial number and tampering status of each device. SCADA must verify the identity and tampering status of each associated device. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each device. The digital test certificate defines the basic security requirements of service provider and device manufacturer in terms of mutually acceptable security policies, certificate formats, naming convention and operational issues [18]. It should aid the deployment of system, operation, system audit, signing and revocation of certificate. Each device should be able to authenticate and authorize other devices without the support of backend security server. A malicious agent may be able to compromise a set of remote terminal units; it may be able to access the compromised RTUs and may launch a coordinated attack by modifying the software of the RTUs. It is also possible for the attacker to hide the attack by reporting correct data to the master terminal unit.
CSVM assumes that SCADA control center knows the exact hardware configuration of the sensor node or RTU like CPU model, CPU clock speed and the memory configuration. The hardware of the RTU is not

corrupted. There is a secure authenticated communication channel between RTU and external verifier. The adversary can control the software and the operating system of RTU; it can access RTUs directly over the Internet or by compromising different devices of SCADA control center. There is at least one trusted external verifier at the SCADA control center which cannot be compromised by the malicious attacker.

A challenge response protocol is employed between a trusted external verifier and RTU [21]. The external verifier sends a random challenge to the RTU. A self checking verification function on RTU computes a checksum over its own instructions and returns the result to the external verifier. If an adversary tampers with the verification function, either the computed checksum will be incorrect or there will be significant increase in computation time. If the external verifier receives the correct checksum within the expected time, it is concluded that the verification function code on RTU is unaltered. The verification function includes a cryptographic hashing function which computes a hash of RTU's memory. The external verifier compares the computed hash with the expected hash to ensure that the device has not been modified. Alternatively, a hash may be computed over a known executable to ensure that it has not been modified.

*False data injection attack***:** The verification mechanism starts with a*uthentication certificate allocation.* SCADA administrator assigns each sensor and communication node an authentication certificate which is a unique ID endorsed with a bootstrapping time. Next step is *neighborhood search.* After the deployment in SCADA network, each new node handshakes with each of its neighbors by establishing a one-hop pair wise signcryption key. Each sensor node handshakes with the leader (L) and each communication node handshakes with the leader / other communication node / MTU. A node validates the IDs and time-stamps of its associated nodes with the help of MTU periodically. Then q number of sensor nodes *sense* the process variables collaboratively when they detect the occurrence of an event of interest. The leader collects the signcrypted data from all participating sensor nodes; unsigncrypts the signcrypted data; wraps them into a message (m) and forwards m to MTU through a set of communication nodes. Next step is relay; each forwarding communication node verifies the message code computed by its lower association node and then unsigncrypts the received message. If the verification fails; it drops the message and informs the instance to MTU. Otherwise, it computes a new message code based on its pairwise signcryption key shared with its upper association node. Finally, it forwards the message to the next node towards MTU. Finally, MTU verifies the message received from the communication node. If MTU detects that q nodes have endorsed the message (m) correctly, it accepts m otherwise discards m.

The basic objective of CSVM is to authenticate each communication node in the SCADA and also to know other valid communication nodes (neighbors) present in the system. A time stamp is involved in the authentication mechanism. The base station system administrator (SA) of SCADA network allocates a certificate to each node and it includes both ID and bootstrapping time to authenticate the identity of a new node. In the certificate, the ID and timestamp are signed by the private key of SA. When a new node is deployed in the SCADA, it shows its certificate to its neighbors. The neighbors can verify the certificate of the new node with the public key of SA. A new node can be accepted into the SCADA if it has a correct identity and a valid time-stamp.

Next, let us consider *Coremelt attack* where the malicious attackers send traffic between each other and not towards a victim host. It is a powerful attack since there are $O(N^2)$ connections among N attackers which can cause significant congestion in core SCADA network. SCADA networks often use web service to enable coordination among physical systems. The malicious attackers are able to flood the end hosts with unwanted traffic to interrupt the normal communication. This is a specific type of Denial-of-Service (DoS) attack where the network link to SCADA server is congested with illegitimate traffic such that legitimate traffic experiences high loss and poor communication performance. Such a poor connectivity between SCADAs can damage critical infrastructure with cascading effect. To address such attacks, it is important to identify the source of excessive traffic and prioritize legitimate traffic. The attackers often rely on distributed denial of service attacks where many subverted machines i.e. botnets are used to generate illegitimate traffic. There are three steps to launch a Coremelt attack [25]. First, the attackers select a link in the SCADA network as the target link. Then, they identify what pairs of subverted machines can generate traffic that traverses the target link. Finally, they send traffic between the identified pairs to overload the target link. Thus, the attacker uses a collection of subverted machines sending data to each other to flood and disable a network link. An efficient SCADA should allow end hosts to identify long-running legitimate traffic. During heavy load, the router forward packets with proper priority and capabilities while dropping packets without capabilities. SCADA requires an efficient tracing and network traffic monitoring system to avoid this attack.

Next let us discuss *multicast attack.* The communication schema of SCADA should support message *broadcasting* and *multicasting*. SCADA may have thousands of sensor nodes or remote terminal units. Therefore, multicasting is a critical requirement of secure SCADA communication. The number and size of keys to be stored in a remote terminal unit should be limited due to memory constraint. The computational and communication cost is O(n) where n is the number sensor nodes or remote terminal units. In SCADA network, actual addition or deletion of a sensor node occurs rarely since the system is commissioned based on a long term plan. But, the remote nodes may be easily compromised by the malicious agents. It needs an efficient *key management mechanism* to preserve group key, forward and backward privacy [15,16]. *Group key privacy* is computationally infeasible for an adversary or malicious agent to discover any group key of SCADA. *Forward privacy* prevents a user which has already left from the SCADA group from accessing future communication within the group all the keys along the path from the leaving point to the root node of the key tree should be changed. It ensures forward privacy. *Backward privacy* prevents a user from accessing past communications of SCADA group, all the keys along the path from the joining point to the root node of the key tree should be changed. The protocols for key management of secure group communication such as join, leave and sub-group change can be found in [37,38,39].

9.4.3 Web Security Verification

Application: Web enabled SCADA; Agents: User of the web application, system administrator;
verify the *design flaws* in service oriented computing schema.
logic attack : check the main flow, sub flows and exception flows as per business rules of the application;
cross site scripting: check whether all parameters of the web application are validated properly; check the risk of phishing attack;
injection flaws : check whether user data modify the meaning of command and queries sent to any interpreters invoked by web application;
malicious file injection : check the use of dangerous application programming interfaces by testing and code review;
insecure direct object reference : check through code review whether the web application allows direct object references;
cross site request forgery : check whether web application generates authorization token that is not automatically submitted by the web browser;
information leakage and improper error handling: check whether web application leaks any data through error messages; check whether the application builds a trusted computing environment;
broken authentication and session management: check through code review whether the web application properly authenticates users and protects their identities and credentials;
insecure cryptographic storage: check whether web application properly encrypts sensitive data; check configuration of the web server;
insecure web communication: check whether the web application ensures private communication between the sending and receiving agents; assess the risk of snooping;
failure to restrict URL access : check whether proper access control is enforced at the presentation layer and business logic for all URLs in the web application;

The web security verification mechanism (WSVM) verifies service oriented computing schema to mitigate the risk of common vulnerabilities. WSVM addresses a set of dangerous attacks against web enabled distributed computing system [36]. The basic objective of WSVM is to protect SCADA from phishing attacks, privacy violations, identity theft, system compromise, data alternation, data destruction, financial and reputation loss. Cross site scripting (XSS) flaw allows an attacker to execute malicious code in the web browser of the user that can hijack user session, deface websites, possibly introduce worms or insert hostile content or conduct phishing attack and take over the browser of the victim through malware. The best protection of XSS is a combination of validation of all incoming data and appropriate encoding of all output data. Validation allows the detection of XSS attacks and encoding prevents injection of malicious script into the browser. Cross site request forgery (CSRF) forces the web browser of the logged on user to send a request to a vulnerable web application which forces the victim's browser to perform a hostile action. Web applications rely solely on automatically submitted credentials such as session cookies, basic authentication credentials, source IP address, SSL certificates or windows domain credentials. CSRF is applicable to any web application that has no authorization checks against vulnerable actions.

Injection flaws allow the attacker to create, read, update or delete any arbitrary data available to the application. Even, it may compromise the web application completely bypassing firewalled protection. SQL injection occurs when the data input of the user is sent to an interpreter as part of a command and query. The hostile data of the attack forces the interpreter to change the data or execute unintended command. The common protection measures are to use strong and safe interpreters, do input validation, use strongly typed parameterized query APIs, enforce least privileges, avoid detailed error messages, use stored procedures, do not use dynamic query interfaces and do not use simple escaping functions.

Web application developers often trust input files improperly and the data is checked insufficiently. Arbitrary, remote and hostile content may be processed or invoked by the web server. It allows an attacker to perform execution of malicious code, installation of tool kit and system compromises remotely. Flawless design is required during the construction of system architecture, design and software testing. The application developers should use indirect object reference map, check errors, validate user's input and implement firewall rules appropriately. Another critical problem is insecure direct object reference; a direct object reference occurs when a reference is exposed to a file, directory, database records or key as a URL or form parameter. A malicious agent can manipulate these references to access other objects without authorization. The web application should avoid exposing direct object reference to the users by using an index, indirect reference map or other indirect validated method that is easy to validate.

An web application can unintentionally leak information about their configuration, internal state or violate privacy through error messages and it can launch dangerous attacks. The application should get support from a standard exception handling mechanism to prevent the leakage of unwanted information; detailed error handling should be limited; errors should be properly checked and should not be exploited by the intruders. Broken authentication and session management is caused due to the failure of protection of credentials and session tokens. It can hijack user's or administration's accounts, undermine authorization and accountability controls and cause privacy violations. The common protective measures are the adoption of efficient authentication mechanisms, secure communication and credential storage, use of efficient session management mechanisms; invalid session identifiers should be rejected.

Insecure cryptographic storage is caused due to the failure in encrypting sensitive data; it leads to disclosure of sensitive data and compliance violation. It is required to avoid inefficient weak cryptographic algorithms and check whether sensitive data are encrypted properly. An web application may fail to encrypt network traffic to protect sensitive communications. The adversary can sniff traffic from the communication network and access sensitive data, credentials, authentication or session token. The application should properly encrypt critical data. The only protection for a URL is that links to a page are not presented to unauthorized users. The adversary may get access to these pages and view private data. All URLs and business functions should be protected by an effective access control mechanism. Web security is a very broad topic; some common critical issues have been discussed above very briefly. There are several open issues in the design of service oriented computing schema. It is an interesting option to interview Internet experts, web developers and programmers and analyze the complexities and challenges in web programming issues.

9.4.4 Access Control

Biometrics are used for automated recognition of SCADA users and system administrators based on their biological and behavioral traits such as finger prints, face image, iris and voice. Traditional authentication methods like passwords and identity documents may fail to meet reliable security and performance of identification systems. Some physical and behavioral attributes of human beings are uniquely associated with an individual. Biometrics captures these traits with sensors; represent them in digital format; compare the recorded data with the data acquired from the same user previously and performs recognition [33]. Biometrics are applicable to VISA verification for regulating international border crossing, welfare distribution, access control at airport and power plant's control room, access control to shared resources and information, remote financial electronics transactions and distribution of social welfare benefits.

SCADA may be attacked at any point such as host or MTU, RTU, communication node or sensor node. It should be protected by a robust access control mechanism. Access control is the process of receiving the requests of the users for specific resources and data and determining whether the request should be granted or denied. The access control system is a combination of access control policy, model and mechanism. Access control may be based on user's identity or role or the regulatory constraints as defined by the system administrator. Credential based access control grant or deny access to the resources by exploiting

digital certificates and make access decisions on the basis of a set of properties that the client should have fulfilled [8]. This trust negotiation process may suffer from privacy problem since the SCADA server discloses its access control policy entirely and the client exposes its credentials certificates to gain access to a resource. An efficient negotiation strategy should restrict the disclosure of information. The service accessibility rules specify the necessary and sufficient conditions for accessing a resource while credential disclosure rules define the conditions that govern the release of credentials and declarations. The SCADA server should discloses the minimal set of policies for granting access while the client releases the minimal set of certificates to access the resource. Prerequisites are the conditions that must be satisfied for a service request. Requisites are conditions that allow the service request to be successfully granted. The SCADA server should not disclose a requisite rule until the client satisfies a prerequisite rule. Biometrics can be also used for credential based access control of distributed computing systems.

Agents: Client (C), SCADA server (S);
check the correctness of *enrollment* and *recognition* mechanisms for biometric access control;
C requests S for the access to a resource r such as data or application;
S requests C for prerequisites;
C informs prerequisites to S;
S requests for requisites to C;
C informs requisites to S;
S verifies the credentials provided by C;
if the verification is true, then S grants C the access to r;
else S asks C the required credentials;
C selects the requested credentials (if possible) and informs S;
S verifies the credentials of C;
if the verification is true, then S grants C the access to r;
else S rejects the request of C;
intrinsic failure: check false match, non-match and failure to enroll or acquire biometric data;
adversary attacks: check collusion, coercion, negligence, enrollment fraud, exception abuse;
infrastructure attacks: check sabotage overloading, attacks on user interface, system modules, databases and interconnections, modification of data and information leakage, spoofing, impersonation, man in the middle attack, replay and hill climbing.

Credential based access control strategy grants or denies access to the resources based on biometric prerequisites and requisites as specified by the client during trust negotiation process.

BACVM mechanism verifies the security intelligence of a biometric access control system associated with SCADA [34,35]. It basically explores the risks of various threats on biometric access control. A *User* presents his or her biometric identity to a biometric system for the purpose of being recognized. Biometric systems can be used efficiently for authentication, nonrepudiation and identity recognition claim. Biometric recognition is the science of establishing the identity of the user based on his or her physical and or behavioral characteristics either in fully automated or a semi-automated way. A biometric system measures one or more physical or behavioral traits such as finger print, palm print, face, iris, retina, ear, voice, signature, gait, hand vein, odor or DNA information of an individual to determine or verify his identity. These characteristics are known as traits, indicators, identifiers or modalities. The biometric mechanism has two phases – enrollment and recognition [33]. During enrollment, biometric data is acquired from the individuals and stored in a database along with the person's identity. During recognition, biometric data is acquired from the individual and compared with the stored data to determine the identity of the user.
The failure to a biometric system is basically a security threat - denial of service (DoS), intrusion, repudiation and function creep. The legitimate users may be prevented from obtaining access to the information assets. An unauthorized user may gain illegitimate access to the system and this intrusion affects the basic integrity of the system. A legitimate user denies the usage of system or data after having access to it. Corrupted users may deny their actions. An adversary may exploit the biometric system for different function. The biometric system may fail due to flaws in enrollment and recognition mechanisms. It may also fail due to manipulation by adversaries which could either be insider or external entities. External entities may be imposters and attackers. Insiders may be system administrators or legitimate corrupter users. Insider attacks may be collusion, coercion, negligence, enrollment fraud and exception

abuse. Infrastructure attacks may be due to sabotage overloading; it may be attacks on user interface, system modules, interconnections and template databases. Attacks on user interface result impersonation spoofing alternation. Attacks on system modules cause modification and exploit faults. Attacks on interconnections cause man-in-the-middle, replay or hill climbing. Attacks on template database result modification and leakage of critical sensitive data.

An adversary may attack human element or system infrastructure associated with a biometric system. The system administrators may do mistakes in enrollment, disenrollment of users or in adjustment of security parameters controlling the performance of a biometric system such as threshold on match scores and minimum limits on the quality of acquired biometric sample. The administrator may do mistakes and breach the security of biometric system. In case of collusion, an authorized user willingly turns malicious and attacks the system either individually or in collaboration with external adversaries. A coerced user does not carry out any attack willingly. An authorized user is forced to turn malicious through physical threat or blackmail. External attackers can also exploit the negligence of authorized users such as log out of the system after completing transactions. In case of enrollment fraud, an adversary may be able to enroll into the biometric system illegally with a false identity and credentials. The system administrator should detect a duplicate identity by matching the biometric traits of a new user against the traits of all enrolled users. Another critical issue is exception abuse where exceptional situations may cause denial of service to legitimate users. It may be the failure of hardware and software components of a biometric system or poor quality of data (e.g. noise, missing data) during enrollment phase.

An adversary may attack the functional modules of a biometric system infrastructure such as sensor, extractor, template database, matches or attacks at the interface of the modules and decision modules. The common types of attacks are overloading and sabotage. A malicious agent may cause physical damage to one or more components of the biometric infrastructure such as putting off power supply, damaging of sensor interfaces or introducing excessive noise that affects the normal operation of biometric system. An imposter may attempt to intrude the biometric system by posing himself as an authorized user either casually or targeted way. The imposter does not modify his biometric traits in the first case. In the second case, the imposter may target an identity whose biometric characteristics are known to be similar to its traits. The imposter may execute mimicry attack by modifying his biometric characteristics. It may adopt the strategy of obfuscation by changing biometric characteristics to avoid detection. It is mainly applicable in negative recognition applications. Obfuscation can be done by presenting a poor quality image or noisy biometric sample. The solution is to improve the robustness of biometric algorithm.

Spoofing is the most common attack at user interface level and it involves the presentation of spoof biometric trait. A spoof is any counterfeit biometric that is not obtained from a live person. It includes the presentation of fake or artificial traits such as gummy finger, thin film on the top of a finger, recorded voice or mask of a face. If the sensor is unable to distinguish between spoofed and genuine biometric traits, an adversary can easily intrude the system under a false identity. Spoof detection is done through liveness detection by checking the signs of human vitality or liveness through blood pulse. Spoofing can be done by directly colluding with or coercing an authorized user, covert acquisition, hill climbing attacks or stealing the biometric template from the database. For spoof detection, common psychological properties used include pulse rate, blood pressure, perspiration, spectral or optical properties of human skin, electrical conductivity of human tissues and skin deformation. A malicious agent can subvert biometric processing by directly undermining the core functional modules of a biometric system such as signal processing or pattern making algorithms or by manipulating the communication between these modules. Template database can be hacked or modified by an adversary to gain unauthorized access or to deny access to legitimate users. There may be leakage of stored biometric template information due to lack of strict database access control.

The biometric system is a costly option in information security management; it requires complex data schema in terms of data warehousing and data structure. It ensures non-repudiation authentication and integrity, only legitimate or authorized users are able to access physical or logical resources protected by it. The imposters cannot access the protected resources or information. Another important issue is availability where authorized users must have timely and reliable access to the protected data. It also ensures confidentiality; it must be used for the intended functionality i.e. credential based access control. A user can be recognized by what he knows (e.g. passwords, PIN or cryptographic key), what he possesses (e.g. passport, driving license, mobile phone, ID card) and who he is intrinsically (e.g. inherent physical and behavioral characteristics). The proliferation of web based services and deployment of distributed computing systems have led to the risks of identity theft significantly. Facial recognition software, voice recognition system and digital fingerprint or palms scanning are emerging trends of biometrics. The traits

such as fingerprints, retina, vein patterns and facial dimensions are generally considered unique user profile but these features may be associated with a fake user ID intentionally or by mistake during registration process. Biometric data management should take care of user privacy and institutional convenience simultaneously.

9.4.5 Privacy Verification

Agents: Client (C), SCADA / ICS administrator;
Input: Query for sensitive sensor data (q);
Output : Private sensor data (d^p_s);
C→SCADA: q;
SCADA: Retrieve sensor data (d_s); Call move (M_i) for privacy preserving data mining;

- M_1: Suppress d_s partially;
- M_2: Randomize d_s;
- M_3: Achieve k-anonymity through generalization, suppression, de-identification;
- M_4: Summarize or aggregate d_s;
- M_5: Replace d_s with a small sample;
- SCADA→ C: d^p_s ;

Verify the performance and efficiency of algorithms: encryption, decryption, digital signature, digital certificate, signcryption;
Verify the degree of information leakage in inference control.

PVM preserves the privacy of SCADA data through efficient secure multi-party computation and privacy preserving data mining.
A client interacts with SCADA through enterprise applications or web; submits simple or complex queries and searches for intelligent information. A malicious agent may be able to attack SCADA server during this communication between sending and receiving agents. PVM tries to protect sensitive data from unsolicited or unsanctioned disclosure of SCADA data by calling different statistical disclosure control and privacy preserving data mining techniques. The privacy of sensitive SCADA data may be preserved by suppressing the data intelligently before any disclosure or computation. Specific attributes of particular records may be suppressed completely. In case of partial suppression, an exact attribute value is replaced with a less informative value by rounding or using intervals. K-anonymity is achieved through generalization, suppression and de-identification [8]. The attribute values are generalized to a range to reduce the granularity of representation. Quasi-identifier attributes are completely or partially suppressed. De-identification is achieved by suppressing the identity linked to a specific record or altering the dataset to limit identity linkage. Summarization releases the data in the form of a summary that allows approximate evaluation of certain classes of aggregate queries while hiding individual records. The sensitive data set may be replaced with a small sample. Aggregation presents data in the form of sum, average or count. Randomization perturbs the data randomly before sending them to the server and introduces some noise. The noise can be introduced by adding or multiplying random values to numerical attributes. SCADA administrator generally preserves the privacy of sensitive data through encryption, decryption, digital signature and certificates and signcryption. PVM checks whether different statistical disclosure control techniques are really able to preserve the privacy of sensitive SCADA data from the adversaries during communication with the client through web or different enterprise applications.

10. CONCLUSION

Intelligent business and technical analysis of IIOT, ICS and SCADA requires the availability of critical up-to-data, analytical models and tools for rational, fair and correct evaluation of technology innovation. This study can be extended in various ways. It is interesting to extend the scope of the aforesaid system in various emerging applications such as banking and financial services, defense and e-governance. ICS / SCADA networks are potentially vulnerable to intrusion and various types of malicious cyber attacks which may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss. It is expected to be a resilient system. This work finds a set of interesting research agenda for future works: how to develop intelligent threat analytics and secure verification

algorithms from the perspectives of method, target, identity and protocol to ensure confidentiality, authentication, integrity, availability, accountability and access control of ICS and SCADA infrastructure? how to quantify various parameters of security intelligence? Is it possible to develop automated verification and model checking algorithms for ICS and SCADA? We need a new broad outlook, imagination and dreams to solve a complex problem through a set of simple mechanisms.

REFERENCES

1. T.J.Parenty. 2003. Digital defense what you should know about protecting your company's assets. Harvard Business School Press.
2. M.Hentea.2008. A perspective on security risk management of DCS control systems. Computers and Their Applications, 222-227.
3. 21 Steps to improve cyber security of SCDA networks. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf accessed on 15.11.2012.
4. W.R.Dunn. 2003. Designing safety critical computer systems. IEEE Computer, 36(11), 40-46.
5. D.Geer. 2006. Security of critical control systems spark concern. IEEE Computer, 39(1), 21-23.
6. S.S.Smith.2006.The SCADA Security challenge: The race is on. http://www.infosecwriters.com/text_resources/pdf/SSmith_DCS.pdf accessed on 15.11.2012.
7. J.L.Hellerstein, Y. Diao, S.Parekh and D.M.Tilbury.2005. Control engineering for computing systems. IEEE Control Systems Magazine. 25(6), 56-68.
8. M.Gertz and S.Jajodia. 2008. Handbook of database security applications and trends.
9. S.Kumar.1995. Classification and detection of computer intrusions. Thesis, Purdue University.
10. J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).
11. S.Zhu, S.Xu and S.Jajodia. 2003. LEAP: Efficient security mechanisms for large scale distributed sensor networks. Proceedings of 10th ACM Conference on Computer and Communication Security, 62-72.
12. W.Du, D.Jeng, Y.Han and P. Varshney. 2003. A pairwise key predistribution schemes for wireless sensor networks. Proceedings of 10th ACM Conference on computer and communication security (CCS'03).42-51.
13. D.Jeng, R.Han and S.Mishra. 2004. Intrusion tolerance strategies in wireless sensor networks. Proceedings of IEEE International conference on dependable systems and networks.
14. H.Chan, A. Perrig and D.Song.2003. Random key predistribution schemes for sensor networks. Proceedings of IEEE security and privacy symposium.
15. D.Choi, S.Lee, D.Won and S.Kim.2010. Efficient secure group communication for SCADA. IEEE Transactions on power delivery, volume 25, no. 2.
16. R.D. Colin, C. Boyd, J.Manuel and J.Nieto, 2006. KMA - A key management architecture for SCADA system. Proceedings of 4th Australian Information Security Workshop, volume 54, 138-197.
17. J. Pollet. 2002. Developing a solid DCS security strategy. SICON'02, Texas, USA.
18. A.R.Metke and R.L. Ekl. 2010. Smart grid security technology, Motorola Inc., USA, IEEE.
19. M.Naedele.2007. Addressing IT security for critical control systems. ABB Corporate Research. Proceedings of 40th HICSS.
20. T.Seki, T.Takehino, T.Tanaka, H.Watanabe and T.Seki. 2000. Network integrated supervisory control for power systems based on distributed objects. SAC'00, Italy.
21. A.Seshadri, A.Perrig, L.van Doorn and P.Khosla.2004. SWATT: Software based attestation for embedded devices. Proceedings of IEEE Symposium on Security and Privacy, Oakland, California.
22. www.theresiliententerprise.com accessed on 15.11.2012
23. Berard, B., Bidoit,M., Finkel,A., Laroussinite, F., Petit, A., Petrucci, L., Schnoebelen, Ph., Mckenzie,P. 2001. Systems and software verification. Springer.
24. Y.Liu, P.Ning and M.K.Reiter. 2009. False data injection attacks against state estimation in electric power grid. CCS'09, Chicago, Illinois, USA.
25. A.Studer and A.Perrig.2008. The Coremelt attack.
26. J.M.Colbert and A.Kott (Editors). 2016. Cyber security of SCADA and other industrial control systems. Springer, Switzerland.

27. S. Forrest et al. 1994. Self-Nonself Discrimination in a Computer. In Proceedings of IEEE; Computer Society Symposium on Research in Security and Privacy, pp. 202–212.
28. J.Kim et al. 2007: Immune system approaches to intrusion detection - a review. Natural Computing 6(4), 413–466.
29. W.Lee, J.S.Salvatore and K.W.Moke 2000. Adaptive intrusion detection: a data mining approach. Kluwer Academic Publishers, Netherlands.
30. P.Matzinger P. 1994. Tolerance Danger and the Extended Family, Annual reviews of Immunology 12, pp 991-1045.
31. P.Matzinger 2002. The Danger Model: A Renewed Sense of Self, Science 296: 301-305.
32. U.Aickelin and S.Cayzer. 2002. The Danger Theory and Its Application to AIS, 1st International Conference on AIS, pp 141-148.
33. A.K.Jain. 2007. Biometric recognition. Nature, 449:38-40.
34. S.Prabhakar, S.Pankanti and A.K.Jain.2003. Biometric recognition: security and privacy concerns. IEEE security and privacy magazine. 1(2):33-42, March - April.
35. R.Bottle, J.Konnell, S.Pankanti, N.Ratha and A.Senior. 2003. Guide to Biometrics. Springer.
36. M.Shema. edited by A.Ely. 2010. Seven deadliest web application attacks. Elsevier.
37. S.Nikoletseas and J.D.P.Rolim.2010. Theoretical aspects of distributed computing in sensor networks. Springer.
38. C.K.Wong, M.Gouda & S.S.Lam. 2000. Secure group communications using key graph, IEEE/ACM Transactions on Networking, 18(1).
39. S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Thesis guided by Prof. A.K.Pal. Indian Institute of Management Calcutta, India.
40. A.K.Pal, D.Nath and S. Chakraborty. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET.
41. H. Sundmaeker, P. Guillemin, P. Friess, P. and S., Woelfflé (eds.), 2010. Vision and Challenges for Realising the Internet of Things. CERP-IoT, European Commission.
42. K. Pretz 2013. The Next Evolution of the Internet. The Institute, IEEE (January 7, 2013), http://theinstitute.ieee.org/technology-focus/technologytopic/ the-next-evolution-of-the-internet
43. P.C. Evans, M. Annunziata 2012. Industrial Internet: Pushing the boundaries of minds and machines. GE report, March. http://www.ge.com/docs/chapters/Industrial_Internet.pdf
44. H. LeHong and J. Fenn. 2012. Key Trends to Watch in Gartner 2012 Emerging Technologies Hype Cycle.

Exercise

1. Define ISI analytics. What is the scope of ISI analytics from the perspectives of IIoT? What are the differences between IoT and IIoT? What are the strength and weaknesses of IIoT?
2. What is the dominant design of ISI analytics?
3. What are the basic elements of the system architecture associated with ISI analytics? How to represent the structure correctly for SCADA and ICS?
4. What do you mean by technology security for IIoT enabled SCADA and ICS ? How to verify the security intelligence? What is the role of adaptive security and dynamic data protection in IIoT? Design an adaptive security architecture. Develop a DDP algorithm.
5. What are the strategic moves of technology innovation, adoption and diffusion of ISI analytics? What is the outcome of technology life-cycle analysis?
6. How to manage resources in SCADA / ICS innovation project? What should be the talent management strategy?
7. What are the skills, leadership style and support demanded by the technological innovation of ISI analytics ?
8. How to manage technology innovation project in ISI analytics efficiently?
9. What should be the shared vision, common goals and communication protocols?
10. How can you ensure a perfect fit among '7-S' elements?

CHAPTER 8: CANCER PREDICTION & PREVENTION – DEEP LEARNING, GENOMICS & PRECISION MEDICINE

Abstract: This chapter shows the application of deep analytics '7-S' model on technology innovation of cancer prediction and prevention. The technology has been analyzed in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. The technology of cancer care is passing through the growth phase of life-cycle. The technology has been analyzed from different dimensions such as proactive and reactive approach, deep learning algorithm, intelligent reasoning and biomedical instrumentation. Intelligent reasoning should be explored in terms of case based reasoning, perception, common sense, genomics, precision and regenerative medicine. It is also essential to adopt a set of reactive strategies such as alternative, integrated, regenerative and precision medicines to fight against cancer. We have presented a deep analytics based cancer prevention mechanism (DACPM) balancing proactive and reactive approaches. It defines human biological system from the perspectives of application, computing, networking, data and security schema.
Keywords: Cancer Prevention, Proactive Approach, Reactive Approach, Bad Luck, Complexity Analysis, Deep Learning, Deep Analytics, CNN, SVM, Intelligent reasoning.

1. INTRODUCTION

This work presents the construction of a deep analytics based cancer prevention mechanism (DACPM) balancing proactive and reactive approaches. It defines human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The strategic moves of DACPM include deep learning, intelligent reasoning, threat analytics, optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan and adaptive secure multi-party computation. The performance of human biological system is expected to be verified through the properties of adaptive secure multiparty computation: fairness, correctness, accountability, transparency, rationality, trust, commitment; authentication, authorization, correct identification, privacy, audit; safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency, robustness and stability of application integration. It analyzes the complexity of the mechanism in terms of computational cost of deep learning algorithm. This work is specifically focused on reasoning nine test cases through DACPM in depth to fight against the epidemic of cancer: The human biological system is assumed to be a computer. It is not a rational thinking that the most of the causes of cancer are due to bad luck; it is still not known enough about the causes and prevention measures of cancer. Deep analytics does not necessarily mean deep learning algorithm, it is also associated with intelligent reasoning – analytical, logical, common sense, case based reasoning and also perception to fight against the epidemic of cancer. A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment, self-confidence, life-style, diet control and right decision making at right time. It demands the necessity of learning the basic concept of reasoning and common sense healthcare through an effective knowledge management system based on deep analytics and intelligent broadcast communication.
The basic objective of this work is to generate a rational cancer prevention plan subject to financial constraints. The work has reviewed the relevant literature on cancer, oncology and deep learning and has adopted analogical reasoning as research methodology. This work is organized as follows. Section 1 defines the problem of cancer prevention. Section 2 -8 analyze cancer prediction and prevention technology in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. Section 9 concludes the work.

2. SCOPE

Recently, there is a trend of cross fertilization between five disciplines: medical science, management information system, artificial intelligence, artificial neural network and management science. This work is associated with the problem of cancer prevention. Cancer is a costly, global and complex problem; it results a major obstacle to human development and well-being [2]. The attack of cancer has increased from 12.7 million (2008) to 14.1 million (2012) and this trend is projected to continue about 25 million cases over next two decades; the greatest impact will be in low and middle income ill equipped countries [1]. The

future of a cancer patient depends on his / her living zone. In less economically developed countries, cancer is diagnosed at more advanced stages while access to effective treatment is limited or unavailable. The highest-income countries often struggle with the spiraling costs of cancer treatment and care. Cancer has a social cost, human potential is lost and cancer care has an escalating economic impact. It is essential to identify the causes and prevention strategies for cancer control [3].

Let us first look at bio-statistics of cancer [1, 20,23,24,34,35]. It is a major cause of morbidity and mortality, with about 14 million new cases and 8 million deaths in 2012, affecting populations in all countries and all regions. Among men, five most common sites of cancer were lung (16.7%), prostate (15.0%), colorectum (10.0%), stomach (8.5%), and liver (7.5%). Among women, five most common sites of cancer were breast (25.2%), colorectum (9.2%), lung (8.7%), cervix (7.9%), and stomach (4.8%). There were 8.7 million people (older than 15 years) alive with cancer diagnosed in the previous year, 22.0 million in the previous 3 years, and 32.6 million in previous 5 years. The worldwide estimate for the number of cancers diagnosed in childhood (ages 0–14 years) in 2012 is 165 000 (95 000 in boys and 70 000 in girls). The highest incidence rates are associated with high income countries of North America and western Europe, Japan, Korea, Australia, and New Zealand. More than 60% of cases and 70% of deaths occur in Africa, Asia, and Central and South America. Cancers are caused by mutations that may be inherited or caused by environmental factors or DNA replication errors [2].

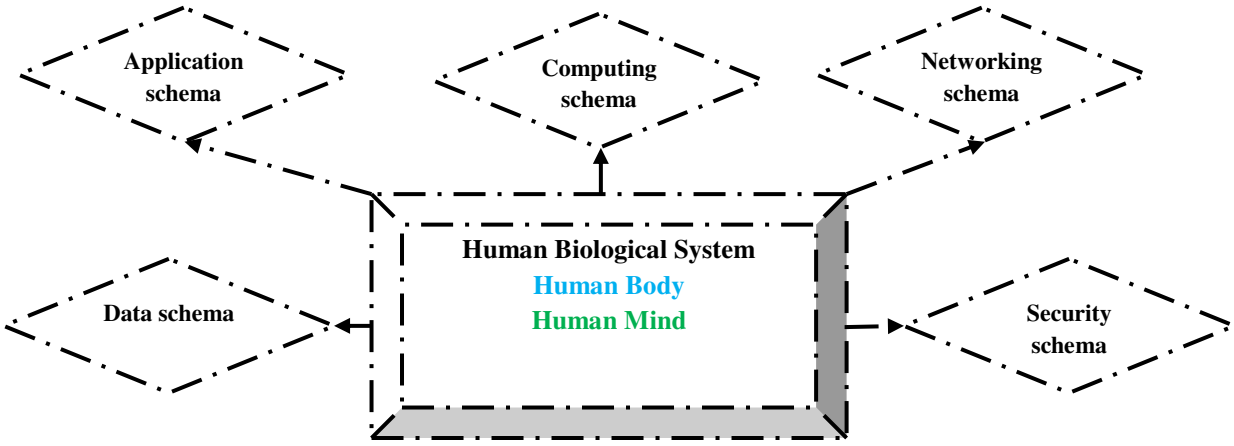


Figure 8.1: Miscellaneous schema of human biological system

This work defines the structure of human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The application schema is related to the function and features of a specific biological system. The networking schema is related to the configuration of the system such as nodes and interconnections among the nodes. The computing schema deals with the protocol, process, procedure and mechanisms of a system and its various components. The data schema is associated with various entities, their attributes and interrelationships, inputs and output of a system. The security schema verifies the disorders of the system and protects the system through various means such as vaccination, regenerative and integrated medicine, chemotherapy and laser.

In this chapter, the scope of cancer has been explored in terms of (i) cancer of mind, (ii) neural control and coordination : brain cancer, (iii) chemical coordination and integration : breast cancer (iv) digestion and absorption : liver, pancreas, stomach and colorectal cancer (v) respiratory : lung cancer, (vi) body fluids circulation : blood cancer, (vii) excretory : renal cancer and urinary bladder cancer, (viii) locomotion and movement: bone cancer and (ix) reproductive system : ovarian and testis cancer.

3. SYSTEM

Artificial intelligence (AI) is basically simulation of human intelligence. An intelligent reasoning system demands new data structure beyond knowledge base with envision, perception and proper assessment of a problem; reasoning is not effective when done in isolation from its significance in terms of the needs and interests of an agent with respect to the wider world. A rational reasoning system needs the support of an intelligent analytics. The basic objective is to evaluate the natural and adaptive immunity of a complex

system. The evaluation of the immunity of a system involves modeling, defining complete specifications and verification.
First, it is essential to model the human biological system by proper representation of its various states and programs. Next, it is important to specify the properties of the system through logical reasoning. Finally, it is essential to develop a verification mechanism which justifies: does the model satisfy the properties indicating a healthy immune system? The evaluation of immunity of a system can be done by exhaustive search of the state space (local, global, initial and goal states and state transition relations) of a system through simulation, testing, deductive reasoning and model checking based on intelligent search. The procedure terminates with positive or negative answer; the positive answer indicates a healthy immune system; the negative results provide an error trace indicating incorrect modeling or specification of the system or the occurrence of malicious threats.
The human immune system is an adaptive, robust, complex and distributed information processing system which protects the health of the biological system from the attacks of malicious foreign pathogens (e.g. virus, bacteria, fungi, protozoa, parasitic worms). It discriminates the self from non-self elements. The immunity is either innate or adaptive; innate immunity detects and kills specific known invading organisms; adaptive immunity responds to previously unknown foreign organisms. AI community needs a new outlook, imagination and dreams to solve a complex problem like prevention of cancer through a set of simple mechanisms. There are some types of cancer due to bad luck. But, we still do not know enough about the causes and preventive measures of different types of cancer. The following section brings to your notice two branches of artificial intelligence: (1) deep learning and (2) case based reasoning.

3.1 Deep Learning

Cancer is a complex global health problem involving abnormal cell growth and a major cause of morbidity and mortality. It is challenging to predict cancer using machine learning algorithms based on gene expression or image data for effective and accurate decision making, diagnosis and detection at early stage. It is basically a classification problem which predicts and distinguishes cancer patients from healthy persons. Recently, deep learning has been explored in terms of ensemble approach that combines multiple machine learning models. It is an interesting strategic option to apply various classification algorithms on informative gene expression and then a deep learning approach is employed to ensemble the outputs of the classifiers. This deep learning-based multi-model ensemble method is an accurate and effective method for cancer prediction as compared to single classifier. One of the critical issues is that it is irrational to mix data of various types of cancer and then apply deep learning based multi-model ensemble method on this mixed data. Rather, it is correct to apply deep learning algorithm on data set of different types of cancer separately such as lung, stomach and breast cancer.
Let us exercise SWOT analysis on deep learning [36-48]. Deep learning is an efficient biomedical research tool in many potential applications such as drug discovery and biomarker development. A neural network may have a single hidden layer where DNN has many hierarchical layers of nonlinear information processing units. A simple neural network does not deal well with raw data whereas deep learning can be largely unsupervised and can, learning intricate patterns from even high-dimensional raw data with little guidance. Only a deep circuit can perform exponentially complex computational tasks without requiring an infinite number of nodes. DNNs can process very large high dimensional, sparse, noisy data sets with nonlinear relationships. DNNs have high generalization ability; once trained on a data set, they can be applied to other, new data sets; this is a requirement for binding and interpretation of heterogeneous multiplatform data. DNNs can be classified into networks for unsupervised learning, networks for supervised learning and hybrid or semi-supervised networks.
But there are some limitations such as black box problem in quality control and interpretation of high dimensional data; selection problem in choosing appropriate DNN architecture, high computational cost of time consuming training method, overfitting problem and the need for large training data sets that may not be readily available. In case of overfitting, training error is low but the test error is high.

Training strategy : Data analysis on gene expression level is one of the research hotspots today. There are various types of machine learning algorithm such as k -nearest-neighbor (kNN), support vector machines (SVM), decision trees (DT), random forests (RF), and gradient boosting decision trees (GBDT). But, each machine learning method has its own flaws in terms of classification accuracy and other performance

measures. It is hard for SVM to find out an appropriate kernel function. DTs have over fitting problems and RFs require more samples to attain high classification accuracy. Each machine learning algorithm may outperform others; it is rational to adopt multiple learning algorithms for better performance. There are various types of ensemble methods such as bagging, boosting, linear regression, stacking, majority voting algorithm and deep learning. Majority voting considers linear relationships among classifiers.
Deep learning has the ability to learn the intricate nonlinear structures from the original large data sets automatically. Deep neural networks can ensemble multiple classification models to predict cancer more accurately. To avoid over fitting, it is required to preprocess the raw data and employ differential gene expression analysis to select important and informative genes, which are fed to various classification models. A deep neural network is used to ensemble the outputs of multiple classification models to obtain the final prediction result. Deep learning-based multi-model ensemble method makes more effective use of the information of the limited cancer data and generates more accurate prediction than single classifiers or majority voting algorithm. There are several open issues. Is it rational to ensemble the outputs of multiple classification models to obtain the final prediction result for same type of cancer across different demographic profile of cancer patients or various zones of the world? Is it possible to ensemble the outputs of multiple classifiers for different types of cancer?

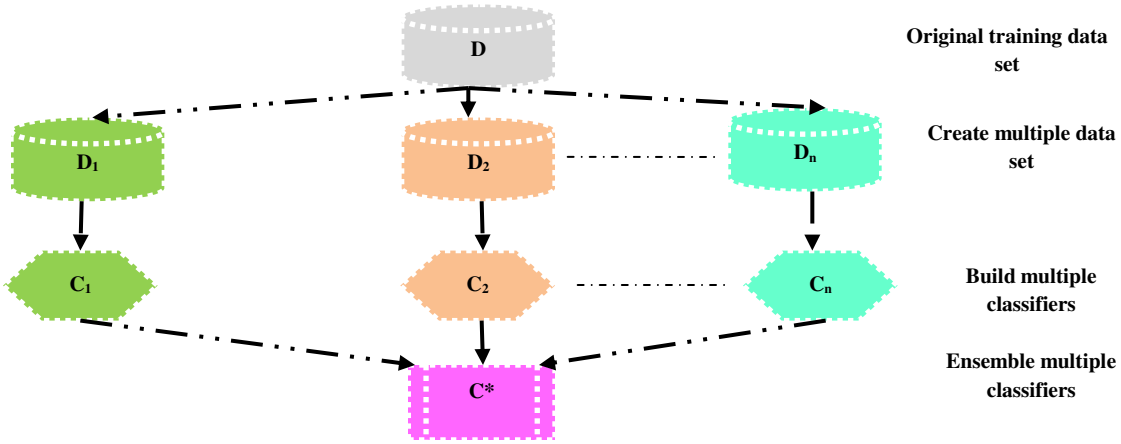


Figure 8.2. Ensemble learning method

Another critical issue is to improve classification accuracy in case of imbalanced, multi-class learning problems. Let us consider the case of bowel cancer data where a large number of examples of normal cases may exist with a much smaller number of positive cases of cancer. This data imbalance complicates the learning process and may result misclassification for the classes with fewer representative examples. Such uneven distribution may create a difficult learning process for finding unbiased decision boundaries. A regularized ensemble model of deep learning employs regularization that accommodates multiclass data sets, automatically determines error bound and penalizes the classifier when it misclassifies examples that were correctly classified in the previous learning phase and can attain superior performance in terms of improvement of overall accuracy for all classes.
Testing strategy: Let us consider three data sets of three kinds of cancers such as Lung cancer (LCD), Stomach cancer (SCD) and Breast cancer data (BCD).

- ROC curve for LCD : True positive rate vs. false positive rate for KNN, SVM, DT,RF, Majority voting, ensemble
- ROC curve for SCD data
- ROC curve for BCDA data
- Dataset, data size, precision (%), recall (%), accuracy(%), CPU time(S)
- Predictive accuracy (%) of various classification algorithms

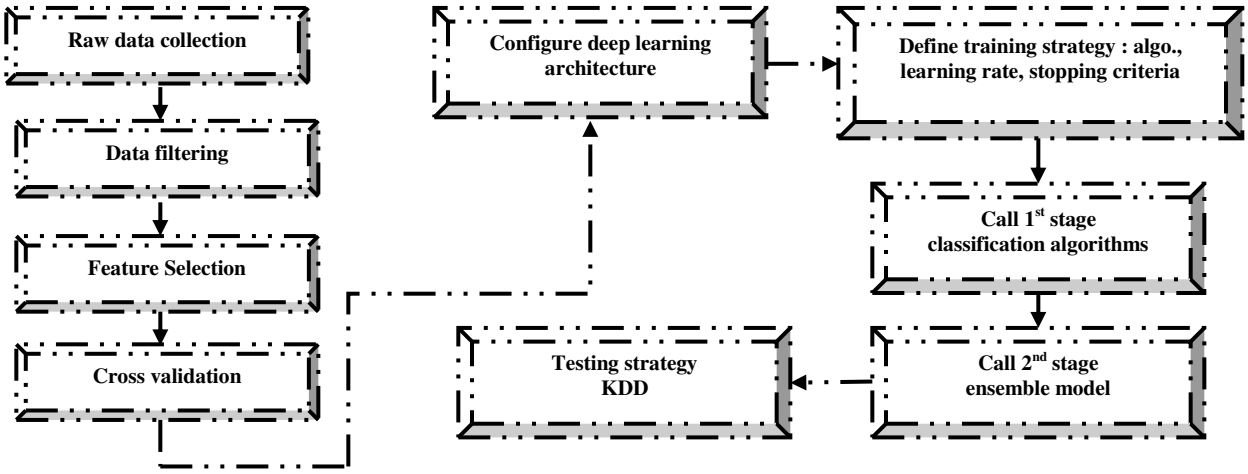


Figure 8.3 : Deep learning based multi-model ensemble method

3.2 Case based reasoning

Case based reasoning (CBR) is a methodology for solving problems by utilizing previous experience. It involves retaining a memory of previous healthcare problems and their solutions and solving new problems by referencing the past cases. A healthcare expert (e.g. oncologist) presents a new query case to CBR system. The system searches its memory of past cases stored in case base and attempts to find a case that has the same problem specification of the current case. If the system does not find an identical case in its case base, it will attempt to find the case or cases that match most closely to the current query case. There are two different types of search such as similarity search and neighborhood search. In case of similarity search, the solution of the retrieved case is directly used for the current problem. The system adapts the retrieved cases if the retrieved case is not identical to the current case. In a complex search, the system requires the access of multiple case bases which are located at various locations. Let us consider a simple CBR algorithm.

Agents: Healthcare consultant (e.g. oncologist);
Input: New case or query (q) regarding the immunity problem a patient;
Protocol:
Retrieve the most similar cases ($c_1,\ldots,c_k$), k nearest neighbors w.r.t. q from the case base;
Adapt the proposed solutions to a solution s(q), compute s(q) by combining the solutions s_j of the cases c_j. s_j is weighted as per the differences between c_j and q;
Learn after applying s(q) to q in reality; Store the new solution in the case base for solving q'.
Evaluate performance: Rejection ratio = no. of unanswered queries / total no. of queries.
Output: Recommended solution;

CBR is selected for cancer due to various reasons. The healthcare domain has an underlying model, the process is not random and the factors leading to the success or failure of a solution can be captured in a structured way. Cases recur in healthcare domain though there may be exceptions and novel cases. Healthcare solutions can be improved through case retrieval and case adaptation. Relevant healthcare cases are available at different healthcare institutes; it is possible to obtain right data. Case retrieval is the process of finding within the case base those cases that are the closest to the current case. There must be criteria that determine how a case is evaluated to be appropriate for retrieval and a mechanism to control how the case base is searched. Most often, an entire case is searched. But, partial search is also possible if no full case exists.
A **case** is a record of a previous experience or problem in terms of problem definition, patient's symptoms, drugs, solution methodology, test results and recommendations. A case base also stores global best practices, standards, valid drugs, price and contacts of specialists. Data is stored based on domain knowledge and objectives of the reasoning system. The cases should be stored in a structured way to

facilitate the retrieval of appropriate case when queried. It can be a flat or hierarchical structure. **Case indexing** assign indices to the cases for retrieval and comparisons. There are different approaches of **case retrieval**. In case of nearest neighbor search, the case retrieved is chosen when the weighted sum of the features that match the query case is greater than the other cases in the case base. A case that matches the query case on n number of features is retrieved rather than a case which matches on k number of features where k < n; different features may be assigned with different weights. Inductive approach is driven by a reduced search space and requires reduced search time. This results reduced search time for the queries. Knowledge based approaches select an optimal set of features of case by using domain knowledge. The complexity of case retrieval depends on multiple factors: (a) number of cases to be searched, (b) domain knowledge, (c) estimation of the weights for different features and (d) case indexing strategy.

Case adaptation is the process of translating the retrieved solution appropriate for the current problem; it adds intelligence to the recommendation process. There are various approaches of case adaptation. The retrieved case can be directly used as a solution to the current problem without any modification. Otherwise, the retrieved solution should be modified according to the current problem. The steps or processes of the previous solution can be reused or modified. The solution of the current case can be derived by combining knowledge of multiple retrieved cases. Case adaptation is a complex decision making task, it considers multiple factors: how close is the retrieved case to the query case? How many parameters are different between the retrieved and the query case? DMAs can apply common sense or a set of rules or heuristics for case adaptation.

Making sense of the information found during an investigational web search is a complex task of case based reasoning. Sense making is to find meaning in a situation; it is the cognitive act of understanding information. The system should support collaborative information search by providing several rich and interactive views of the search activities of a group. One of the problems is the design of computer interfaces to enable sense making of the processed information. Sense making is not only important for individuals, but also for groups to achieve shared goals. Traditional sense making tools focus on data mining, provide better information representation, visualization and organization of search results. But, it is also required to support the collaboration and communication that occurs among the investigators when they make sense of information together.

4. STRUCTURE

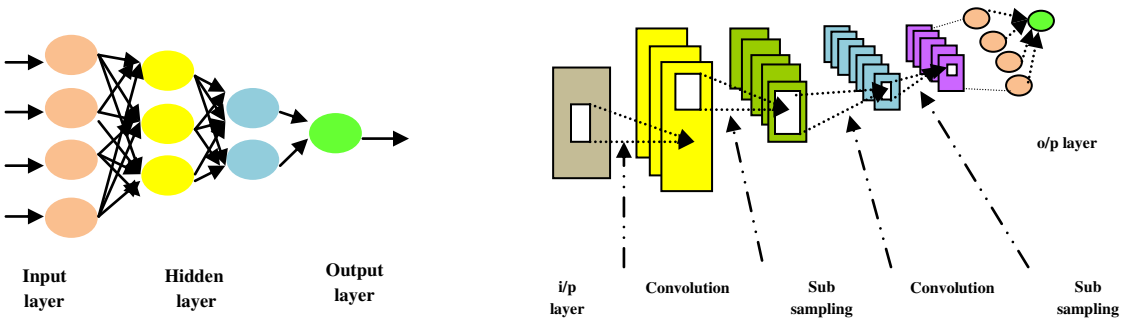


Figure 8.4: Deep learning architecture

DNN System Architecture: There are several classes of deep learning architectures used for biological data analysis. A convolution neural network (CNN) has a deep architecture with several convolutional and sub-sampling layers. Stacked auto-encoder consists of multiple sparse autoencoders. A deep belief network (DBN) freezes the weights of previous layers and feed the output to the next layer. Restricted Boltzmann machine includes a visible layer and a layer of hidden units. Mammography is a method to screen breast cancer. Breast masses are often misdiagnosed due to variability in mass appearance and low signal-to-noise ratio. Convolutional Neural Networks can be an interesting option to classify breast masses in mammograms as benign or malignant using transfer learning, and efficient data processing strategies.

Deep learning represents a class of machine learning techniques that exploit many layers of non-linear information processing for supervised or unsupervised feature extraction and transformation, pattern recognition (e.g. classification) [4]. It is used for learning multiple levels of representation to model

complex relationships among data. Higher level features and concepts are defined in terms of lower level ones and such a hierarchy of features is known as deep architecture [5]. Deep learning is based on learning representations. An observation such as an image can be represented in many ways like a vector of pixels, but some representations make it easier to learn from examples. Deep learning is a set of algorithms in machine learning to learn in multiple levels and at different levels of abstraction. It typically uses artificial neural networks such as multi-layer feedforward neural network and convolutional neural network.
There are three classes of deep learning architectures and techniques: (a) Deep networks for unsupervised or generative learning, (b) Deep networks for supervised learning and (c) hybrid deep networks [6]. Unsupervised learning is used to capture high order correlation of the visible data when no information about target class labels is available. In case of supervised learning, target label data are always available in direct or indirect forms. Hybrid deep networks use both unsupervised and supervised learning techniques. Many machine learning techniques use shallow structured architectures consisting of at most one or two layers. Shallow architectures are effective in solving simple problems are not effective for complicated applications due to limited modeling and representational power. Human information processing mechanisms needs deep architectures for extracting complex structure and building internal representation from rich sensory inputs. The basic concept of deep learning comes from the domains of ANN, AI, graphical modeling, optimization, pattern recognition and signal processing. Deep learning has several advantages as compared to shallow architecture: increased chip processing abilities, significantly increased size of training data and recent advances in machine learning research have enabled the deep learning methods to exploit complex and nonlinear functions, to learn distributed and hierarchical feature representations and effective use of both labeled and unlabeled data.
Deep Learning is basically credit assignment in adaptive systems with long chains of causal links between actions and consequences. It is accurately assigning credit across many stages. A standard neural network consists of many simple connected processors or units each producing a sequence of real valued activations. Input units get activated through sensors perceiving the environment, other units through connections with weights from previously active units. Learning or credit assignment is to find weights that make the neural network exhibit desired behavior [7]. A complex problem may require long causal chains of computational stages. Convolution Neural Networks (CNN) architecture are widely used for computer vision. The receptive field of a unit with given weight vector is shifted step by step across input values. The resulting array of subsequent activation events of a unit can provide inputs to higher level units.

5. SECURITY

One of the most critical elements of deep analytics is security; it is essential to verify security intelligence of the technological innovation associated with cancer prevention collectively through rational threat analytics at five levels : L1, L2, L3, L4 and L5. At level L1, it is important to audit the access control mechanism for the biological system of cancer patients in terms of authentication, authorization, correct identification, confidentiality and data integrity. At level L2, it is required to verify fairness, robustness, correctness, transparency, accountability, trust and commitment. Next, it is required to verify the system performance at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety. At level L4, it is required to assess the risks of various types of malicious attacks by adversaries on the human biological system such as Denial of Service (DoS), false data injection attack and sybil attack. At level L5, it is required to assess the risks of various types of corruptions such as agents, system administration and payment function associated with cancer treatment. It is rational to adopt an optimal mix of proactive and preventive i.e. sense-and-respond approaches to fight against cancer; the following section outlines a Deep Analytics based Cancer Prevention Mechanism (DACPM).

Deep Analytics based Cancer Prevention Mechanism [DACPM]

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human biological system – (a) body, (b) mind;
Objectives: cancer prevention at optimal cost;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;

Strategic moves:

- optimal mix of proactive and reactive approaches;
- deep learning algorithm;
- intelligent reasoning : case based reasoning (CBR), perception, analytical, logical, common sense, biomedical instrumentation;
- rational healthcare payment function and budget plan;
- adaptive secure multi-party computation;

Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively.
- **Attacker:** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets** : computing, data, networking, security and application schema;
  - **Threat modeling**
    - Call threat analytics function (f_a) and assess miscellaneous risk elements;
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
      - Auto-immunity and vaccination;
      - Optimal diet intake (e.g. fruits : amla, vegetables, nutrients) to fight against malnutrition;
      - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities, stress control through meditation;
      - Self-healing mechanism through wearable computing based health monitoring devices which measure several health parameters in real-time such as pulse rate, temperature, blood pressure, respiration rate, heart bit and oxygen saturation rate;
      - Yoga for physical pain and treatment of psychological, social and spiritual trauma (as side effects of radiation and chemotherapy)
        - 'Suryanamaskar'
        - 'Pranayam' and deep breathing exercises for stress management
        - Free hand exercises for muscle relaxation
          - standing postures (e.g. 'chakrasan', 'pada hastasan')
          - sitting postures (e.g. 'ustrasan' or camel pose, 'shashangasan' or rabit pose)
- **Reactive approach**:
  - adopt sense-and-respond strategy.
  - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
  - verify security intelligence of application, computing, networking, security and data schema of biological system.

- **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
- **Level2**: authentication, authorization, correct identification, privacy, audit;
- **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
- **Level4:** stability, system dynamics, quality of application integration.

- Explore risk mitigation plan (P^r_d and P^r_m).
  - Do medical testing → Data visualization (Refer Deep Leaning Algorithm of section 2.1)
  - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
  - Integrated medicine
  - Regenerative medicine
  - Chemotherapy and radiation
  - Laser

Fight against bad luck : Identify critical risk elements.

- Genetic disorder (sex, race, ethnicity, somatic mutation)
- Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
- Injuries from accidents, sports and games, war and crime
- Side effects of medical treatment (e.g. hormone therapy)
- Occupational exposure (e.g. at nuclear power plant; alternative option : solar power)
- Environmental pollution (e.g. nuclear and thermal power plant)
- Hostile climate, weather and other locational disadvantages, exposure to sunshine
- Malnutrition due to poverty

- Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Cost of illness (COI) : health sector costs (direct cost) + decreased or lost productivity by the patient (indirect cost) + the cost of pain and suffering (intangible cost);
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;
- Crowd funding campaign through social media (e.g. pediatric cancer treatment appeal at social networking site or crowd funding portal.

Output: Cancer prevention plan

5.1 Deep Learning Algorithm

Objective: Computer aided cancer detection and diagnosis with improved accuracy;
Input : Medical images with optimal number of correct features;
Data preprocessing : Filter raw data from noise and incompleteness;
System Architecture: Deep Convolution Neural Network (CNN);
Training strategy : Ensemble learning

- Create multiple data sets from original training data;
- Build multiple base classifiers (e.g. kNN, SVM, DT, RF, GBDT) for each data set;
- Combine classifiers;

Algorithm :

D: Original training data , n : no. of base classifiers, D_t: Test data;

for i = 1 to n do

create training data set D_i from D;

build base classifier C_i on D_i;

end for

for each test data $x \in D_t$

$C^*(x) = C_1(x) \oplus \ldots \oplus C_n(x)$; /* $\oplus$: combination operator */

end for

Testing strategy : Predictive accuracy analysis;

Output: Pattern recognition for cancer location identification, cancer tissue classification, cancer image segmentation, cancer image retrieval, big image data analysis

DACPM is basically a security game i.e. fight against cancer. It is defined by various types of elements: a group of agents, model, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payments, a strategy profile, a dominant strategy which maximizes the utility of an agent for all possible strategies of other agents involved in the mechanism, security intelligence and revelation principle [8]. There are two agents in the security game: a defender (D) and the attacker (A). Each agent adopts and executes a or a set of strategies. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy. The best strategy may depend on the knowledge of the defender about prospective attacks and the sunk costs incurred when upgrading information security schema reactively. The payment function of the mechanism estimates an optimal investment plan for the protection of human biological system. The mechanism verifies the security intelligence of human biological system; it is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy [please refer chapter 1].

The DACPM mechanism evaluates security intelligence of the human biological system based on proactive and reactive approaches. The system is expected to be a resilient system. The resiliency measures the ability to and the speed at which the information system can return to normal performance level following a disruption. Adaptability is about responding to change effectively and decisively through reactive approach: the ability to identify the change in search space for the adversaries, understanding the probable impacts of the hit by the adversaries, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The vulnerability of the system to a disruptive event such as cancer should be viewed as a combination of likelihood of a disruption and its potential severity. The defender must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the defender should explore what can go wrong in the operation of the system? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences.

The defender tries to define the payment function associated with healthcare in terms of aspiration point, reservation point and adjustment of various preferential thresholds (e.g. indifference, strong preference, weak preference, veto) and preferred solutions. Cost of illness may be estimated based on direct cost (e.g. health sector costs), indirect cost (e.g. loss of productivity of the patient) and intangible cost (e.g. cost of pain and suffering). Direct costs include hospitalization, medication, emergency transport, and medical care. Decreased or lost productivity may be the result of illness, premature death, side effects of illness or treatment or time spending receiving treatment. With premature death, the indirect cost is the loss in wage and benefits.

The computational cost of deep learning mechanism depends on the complexity of threat analytics function, deep learning algorithm and payment function. The cost of computation is a function of the complexity of threat analytics. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. Another major computational burden of the deep learning mechanism is the complexity of verification or model checking algorithms. The cost of computation also depends on the complexity of payment function. The appendix shows the application of DACPM for nine types of cancer as stated in scope (section 2).

6. STRATEGY

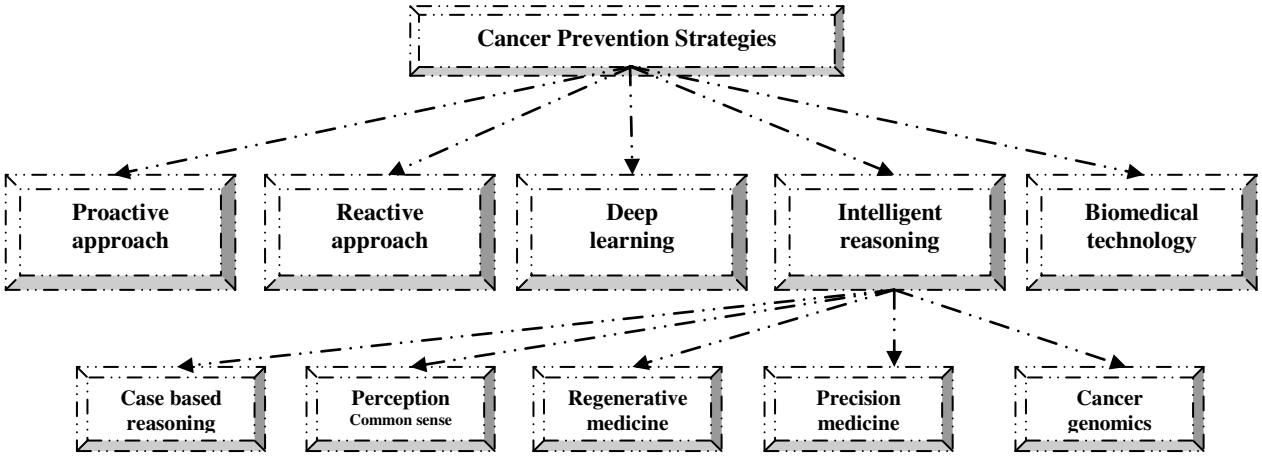


Figure 8.5: Strategic moves of cancer prevention

The fifth element of deep analytics is strategy; it can be analyzed from different dimensions such as proactive self-healing approach, reactive approach, deep learning algorithm, intelligent reasoning and biomedical instrumentation. Intelligent reasoning should be explored in terms of case based reasoning, perception and common sense, logical and analytical reasoning and rational payment function. It is essential to adopt a set of reactive strategies such as alternative, integrated, regenerative and precision medicines to fight against cancer. It is rational to evaluate strength, weakness, opportunities and threats for various strategic options. The evolution and diffusion of cancer prevention technology depends on R&D policy, organization learning, knowledge management strategy and technology life-cycle analysis. An intelligent R&D policy should be explored through shared vision, goal and strategic alliance, collaborative and collective intelligence. There are various strategies of learning such as learning-by-doing and learning-before-doing. Learning-by-doing is effective in cancer care through deep learning on big data; it is also essential to attain deep practical and theoretical knowledge on cancer therapy through experimental medicines. In fact, it is clear from the aforesaid case analysis that different types of cancer demand different types of prediction and prevention technologies, best practices and therapies.

Technology trajectory is the path that the cancer prevention technology takes through its life-cycle from the perspectives of rate of performance improvement, rate of diffusion and rate of adoption in cancer care. It is really complex to analyze the impact of various factors on the trajectory of cancer prevention technology today. From the view of life-cycle, the technology of cancer prevention is at the growth phase of S-curve. The technology has evolved from the birth phase and going though growth phase. Initially, it may be difficult and costly to improve the performance of the new cancer prevention technology. The performance is expected to improve with better understanding of the fundamental principles and mechanisms of human biological system. Initially, the technology may be costly for the adopters due to various uncertainties and risks. Gradually, it is expected to be adopted by large segments of the market due to reduced cost and risks. The evolution of the technology is passing through a phase of turbulence and uncertainty; various entities are exploring different competing options of cancer care and a dominant therapy is expected to emerge through a consensus and convergence of the best practices. The dominant therapy must consider an optimal set of technological advancements which meet the demand of the cancer patients, cancer care experts, supply chain and design chain in the best possible way.

Let us consider the strategy of surgical operation for cancer care. It is essential to operate hard and soft tissues with proper care, precision, consistency, speed and control. The surgical operation is expected to be minimally invasive, less painful and faster healing. An innovative technological solution and surgical method for cancer care is expected to have higher success rate; lower recurrence rate, more precision, accuracy and effectiveness, less treatment time, faster recovery and healing, unmatched cutting, speed and control with high consistency and reliability, greater precision and control, efficiency and safety, less post operative problems due to minimally invasive procedure preventing damage to nearby tissues and less bruising, numbness and post operative pain, minimal invasion and no scars, simple OPD procedure, better

patient experience and thus high credibility and high patient satisfaction. Laser technology is an emerging solution for the aforesaid desired surgical operation in cancer care.
Laser (light amplification by stimulated emission of radiation) is an effective solution as compared to conventional methods. Laser has a specific wavelength; it is focused in a narrow beam and creates a very high intensity light which is used for cutting through tissue in surgical operation. Laser therapy is used to destroy tumors or precancerous growths in skin, cervical, penile, vaginal, vulvar and lung cancer [49]. It may be also used for cancer related to brain, prostate, piles, fissures, fistula and dental problems. Laser therapy can be used in standalone mode or in combination with chemotherapy or radiation therapy. It is used to relieve certain symptoms of cancer such as to remove a tumor blocking trachea or esophagus or colon polyps or stomach. It can also be used to seal nerve endings and to reduce pain after surgical operation and seal lymph vessels to reduce swelling and limit the spread of tumor cells. Laser therapy is given through a flexible endoscope fitted with optical fiber. It is inserted through mouth, nose, anus or vagina. Laser is then precisely focused to remove a tumor.
There are various types of laser therapies such as Laser-induced Interstitial Thermotherapy (LITT) and Photodynamic Therapy (PDT). Generally, CO_2, argon and neodymium: yttrium-aluminum-garnet (Nd:YAG) lasers are used for cancer care. Laser therapy provides several benefits such as minimally invasive procedure, faster recovery, minimal recurrence, blood loss, pain and post operative discomfort and high success rate. Laser therapy demands specialized training of the surgeons and strict safety precautions. It is expensive; the effects may not last long and may be repeated for recovery.

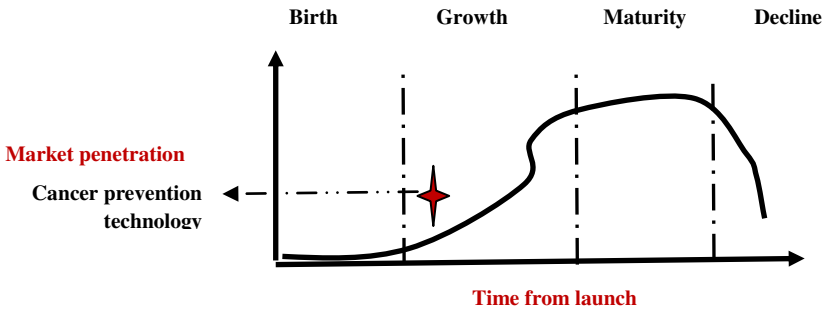


Figure 8.6 : Technology life–cycle analysis

7. STAFF - RESOURCES

This element can be analyzed in terms of sources of innovation and roles of biomedical engineering, pharmacy and life-science firms, oncology departments of healthcare institutes, government research laboratories and collaborative networks; optimal utilization of man, machine, material, method and money, dominant design factors of artificial organs and biomedical devices, process innovation in cancer treatment and technological spillover. The innovation demands the commitment of creative experts of oncology, bio-medical engineering, healthcare and life-science sectors who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab, start-ups (e.g. science parks, incubators), academic institutions, ministries of state and central government, patients, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. bio-medical engineering, pharmacy, life-science, oncology, deep learning and artificial neural network), healthcare and medical science domain such as research and development, knowledge management, product design,

project management, supply chain management, sales and distribution. It is essential to teach deep learning innovatively in various programmes of Electrical, Electronics and Biomedical engineering as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as digital libraries having good collection of books, journals and magazines, software and experimental set up. The workforce of R&D labs can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The healthcare professionals are expected to be people, information and action oriented. Next, let us consider the element support.

Caution from malicious learning system : The basic objective is to protect learning systems in adversarial setting from various types of threats such as use of flawed learning algorithm or intentional change of training and testing data distribution [14,15]. The malicious agents may act consciously to limit or prevent accurate performance of the learning system for economic incentives. It is a common problem where machine learning is used to prevent illegal or unsanctioned activities. Traditional techniques (e.g. efficient algorithm, linear classification) are necessary but not sufficient to ensure the security of the machine learning system. It is a hard problem and needs the support of an efficient mechanism equipped with intelligent threat analytics and adaptive secure multi-party computation algorithms. Malicious business intelligence is a critical threat to machine learning system. The conflict between security intelligence and business intelligence is inevitable. It needs fair, rational and intelligent business model innovation [16].

Example : Malicious business intelligence may attack a life-science supply chain and healthcare service chain through greedy heuristics in payment function for revenue and profit optimization, economic pressure and incentive policy, fraudulent health insurance model, flaws in investment decision on technology management, irrational and dull HR policy in talent management and chaotics in formulation of public policy, mechanisms and corporate governance. In fact, the conflict between business intelligence and security intelligence is inevitable; the deep learning mechanism is expected to resolve this conflict between security and business intelligence.

Let us consider a specific instance of machine learning in healthcare service chain. The deep learning mechanism must call the threat analytics to audit various critical processes associated with a healthcare service chain in cancer care such as registration, consulting, testing, surgical operations, billing, payment processing and follow-up. Generally, different types of information systems are commonly used to support these processes such as transaction processing system (TPS), decision support system (DSS), group decision support system (GDSS), knowledge management system (KMS) and business intelligence (BI) system. The primary objective of these information systems is to ensure fairness and correctness in computation of registration card, appointment slip for consulting, prescription by consultant, surgery schedule, quality control certificate, medical test report, discharge certificate, bills and payment receipt, feedback form and patient's guide. The other important issue is to preserve the privacy of patient's personal and medical data. The deep learning mechanism should verify the security of the computing schema associated with the machine learning system in healthcare service chain to identify probable sources of errors in cancer care.

a. Incorrect data provided by the cancer patients to the registration associate during registration intentionally or due to lack of knowledge or incorrect perception of the patients or their attendants; the patients or their attendants may be irrational in information sharing properly with the service providers.
b. No verification of patient's identity correctly during registration; the cases of emergency situation or accidents may skip verification due to unavailability of data about the patients.
c. Wrong entry of data into various information systems by the healthcare associates due to time and resource constraints or misunderstanding or lack of validation of input data.
d. Computational errors due to wrong configuration of enterprise applications and / or errors in the heuristics, deep learning algorithms and quantitative models and / or no updating of data (e.g. service charge, tariff of testing, price of drugs and healthcare products; low accuracy of pattern recognition algorithms in image processing system may result incorrect medical diagnosis.
e. Access control problem causing dangerous errors in information system; a malicious agent may enter false data into HIS during the absence of authorized users.

f. A malicious agent may launch attacks on TPS, DSS, GDSS, KMS and BIS through malicious data mining, insecure data storage, flaws in data visualization and image processing algorithms and transaction processing logic.
g. Swap or mixing of test data of various patients or drugs administration due to confusion, poor document management, lack of clear understanding or training of the healthcare workforce; false data injection on viruses in test reports are serious threats in today's healthcare practice. The patients are not often given test reports today by the service provider to hide malicious trading practice or to charge extra amount. Testing of uncommon viruses enhance the cost of testing unnecessarily. Sometimes, broadcast of epidemic results panic among the public and this critical and helpless situation is exploited by malicious testing and medicare practice inhumanly.
h. Errors in decision making by the health consultants due to lack of proper knowledge management system (e.g. case based reasoning, intelligent DSS and GDSS) or misperception or lack of coordination among the workforce of various departments or inappropriate enterprise application integration or error in test reports; incomplete prescription due to memory failure or silly mistakes.
i. Errors in scheduling due to exceptions (e.g. unfit patients, non-availability of healthcare experts), flawed and inadequate doctor-patient ratio;.
j. surgical operation by unauthorized and unskilled workforce, intentional errors due to malicious business practice, lack of ethics, casual approach and dull HR policy; unintentional errors due to physical and mental fatigue for excessive workload and sickness, non-availability of basic infrastructure and logistics arrangements;
k. Lack of verification of correctness of computation in medical billing and payment processing by the service provider and / or service consumer;
l. Incorrect data in patient's help guide may cause confusions and mismatch between the computed results and perceived one;
m. Incorrect feedback by the patients or their attendants due to misperception, misunderstanding of feedback form, lack of knowledge and critical observations or casual attitude.
n. Sybil attack: It is really complex to trace the corrupted players in healthcare domain. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt an application that relies on redundancy by injecting false data or suppressing critical data; it is *sybil attack*. The patients may be treated incorrectly and diagnosed as cancer casually though there is another simple medical problem. Natural intuition and perception may not be applied for simple medical problems. The patients may be incorrectly recommended for costly treatment. They may be recommended for costly treatment procedure repeatedly (e.g. CT scan, X-ray), drugs and surgical operations. The poor and helpless patients may be forced to validate and verify the test reports and medical diagnosis at various healthcare institutes. This is an instance of modern biological, chemical and radiological terrorism today.

Fairness and correctness of computation and testing is a critical concern in cancer therapy. Knowledge management is another critical success factor; case based reasoning may be a good solution for correct clinical decision making. For effective deep learning system, digital technology management is not only the critical success factor (CSF). There are other several CSFs such as HR policy in talent management, motivation and commitment, quality of education in terms of trust, ethics and values, intelligent public policy, mechanisms and corporate governance.

9. CONCLUSION

This work explores the importance of a deep analytics based mechanism for cancer prevention in the context of human biological system. It presents a new framework of human biological system in terms of computing, data, networking, application and security schema of an information system based on analogical reasoning. DACPM promotes a hybrid approach which recognizes the role of both proactive and reactive approaches in making decisions on healthcare investment for cancer prevention. The reactive approach may outperform proactive one against the threats that never occur actually. Sometimes, reactive approach may be cost effective as compared to proactive approach. The basic building blocks of the proposed mechanism are threat analytics and adaptive secure multiparty computation. The threat analytics monitor the system performance of human biological system based on time series data, detects and analyzes different types of vulnerabilities on the biological system.

This work finds a set of interesting research agenda for future work: (a) explore new risk factors and causes of cancer, classifying cancers, opportunities for early detection and prevention and cost reduction of cancer care; (b) how to design an intelligent threat analytics; (c) how to design intelligent verification mechanisms; (d) how to rationalize DACPM, (e) how to quantify and code miscellaneous security intelligence parameters, (e) check the performance of kernel based learning algorithms with CNN, (g) how to apply integrated medicine for critical case (e.g. multiple organ failure syndrome) and exercise allopathic, homeopathy, herbal, yoga and naturopathy effectively for various purposes such as pain management, combating side effects of radiation and chemotherapy (e.g. hair fall, nausea, vomiting), every cancer patient requires specific treatment considering complexity of disease and (g) explore new approaches of cancer prevention such as vaccination for auto-immunity, laser therapy, integrated and regenerative medicine, precision medicine, gene therapy and stem cell therapy and (h) is it possible to imagine the security schema of human biological system based on antivirus, firewalls and various cryptographic tools (e.g. encryption, decryption, digital signature and signcryption) apart from secure multi-party computation? The next chapter explores the strategic option of bio-medical instrumentation and organ transplantation for various types of cancers such as pancreatic and liver cancer.

REFERENCES

1. B. W. Stewart, C. P. Wild, Eds., World Cancer Report 2014, IARC, France.
2. C.Tomasetti and B.Vogelstein. 2015. Cancer etiology. Variation in cancer risk among tissues can be explained by the number of stem cell divisions. *Science,* 347(6217):78–81.
3. A.Albini, F. Tosetti and VW Li. 2012. Cancer prevention by targeting angiogenesis. *Nat Rev Clin Oncol*. 9(9):498–509.
4. G. Anthes. 2013. Deep learning comes of age. *Communications of the Association for Computing Machinery (ACM)*, 56(6):13–15.
5. I. Arel, C. Rose, and T. Karnowski. 2010. Deep machine learning — a new frontier in artificial intelligence. *IEEE Computational Intelligence Magazine*,5:13–18.
6. Y. Bengio. 2013. Deep learning of representations: Looking forward. In *Statistical Language and Speech Processing*, pages 1–37. Springer.
7. L. Deng. 2011. An overview of deep-structured learning for information processing. In *Proceedings of Asian-Pacific Signal & Information Processing Annual Summit and Conference (APSIPA-ASC)*. October 2011.
8. N. Nisan and A.Ronen. 1999. Algorithmic mechanism design. In 31st Annual ACM symposium on Theory of Computing, pp 129 -140.
9. S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Indian Institute of Management Calcutta, India.
10. A.Barth, B.Rubinstein, M.Sundararajan, J.Mitchell, D.Song and P.L. Bartlett. 2010. A learning-based approach to reactive security. In: Radu, S. (ed.) Financial Cryptography' 2010. LNCS, vol. 6052, pp. 192–206. Springer.
11. R.Bohme and T.W.Moore. 2009. The iterated weakest link: A model of adaptive security investment. In: Workshop on the Economics of Information Security (WEIS), University College, London, UK.
12. Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.
13. R.Canetti, U.Feige, O.Goldreich and M.Naor. 1996. Adaptively secure multi-party computation.
14. M.Kearns and M. Li. 1993. Learning in the presence of malicious errors. SIAM Journal on Computing 22(4), 807–837.
15. M.Barreno, B.Nelson, R. Sears, A.D. Joseph and J.D.Tygar. 2006. Can machine learning be secure? In Proceedings of the ACM symposium on Information, computer, and communications security.
16. S.Chakraborty. 2015. Secure multi-party computation: how to solve the conflict between security and business intelligence. Technical report.
17. S.K.Chaturvedi. 2012. Psychiatric oncology: cancer in mind. Indian Journal Psychiatry. Apr-Jun; 54(2): 111–118.
18. T.V.Borght, S. Asenbaum, P.Bartenstein, C.Halldin, Ö. Kapucu, K.V. Laere, A. Varrone and K.Tatsch. 2010. Brain Tumor Imaging: European Association of Nuclear Medicine Procedure Guidelines.
19. M. Havaeia, A. Davyb, D. Warde-Farley, A. Biard, A. Courvillec, Y. Bengioc, C. Pal, P.Jodoina and H. Larochelle. 2016. Brain Tumor Segmentation with Deep Neural Networks.

20. R.L.Siegel, K.D.Miller and A. Jemal. 2015. Cancer statistics. CA Cancer J Clin. 65(1):5–29.
21. American Cancer Society. 2015. Breast Cancer Facts and Figures 2015–2016: Atlanta: American Cancer Society, Inc.
22. D. Wang, A. Khosla, R. Gargeya, H.Irshad and A.B. Beck. 2016. Deep Learning for Identifying Metastatic Breast Cancer.
23. American Cancer Society. 2014.*American Cancer Society: Cancer Facts and Figures 2014*. Altanta, GA: American Cancer Society..
24. R.Siegel, D.Naishadham and A. Jemal. Cancer statistics, 2012. *CA Cancer J Clin*. 62(1):10-29.
25. S.Deuffic, et al. 1998. Trends in primary liver cancer. *Lancet.* 1998;351(9097):214-215.
26. R.Govindan, N. Page and D. Morgensztern. 2006. Changing epidemiology of small-cell lung cancer in the United States over the last 30 years: analysis of the surveillance, epidemiologic, and end results database. *J Clin Oncol*. 24(28):4539-4544. PMID: 17008692.
27. LC Caprario, DM Kent and GM Strauss. 2013. Effects of chemotherapyon survival of elderly patients with small-cell lung cancer: analysis of the SEER-medicare database. *J Thorac Oncol*. 8(10):1272-1281. PMID: 24457238. PMCID: 3901951.
28. F.Barbone, M. Bovenzi, F Cavallieri and G. Stanta. 1997. Cigarette smoking and histologic type of lung cancer in men. Chest. 112(6):1474-1479. PMID: 9404741.
29. S. Faderl S, S. O'Brien S and C-H Pui 2010. Adult acute lymphoblastic leukemia: concepts and strategies. *Cancer*. 116(5):1165-1176.
30. T.J. Lightfoot and E. Roman. 2004. Causes of childhood leukemia and lymphoma. *Toxicol Appl Pharmacol*. 199(2):104-117.
31. M. Murai and M. Oya. 2004. Renal cell carcinoma: etiology, incidence and epidemiology. Curr Opin Urol ;14: 229–33.
32. JD Mulder, HE Schütte, HM Kroon and W.K., Taconis. Radiologic atlas of bone tumors. 2nd edn. Amsterdam: Elsevier; 1993.
33. A.G. Huvos 1991. Bone tumors. Diagnosis, treatment, and prognosis. 2nd edn. Philadelphia: W.B. Saunders Company.
34. J.Ferlay, I.I.Soerjomataram and R. Dikshit 2015. Cancer incidence and mortality worldwide: sources, methods and major patterns in GLOBOCAN. *Int J Cancer*. 2015;136:E359–E386.doi:10.1002/ijc.29210.
35. BK Edwards, A-M Noone, AB Mariotto et al. 2014. Annual Report to the Nation on the status of cancer, 1975-2010, featuring prevalence of comorbidity and impact on survival among persons with lung, colorectal, breast, or prostate cancer. *Cancer*.120(9):1290–1314.
36. D. Hanahan , R.A. Weinberg, Hallmarks of cancer: the next generation, Cell 144 (5) (2011) 646–674 .
37. K. Kourou , T.P. Exarchos , K.P. Exarchos , M.V. Karamouzis , D.I. Fotiadis , Ma- chine learning applications in cancer prognosis and prediction, Comput. Struct. Biotechnol. J. 13 (2015) 8–17 .
38. E. Sayed , A. Wahed , I.A . Emam , A . Badr, Feature selection for cancer classifica- tion: an SVM based approach, Int. J. Comput. Appl. 46 (8) (2012) 20–26.
39. A. Statnikov , L. Wang , C.F. Aliferis , A comprehensive comparison of random forests and support vector machines for microarray-based cancer classification., BMC Bioinform. 9 (1) (2008) 1–10 .
40. S.B. Cho , H.H. Won , Machine learning in DNA microarray analysis for cancer classification, in: Asia-Pacific Bioinformatics Conference, 2003, pp. 189–198 .
41. H. Hijazi , C. Chan , A classification framework applied to cancer gene expression profiles, J. Healthc. Eng. 4 (4) (2012) 255–284.
42. N. C. F. Codella, Q. B. Nguyen, S. Pankanti, D. A. Gutman, B. Helba, A. C. Halpern, J. R. Smith, Deep learning ensembles for melanoma recognition in dermoscopy images, IBM Journal of Research and Development 61 (4) (2017) 5:1 – 5:15.
43. G. Karakoulas, J. Shawe-Taylor, Optimizing classifiers for imbalanced training sets, in: The Conference on Advances in Neural Information Processing Systems II, MIT Press, Cambridge, MA, USA, 1999, pp. 253– 259.
44. [42] R. Rasti, M. Teshnehlab, S. L. Phung, Breast cancer diagnosis in dce-mri using mixture ensemble of convolutional neural networks, Pattern Recognition 72 (2017) 381–390.
45. Nussinov, R. Advancements and Challenges in Computational Biology. PLoS Comput. Biol. 2015, 11 (1).
46. LeCun, Y.; Bengio, Y.; Hinton, G. Deep Learning. Nature 2015, 521 (7553), 436−444.

47. Schmidhuber, J. Deep Learning in Neural Networks: An Overview. Neural Networks 2015, 61, 85−117.
48. Fakoor, R.; Huber, M. Using Deep Learning to Enhance Cancer Diagnosis and Classification. In Proceeding 30th Int. Conf. Mach. Learn. Atlanta, GA, 2013, Vol. 28.
49. https://www.cancer.gov/about-cancer/treatment/types/surgery/lasers-fact-sheet

Exercise

1. **Explain the technology of deep learning on prediction and prevention for cancer care? Justify it as a technology for humanity. What is the scope of this technology?**
2. **What is the dominant design of the technology?**
3. **What are the basic elements of the system architecture?**
4. **What do you mean by technology security in cancer care? How to verify the security intelligence?**
5. **What are the strategic moves of technology innovation, adoption and diffusion for cancer care? What is the outcome of technology life-cycle analysis?**
6. **How to manage resources for this innovation project?**
7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
9. **Develop a deep learning algorithm for the prediction of cancer correctly?**
10. **Explain the scope of genomics, regenerative and precision medicine for cancer care.**

APPENDIX

This section highlights the application of DACPM for nine different types of cancer.

A. Cancer of Mind

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human mind;
Objectives: cancer prevention at optimal cost;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: intelligent reasoning, optimal mix of proactive and reactive approaches, rational payment function and budget plan;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively.
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets** :
    - application schema – human mind;
    - networking schema – brain and nervous system;
    - computing schema – nerve impulse and release of neurotransmitter;
    - data schema – symptoms of abnormal, selfish behavior, narrow outlook, jealousy, negative mechanical robotic thinking, devil's thought, fear of death, anxiety, impatience, restlessness, hyperactive behavior, depression;
    - Security schema – auto immunity, hormones, vitamins, minerals, genetic traits;
  - **Threat modeling**
    - Call threat analytics and assess miscellaneous risk elements :
      - change in behavior, physical appearance and personality;

        - psycho-oncology disoder;
        - Schizophrenia : multiple personalities, severe mental disorder in thinking, perception, emotion, sense of self and violent behavior;
    - Estimate demand plan;
    - Explore risk mitigation plan : accept / transfer / remove / mitigate risks.
        - Vaccination (option to be explored);
        - Optimal diet intake to fight against malnutrition;
        - Life-style : Avoid smoking, alcohols and drug addiction;
        - Stress control through yoga and meditation, deep sleep;
        - Listen soft relaxation music during idle time in subconscious mind.

- **Reactive approach**:
    - adopt sense-and-respond strategy.
    - assess risks of single or multiple attacks on the mind; analyze performance, sensitivity, trends, exception and alerts.
        - what is corrupted or compromised?
        - time series analysis : what occurred? what is occuring? what will occur?
        - insights : how and why did it occur? do cause-effect analysis.
        - recommend : what is the next best action?
        - predict: what is the best or worst that can happen?
    - verify security intelligence of application, computing, networking, security and data schema of human mind.
        - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
        - **Level 2**: authentication, authorization, correct identification, privacy, audit;
        - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
        - **Level4:** stability, system dynamics, quality of application integration.
    - Explore risk mitigation plan.
        - Do medical testing → Data visualization of brain scan;
        - Integrated medicine
        - Psychiatric oncology
        - Behavioral and cognitive therapy
- **Fight against bad luck:** Identify critical risk elements.
        - Genetic disorder
        - Reproductive disorder (personal, hormonal and family history)
        - Occupational exposure
        - Injuries from accidents, war and crime
        - Environmental pollution (e.g. air, sound)
        - Hostile climate, weather and other locational disadvantages, exposure to sunshine
    - Develop risk mitigation plan in terms of deaddiction and rehabilitation.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements.
- Trade-off proactive vs. reactive security: assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Prevention plan of cancer of mind

Drug Addiction: Let us analyze DACPM in the context of cancer of mind caused by drug addiction. There is slight difference between cancer of mind and madness. A human agent suffering from cancer of

mind may act selfishly with narrow outlook and malicious business intelligence. But, a mad man generally acts irrationally. Any chemical substance other than food used for the prevention, diagnosis, alleviation, treatment or cure of a disease of human agents or animals is called a *drug* or medicine or therapeutic agent. Drug addiction is the habitual, physiological and psychological dependence on a substance or a practice which is beyond voluntary control of an addict. Addictive drug modifies the biological, psychological and social behavior of the addicted person by stimulating, depressing or distorting the function of their body and mind. Use is basically taking a drug for medical treatment like disorder or injury. Drug abuse is the wrong, improper, injurious and misuse of drugs for non-medical purposes which affects physical and mental health of the drug abuser. They use drugs without the prescription of the doctors secretly; taken frequently and regularly; habituating substances; may affect brain and nervous system and changes behavior; gives temporary pleasure or relief from stress. A doctor prescribes drugs for the treatment of diseases or for the improvement of physical and mental health and the drugs are withdrawn as soon as the desired effect is achieved. Repeated use of some drugs on a periodic or continuous basis may make the body dependent on those drugs, It is *drug dependence*. The drug action is affected by a set of factors such as the form, type, dose, mode of use, period of consumption and susceptibility of the addicted person. The addicted person becomes drug dependent through various stages such as experimental use for curiosity, recreational use, situational use, compulsive use and dependence. The addicted person shows some abnormal symptoms such as poor academic performance, indifference in the duties and responsibilities, change in behavior (e.g. telling lies, violence, unrest), change of physical appearance (e.g. loss of weight, vigor and appetite) and change in personality. There are two types of drug dependence - psychological and physical or neuroadaptation. In case of physical dependence, intake of drugs is essential to maintain physiological equilibrium. In case of psychological dependence, a person believes that the normal state can only be achieved with the action of the drugs.

There are several critical *causal factors* of drug addiction such as curiosity, the pressure from friends and relatives, high stress, pleasure, temporary relief from mental stress, frustration and depression, poor academic performance, problems in relationship management, job loss, unemployment, desire for more work, looking for a different world, relief from pain, family history, easy availability of drugs and money and excitement and adventure. Some students take drugs to keep awake the whole night for the preparation of their examinations or to manage high work load or backlog. It is a malpractice and bad habit.

Drugs act on brain and central nervous system. The structural and functional units of nerve cells are neurons; the message passes from one neuron to the other through synapses. Arrival of the nerve impulse causes the release of a chemical neurotransmitter. The drugs act at the synapses. The depressant drugs (e.g. alcohol, narcotics) inhibit the production of neurotransmitter or inactivation of the neurotransmitter more quickly or modify postsynaptic membrane. The stimulants increase the production of neurotransmitter and increase stimulation of the neurons. The general symptoms of drug addiction include excitement, violent nature, exhausted and drowsy appearance, poor concentration, memory loss, loss of interests in works, studies and social life, reduced appetite, vigor and weight and disorder of sleep. Ultimately, it results the cancer of mind of drug addicted people.

The addicts often suffer from the problems of central nervous system, psychosis, Hepatitis-B, AIDS, impotency, chromosal abnormalities and genetic disorder. Many of them have a dull unhappy life. They create problems for their families, neglect duties and may lose jobs. It may deprive a family of basic needs and may result frustration and insecurity of the children. The family members may suffer from physical and psychiatric problems such as headache, anxiety, insomnia and depression. The drug users get drugs from illegal sources encouraging smuggling, criminal activities, bio-terrorism and accidents. The drug addicts are less efficient and unreliable as workers and often lose their job or may not get employment anywhere.

Life-science supply chain is a soft target of bio-terrorism. The drugs and medicines sold through popular distribution channels may be tainted, compromised and mislabeled. It needs strong support of drug quality and security act. The life-science supply chain has developed and produced breakthrough drugs and medicines that enhance the average life span in the world. Unfortunately, when bad things happen in life-science supply chain, the public get hurt. Today's life science supply chain requires an effective *'Drug Quality and Security Act and Standards'* which is able to clarify with transparency the authority, roles and responsibilities of food and drugs administration and consumer protection ministry, regulate pricing of drugs, develop a national track-and-trace system to audit the functions of the life-science supply chain and minimize the risks of contamination, adulteration, diversion or counterfeiting.

It is essential to adopt a set of *good habits* by the students and youth as proactive approach through a value based education system at school and colleges to mitigate the risks of drug abuse.

a. Intelligent reasoning through common sense, logical and analytical mind set;
b. Be proactive and take responsibility of your life. Avoid bad habits and negative thinking; adopt good habits;
c. Be dedicated, motivated and committed in learning;
d. Define vision, mission and goals in life rationally and innovatively;
e. Control physical and mental stress through yoga, meditation, relaxation music and extracurricular activities;
f. Be conscious of physical, mental and social health;
g. Prioritize multiple tasks through proper planning and time management and do the most important things first;
h. Think win-win; have an everyone-can-win attitude with confidence, patience and perseverance;
i. Listen to the other people carefully and sincerely. First try to understand and then to be understood;
j. Promote synergy and collaborative intelligence, work together to achieve more through group dynamics;
k. Sharpen the saw - renew yourself regularly. Analyze as-is state; find out gap and innovate to-be-state;
l. Contribute to the society and environment through activities, thoughts and plans.

There are various strategies to mitigate the risk of drug abuse and drug addiction for reactive approach: deaddiction, childcare, drugs as social stigma, legal punitive action, strict regulatory compliance through effective corporate governance, corporate social responsibilities and good habit development through an effective education system. The physicians should prescribe drugs with responsibility and the pharmacists should not sell drugs without the valid prescriptions of the doctors. The parents should keep a watch and monitor the activities, attitude and behavior of their children. The social workers and policemen should be alert and inform the parents or deaddiction centers in time. In fact, law and the public should take joint responsibility against drug abuse.

Deaddiction is basically treatment of drug addiction or withdrawal symptoms of drugs. The major steps of deaddiction include master health check up (e.g. blood test, brain scanning), pharmacotherapy, psychosocial therapy, health restoration, psychological treatment and prevention of relapse. If a drug dependent person fails to get drugs, feels severe physical severe physical and psychological disturbances depending on the type and dosage of drugs. The general treatment of *withdrawal symptoms* of a drug is to replace the drug with a less reinforcing and legally available drug that can be gradually eliminated with decreasing doses. It is Pharmacotherapy. For the drug combination addiction, it is required to withdraw one drug at a time and maintain the others. After the withdrawal symptom subsides, psychological treatment persists and cause craving for the drugs. At this stage, the drug addicts need the moral support of their parents, relatives and friends. They may need the treatment at rehabilitation centers; it is a long term treatment requiring behavioral training of the patients. *Rehabilitation* involves the psychological and social therapy in the form of counseling by relatives, friends and physicians in a sympathetic manner. The patients should learn the ill effects of drug addiction through Psychosocial therapy. The patient also needs supportive measures such as administration of vitamins, proper nutrition, restoration of electrolytic balance and proper hydration. Vitamin C checks the rise of the level of cAMP in human brain. The patient may also need Psychological treatment. Finally, *readdiction* may occur; many addicts restart taking drugs after deaddcition. They should be watched by their near and dear ones.

Psycho-oncology : Psychiatric oncology is the study of psychiatric and social aspects of cancer such as cause, maintenance and prognosis of cancer, emotional reactions, psychiatric disorders, stress management and communication skills of the oncologists in revealing bad news and handling difficult questions and counseling. It is essential to understand psycho-neuro-endocrino-immunological mechanisms of the cancer patients. The psychological responses to cancer arise from knowledge of life-threatening diagnosis, uncertainty, financial burden and fear of death. The emotional responses arise from pain, nausea and unwanted side-effects of medical, surgical, and radiation treatments [17]. This treatment also addresses various issues such as diet and nutritional supplements, yoga, meditation and physical exercises and aromatherapy.

B. Neural control and coordination

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human nervous system, sensory system;
Objectives: cancer prevention at optimal cost; focus : brain cancer [18,19];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets**
    - application schema : Nervous and sensory system;
    - networking schema :
      - Nervous system : CNS – Brain, spinal chord; PNS, Neurons, nerves, cerebrospinal fluid, brain stem, meninges, neuroglia, ependymal cells, neurosecretory cells;, cerebral nerve, spinal nerve;
      - Sensory organs : eye, ear, nose, toungue, skin;
    - computing schema : nerve impulse, reflex, neurotransmitter, neurosecretion, chemoreception; control and coordination, integration, memory, mechanism of sensory organs – see, hear, smell, feel, taste;
    - data schema : sensory receptors – photo, chemo, thermo, electro and mechanoreceptors; structure of sensory organs;
    - security schema : immunity, hormones, vitamins, minerals, blood, CSF;
  - **Threat modeling**
    - Call threat analytics and assess miscellaneous risk elements
      - brain tumors : astrocytic, neuronal, embryonic and pineal;
      - disorders of nervous system : memory loss, poliomyelitis, meningitis, sciatica, neuritis, synaptic delay, synaptic fatigue;
      - eye defects – myopia, hypermetropia, astigmatism, presbiopia, cataract, glaucoma;
      - skin cancer;
      - throat cancer;
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
      - Optimal diet intake to fight against malnutrition;
      - Life-style : yoga and physical activities, stress control through meditation;
      - Eye, ear and skin care against hostile climate (e.g. snowfall, scorching sunshine)
      - Autoimmunity through vaccination
- **Reactive approach**:
  - adopt sense-and-respond strategy based on following *symptoms* of brain cancer : headache, weakness, clumsiness, difficulty in walking, seizures, altered mental status like changes in

concentration, memory, attention or alertness, intellectual capacity or emotional response, nausea, vomiting, lethargy, blurred vision and difficulty with speech;

- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised : Is the brain tumor malignant or benign?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
        - genetic factors
        - environmental effects
        - radiation
        - HIV infection
        - smoking
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
- verify security intelligence of application, computing, networking, security and data schema of biological system.
    - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
    - **Level 2**: authentication, authorization, correct identification, privacy, audit;
    - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
    - **Level4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan (P^r_d and P^r_m).
    - Detection of viable tumor tissue $\rightarrow$ tumor delineation $\rightarrow$ selection of the best biopsy site $\rightarrow$ non-invasive tumor grading $\rightarrow$ therapy planning $\rightarrow$monitoring tumor response;
    - MRI and CT scan of brain tumor (Refer Deep Leaning Algorithm of section 5.1);
    - Biopsy trough surgery of brain tumor;
    - Treating viral and bacterial infection, chronic inflammation, pain;
    - Automatic drug injection into malignant brain tumor through nano-chip implanted into brain.

- **Fight against bad luck :** Identify critical risk elements.
    - Genetic disorder (sex, race, ethnicity, somatic mutation)
    - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
    - Injuries from accidents, war and crime
    - Occupational exposure
    - Environmental pollution (e.g. dust, sound pollution)
    - Hostile climate, weather and other locational disadvantages, exposure to sunshine
    - Malnutrition due to poverty
- Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

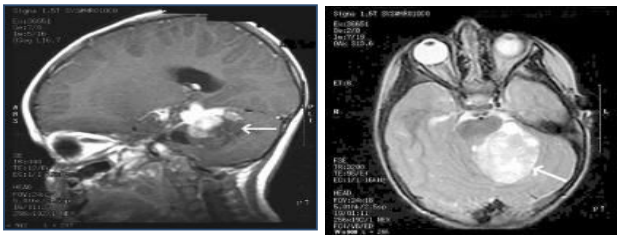


Figure 8.7 : MRI scan of a brain tumor

C. Chemical coordination and integration

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human endocrine system;
Objectives: cancer prevention at optimal cost; Focus : breast cancer [20,21];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM);
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
    - **Identify targets** :
        - application schema : Endocrine, Exocrine and Heterocrine system, Breast;
        - networking schema : Glands – hypothalamus, pituitary, pineal, thyroid, parathyroid, thymus, adrenals, pancreas, gonads : testes and ovaries, kidneys;
        - computing schema : coordination between endocrine and nervous system, interaction among glands, hormone action mechanism (formation of Camp);
        - data schema : hormones (informational molecules secreted by endocrine cells), hypothalamus – neurohormones > release hormones (RH), inhibitory hormones (IH); pituitary – FSH LH, GTH, TSH, ACTH, GH (*),LTH, OT; pineal – melatonin; thyroid – thyroxine (**), calcitonin; parathyroid – PTH (#), thymus - thymosine, adrenals - aldosterone, glucocorticoids, sexcorticoids (##); pancreas – insulin ($), glucagon, SS; gonads : testes – LH and ovaries – Estrogen, Progesterone and Relaxin; kidneys - Renin; primary, secondary and final targets;
        - security schema : innate and adaptive immunity, hormones, vitamins, minerals;
    - **Threat modeling**
        - Call threat analytics, understand *molecular switches* and assess miscellaneous risk elements of breast cancer:
            - age (old age increases risk)
            - gender (females with higher risk)
            - race
            - reproductive factors (e.g. infertility, menarche age, menopause age, age of first pregnancy)

- parity (nulliparous women at higher risk)
- family history (inherited genetic mutation)
- obesity and weight
- breast density (higher density with higher risk)
- radiation exposure
- side-effects of hormone replacement therapy, cross-sex hormone therapy and birth controlling pills

♦ Assess the risks of other disorders
- over secretion : gigantism (*); grave's disease(**), osteoporosis (#);
- deficiency : dwarfism(*), goitre(**), addison's disease (##), diabetes mellitus ($);

♦ Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];
♦ Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
♦ Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
♦ Estimate requirements of healthcare in terms of demand plan (P^p_d);
♦ Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
- Optimal diet intake to fight against malnutrition;
- Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities, stress control through meditation;
- Proactive risk mitigation strategies for breast cancer
  - Early detection through self-breast examination (SBE) : 'know your breast';
  - Rational diet chart, yoga and physical exercises;
  - Diabetes control;
  - Avoid wearing tight dress;
  - Safe massage for beast development exercises;
  - Caution: violent love-life

Reactive approach:
- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
  - ♦ what is corrupted or compromised?
  - ♦ time series analysis : what occurred? what is occuring? what will occur?
  - ♦ insights : how and why did it occur? do cause-effect analysis.
  - ♦ recommend : what is the next best action?
  - ♦ predict: what is the best or worst that can happen?
- verify security intelligence of application, computing, networking, security and data schema of biological system.
  - ♦ **Level 1**: correctness, fairness, accountability, transparency, rationality, commitment;
  - ♦ **Level 2**: authentication, authorization, correct identification, privacy, audit;
  - ♦ **Level 3:** reliability, consistency, liveness, resiliency;
  - ♦ **Level 4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan (P^r_d and P^r_m).
  - ♦ Breast cancer : Personalized screening
  - ♦ Do clinical breast examination (CBE) → Data visualization
    - Convolutional network for tumor detection in breast mammography (Refer Deep Leaning Algorithm of section 5.1);
    - Caution of mammography screening : radiation exposure, anxiety, false positives and over diagnosis;
  - ♦ Integrated medicine

- Mastectomies

- **Fight against bad luck :** Identify critical risk elements.
  - Genetic disorder (sex, race, ethnicity, somatic mutation)
  - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
  - Side effects of medical treatment (e.g. hormone therapy)
  - Malnutrition due to poverty
- Develop risk mitigation plan in terms of surgical operation, gene therapy, stem cell therapy.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

Deep learning algorithm for breast cancer [22] :
Objective: Computer aided breast cancer detection and diagnosis with improved accuracy; avoid the limitations of qualitative visual analysis with microscope like lack of standardization, diagnostic errors and excessive cognitive load, precision medical treatment through computational image analysis;
Input : millions of training patches;
System Architecture: Deep Convolutional Neural Network;
Procedure of cancer metastasis detection :

- a patch-based classification stage
- a heat map based post processing stage

Output: identification of cancer metastases from whole slide images of breast sentinel lymph nodes; make patch-level predictions to discriminate tumor patches from normal-patches.

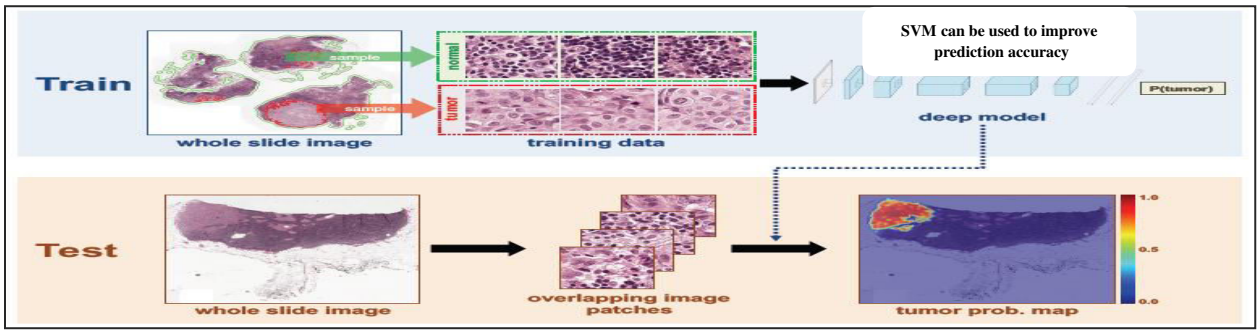


Figure 8.8 Deep learning for breast cancer detection

D. Digestive system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human digestive system;
Objectives: cancer prevention at optimal cost;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of digestive system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;

Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets**
    - application schema : digestive system;
    - networking schema :
      - alimentary canal – mouth, vestibule, oral cavity – tongue, teeth, pharynx, oesophagus, stomach, small intestine, large intestine;
      - digestive glands – salivary gland, gastric glands, liver, pancreas, intestinal glands;
    - computing schema :
      - nutrition mechanisms – autotrophic, holophytic, heterotrophic, symbiotic and holozoic;
      - movement of alimentary canal;
      - hormonal control of digestive secretion;
      - ingestion, digestion - intracellular, extracellular and mixed, egestion, absorption and assimilation;
    - data schema : nutrients – food (carbohydrates, protein, fat), minerals, vitamins, bile;
    - security schema : immunity, enzymes, bile, gastric juice, hormones, vitamins, minerals;
  - **Threat modeling**
    - Call threat analytics and assess miscellaneous risk elements:
      - malnutrition, over nutrition,
      - incomplete digestive tract,
      - Gastrointestinal cancer [23,24,25]
        - gastric, gastro esophageal junction and esophageal cancer (adenocarcinoma) with risk elements like low consumption of fruits and vegetables, high intake of N-compounds in salted and preserved foods and occupational exposure in coal mining and nickel, rubber and timber processing industries, high meat consumption, smoking, alcohol consumption, gastric surgery and reproductive hormones
        - oral cancer
        - pancreatic Cancer with risk elements like tobacco smoking, diabetes and chronic pancreatitis, diet, body mass index and genetic syndrome
        - hepatocellular carcinoma (HCC) or liver cancer caused by chronic viral hepatitis, alcohol and cirrhosis, aflatoxin, OCP and genetic metabolic factors, toxic exposures of medicine
        - small bowel cancer and appendiceal tumors
        - colorectal cancer with risk factors such as somatic or inherited genetic mutation, diet, obesity, inflammatory bowel diseases,
        - anal cancer
        - neuroendocrine tumor
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^{p}_{d});

- Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
  - Auto-immunity and vaccination against hepatitis B and C;
  - Optimal diet intake to fight against malnutrition;
  - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities
  - Oral cancer from wild polygamy;

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
  - what is corrupted or compromised?
  - time series analysis : what occurred? what is occuring? what will occur?
  - insights : how and why did it occur? do cause-effect analysis.
  - recommend : what is the next best action?
  - predict: what is the best or worst that can happen?
- verify security intelligence of application, computing, networking, security and data schema of biological system.
  - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
  - **Level 2**: authentication, authorization, correct identification, privacy, audit;
  - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
  - **Level4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan.
  - Gastric cancer : surgery, perioperative chemotherapy, postoperative chemoradiotherapy;
  - Pancreatic cancer : immunotherapy, CT scan, biopsy, surgery, systemic therapy or chemoradiation;
  - Liver cancer : systemic chemotherapy, hormonal therapy, clinical trial of antiangiogenesis agents, radiation therapy;
  - Colorectal cancer : fecal occult blood testing, barium x-ray, colonoscopy, sigmoidoscopy, genetic testing, radiotherapy, surgery;
  - Do medical testing $\rightarrow$ Data visualization of images (e.g. liver, pancreas and alimentary canal, Refer Deep Leaning Algorithm of section 5.1)
  - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
  - Insulin injection
  - Artificial liver and pancreas transplantation

Fight against bad luck : Identify critical risk elements.

- Genetic disorder (sex, race, ethnicity, somatic mutation)
- Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
- Injuries from accidents, war and crime
- Occupational exposure
- Water and soil pollution
- Hostile climate, weather and other locational disadvantages, exposure to sunshine
- Malnutrition due to poverty

- Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.

- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

Figure 8.9 : Gastric cancer

Figure 8.10 : Liver cancer

E. Respiratory system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human respiratory system;
Objectives: cancer prevention at optimal cost; focus : lung cancer [26,27,28];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets**
    - application schema : respiratory system;
    - networking schema : respiratory tract, respiratory organs – lungs, tissues, larynx;
    - computing schema : breathing mechanism – inspiration, air filtering, exchange of gases in alveoli, expiration; nervous and chemical control of respiration, transport of gases in blood (O_2, CO_2), artificial respiration mechanism;
    - data schema (^) : respiratory rate, pulmonary air volume and capacity, composition of inspired, expired and alveolar air, TV, IRV,ERV,RV,VC,IC,FRC,TLC;
    - security schema : innate and adaptive immunity, hormones, blood;
  - **Threat modeling**
    - Call threat analytics function and assess miscellaneous risk elements : lung cancer,
      - Lung cancer : small cell and non-small cell lung cancer
        - Tobacco exposure: duration and intensity of tobacco use;
        - Exposure to asbestos, benzene, coal tar and radon gas;
        - Environmental or industrial exposure to arsenic, chromium, chloromethyl ether, vinyl chloride and polycyclic aromatic hydrocarbons;
        - Genetic predisposition

        - Other disorders of respiratory system : hypoxia, asphyxia, bad cold, bronchitis, bronchial asthma, pneumonia, emphysema, occupational respiratory disorder, carbon monoxide poisoning;
        - Throat cancer and ENT
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
        - Auto-immunity and vaccination;
        - Optimal diet intake to fight against malnutrition;
        - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control, yoga (deep breathing exercises) and physical activities, stress control through meditation;

- **Reactive approach**:
    - adopt sense-and-respond strategy.
    - assess risks of single or multiple attacks on the human respiratory system; analyze performance, sensitivity, trends, exception and alerts.
        - what is corrupted or compromised?
        - time series analysis : what occurred? what is occuring? what will occur?
        - insights : how and why did it occur? do cause-effect analysis.
        - recommend : what is the next best action?
        - predict: what is the best or worst that can happen?
    - verify security intelligence of application, computing, networking, security and data schema of biological system.
        - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
        - **Level 2**: authentication, authorization, correct identification, privacy, audit;
        - **Level3:** safety, reliability, consistency, liveness, deadlock freeness, reachability, resiliency;
        - **Level4:** stability, system dynamics, quality of application integration.
    - Explore risk mitigation plan.
        - Prevention measures of lung cancer : stop smoking , early detection and screening and chemoprevention;
        - Do medical testing of data schema (^);
        - Data visualization of X-ray report of lungs and also biopsy report;
        - Treating tobacco induced injuries in the air way, viral and bacterial infection, chronic inflammation; medication against chronic disease;
        - Limited disease of lung cancer (LD) :
            - combined chemo radiation therapy
                - radiation intensity
                - timing of chemotherapy : Sequential, concurrent, and alternating chemotherapy
            - surgery
        - Extensive disease of lung cancer (ED):
            - Select correct treatment algorithm
            - systematic chemotherapy
            - immunotherapy through tumor vaccines
- **Fight against bad luck :** Identify critical risk elements.
    - Genetic disorder
    - Reproductive disorder (flaws in organ formation and development since birth)
    - Injuries from accidents, war and crime

- Occupational exposure
- Air and soil pollution
- Hostile climate, weather and other locational disadvantages, exposure to sunshine, snowfall and very cold climate;
- Malnutrition due to poverty

- Develop risk mitigation plan in terms of surgical operation and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

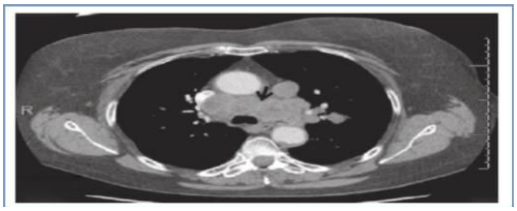


Figure 8.11: CT scan of lung cancer

F. Body fluids circulation – Cardiovascular system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human biological system – (a) body, (b) mind;
Objectives: cancer prevention at optimal cost; focus : leukemia or blood cancer [29,30];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets**
    - application schema : cardiovascular system;
    - networking schema : heart, blood vascular system – open and closed circulatory system, arterial and venous system, blood, tissue fluid, lymphatic system – spleen, thymus, tonsils;
    - computing schema : pulmonary and systemic circulation, blood clotting or coagulation mechanism, blood flow mechanism;
    - data schema : blood group, efficiency of heart, heart rate, heart output, pulse, heart sound;
    - security schema : blood, lymph, water, minerals, vitamins, hormones;
  - **Threat modeling**

- Call threat analytics and assess miscellaneous risk elements :
  - blood cancer / lukemia
    - **Acute lymphoblastic leukemia (ALL) :** proliferation and accumulation of lymphoid progenitor cells in blood, bone marrow and tissues for both the children and adult; bone marrow failure, malaise, fatigue, bleeding fever, night sweats, weight loss and abnormal White blood cell (WBC) count;
    - **Adolescent and young adult acute lymphoblastic leukemia;**
    - **Acute myeloid leukemia (AML)** due to genetic mutations and chromosomal aberrations with symptom of Fanconi anemia;
    - **Chronic lymphocytic leukemia (CLL):** clonal hematopoietic disorder;
    - **Chronic myeloid leukemia (CML)**
  - blood pressure disorder (SP, DP)
  - cardiovascular diseases : Stroke (CVA or cardiovascular accident), rheumatic heart disease (RHD), coronery artery disease (CAD), hypertensive heart disease, atrial fibrillation, tachycardia, vaculities;
- Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
- Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
- Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
- Estimate requirements of healthcare in terms of demand plan (P^p_d);
- Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
  - Auto-immunity and vaccination
  - Optimal diet intake to fight against malnutrition
  - Life-style : Avoid smoking and alcohols, food habit, drug addiction control

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
  - what is corrupted or compromised?
  - time series analysis : what occurred? what is occuring? what will occur?
  - insights : how and why did it occur? do cause-effect analysis.
  - recommend : what is the next best action?
  - predict: what is the best or worst that can happen?
- verify security intelligence of application, computing, networking, security and data schema of biological system.
  - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
  - **Level 2**: authentication, authorization, correct identification, privacy, audit;
  - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
  - **Level4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan (P^r_d and P^r_m).
  - Diagnosis of ALL: immunophenotyping, cytogenetic-molecular profiling, allogeneic stem cell transplantation, salvage therapy, immunotherapy;
  - Risk stratification of AML based on patient related variables (age and performance) and disease related predictors (cytogenetic and molecular characteristics);

- Induction therapy, supportive care and stem cell transplantation for AML;
- Do medical testing → Data visualization of ECG
- Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance
- Medication for blood pressure control
- Integrated medicine
- Regenerative medicine

Fight against bad luck : Identify critical risk elements.

- Genetic disorder (sex, race, ethnicity, somatic mutation)
- Reproductive disorder (personal, hormonal and family history)
- Occupational exposure
- Air, water and sound pollution
- Hostile climate, weather and other locational disadvantages, exposure to sunshine
- Malnutrition due to poverty

- Develop risk mitigation plan in terms of organ transplantation, surgical operation, blood substitution and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

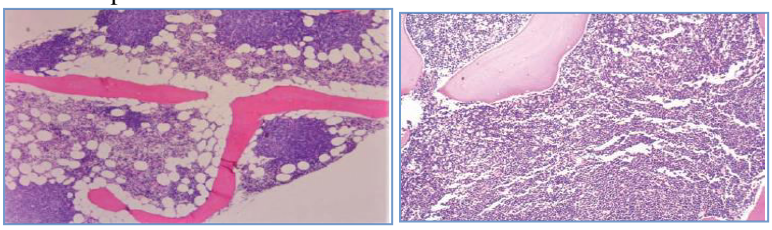


Figure 7.8: Bone marrow biopsies of leukemia

G. Excretory system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human excretory system;
Objectives: cancer prevention at optimal cost; focus : renal cancer, skin cancer [31];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

Proactive approach:

- **Identify targets**
  - application schema : excretory system;

- networking schema : kidney - nephron, ureters, urinary bladder and urethra; skin – sweat, lungs – CO_2;
- computing schema : urea and urine formation, mechanism of kidney;
- data schema : urine and stool – quantity, physical properties, chemical composition and renal threshold;
- security schema : immunity, water, vitamins, minerals;

- **Threat modeling**
  - Call threat analytics function and assess various risk elements :
    - renal cancer : tobacco smoking, regular alcohol consumption, food habit (e.g. high intake of animal protein and fat), polluted drinking water, obesity, lack of physical activities, reproductive factors and hormones, medical conditions : hypertension, diabetes, urinary tract disease, drug addiction, radiation , occupational exposure : chemical, oil and gas, Pb, Cd, asbestos, gasoline and hydrocarbons, genetic susceptibility;
    - kidney disorder - renal failure, kidney stone; uremia, cystitis, glomerrulonephritis, pyelonephritis;
    - urinary bladder cancer
    - prostate cancer
    - skin cancer : actinic keratosis, melanoma skin cancer, non-melanoma skin cancer;
  - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
  - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
  - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
  - Estimate requirements of healthcare in terms of demand plan (P^p_d);
  - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
    - Auto-immunity and vaccination;
    - Optimal diet (e.g. fruits, vegetables) and water intake to fight against malnutrition;
    - Life-style : Avoid smoking and alcohols, food habit (e.g soft drinks), drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities;

- **Reactive approach**:
  - adopt sense-and-respond strategy.
  - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
  - verify security intelligence of application, computing, networking, security and data schema of biological system.
    - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
    - **Level 2**: authentication, authorization, correct identification, privacy, audit;
    - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
    - **Level4:** stability, system dynamics, quality of application integration.
  - Explore risk mitigation plan.
    - skin cancer :
      - actinic keratosis – cryotherapy, topical treatment;

        - melanoma skin cancer : biopsy – shave, punch, excisional, incisional, wound care;
        - non-melanoma skin cancer : topical treatment, ED&C, excision, radiotherapy;
    - renal cancer: immunotherapy, radiotherapy and supportive care, systemic therapy of metastatic disease, adjuvant therapy, surgical treatment of renal cell carcinoma, interventional radiology, laparoscopic radical nephrectomy;
    - Do medical testing → Data visualization of kidney scan (Refer Deep Leaning Algorithm of section 5.1, transferring a Convolutional Neural Network, trained on images for detection of kidney problem in ultrasound images); detection of renal tumor by USG, MRI and CT scan;
    - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
    - Artificial kidney or kidney transplantation
    - Integrated medicine
- **Fight against bad luck :** Identify critical risk elements.
    - Genetic disorder (sex, race, ethnicity, somatic mutation)
    - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
    - Injuries from accidents, war and crime
    - Occupational exposure
    - Water pollution
    - Hostile climate, weather and other locational disadvantages,
    - Malnutrition due to poverty
- Develop risk mitigation plan in terms of organ transplantation and surgical operation and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

Figure 8.12: Skin cancer

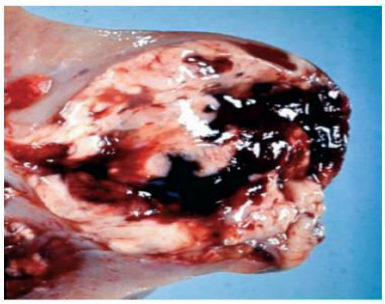


Figure 8.13: Renal cancer

H. Locomotion and Movement

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human biological system – (a) body, (b) mind;
Objectives: cancer prevention at optimal cost; focus: bone cancer [32,33];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;

Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender :** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker :** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets** :
    - application schema : human skeletal and mascular system;
    - networking schema :
      - skeleton – bone (skull, spinal column, ribs, sternum, girdles, limb), cartilage, joints;
      - muscles – red and white;
    - **computing schema :**
      - Mechanism of metastasis to bone, inflammatory cytokines in osteolysis, prostate cancer bone colonization causing metabolic imbalance between osteoblasts and osteoclasts, tumor-bone interaction, suppression of bone formation;
      - locomotion and movement mechanism, autonomic and induced movement,
      - muscle contraction mechanism;
    - data schema : oxygen debt, muscle fatigue;
    - security schema : bone marrow, minerals, vitamin D;
  - **Threat modeling**
    - Call threat analytics and assess miscellaneous risk elements :
      - Risk factors : age, gender, race, site distribution;
      - bone cancer : bone pain, spinal chord suppression;
      - osteosarcoma (primary and malignant bone tumor);
      - multiple myeloma : bone destruction, hypercalcemia, neurological disorder;
      - head and neck cancer, cervix cancer ;
      - Other disorders: sprain, arthritis, osteoporosis, dislocation, slipped disc, fracture of bones, bursitis, tetany, myasthenia gravis and muscular dystrophy.
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
      - Auto-immunity and vaccination;
      - Optimal diet intake to fight against malnutrition;
      - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control;
      - Fairplay : Take less risk in sports, games and adventure;
      - yoga and physical mascular activities, stress control through meditation;
      - Use computers, tablets and laptops with a safe posture.
- **Reactive approach**:
  - adopt sense-and-respond strategy.
  - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.

- what is corrupted or compromised?
- time series analysis : what occurred? what is occuring? what will occur?
- insights : how and why did it occur? do cause-effect analysis.
- recommend : what is the next best action?
- predict: what is the best or worst that can happen?

- verify security intelligence of application, computing, networking, security and data schema of biological system.
  - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
  - **Level 2**: authentication, authorization, correct identification, privacy, audit;
  - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
  - **Level4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan .
  - Bone cancer treatment : radio graphy, radio surgery, bone marrow transplant, treatment against side effects of hormonal therapy in breast and prostate cancer, bone pain management;
  - Bone pain management through eradication of bone tumors, decreasing the impact of tumor induced bone loss, surgical stabilization of fractures and pain medications;
  - Optimal therapy and treatment outcomes in head and neck cancer through precise identification of the primary tumor and also local, regional, and distant extent of disease.
    - Combined modality therapy
      - Induction chemotherapy
      - Concomitant radiotherapy and chemotherapy
      - Adjuvant Chemoradiotherapy
  - Do medical testing → Data visualization of digital x-ray, molecular images of cancer cells growing in bones, detection of tumor cells in bone marrow;
  - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
  - Physiotherapy
  - Integrated medicine

- **Fight against bad luck :** Identify critical risk elements.
  - Genetic disorder (sex, race, ethnicity, somatic mutation)
  - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
  - Injuries from accidents, war and crime
  - Bone fracture in sports and games (e.g. football, rugby, boxing)
  - Occupational exposure (e.g. mason)
  - Environmental pollution
  - Hostile climate, weather and other locational disadvantages;
  - Malnutrition due to poverty
- Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan

I. Reproductive System

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human reproductive system;
Objectives: cancer prevention at optimal cost; focus : (a) ovarian cancer; (b) testicular cancer; [34,35]
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender:** The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).
- **Attacker:** The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.

Cancer Prevention Approaches:

- **Proactive approach**:
  - **Identify targets** :
    - application schema : human reproductive system;
    - networking schema :
      - male : scrotum, testes, vasa efferentia, epididymes, vasa deferntia, ejaculatory ducts, urethra, penis; prostate glands;
      - female : ovaries, fallopian tube, uterus, vagina, vulva, breast;
    - computing schema : spermatogenesis, oogenesis, menstrual cycle, menopause, fertilization, cleavage, implantation, gastrulation, organogenesis, parturition, lactation;
    - data schema : sperm, ovum, egg, zygote;
    - security schema : hormones, minerals, vitamins;
  - **Threat modeling**
    - Call threat analytics and assess miscellaneous risk elements :
      - Testicular cancer
        - Metastatic germ cell cancer
        - CSI Non-seminoma
      - Ovarian cancer
        - genetic risk factors : inherited susceptibility,
        - hormonal risk factors (estrogen and progesterone)
        - age at menarche and age at menopause, gender, race
        - pregnancy, parity and infertility
        - lactation, benign gynecologic conditions and gynecologic surgery
        - oral contraceptives
        - hormone replacement therapy
        - anthropometric factors
        - diet and nutrition, lack of exercise and physical activity, life-style and environmental factors : smoking, alcohol consumption, asthma, drug use, occupational exposure
      - other disorders : impotence, sterility, menstrual irregularity, prostetomegaly;
    - Estimate probability (p) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;

- Estimate requirements of healthcare in terms of demand plan;
- Explore risk mitigation plan : accept / transfer / remove / mitigate risks.
    - Auto-immunity and vaccination;
    - Optimal diet intake to fight against malnutrition;
    - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control;
    - yoga and physical activities, stress control through meditation;
    - secure multi-party computation

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
    - what is corrupted or compromised?
    - time series analysis : what occurred? what is occuring? what will occur?
    - insights : how and why did it occur? do cause-effect analysis.
    - recommend : what is the next best action?
    - predict: what is the best or worst that can happen?
- verify security intelligence of application, computing, networking, security and data schema of biological system.
    - **Level1**: correctness, fairness, accountability, transparency, rationality, trust, commitment;
    - **Level 2**: authentication, authorization, correct identification, privacy, audit;
    - **Level3:** safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
    - **Level4:** stability, system dynamics, quality of application integration.
- Explore risk mitigation plan.
    - Testicular cancer
        - USG detecting a painless swollen mass in testes
        - Determination of AFP, LDH and hCG
        - Surgical exploration in testis to detest germ cell tumor
        - Orchiectomy
        - Organ preserving surgery in case of benign histology
        - Surveillance for low risk patients and adjuvant BEP chemotherapy for high risk patients and also risk adapted treatment
        - First line treatment for metastatic disease and residual tumor resection
        - Salvage treatment, late relapse and follow up
        - Treatment of fertility and sexuality : hypogonadism, ejaculatory disorder, disorder with erectile function and libido, metabolic syndrome (MBS)
    - Ovarian cancer:
        - screening and early detection,
        - early stage treatment : staging, adjuvant chemotherapy,
        - advanced stage treatment : surgical debulking principle,
        - chemotherapy for recurrent ovarian cancer;
        - targeted molecular therapy (TMT)
    - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
    - Radiotherapy
    - Integrated medicine

Fight against bad luck : Identify critical risk elements.

- Genetic disorder (sex, race, ethnicity, somatic mutation)
- Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)

- Occupational exposure (e.g. high workload, stress)
- Environmental pollution
- Hostile climate, weather and other locational disadvantages
- Malnutrition due to poverty

- Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.
- Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;

Output: Cancer prevention plan.

CHAPTER 9: BIOMEDICAL TECHNOLOGY for CANCER CARE - SURGICAL ROBOTICS, LASER, PERVASIVE & WEARABLE COMPUTING

Abstract: This chapter shows the application of deep analytics '7-S' model on the innovation of bio-medical technology for cancer care. The potential of biomedical instrumentation technology has been analyzed in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. The scope of biomedical technology has been explored in terms of artificial pancreas, artificial liver, artificial kidney, artificial cardiovascular system and artificial limbs. The critical observation is that oral insulin is a rational, simple, practically feasible and safe option as compared to artificial pancreas. It is hard to develop artificial kidney, liver and pancreas which can mimic all the functions of related biological organs. The concept of oral insulin is now at emergence phase of technology life-cycle; artificial cardiovascular devices and limbs. It is rational to adopt proactive and reactive approaches to overcome the constraints of biomedical technology. This work also explores the scope of laser therapy, pervasive and wearable computing and surgical robotics for cancer care. Can AI promote such complex innovations in future?

Keywords: Bio-medical technology, oral insulin, artificial pancreas, artificial kidney, artificial liver, artificial cardiovascular devices, artificial limbs, Laser, concurrent engineering, Technology innovation

1. INTRODUCTION

Technological innovations are practical implementation of creative novel ideas into new biomedical devices. Many potential ideas pass through the wide end of an innovation funnel but very few may become successful, profitable, economically and technically feasible products in future. It is an interesting research agenda whether deep analytics may be an effective tool for the diffusion of biomedical technology technology in future. It is a multi-dimensional analysis wherein seven factors must be integrated, coordinated and synchronized. This chapter shows the application of deep analytics '7-S' model on technology innovation of bio-medical technology. Sections 2-8 show the analysis on biomedical technology technology in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. Section 9 concludes this chapter.

2. SCOPE

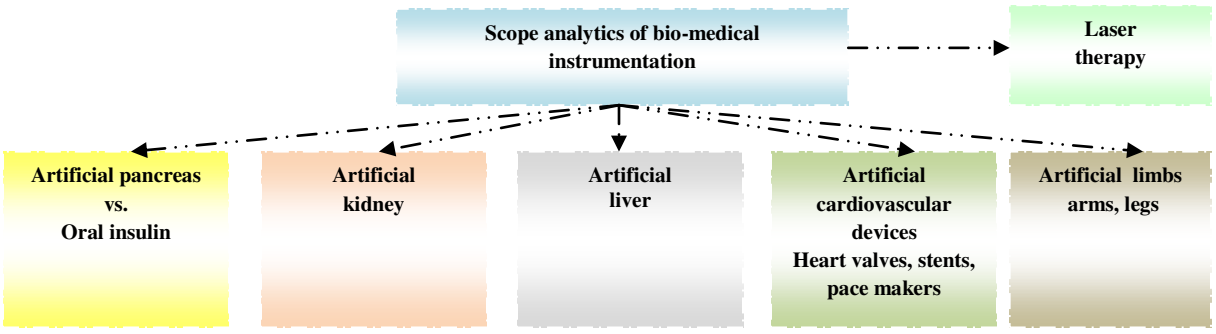


Figure 9.1 **:** Scope analysis of biomedical technology for cancer care

The first element of the deep analytics is scope. The scope of innovation on biomedical technology technology should be explored rationally through intelligent analysis of the basic objectives, goals, needs, constraints and mechanisms; strength, weakness, opportunities and threats of various strategic options [27,37,38]. First, it is essential to understand the mechanisms of various human organs (e.g. pancreas, liver, kidney, heart, limb, brain) in terms of human physiology, input, output, feedback control, function, process,

chemical reaction, secretion of enzymes and hormones, coordination, integration and system performance. Next, it is rational to analyze whether it is practically feasible to make artificial organs which can mimic various functions of biological organs of human body in the best possible ways. The scope of biomedical technology spans over several domains such as artificial pancreas, liver, kidney, cardiovascular system and limbs [Figure 9.1]

2.1 Artificial Pancreas : Let us first do scope analysis on oral insulin vs. artificial pancreas for the treatment of diabetes; which is more feasible technology innovation and why [1-17]? Pancreas synthesizes insulin which extracts glucose from carbohydrate for the supply of energy and storage. It controls blood sugar level and prevents hyperglycemia or hypoglycemia. Insulin is a collection of 51 amino acids with two chains A (21 amino acid) and chain B (30 amino acid) linked by disulfide bridges. Diabetes is a chronic disease, it arises when sufficient amount of insulin is not produced by the pancreas (Type 1 diabetes) or insulin which is formed is not utilized properly by the body (Type 2 diabetes). It leads to an elevation of blood glucose level (hyperglycemia). Diabetes is the most common endocrine disorder. It is a real challenge to find out effective administration and delivery mechanism of Insulin. Subcutaneous (SC) route may lead to hyperinsulinemia. Repeated injections if insulin may result various types of health problems such as lipoatrophy or lipohypertrophy, peripheral hyperinsulinemia, peripheral hypertension, atherosclerosis, cancer, hypoglycaemia and other adverse metabolic effects. Can an artificial pancreas mimic all the functions of a biological pancreas? It is essential to explore alternative route such as oral insulin which mimics the typical insulin pathway within the body after endogenous secretion subject to various constraint such as good bowel absorption and very low oral bioavailability of insulin. Section 5.1 shows detailed SWOT analysis on artificial pancreas vs. oral insulin

2.2 Artificial Liver : Next, let us consider the scope analysis of **artificial liver** [31-36]. Liver is a complex organ doing various vital functions such as synthesis, detoxification and regulation; its failure may result a life threatening condition. Liver failure (LF) can either occur as acute liver failure (ALF) due to intoxication or as acute-on-chronic liver failure (AoCLF). The common symptoms are icterus, hepatic encephalopathy and impairment of coagulation and may result even multi organ failure. In case of liver failure, water-soluble toxins (e.g. ammonia) and albumin-bound toxins (e.g. bilirubin, amino and fatty acids) may accumulate and cause encephalopathy and dysfunction of other organs. Detoxification and regulation can be addressed by artificial devices similar to dialysis, the synthetic function of the liver can only be provided by living cells. In section 5.1, we have done analysis on strength, weakness, threats and opportunities of artificial liver and have also outlined a liver protection mechanism by adopting an optimal mix of proactive and reactive approaches.

2.3. Artificial Kidney: Next, let us consider the innovation of artificial kidney. There are various therapies of kidney problems [e.g. end-stage renal disease (ESRD, continuous renal-replacement therapy (CRRT)] which cause sepsis, systemic inflammatory response syndrome, acute respiratory distress syndrome, congestive heart failure, tumorlysis syndrome and genetic metabolic disturbances [19-24]. The dominant therapies are hemodialysis and hemofiltration [18]. An artificial kidney should perform three physical processes efficiently that determine the removal rate for uremic toxins through membrane-based devices: c*onvection* removes toxin through a semipermeable membrane; d*iffusion removes* smaller molecules with high diffusion coefficients and a*dsorption*.

2.4 Artificial Cardiovascular Devices: Next, let us consider the technological innovation of artificial cardiovascular devices. Cardiovascular disease (CVD) is the leading cause of death worldwide. In this domain, the technological innovation is facing several challenges such as improved device function (e.g. cardiac valves, stents, pacemakers and defibrillators, vascular grafts, hemodialyzers, catheters, circulatory support devices and blood oxygenators), complex and challenging cardiovascular surgical procedures (e.g. open- heart surgery), medical therapies (e.g. dialysis), valve replacement problems (e.g. thromboembolism, hemolysis, paravalvular regurgitation, endocarditis and structural failure of the valve); artificial heart valves design (e.g. percutaneous or minimally invasive valve implantation and tissue engineering), progress in stent technology to reduce restenosis and improvement of stent outcome, development of pacemakers, cardioverter-defibrillator (AICD), cardiac electrophysiologic devices from the perspectives of improved device function, dual chamber activity, advances in technology and implantation techniques, development of artificial lung for acute cardiopulmonary bypass and improved biocompatibility [28-30].

2.5 Artificial Limbs: The basic objective of prosthetics research is to design and develop artificial arms, hands and legs which can be used flexibly with physiological speeds-of response and strength and controlled almost without thought [41,43]. The current state is basically a tool rather than a true limb replacement. The prosthesis is an interchangeable device that is worn and used as needed and then ignored. The major constraints of prostheses are weight, power, size and sufficient number of appropriate control sources to control the requisite number of degrees of freedom [47,48]. The system requires better sensors, actuators and multifunctional control mechanisms. The basic building blocks of artificial limbs are mechatronics and robotics; current prosthetic components and interface techniques are still a long way from realizing the aforesaid objectives [51,52].

3. SYSTEM

The second element of deep analytics is system which should be analyzed in terms of state, complexity, feedback loop, physical and information flows**.** The basic objectives of system analytics are to analyze complex and dynamic interactions among various components of different types of biomedical devices such as artificial pancreas, liver, kidney, cardiovascular devices and limbs.

3.1 **Artificial pancreas :** An artificial pancreas is expected to perform various types of functions such as continuous blood glucose monitoring without manual intervention of the user, monitoring trends of rising and falling blood sugars for the prediction of blood glucose levels in the immediate future, comparing blood sugar levels against a high threshold, and prompting for a correction bolus from the insulin pump and also comparing blood sugar levels against a low threshold and prompting to reduce the basal insulin from the pump. A stream of real-time data is used for close loop control of the insulin pump. The critical components of artificial pancreas are sensors, control algorithm and insulin pump.

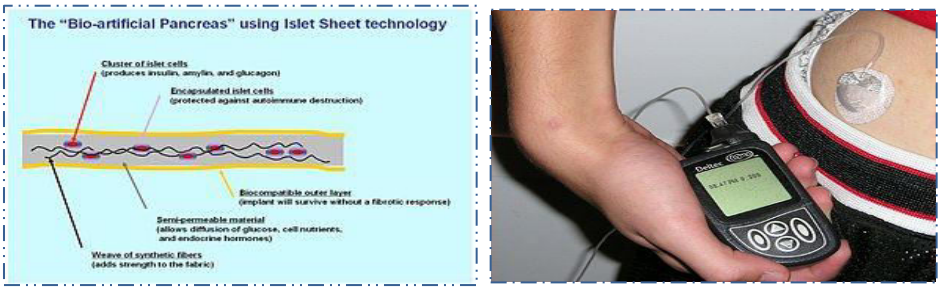


Figure 9.2 : (a) Artificial pancreas (b) Insulin pump

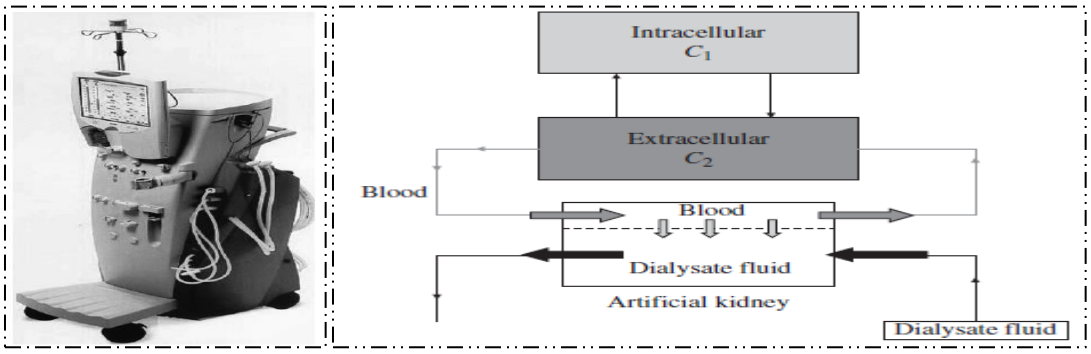
3.2 Artificial liver: Next, let us consider the innovation of artificial liver. Liver failure can be overcome by orthotropic liver transplantation and this motivates the development of various artificial and bioartificial liver support devices [33-35, 36]. Artificial systems are based on the principles of adsorption and filtration; bioartificial devices are based on the provision of liver cells. Such artificial livers support detoxification, synthetic and regulative functions. In case of orthotropic liver transplantation, many patients may not survive until a suitable donor organ is available since donor organs are rare. Contraindications do not permit liver transplantation. For these problems, artificial devices are essential to bridge the patient to transplantation or temporarily support the failing organ. Cell free artificial systems use adsorption and filtration through removal of toxins from the patient's plasma. Haemodialysis is used for treatment of liver failure to remove water soluble toxins.

A bioartificial liver device (BAL) is an artificial supportive device based on bioengineering for acute liver failure patient. Is it really feasible to develop a complex artificial liver which can mimic each function of normal and healthy liver? Dr. Kenneth Matsumara developed BAL based on liver cells obtained from an animal; a semipermeable membrane allows toxins and blood proteins to pass. Advancements in bioengineering techniques have led to improved membranes and hepatocyte from various cell sources such as primary porcine hepatocytes, primary human hepatocytes, human hepatoblastoma (C3A), immortalized human cell lines and stem cells. But, BAL can not replace liver functions permanently and serve as a supportive device for acute liver failure.

There are several limitations of bioartificial liver support. In most cases, the liver cells are separated from the patient's blood or plasma by at least one membrane which provides an immunological barrier limits the

exchange of substances and reduces the effectiveness of the system. The blood/plasma flow is limited to 100–300 mL/min whereas the blood flow in a normal human liver is about 1500 mL/min. Then, what should be rational risk mitigation strategies for the problems of liver?
In charcoal haemoperfusion, there is risk of biocompatibility, loss of thrombocytes and clotting problems. Plasma exchange using filters requires a large plasma stock and bears the risk of infections. But, improved biochemical and clinical conditions and removal of toxins may not ensure survival benefit for the patients. It is essential to explore more sophisticated detoxification systems like albumin dialysis, fractionated plasma separation, continuous albumin purification system (CAPS) and Single Pass Albumin Dialysis (SPAD). Bioartificial systems give support in synthetic and regulatory function of the liver besides detoxifying the patient's plasma. Primary human cells meet the demand of biocompatibility. But, there is risk of infections and metastasis formation; the metabolic compatibility is not assured. It is really hard to find ideal cell source.

3.3 Artificial kidney : Let us now consider the technological innovation of artificial kidney. The system needs focus on several areas such as maturation of hemodialysis and hemofiltration therapy, improvements in materials and hemodynamic areas, biocompatible materials, superior transport methods for toxin removal, bioartificial renal tubule, homeostatic functions, selective toxin removal without concomitant elimination of beneficial proteins, absorption removal pathway (with affinity methods to eliminate uremic toxins), tissue engineering and improved patient management techniques [18-24]. An artificial kidney is expected to perform a number of important metabolic, endocrine and active transport functions of living kidney.

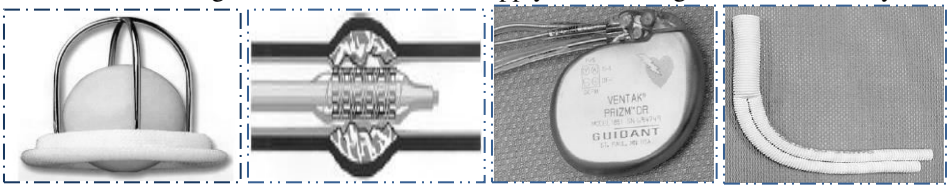


(a) (b)

Figure 9.3: (a) Hemodialyzer; (b) Basic mechanism of artificial kidney

3.4 Artificial cardiovascular devices: The basic objectives and challenges of the design of artificial cardiovascular devices is to replace various lost functions of heart, improve the performance of artificial valves, stents and pacemakers and to minimize the side effects and risks of complex surgical procedures. The number of surgical operations of valve replacement, stents and pacemakers has been increasing day-by-day due to various reasons like congenital valve defects and acquired valve disease of various patient groups and valve location. Valve replacement can be done for aortic or mitral valves. The design of artificial valves is evolving based on minimally invasive valve implantation and valvular tissue engineering through the advancement of computational fluid dynamics and computationally intensive simulation modeling techniques. Simulations can predict the performance of both bioprosthetic and mechanical valves and analysis of various complications such as structural failure, thromboembolism, hemolysis, paravalvular regurgitation and endocarditis [27,59-62].
Stent is used to hold tissue in place or provide a support for a graft and applicable to the diseases of peripheral and coronary arteries. Stents may be of two types such as balloon-expandable and self-expanding. The design of stent is evolving in terms of advanced material science [metal, alloys (e.g. tantalum, steel, Nitinol), biodegradable and nondegradable polymeric stents], improvement of system performance, reduction of the risks of restenosis, ease of handling and stable long term system performance, simple and effective deployment method. Percutaneous Transluminal Coronary Angioplasty (PTCA) moves a catheter mounted balloon to specific site and inflated to displace the tissue and create a wider lumen in the blood vessel. Percutaneous coronary intervention (PCI) refers to a set of procedures like PTCA, atherectomy, thrombolysis, intravascular radiation and correct placement of stents.

The technology of pacemakers and ICDs (cardioverter defibrillators) is evolving in terms of dual chamber activity, cost reduction, potential harmful interactions, reduction in number of leads, improved device function, advances in technology and implantation techniques. A pacemaker delivers an electrical impulse to depolarize the heart chamber in a spreading and coordinated way like a normal heartbeat. In contrast, defibrillators are used to depolarize the entire heart at once to terminate uncoordinated contractions. It is extremely useful while electric impulse conduction or initiation in the heart is blocked, slowed or triggered irregularly. The technology of artificial vascular grafts is passing through technological and clinical advancements such as endovascular therapies (angioplasty, stent), less invasive interventions for vascular repair and reconstruction, reduction in open excision and replacement, development of tissue engineered blood vessels (TEBV), performance improvement of vascular graft designs, novel coatings, improved biocompatibility and minimization of hematologic alterations. The other critical technologies are circulatory support devices for chronic congestive heart failure, artificial lungs, intra-aortic balloon pump (IABP), ventricular assist devices (VADs) and total artificial hearts (TAH). The technology is evolving with the advancement of electronics and software engineering. IABP requires that a patient maintains some native pumping capacity. A cardiac transplant is the last resort for critical patient care which fails conventional medical and surgical treatment. But, the supply of donor organs is limited today.



(a) (b) (c) (d)

Figure 9.4: (a) Artificial heart valve, (b) stent, (c) cardioverter defibrillator, (d) artificial vascular graft

3.5 Artificial limbs : Is it possible to design artificial limbs from the concept of robotic arms? what are the similarities and differences? What are the mechanical constraints: size, weight and power? What are the other design constraints: interface between artificial limbs and human body, sensors, strong light weight materials for prosthetic socket and interfaces; how to mimic the functions of biological limbs of human beings from the perspectives of ease of use, comfort and flexibility? what should be the system control mechanisms? Is it possible to design artificial limbs through CAD / CAM software? An intelligent system analytics is expected to resolve these issues accurately [39-58].

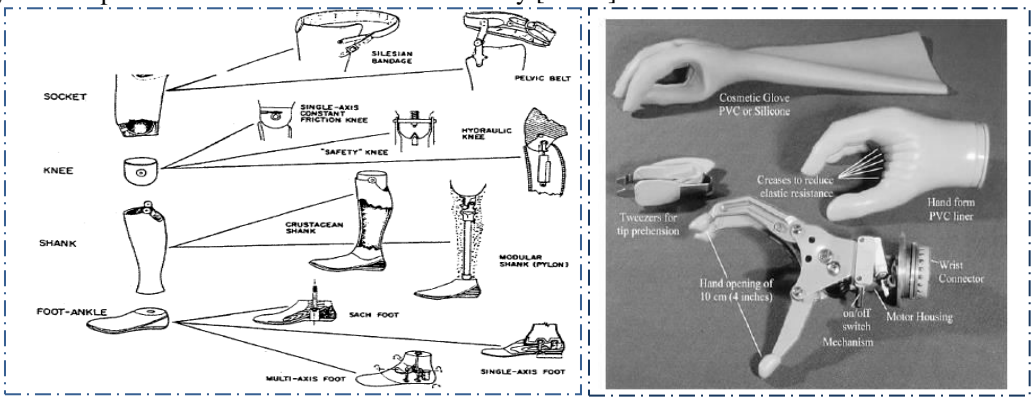


Figure 9.5: Artificial limbs - (a) artificial legs, (b) artificial arms

4. STRUCTURE

The third element of deep analytics is structure i.e. the backbone of a system associated with a specific technological innovation of a biomedical device. The topology of technology should be analyzed in terms of circuit intelligence: nodes, connectivity, type of connections; layers, interfaces between layers and organization of layers. Today, it is hard to perceive a concrete picture of the aforesaid artificial biomedical devices from conceptual stage. The system architecture of the aforesaid biomedical devices is not yet

transparent; it is not a simple design. The architecture depends on the mechanism of the biomedical device; and also computing, data, networking, application and security schema.
Tissue engineering is expected to be a good solution to the innovation of aforesaid artificial organs (e.g. artificial kidney, liver and pancreas) through cell and gene therapies. It is an emerging trend of biomedical engineering; the basic building blocks are cellular, organ and molecular biology, biotechnology, chemical and mechanical engineering and material science [25]. It may be possible to reconstitute, maintain, simulate and improve tissue or organ functions in building artificial organs. It is an interesting research agenda whether it will be possible to replace physiological functions of diseased tissues and living organs with synthetic materials, biological compounds and cells.

5. SECURITY

It is essential to design biomedical devices in terms of security at various levels – L_1, L_2, L_3, L_4 and L_5. Level L_1 verifies system performance in terms of correctness of measurement of health parameters by sensors, safety, reliability, consistency, stability and robustness. The device should be safe. Safety is the most important consideration in the design of any biomedical device. Let us consider the safety aspects of artificial kidney in terms of biological, chemical, mechanical and human factors. The device should have high biocompatibility and blood compatibility; the device should not cause hemolysis i.e. destruction of red blood cells. Water quality is a major safety concern for dialysate fluid. The dialysis membrane should have high shear and ultimate strength. The device should be easy to operate and should be fool-proof. The design of artificial limbs is expected to satisfy several critical requirements such as subconscious control, user friendliness for simple learning and use, independence in multifunctional control, parallel control of multiple functions, direct access, speed of response, no sacrifice of human functional ability and natural appearance.

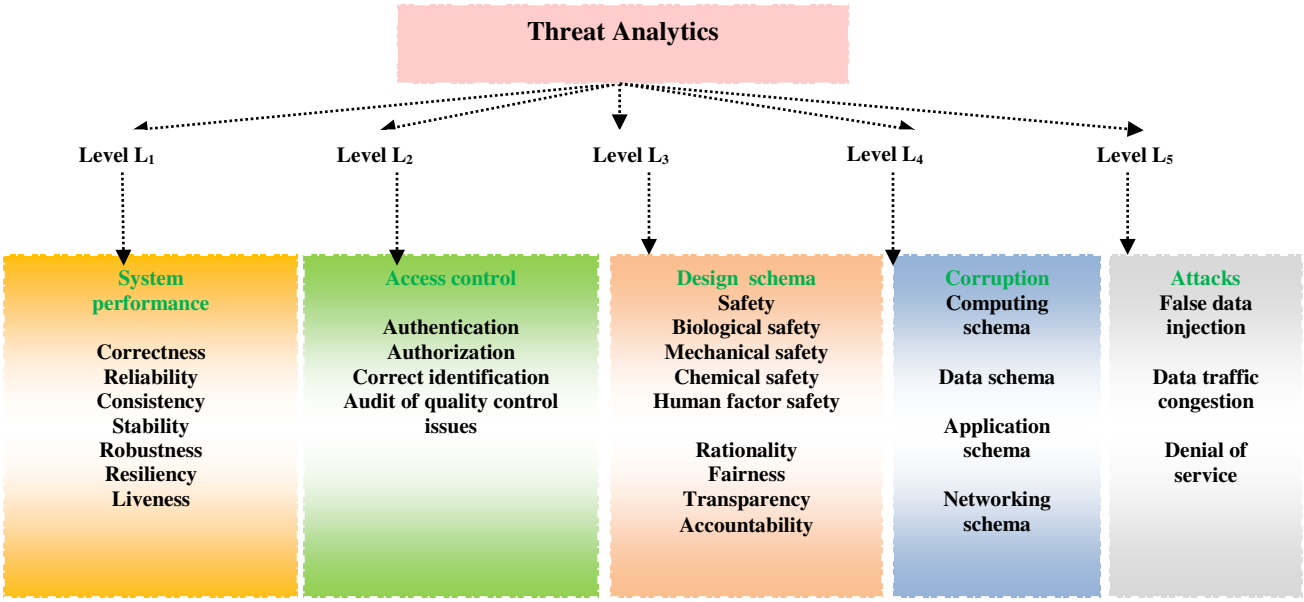


Figure 9.6 Security analyses for biomedical technology

The other critical design issues are also associated with resiliency, deadlock-freeness, synchronization and interactive intelligent communication protocol. The safety of bio-medical devices depends on access control at level L_2 in terms of authentication, authorization, correct identification of system components and audit of quality control issues. The security schema is also designed and verified at level L_3 in terms of rationality, fairness, transparency, accountability, trust and commitment.
The safety of the bio-medical devices may be threatened at level L_4 through corruption of computing, data, application and networking schema. The design of the bio-medical devices is also expected to assess and mitigate the risks of various types of attacks at level L_5 such as false data injection, shilling and data traffic congestion. A biomedical device should be safe from the perspectives of biological, chemical, mechanical,

human factor safety. Safety is one of the most important design criteria. A biomedical device should have high biocompatibility and blood compatibility. For example, an artificial kidney should not result hemolysis i.e. destruction of RBC; should not adsorb or filter blood cells; should not introduce any foreign toxic materials into blood; also remove toxic material. The quality of *w*ater is a major safety concern for dialysate fluid. The dialysis membrane should have high shear and ultimate strength and dimensional stability. A biomedical device should be easy to operate and should be fool-proof. Alarms should be incorporated into a biomedical device the dialysis machine to signal any malfunctioning of the system components.

6. STRATEGY

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision and goal,. Biomedical innovations are closely associated with various strategies of organization learning and knowledge management. The aforesaid biomedical innovation is closely associated with R&D policy and organizational learning strategies in new product development. There are various strategies of learning such as learning by doing and learning before doing. Learning before doing is possible through laboratory experiments, prototype testing and simulation. Deep practical and theoretical knowledge can be achieved through laboratory experiments. Learning by doing is also important to understand the impact or side-effects of the implantation of biomedical devices and oral insulin.

Technology innovation on biomedical technology is associated with various strategic moves and functions such as scope analysis, requirements engineering, quality control, product design, concurrent engineering, talent management, team management and coordination, resources planning, defining products specification, concept development, concept evaluation, system architecture design, detailed design, production plan development, roll out, prototyping, testing, documentation, tools development and regulatory issues [37-38].

The design of a medical product is a complex task having uncertain information, high stakes and conflicts, varieties in size, scope, complexity, importance and cost and various constraints in terms of product quality, product cost, development cost, development time and development capability. It is essential to adopt concurrent engineering approach which considers all aspects of the problems faced and a clearly defined role. It is challenging to develop a product development team with specific skills and group dynamics. The next step in our process is to transform these needs into specifications that can be used to guide the design decisions. These product specifications become the targets for the product development. The concept development phase is the time to search out ideas that will meet the need. Next important steps are concept evaluation through SWOT analysis, design of system architecture, prototyping and product testing. Finally, it is essential to satisfy various issues of regulatory compliance such as approval of FDA. It is not a simple task to make rational decisions on strategic technologies, ICT, technology infrastructure development and renewal of existing technologies.

6.1 SWOT Analysis: It is an interesting research agenda to analyze strength, weakness, opportunities and threats of innovation on biomedical technology. Strength indicates positive aspects and benefits; weakness shows negative aspects and limitations of the same; opportunities explore the growth potential and threats assess the risks of the technology. Let us compare two strategic options for the treatment of diabetes: oral insulin vs. artificial pancreas based on biomedical technology [2,7,8,11,12]. The critical observation from this deep analytics is that oral insulin is a rational, simple, practically feasible and safe option as compared to artificial pancreas. But in case of pancreatic cancer, artificial pancreas may be an essential option. However, the concept of artificial pancreas is a very complex and costly strategic option and there is threat of immunity and safety from the perspectives of adaptability of human biological system. But, both the aforesaid options are not matured at their technology life-cycle; they are now at emergence phase. It is also essential to adopt a set of proactive and reactive measures to fight against diabetes such as herbal and homeopathic medicines, yoga, meditation, healthy life-style, obesity control and organ replacement.

Diabetes is a disorder of deficiency in insulin, a peptide hormone of pancreas. Insulin is generally given by subcutaneous (SC) route; the non-compliance of diabetic patients is a common occurence. Oral insulin is an alternative option but it is essential to identify appropriate delivery mechanism. Oral insulin is the dream of

diabetic patients. Nanotechnology may be an innovative strategic option in this connection due to the size of particles in nano range and greater surface area [3,4]. These physical and chemical properties improve the absorption of nanoparticles as compared to larger carriers. This is a real challenge of today's research on oral insulin from the academic and industrial community. Is it possible to use nanoparticles as a carrier to deliver insulin orally?

Let us analyze the strength and opportunities of oral insulin delivery mechanism which support a cost effective, convenient, simple and painless treatment; it reduces the risk of hypoglycemic incidents, immune responses and obesity. The threat and weaknesses of SC route mechanism may be considered from various aspects such as hyperinsulinemia, lipoatrophy, lipohypertrophy, patient noncompliance, painful procedure of injections and cost for the treatment for hyperglycemia, retinopathy, neuropathy and nephropathy. There are various types of Diabetes Mellitus such as Type I, Type II, gestational and secondary.

Now, let us consider the strength of nanomedicines. For oral insulin delivery, it is possible to explore various types of options such as nanoparticles (NPs), liposomes, microemulsions (MEs), self-nanoemulsifying drug delivery systems (SNEDDS), micelles, nanogels (NGs), microspheres, niosomes, and superporous hydrogels (SPHs). A NP is a small entity, particle size ranges from 10 to 1000 nm. Two major pathways by which NPs pass through intestinal epithelium are paracellular and transcellular. Transcellular route is the most common route of absorption. NPs can be classified into polymeric and lipid-based systems. Biocompatible and biodegradable polymeric NPs may be an ideal carrier for delivering proteins and peptides orally. It improves bioavailability of oral insulin. It may be Nanospheres and nanocapsules. Solid lipid nanoparticles (SLNs) offer some advantages like nano size range and comparatively narrow size distribution, controlled release of drug over a long period of time, protection of drug against chemical degradation, nontoxic, relatively cheaper and stable and can be easily freeze or spray dried. Liposomes offer several advantages such as nanosize, able to incorporate both hydrophilic and hydrophobic drug, improved effectiveness, better stability by encapsulation, non-hazardous, compatible in biological environment, biodegradable, and nonantigenic; biotinylated liposomes (BLPs) enhance the delivery of insulin.

Nanocarrier based systems for mucoadhesive drug delivery systems prevent degradation of entrapped drug and improve the circulation time of drug at absorption site. Polyionic polymers show mucoadhesive properties. From such polymers, alginate has shown the best candidate for the intestinal mucosal system. Alginate is a nontoxic, biodegradable, and mucoadhesive polysaccharide polymer that possesses mucoadhesive properties than carboxymethylcellulose, chitosan, poly (lactic acid), and other polyionic polymers.

It is essential to improve oral insulin delivery mechanism due to incomplete and unpredictable absorption through gastrointestinal tract, degradation due to varying pH of the stomach and enzymatic degradation lead to poor oral bioavailability. The structure of insulin is very delicate. Stability is affected by component and processing elements; the common degradation pathways are oxidation, photodegradation, disulfide scrambling, deamidation, aggregation, precipitation, dissociation and fragmentation.

Next let us focus on strength and weakness of artificial pancreas. Artificial pancreas is a technology that controls blood sugar level of diabetes patients and acts as the substitute of a healthy. A pancreas performs various exocrine digestive and endocrine hormonal functions There are alternative options of treatment such as insulin replacement therapy having life saving capability and manual control of blood sugar level with several limitations. The basic objectives of artificial pancreas is to improve insulin replacement therapy and to ease the burden of therapy. There are various types of approaches such insulin pump through close loop control based on real-time data from a continuous blood glucose sensor, bioengineering approach through surgical implantation of a biocompatible sheet of encapsulated beta cells and gene therapy approach through therapeutic infection by a genetically engineered virus which changes DNA of intestinal cells to insulin producing cells.

Artificial pancreas is used to deliver basal insulin automatically and continuously at meal time by pressing the buttons of insulin pump. Blood sugar data is given to the insulin pump before meals. It calculates the correction bolus to bring the blood glucose level back to the target. But there are several complexities of artificial pancreas such as calibration for sensor correction, correctness in measurement of blood sugar levels, skill, intellect and knowledge of the diabetic patients, maintenance of medical equipments and verification of the correctness of automatic control of basal rate of insulin pump, adaptive filtering for learning unique basal rate, feedback from a continuous blood glucose sensor and adjustment of correction bolus during increase or decrease of blood sugar level. Typically, implantable insulin pumps work for an average of eight years and the sensors stop working after an average of nine months. From the aforesaid

analysis, it is clear that oral insulin is a much more simple and rational strategic option as compared to artificial pancreas and demands much more focus of R&D.

It is an interesting research agenda to do SWOT analysis on **artificial liver** vs. biological liver transplantation [35,36]. Both the options may be essential for various types of liver diseases such as liver cancer, cirrhosis of liver, jaundice, hepatitis, alcoholic liver problem, chronic liver problem, autoimmune hepatitis, Wilson's disease, black stool, blood vomit, swollen legs and heals and water accumulation. But, there are several constraints such as adaptability and immunity. Can an artificial liver mimic all the functions of a biological liver?

Generally, the patients suffer from liver cirrhosis due to regular consumption of booz; liver cells are destroyed and the liver is scarred due to the effect of alcohol. Non-alcoholic fatty liver disease (NAFLD) is the accumulation of fat in the liver not triggered by alcohol but caused by erratic life-style, high blood sugar, cholesterol and obesity. It often remains undetected and may lead to liver cancer. There are other various types of liver problems such as liver cirrhosis and acute hepatitis [B or C type]. Acute hepatitis are treatable and can be prevented with vaccines but chronic hepatitis or NAFLD are not fully reversible. It can not be cured but can be merely controlled. The common prevention strategies for NAFLD include avoiding fatty food, daily physical exercise, periodic screening of liver and control of blood sugar and cholesterol levels. It is technologically hard to develop an artificial liver that can mimic all the functions of biological liver in human body. Alternatively, it is rational to adopt an optimal mix of proactive and reactive approaches which can protect liver from various toxic effects.

Liver Protection Mechanism:

Proactive approach:

- Control consumption of booz / country liquor / wine / alcohol for the treatment of cirrhosis of liver;
- Avoid excessive consumption of non-vegetarian food (e.g. red meat, egg, fish);
- Take fruits regularly (e.g. Jambura or 'batabi lebu', mousambi, orange);
- Take herbal medicine periodically and vitamins;
- Acute hepatitis are treatable with vaccines;
- Avoid fatty food, daily physical exercise, periodic screening of liver and control of blood sugar and cholesterol levels for prevention of NAFLD;

Reactive approach

- **Acute liver failure:** Organ transplantation is a feasible option but it should consider following issues carefully.
    - Is there any problem of immunity and infection in case of liver transplantation from other animals?
    - Which animal should be considered for organ transplantation: human being, goat, lamb, cow, pig?
    - Is it possible to transplant a healthy liver from a dying person to a liver patient?
    - Is it possible to set up animal liver bank to preserve animal livers in advance?
    - Liver dialysis : BAL can replicate several metabolic functions such as detoxification, lipid and plasma lipoprotein synthesis, carbohydrate homeostasis and production of serum albumin and clotting factors wi9thout using multiple devices. BAL device reduced mortality by about half in acute liver failure cases.
    - Is it possible to develop artificial liver that can mimic all the functions of normal and healthy biological liver? It is a promising but challenging task in terms of product design, clinical study and identification of ideal cell source that can grant patients substantial survival benefits compared to standard intensive care.

Liver transplantation is a feasible solution to acute liver failure but severe shortage of donors is a major constraint. Artificial hepatic support systems should provide optimal cell survival, proliferation and maintenance of sufficient liver functions. Liver is one of the most sophisticated organs in human body, the science of liver tissue construction is also very complex.

The evolution of technological innovation of **artificial kidney** depends on various factors such as tissue engineering, biocompatible materials, transport mechanism; hemodynamic, absorption, hemodialysis and hemofiltration therapy, animal studies and extensive clinical trials [20-22,25]. Can an artificial kidney mimic the metabolic, endocrine, and transport functions of a healthy living kidney efficiently? The present technology cannot replace an ailing kidney with artificial one. It is technically hard and complex to develop

artificial kidney and install the same in human body. What are the side-effects of an artificial kidney on human biological system? Is it possible to explore proactive and reactive approaches for the protection of kidneys rationally? Generally, it is recommended to drink water sufficiently and avoid excessive consumption of salts. Is it possible to improve the functions of a kidney artificially using medicines – it may be herbal, allopath or integrated medicine? Dialysis is a popular method of treatment. Acute kidney failure needs organ transplantation and surgical operation. Is there any problem of immunity and infection in case of transplantation of kidney from other animals? Which animal should be considered for organ transplantation? Is it possible to transplant a healthy kidney from a dying person to an ailing patient? These are alternative feasible options as compared to artificial kidney.

It has been possible to simulate the functions of a kidney through renal substitution therapy with hemodialysis or chronic ambulatory peritoneal dialysis (CAPD) and transplant it from a donor to a patient successfully. Dialysis is basically renal substitution rather than renal replacement therapy. It only mimics the filtration function but can not replace homeostatic, regulatory, metabolic and endocrine functions of a healthy kidney. So, dialysis has major medical, social, and economic problems. A biohybrid kidney may have biological and synthetic components. It is expected to offer many benefits such as reduced cost, time and infection and increased flexibility, mobility and life expectancy.

6.2 Technological life-cycle analysis

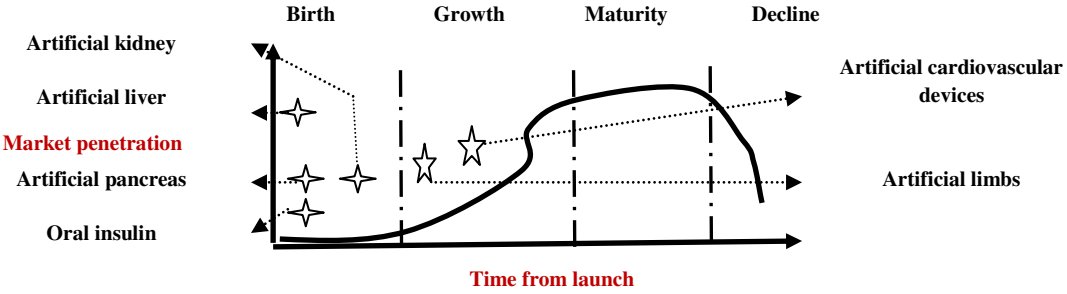


Figure 9.7 : Technology life-cycle analysis

The basic objective of deep analytics is how to manage evolution of the aforesaid technological innovations effectively. It is really interesting to analyze the impact of various factors and patterns of trajectories of biomedical innovations. It is possible to do the analysis of life-cycle based on S–curve, trajectory, diffusion and dominant design of the aforesaid innovations. Technology trajectory is the path that the new technology follows based on rate of improvement in performance, diffusion and adoption. It is perceived today that the innovations of oral insulin, artificial pancreas, artificial liver and artificial kidney may be at emergence phase of S-curve. On the other side, the innovations on artificial cardiovascular devices and limbs may be at growth phase of the curve. The emergence of such new technologies follow a complex process. It is really hard to understand how the life-cycle of a new technology interacts with other technologies and impacts on healthcare and life-science sectors. The next phase is growth if the technology; initially it is difficult and costly to improve the performance of a new biomedical device. The performance is expected to improve with better understanding of the fundamental principles of the technology and system architecture. Initially, the new technology may be costly and risky for the early adopters. Gradually, it should reduce the cost and risks of the biomedical devices and penetrate the market rapidly.

The diffusion of biomedical technology and oral insulin depends on how new technologies can spread through potential adopters such as the patients and healthcare consultants. Diabetes is a very common healthcare problem today; the size of the market of oral insulin is expected to be big. The rate of diffusion depends on the effectiveness, reliability, consistency and flexibility in system performance and the economic and demographic profile of the adopters. The rate of improvement of the aforesaid biomedical technology technologies and oral insulin should be faster than the rate of market demand over time; the market penetration is expected to increase with high performance and efficiency of the bio-medical devices and oral insulin. At present, the evolution of these technologies are going through a phase of turbulence and uncertainty; the firms are exploring a set of competing options; a dominant design is expected to emerge through consensus and convergence of biomedical system. The dominant design must consider an optimal

set of features which should meet the demand of the patients and healthcare experts in the best possible way.

7. STAFF-RESOURCES

The sixth element of deep analytics is staff-resources which can be analyzed in terms of sources of innovation and roles of biomedical engineering and pharmacy firms, healthcare institutes, government and collaborative networks; optimal utilization of man, machine, material, method and money, dominant design factors and technological spillover. The innovation demands the commitment of creative experts of bio-medical engineering, healthcare and life-science sectors who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab, start-ups (e.g. science parks, incubators), academic institutions, ministries of state and central government, patients, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

8. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. bio-medical engineering, pharmacy, life-science), healthcare and medical science domain such as research and development, knowledge management, product design, project management, supply chain management, sales and distribution [37]. It is essential to teach Biomedical technology innovatively in various programmes of Electrical, Electronics and Biomedical engineering as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented.
It is essential to develop skill in new product development through proper coordination among design, supply and patient chain and R&D, production and marketing functions. The basic objectives are to maximize fit with customer's needs and demands, ensure quality assurance, minimize time to market, and control product development cost. It may be an intelligent initiative to involve the suppliers and the customers in the development process, beta testing, fault tree and failure mode effects analysis and TFPG as part of quality control measures. It is really challenging to manage new product development team through diversity, knowledge base, multiple skills, problem solving capability, cooperative corporate culture and intelligent communication protocol at optimal administrative costs.

9. CASE BASED REASONING on BIOMEDICAL TECHNOLOGY for CANCER CARE

Let us consider three emerging technologies based on biomedical instrumentation, computer science and AI : (a) Laser therapy, (b) Wearable & Pervasive computing and (c) Surgical robots. These technologies may be interesting and good solutions for cancer care in future.

9.1 CASE STUDY 1 : LASER THERAPY FOR CANCER CARE

This section analyzes the emerging trend of laser technology for various biomedical applications such as dental problems, piles, fissures and fistula [63]. In previous chapter, we have already shown the application of laser for cancer care alongwith details of various advantages. In case of dental problems, smart diode

laser is effectively used for the treatment of both hard and soft tissues with utmost care, precision, consistency, speed and control. The diode laser is a solid state semiconductor which produces laser wavelength (e.g. 980 nm). Laser therapy is minimally invasive, less painful, takes shorter time, reduces number of seating and ensures better healing and changes the experiences of the dental patients positively.
This laser system uses two wavelengths of 635 nm and 980 nm through transmission or absorption effects (Figure 9.8). 635 nm shows excellent photo biological effects due to high transmission in water. It is also optimally selected for photochemical effects and local ozone therapy activated by tolonium chloride. 980nm wavelength shows high soft tissue absorption efficiency and excellent safe surgical results for soft tissue cutting at low power radiation. Smart diode laser is expected to be cost effective (e.g. low operating cost), light weight, easy to handle, supporting preset procedures and customized programmes; equipped with large touch screen and LCD display, high storage space and advanced security features. 980 nm 10W is used for *soft tissue cutting* (e.g. coagulation, gum contouring and reshaping, gingive retraction, Haemostasis in gingival sulcus for prosthodontics impression, exposure of implants, lingual and fabial frenotoma and frenectomy, abscess opening, Epulis papiloma and fibroma removal periodontology, elimination of bacteria in periodontal pockets endodontic, sterilization of root canal and closure of microhannels); *aesthetic dentistry* (e.g. power bleaching of viral and non viral teeth) and *biostimulation* (e.g. wound healing, root canals, support in treatment of periapical lesions, periodontitis and periimplantitis, decontamination of cavities before filing treatment of chronic and recurrent aphthae, hygienisation of cervical area after scaling) and photoactivated disinfection (e.g. : root canals, periodontal pockets, support in the treatment of periapical lesions, periodontitis and periimplantitis, decontamination of cavities before filing treatment of chronic and recurrent aphithae, widespread and local inflammation of the mouth caused by herpes virus) [64].

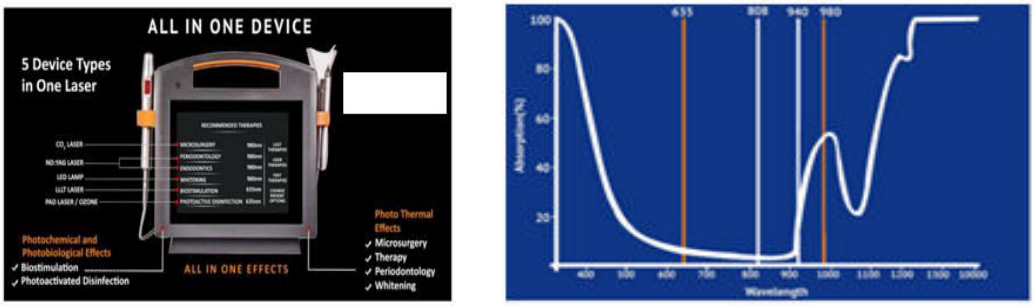


Figure 9.8: Laser diode for dental care

Diode laser therapy offers various types of benefits such as less invasive, less painful, less bleeding, less trauma, faster healing, no scars , less time (e.g. not more than an hour) and can be treated in an ambulatory condition with local anesthesia. It provides the choice of two specific wavelengths: 980nm, 10/15 W for haemorroids and fistula as safe and efficient absorption coefficient and 1470nm, 15W for varicose vein and 2 types of fibres with open end or radial (Figure 9.8). It is a cutting edge technology; has low operating cost, very compact and small sized device and may have extendable database of predefined therapy protocols and flexible customized parameters. In case of fistula, laser energy is delivered via radial fibre into the anal fistula tract and is used to thermally ablate and close off the abnormal pathway. It gives good control to the operator in surgical operation and ensures fast healing process. The tissue is destroyed and the fistula tract collapses to a very high degree. So, laser therapy can be effectively used for colone cancercare.

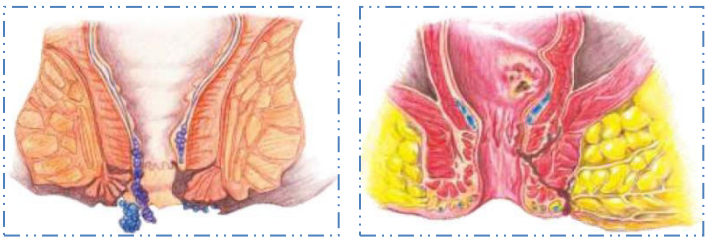


Figure 9.9: Hemorrhoids and piles; (b) Fistula

9.2 CASE STUDY 2 : PERVASIVE & WEARABLE COMPUTING for CANCER CARE

One of the most promising emerging digital technology is health monitoring smart wearable systems (SWS) through advances of microelectromechanical systems, electrical simulation, mechatronics, sensors, actuators, biomedical instrumentation and nanotechnology. SWS is an interesting cost-effective solution which can monitor a patient's health status in real-time and support complex healthcare applications for disease prevention, symptom detection and medical diagnosis. Let us consider the structure of smart wearable system (SWS). The system may have various types of digital and mechatronics components such as sensors, actuators, power supplies, wireless communication and processing units, algorithms, software, UI and smart fabrics to capture and process data and make intelligent decisions based on the measurement of various parameters of human body such as temperature, blood pressure, heart rate, respiration rate, blood oxygen saturation, EEG and ECG. The measured data are sent to a central node (e.g. PDA, medical centre) through wireless communication system. SWS is expected to monitor the state of the health of human agents (e.g. patients, athletes), issue alerts and send feedback to the medical staff in real-time. The healthcare experts and consultants can take rational decisions on patient care accordingly. There are various issues and challenges in wearable and pervasive computing, telecare, tele-health and telemedicine through new models, prototypes, test beds and industrial products to enhance the performance of healthcare system and minimize the risk of illness, injury, inconvenience and rehabilitation. There are some constraints in terms of high cost, size, weight, energy consumption, complexity of sensor implementation and connectivity, ethics, laws, information security and privacy, freedom, autonomy, reliability, consistency, safety and service issues.

9.3 CASE STUDY 3 : SURGICAL ROBOTICS for CANCER CARE

Artificial intelligence simulates human intelligence and develops algorithms that can learn and perform intelligent behavior with minimal human intervention, high precision, accuracy and speed. Robotics is an interdisciplinary branch of mechanical, electrical and electronics engineering and computer science. Various domains of AI are used in medical robotics such as computer vision, edge computing, deep, transfer and reinforcement learning. A medical robot is a programmed machine designed to execute one or more tasks automatically and repeatedly with speed and precision for delicate and complicated surgical operations where human skills may not be applicable appropriately. The basic objectives of medical robotics are design, construction, operation and use of robots and related information system for control, feedback and information processing and development of sensors and human robot interface. The critical components of a robot are controller or brain run by a computer program; robotic operating system; electrical parts such as motors, sensors for sensing and touch, power sources: batteries, solar power; mechanical parts such as actuators, effectors, grippers, manipulators, locomotion devices, air muscles, muscle wire, pistons, grippers, wheels, and gears that make the robot move, grab, turn and lift.

SWOT analysis on various surgical methods: Robotic surgery allows surgeons to perform complex, delicate and minimally invasive surgical tasks with more precision, flexibility and control as compared to conventional methods through tiny incisions using robotic technology. Surgical robots (e.g. da Vinci Surgical System) are self powered, computer controlled devices that can be programmed to aid in the positioning and manipulation of surgical instruments. The system includes a camera arm and mechanical arms with surgical instruments. The surgeon controls the arms while seated at a computer console near the operating table. The console gives the surgeon a high definition and magnified 3-D view of the surgical site. The surgeon leads other assisting team members. There are various types of benefits as compared to conventional open surgery such as enhanced precision, flexibility and control, transparency in view, minimally invasive prostate and heart surgery, safe, fewer complications (e.g. surgical site infection, less pain and blood loss, quicker recovery, smaller, less noticeable scars). Medical robotics is being widely used in USA and Europe. But, there are several constraints such as skill, knowledge and cost. A single robot may cost $2'. There may be risk of death in critical cases. Robotic surgery may cost $3,000 - $6,000 more than traditional laparoscopic surgery. Robotic surgery offers a greater range of motion and precision,

less bleeding and post operative pain as compared to laparoscopic surgery. Is it really possible to replace surgeons by robots in future?

10. CONCLUSION

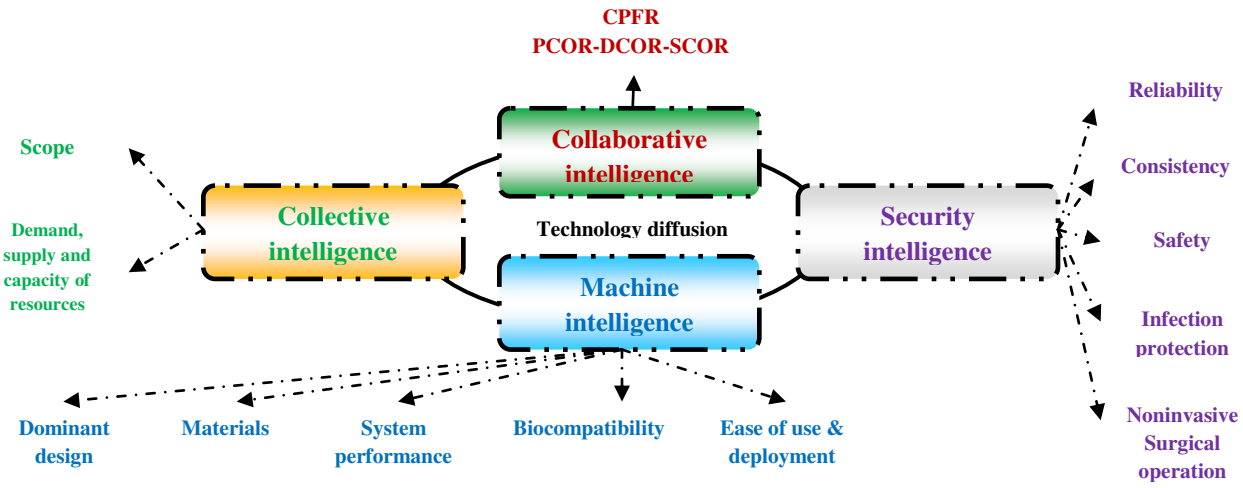


Figure 9.10: Technology diffusion of biomedical technology

Let us summarize the outcome of deep analytic on the evaluation of today's biotechnology technology. The diffusion of the technology is controlled by four factors: machine intelligence, security intelligence, collaborative intelligence and collective intelligence. The machine intelligence considers a set of important criteria such as dominant design features, construction materials, system performance, biocompatibility and ease of use and deployment. It is essential to understand the fundamental principles, functions and mechanisms of the aforesaid biological organs through innovative experimental set up. The security intelligence considers safety, reliability, consistency, efficient surgical operation and reduced risk of infection. The design of biomedical devices must consider biological, chemical, mechanical, electrical and human factors of safety rationally. The collaborative intelligence demands proper integration and coordination among patient care chain, design chain and supply chain of biomedical engineering. The collective intelligence is determined by efficient demand, supply and capacity management of critical resources. Another critical success factor of technology diffusion is correctness and rationality of scope analytics. For example, oral insulin has more strength and opportunities of growth as compared to artificial pancreas. The technology of artificial kidney and liver should explore the hidden potential of tissue engineering. On the other side, the technology of artificial cardiovascular devices and limbs should explore the strength of mechanical and electrical engineering and mechatronics. It is also an interesting research agenda to explore the scope of living biological organ transplantation through organ donation, organ banks and alternative medicines (e.g. integrated medicine, regenerative medicine, precision medicine) as a part of proactive and reactive healthcare approaches. Finally, deep analytics can streamline the diffusion of biomedical technology through efficient coordination and integration among 7-S elements.

REFERENCES

[1] A. Nautiyal, N.V.M. Satheesh and S. Bhattacharya. 2013. A detailed review on diabetes mellitus and its treatment in allopathic and alternative systems. Int J Adv Pharm Sci ;4:16-43.
[2] H. Iyer, A. Khedkar and M. Verm. 2010. Oral insulin – a review of current status. Diabetes, Obesity and Metabolism. 12: 179–185.
[3] C. Reis, R. Neufeld, A. Ribeiro A and F. Veiga . 2006. Nanoencapsulation I. Methods for preparation of drug-loaded polymeric nanoparticles. Nanomedicine; 2: 8-21.
[4] M.S. Bhadoria and P. Mishra. 2013. Applications of nanotechnology in diabetes. Int. J. Res. Comput. Eng. Electron., 2.

[5] P. Home. Insulin therapy and cancer. Diabet. Care, 2013, 36(Suppl2), S240-244.
[6] S.Kalra. 2013. Advances in insulin therapy. J. Pak. Med. Assoc., 63, 925-927.
[7] S. Kalra, B.Kalra and N. Agrawal. 2010. Oral insulin. Diabetol. Metab.Syndr., 2, 66.
[8] P.Mukhopadhyay, R.Mishra, D.Rana and P.P. Kundu. 2012. Strategies for effective oral insulin delivery with modified chitosan nanoparticles: A review. Prog. Polym. Sci., 37, 1457-1475.
[9] S.R.Joshi, R.M.Parikh and A.K. Das. Insulin - History, biochemistry, physiology and pharmacology. J Assoc Physicians India 2007;55 Suppl:19-25.
[10] A. Akbarzadeh, R. Rezaei-Sadabady, S.Davaran, S.W. Joo, N. Zarghami and Y. Hanifehpour. Liposome: Classification, preparation, and applications. Nanoscale Res Lett 2013;8:1-9.
[11] X. Zhang, J. Qi , Y.Lu , W.He, X. Li and W. Wu 2014. Biotinylated liposomes as potential carriers for the oral delivery of insulin. Nanomedicine 2014;10:167-76.
[12] E. Zijlstra, L. Heinemann and L. Plum-Mörschel. Oral insulin reloaded: A structured approach. J Diabetes Sci Technol 2014;8:458-65.
[13] X.Xiongliang, Z. Hongyu, Z., L. Long and C. Zhipeng. 2012. Insulin nanoparticle and preparation method thereof. Chinese Patent 1,026,144,98, August.
[14] L. Huixia, S.LA, Z. Zhenhai and Z. Jianping. 2011. Preparation and application of novel oral insulin nanoparticles. Chinese Patent 1,021,207,81, July 13, 2011.
[15] P. Wang, Y. Cheng, Y. and D. Du. 2003. Nano-insulin oral preparation. Chinese Patent 2,566,851, August. .
[16] Z. Zhang, Z. Hou, Z and J. Niu. 2003. Process for preparing oral insulin nanomaterial. Chinese Patent 1,425,464, June .
[17] R.Margalit. 2003. Liposome-encapsulated insulin formulations. Australian Patent 2,002,330,273, April.
[18] P.D.Light. 2004. Dialysate composition in hemodialysis and peritonial dialysis, in Henrich WL (ed.), Principles and Practice of Dialysis. pp. 28–44.
[19] W. Henrich. 2004. Prinicples and Practice of Dialysis, Philadelphia, Pa. Lippincott Williams & Wilkins.
[20] C.Ronco and N.W. Levin. 2004. Hemodialysis, Vascular Access, and Peritoneal Dialysis Access. New York.
[21] N.A.Hakim. 1998. Influence of hemodialysis membrane on outcome of ESRD patients. Am. J. Kidney Dis.32:71–75.
[22] M. Misra. 2005. The basics of hemodialysis equipment. Hemodial. Int. 9:30–36,.
[23] A. O'Connor and B. Wish. 2004. Hemodialysis adequacy and timing of dialysis initiation, in Henrich WL (ed.), Principles and Practice of Dialysis. Philadelphia, pp. 111–127.
[24] V.A. Kumar and T.A. Depner. 2004. Approach to hemodialysis kinetic modeling, in enrich WL (ed.), Principles and Practice of Dialysis, Philadelphia, Pa. Lippincott Williams & Wilkins, 3d ed., 2004, pp. 82–102.
[25] J.K. Leypoldt. 1999. The Artificial Kidney: Physiological Modeling and Tissue Engineering, Austin, Tex, R.G. Landes.
[26] O.F. Bertrand and R. Sipehia. 1998. Biocompatibility aspects of new stent technology. J Am Coll, Cardiol, 32(3):562–71.
[27] M. Kutz (Ed.). 2009. Handbook of Biomedical Engineering and Design. McGraw-Hill
[28] N. L'Heureux and N. Dusserre,. 2007. Technology insight: the evolution of tissue-engineered vascular grafts - from research to clinical practice. Nat Clin Pract Cardiovasc Med, 4(7):389–95.
[29] A. J. Makarewicz and L. F. Mockros. 1994. A pumping artificial lung. ASAIO J, 40(3):M518–21.
[30] M.A. Mattos and K. J. Hodgson. 1999. Vascular stents. Curr Probl Surg, 36(12):909–1053.
[31] A.W. Holt. 1999. Acute liver failure. Crit Care Resusc. 1:25–38. [PubMed]
[32] JG Freeman , K.Matthewson and C.O. Record. 1986. Plasmapheresis in acute liver failure. Int J Artif Organs. 9:433–438. [PubMed]
[33] L.J. Li, Y.M. Zhang, X.L. Liu, W.B.Du, J.R. Huang, Q.Yang, X.W. Xu XW and Y.M. Chen . 2006. Artificial liver support system in China: A review over the last 30 years. Ther Apher Dial.10:160–167.
[34] C.D.Campli, R. Gaspari, V. Mignani, G.Stifano, A. Santoliquido , L.Z. Verme, R. Proietti, P. Pola, N.G. Silveri, G.Gasbarrini and A. Gasbarrini. 2003. Successful MARS reatment in severe cholestatic patients with acute on chronic liver failure. Artif Organs. 27:565–569.

[35] C.Doria, L.Mandala, V.L. Scott, S.Gruttadauria, I.R. Marino. 2006. Fulminant hepatic failure bridged to liver transplantation with a molecular adsorbent recirculating system: A single-center experience. Dig Dis Sci.;51:47–53.
[36] M.P. van de Kerkhove, E. Di Florio, V. Scuderi, A. Mancini, A. Belli, A. Bracco, D. Scala, S. Scala, L. Zeuli, G. Di Nicuolo, P. Amoroso, F.Calise, R.A. Chamuleau. 2003. Bridging a patient with acute liver failure to liver transplantation by the AMC-bioartificial liver. Cell Transplant.12:563–568.
[37] T.K. Ulrich and S.D. Eppinger. 2000. Product Design and Development, 2nd ed., McGraw-Hill.
[38] S.C. Wheelwright and K.B. Clark. 1992. Revolutionizing Product Development. Free Press.
[39] A.L. Swiffin et al. 1987. Adaptive and predictive techniques in a communication prosthesis, *Augmentative and Alternative Communication,* **3**(4):181–191.
[40] J. Kumagai . 2004. Talk to the machine, *IEEE Spectrum,* **39**(9):60–64, 2004.
[41] R.W. Beasley and G.M. de Bese. 1990. *Prosthesis for the Hand. Surgery of the Musculoskeletal System*, 2nd ed. New York
[42] C.D. Brenner. 2004. Wrist Disarticulation and Transradial Amputation: Prosthetic Management. In: *Atlas of Amputations and Limb Deficiencies*, 3rd ed. (Smith DG, Michael JW, Bowker JH, eds.), pp. 223–230.Rosemont, Ill.: American Academy of Orthopaedic Surgeons.
[43] D. Childress. 1985. Historical aspects of powered limb prosthetics. *Clinical Prosthetics and Orthotics* **9**:2–13.
[44] w. Daly. 2004. Elbow Disarticulation and Transhumeral Amputation: Prosthetic Management. In: *Atlas of Amputations and Limb Deficiencies*, 3rd ed. (Smith DG, Michael JW, Bowker JH, eds.), pp. 234–249.Rosemont, Ill.: American Academy of Orthopaedic Surgeons.
[45] M.J. Fletcher. 1954. New Developments in Hands and Hook. In: *Human Limbs and Their Substitutes* (Klopsteg PE, Wilson PD, eds.), pp. 359–408.McGraw-Hill.
[46] Kenworthy G. 1974. An artificial hand incorporating function and cosmesis. *Bio-Medical Engineering,* 9:559–562.
[47] Y. Lozac'h, S. Madon, S. Hubbard and G. Bush. 1992. On the Evaluation of a Multifunctional Prosthesis. In:*Proceedings of the 7th World Congress of the International Society for Prosthetics and Orthotics (ISPO)*, p. 185.Chicago, Ill.
[48] J.W. Michael. 1986. Upper-limb powered components and controls: current concepts. *Clinical Prosthetics and Orthotics* **10**:66–77.
[49] D.G. Smith, J.W. Michael JW and J.H. Bowker. 2004. *Atlas of Amputations and Limb Decifiencies*, 3rd ed. Rosemont, Ill.: American Academy of Orthopaedic Surgeons.
[50] C.L.Taylor.1954. The Biomechanics of the Normal and of the Amputated Upper Extremity. In: *Human Limbs and Their Substitutes* (Klopsteg PE, Wilson PD, eds.), McGraw-Hill, New York.
[51] D. G. Shurr and T. M. Cook. 1990. *Prosthetics and Orthotics,* Appleton & Lange, East Norwalk, Conn.
[52] A. B. Wilson. 1989. *Limb Prosthetics,* 6th ed., Demos Publications, New York, N.Y.
[53] B. J. May. 1996. *Amputations and Prosthetics: A Case Study Approach,* F. A. Davis, Philadelphia, Pa.
[54] W. Loob. 2001. Robotics and electronics research aid building "smart" prostheses, *in Medical Device and Diagnostic Industry,* Jan., 64.
[55] K.S. Katti 2004. Biomaterials in total joint replacement. *Colloids Surf B Biointerfaces*, **39**:133–142.
[56] I.C.Clarke, T.Donaldson, J.G.Bowsher, S.Nasser and T.Takahashi. 2005. Current concepts of metal-onmetal hip resurfacing. *Orthop Clin N Am*, 36:143–162.
[57] M.P. Gispert, A.P. Serro, R.Colaco, E. Pires and B. Saramago. 2007. Wear of ceramic coated metal-on-metal bearings used for hip replacement. *Wear*, 263:1060–1065.
[58] I.D. Learmonth, C.Young and C. Rorabeck. 2007. The operation of the century: total hip replacement. *Lancet*, **370**:1508–1519.
[59] Abiomed Inc. 2007. Heart Replacement.
[60] J. Al Suwaidi, P. B. Berger et al.. 2000. Coronary artery stents. *JAMA*, 284(14):1828–36.
[61] J. Bai and H. Lin et al. 1994. A study of optimal configuration and control of a multi-chamber balloon for intraaortic balloon pumping. *Ann Biomed Eng*, 22(5):524–31.
[62] O.F.Bertrand, R. Sipehia et al. 1998. Biocompatibility aspects of new stent technology. *J Am Coll, Cardiol*, **32**(3):562–71.
[63]https://www.cancer.gov/about-cancer/treatment/types/surgery/lasers-fact-sheet
[64] http://lasermart.in/lasotronix-smart-pro-dental.html

Exercise

1. **Explain the technology of biomedical instrumentation for cancer care? Justify it as a technology for humanity. What is the scope of biomedical instrumentation technology?**
2. **What is the dominant design of the technology?**
3. **What are the basic elements of the system architecture?**
4. **What do you mean by technology security in biomedical instrumentation? How to verify the security intelligence?**
5. **What are the strategic moves of technology innovation, adoption and diffusion of biomedical instrumentation for cancer care? What is the outcome of technology life-cycle analysis?**
6. **How to manage resources for this innovation project?**
7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently for biomedical instrumentation What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
9. **Explain the scope of laser therapy, pervasive computing and surgical robotics for cancer care.**

CHAPTER 9 : ARTIFICIAL RAINFALL – CLOUD PHYSICS, LASER & MULTI-AGENT COLLABORATIVE RESOURCE SHARING

Abstract : Can You recall the tune of 'The rain must fall' by Yanni? This chapter has analyzed the technological innovation associated with the problem of water security through artificial rainfall and rational, fair and correct resource allocation and sharing among multiple entities. Such type of technological innovation is essential to fight against natural calamities such as drought and flood. It is an emerging technology for humanity. We have analyzed the technological innovation through seven elements of the deep analytics i.e. scope, system, structure, security, strategy, staff-resources and skill-style support of the deep analytics. We have shown various strategic moves of artificial rainfall such as weather modification and rain enhancement through cloud seeding, glaciogenic seeding, hygroscopic seeding and laser induced rainfall. At present, the technology is at emergence phase of technological life-cycle. This work also outlines a water sharing mechanism (WSM) based on collaborative intelligence. However, the efficiency of the resource sharing mechanism is associated with several critical success factors such as good governance, corporate social responsibilities, law and order, rational positive thinking and political goodwill. An intelligent broadcast protocol is expected to enhance public awareness of rational usage of water by the common people and restrict wastage of water in swimming pools, water amusement parks, luxurious use of air conditioners and air coolers by the rich and super rich classes of our society; tap at roadside and construction works and leakage from pipelines, saving water bodies and conservation of water. Academic institutes are expected to play responsible and rational role in regional urban and rural development planning globally.

Keywords : Artificial rainfall, Cloud seeding, Collaborative intelligence, Resource sharing mechanism, Water sharing, Compensation, Collaborative Planning, Forecasting & Replenishment, Political will, Power play, Conspiracy for war, Corporate social responsibilities

1. SCOPE

In this chapter, we are considering the problem of water security. The people in today's world are facing with significant challenges in this utility sector such as shortage of water, high cost of generation, storage and distribution, wastage or loss and pollution. We must set an efficient national and global utility policy to promote the development of a sustainable system which should be viable environmentally, socially and economically. The sustainability in such resource management not only requires a balanced approach between natural and artificial rainfall but also encourages rational and efficient use of water by minimizing wastage and pollution. There are many strategic moves of efficient water resource management. This work is focused on two specific strategic moves to fight against flood and drought: artificial rainfall and multi-agent collaborative resource sharing. Can we dream of a collaborative enterprise model in this context?

2. SYSTEM

Natural rainfall requires conservation of forests and green plantation in smart cities and villages and along riverside. It is essential to save the rivers. Massive cut of trees and green plants in urban zone occurs due to construction of residential flats and other civil infrastructure (e.g. flyovers, bridges and transportation infrastructure). It may lead to droughts. The basic objectives of rainmaking or artificial precipitation or artificial rainfall is to artificially induce or increase precipitation using airplanes or rockets to sow to the clouds with catalysts. This method makes rain or increase precipitation and drought like situation.
Cloud seeding is a weather modification method by dispersing substances into the air ; results condensation of cloud and alter the microphysical processes within the cloud [6-10]. The most common chemicals used for cloud seeding are salt powder (e.g. silver iodide, potassium iodide), dry

ice and liquid propane. Cloud seeding chemicals may be dispersed by aircraft or drones or by dispersion devices located on the ground (e.g. firing from anti-aircraft guns or rockets) (Figure 9.1).

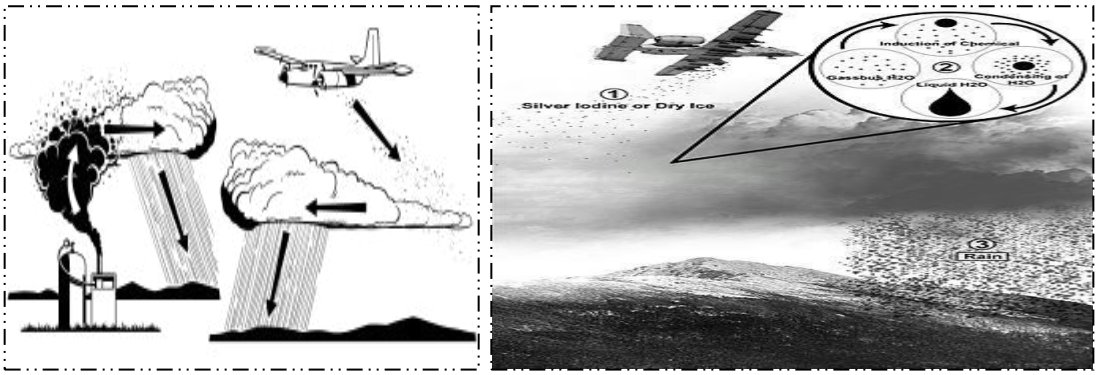


Figure 10.1: Cloud Seeding

Glaciogenic cloud seeding use glaciogenic materials such as Silver Iodide which increase the ice crystal concentration in clouds by freezing cloud droplets. Static cloud seeding is applicable to cold cloud. Dynamic seeding results increased rainfall as compared to the static approach. The seeding of super cooled cloud with large amount of ice nuclei cause glaciation of the cloud. The super cooled liquid water is converted into ice flakes releasing latent heat, increasing buoyancy, growing larger and increased precipitation. *Hygroscopic cloud seeding* is a form of warm cloud seeding which enhances rainfall through coalescence process using fine spray of hygroscopic salt.

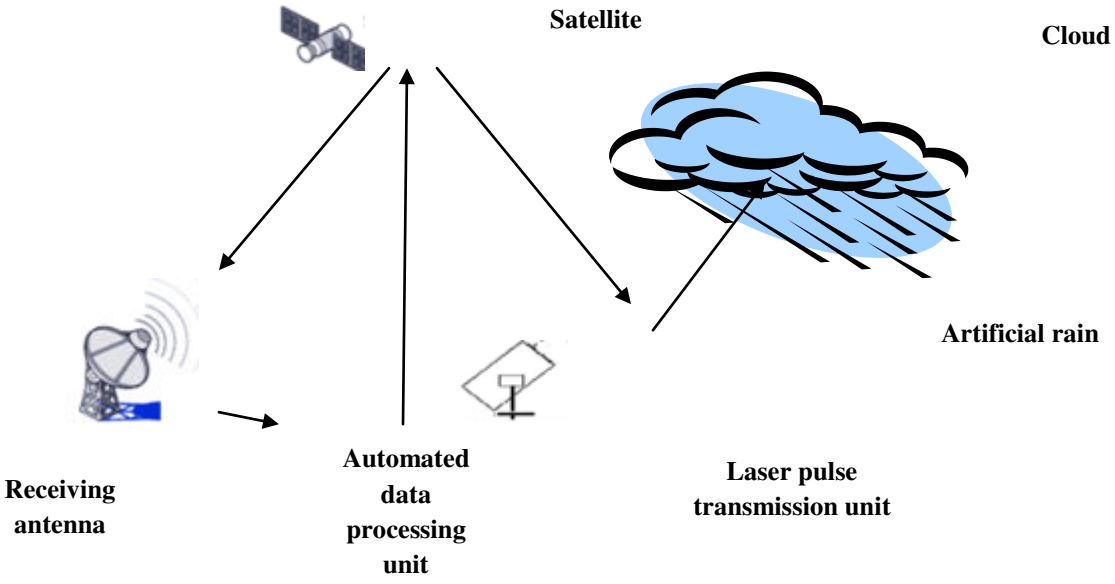


Figure 10.2 : Laser induced artificial rain

The other emerging techniques for artificial rainfall are *laser induced cloud generation* and *ion generation method* [11]. Lasers may help cause rain; rainclouds form when airborne pockets of tiny particles condense water vapor around them (Figure 10.2). It is possible to control over moisture using lasers. Weather control may get their next rainmaking tool in the form of an infrared laser. Precipitation is formed after lightning and heavy rain follows due to dissociation, ionization and natural seeding process in the atmosphere. Plasma laser pulse can be used for artificial rain making; for example 2.2 x 10^{19} gm of water drops are formed in the atmosphere by laser pulse of energy 500 mJ. Plasma laser pulse creates high temperature (up

to 3000^{o}C) which breaks bonds N_2 and O_2 into excited and unstable N^* and O^* and form NO and O_3. These endothermic reactions absorb heat from the clouds and condensation creates water drops. Simultaneously N_2 and O_2 will be ionized and become big clustered ions through several reaction. The big ions act as seed and results precipitation and rain.

3. STRUCTURE

The next element of the deep analytics is structure which should be analyzed from the perspectives of organization structure and system architecture. The technological innovation related to the artificial rainfall and multi-agent resource sharing mechanism is suitable for a collaborative enterprise model. The system architecture is shown in figure 8.2 at an abstract level. Let us also consider the structure of an information system to be used in allocation and sharing of water. The information system should monitor a set of entities such as various water bodies, rivers, canals, lakes and dams; demand of water in agriculture, industrial plants and domestic uses, supply of water, rainfall data, water level in rivers, lakes and storage systems, pollution levels and water sharing data (Table 9.1). It may be integrated with GIS. The information system is expected to support the decision making process associated with artificial rainfall i.e. what initiatives are essential to fulfill the demand-supply gap. The resource sharing system should be able to interact with various types of sensors and measuring instruments like water level indicator, inflow and outflow measuring instruments physically for real-time supply chain optimization in water resource management. The resource sharing mechanism may also require an intelligent negotiation support system (NSS) for multi-party negotiation in water sharing; it is basically a group decision support system; it permits collection of different views of the negotiating agents; defines the structure of the problem, generates alternatives for compromise and improves the quality and the acceptability of a negotiated agreement.

Entities	Demand of water	Supply of water	Rainfall data	Water level	Pollution level	Water sharing
Water bodies	Agriculture	Rainfall	Natural rainfall	Water bodies : rivers, lakes	Pollutants, plastic, paper	Inflow
Canals	Industry	Sharing from other sources	Artificial rainfall	Dams	Drainage system	Outflow
Rivers	Domestic use of population	Capacity utilization		Storage system	Congestion	Shared data
Lakes	Drinking, cooking	Loss or wastage			Encroachment statistics	Surplus
Dams	Washing and cleaning					Shortage
Lock gates	Natural activities and bathing					

Table 10.1: Analytics for resource allocation and sharing

4. SECURITY

The security of the technological innovation related to artificial rainfall and multi-agent collaborative resource sharing mechanism should be analyzed from the perspectives of fairness, correctness, transparency, accountability, reliability, consistency, resiliency, authorization and authentication in access control, trust and commitment. It is really a hard task to estimate the resource to be allocated and shared fairly and correctly in time. The resource sharing mechanism should be transparent to all the stakeholders through intelligent broadcast communication. The operators and the administrators of the system should be accountable for any mishap due to the natural disaster such as timely release of water from the dam during heavy rainfall in the rainy season or proper storage of water in the dam during the summer and the winter for proper irrigation to the fields of agriculture. The performance of the system is expected to be evaluated

in terms of reliability and consistency. Who will take the decision of artificial rain? The system should be operated by the authenticated and authorized decision making agents only since it is a very sensitive issue, which is related to the safety and security of a large number of human beings, plants and animals over a specific zone (e.g. it may be a district or a state or even a country).

Let us explain the security element of the deep analytics through a case of water sharing conflict between two states U (upstream state) and D (downstream state) associated with a river (R). There is lack of mutual cooperation and trust between two states in the context of water sharing of river R. Initially, the Supreme Court (SC) orders the state government of U to release water of 15000 cusec / day; then 12000 cusec / day; then 6000 cusec water / day to the state D. There was a water riot in state U; the mob torched 42 buses; a leader was killed. Inlow from U was 15000 cusecs/ day last week. 12000 cusecs was being released everyday from Dam X from 20.9.2016. Release amounts to 1 tmcft; paddy raised in 14.9 L acres. Then, the inflow from U was reduced to 3000 cusecs on Wednesday evening; 21.9.2016. SC orders U to release 6000 cusec water / day for rest of September'2016. The State Govt. of U called all party meeting and had taken decision collectively; a legislative resolution was taken to defy SC order; stop release of water for agriculture (e.g. samba cropping) and water to be released only for drinking purpose.

The State Govt. of D did not call any all party meeting. This is a fresh controversy. Defiant U triggers a constitutional crisis since it is defying SC order to release 6000 cusecs per day to TN. The special legislature session is expected to adopt a resolution that SC order cannot be implemented as it is contrary to the public interest in the state U. U does not have adequate drinking water. By projecting it a legislature-judiciary confrontation, the state Govt. of U hopes to escape the charge of commitment to the court.

Many in U are concerned with the silence of the central government. The centre can not be a bystander since the issue is with the Supreme Court (SC). The PM should take initiatives to prevent a constitutional crisis. It is his duty to protect the federal structure. The decision of the Govt. of U cannot be seen as an act of defiance but as the helplessness of a state ravaged by a court order that cannot be implemented. If U defies SC order, then there are serious risks for river sharing agreements. The tension between U and D will grow since both states are feeling pressure. Outright defiance of SC may boomerang and set an extremely dangerous precedent. SC directs to form river R board having representatives from four neighboring states U,D, Y and Z. Even in the absence of state representative, the board can take decisions by majority option. So, it is in the interest of the riparian states to nominate the members otherwise they will lose the opportunity to protect their rights.

The output of the analytics is as follows: Irrigation in state D is more than 20L acres which is now 18L acres; the same in state U is 6.5L acres which is now 15 L acres. About 80% of the annual yield from river R is utilized by the farmers of D. It has now come down to 57%. The state U was using 16% now gets 37%. The water received from U by D is 4.57 tmcft during 2010-11; 28.06 during 2011-2012; 135.77 during 2013-2014 and 76.31 during 2014-15. The major cities of U consume drinking water as 26 tmcft by city B; 6 tmcft by city E; the city C of state D consumes 7 tmcft. Present water level at X Dam : 86.94 ft; storage now 44.21 tmcft. Sharp increase in irrigated farm acreage and drinking water use in the state U has deprived D of what it considers its right share. Rainfall in D in September'2016 is high. What should be the water sharing mechanism among states U, D, Y and Z?

5. STRATEGY

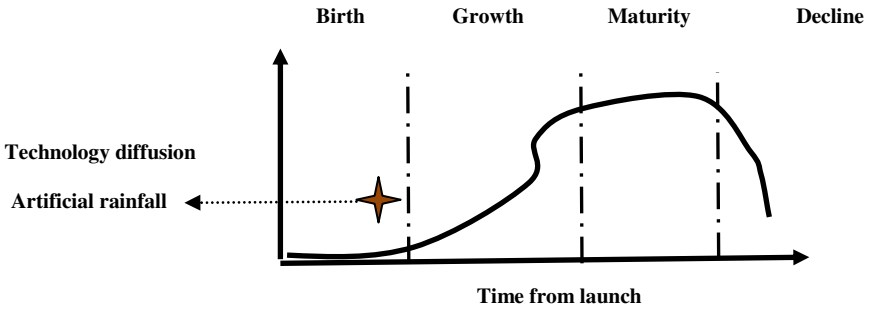


Figure 10.3 : Technology life–cycle analysis

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, shared vision and goal, learning curve, technology life-cycle analysis, technology diffusion and knowledge management strategy. At present, the technology of artificial rainfall is at emergence phase of S-curve [Figure 10.3]. We need fast diffusion of this technology globally to fight against flood and droughts. It is possible to explore different strategic moves for efficient water management; this is basically a natural resource planning (NRP).

- Natural rainfall control thorough green plantation, conservation of forests and rational rural and urban development planning against building of concrete jungles by cutting trees and plants at mass scale;
- Artificial rainfall such as weather modification, rain enhancement through cloud seeding, glaciogenic seeding, hygroscopic seeding and laser induced rainfall;
- Transportation of water by rail and truck to the zone with water scarcity;
- Save water bodies through pollution control;
- Develop smart water grid and irrigation system;
- Rational storage, distribution, recycling and reuse of water;
- Demand and supply management through capacity utilization, drainage system, water irrigation system and smart water grid;
- Collaborative intelligence in water sharing among multiple entities (e.g. districts, states, countries).
- Intrusion and migration control of refugees
- Restrict wastage of water in swimming pools, water parks, luxurious use of air conditioners and air coolers, by the rich and super rich classes; tap at roadside, leakage from pipelines and construction works.

Save water bodies : It is essential to adopt multi-dimensional strategies to save existing water bodies such as intelligent and rational capacity utilization of water from both artificial and natural rainfall; efficient water storage in lakes, ponds, reservoirs, water distribution channels and canals; desalination of sea water; restrict wastage of water in swimming pools, water parks, luxurious use of air conditioners and air coolers, by the rich and super rich classes; tap at roadside and leakage from pipelines; conservation of water to tackle flood and drought, water pollution control (e.g. tube well equipped with water purifier, filter at pumping stations), cleaning of drainage system and riverbed deepening, mutual agreement and dialogue, restriction of illegal encroachment of water bodies, dredging of rivers or canals, collaborative planning, forecasting and replenishment and banning restriction on natural flow of water in river, canals, seas and ocean across borders or boundaries.

Demand & supply management: It is essential to estimate the gap between demand and supply of water for a specific zone (e.g. district, state, country). The demand plan is estimated considering various application domains such as agriculture, industries (e.g. manufacturing plants, retail outlets, life-science industry), construction projects, energy (e.g. power plants), drinking water consumption (e.g. mineral water, fruit juice, beverages, soft drinks), cooking food, washing and cleaning of bodies, garments and cars, religious and cultural events (e.g. marriage, parties), entertainment (e.g. swimming pool, sports and games events, infrastructure and ground maintenance), service sector (e.g. education institutes, student's hostels, healthcare institutes, hospitals, offices of private and public sectors, banks and financial services, communication, IT firms, travel and hospitalities, hotels, restaurants) and miscellaneous purposes like transport and logistics services, workshops, seminars, conferences, administration and governance. The supply plan is estimated based on real-time data on natural and artificial rainfall, inflow and outflow of water in a river, availability of water in the reservoirs, wastage or loss due to pollution and disposal of water through drainage system.

Collaborative intelligence: Let us first explain the problem of resource allocation and sharing among multiple entities [2]. It is basically a problem of supply chain management. Let us first consider the concept of supply chain in manufacturing sector. Then, the concept can be extended to river water sharing mechanism. Typically, a supply chain is a network of organizations that satisfies the demand of ultimate customers by producing values in the form of products and services. Supply chain management is a novel management paradigm; the basic objective is to improve the competitiveness of the supply chain and to

fulfill ultimate customer demands by integrating a network of organizational units through systematic coordination of material, information and financial flows. A supply chain includes all the stages involved directly or indirectly in a business process - suppliers, manufacturers, distributors and customers. Each stage performs different processes and interacts with other stages of the supply chain; there is a flow of material, information and funds between different stages. The ultimate objective is to maximize the value, which is measured in terms of the difference between revenue generated from the customer and. the overall cost across the supply chain. In case of river water sharing, a supply chain is a network of upstream and downstream states or countries that satisfies the demand of water of consumers (e.g. agriculture, industrial plants, common people). It is essential to integrate and coordinate the flow of water among various entities through appropriate infrastructure such as distribution channels, irrigation system, dams, storage and drainage system.

Integration of organizational units and coordination of flows of material, information and funds are the basic building blocks of supply chain management. A lack of coordination occurs if information is distorted as it moves across the supply chain or if different stages of the supply chain focus on optimizing their local objectives. The phenomenon in which demand variability is amplified as one moves up the supply chain is known as Bullwhip effect. There are five main causes of Bullwhip effect – error in demand forecasting, high lead-time, batch ordering, supply shortage and price variations. This problem moves the partners of the supply chain away from the efficient frontier and results in a decrease of profitability and quality of service. It is essential to define frameworks for tighter integration and improved coordination of business processes along the supply chain. Successful integration depends on three factors - choice of partners, inter-organizational collaboration and leadership. Effective use of information and communication technology, integration of advanced planning system and enterprise resource planning (ERP) system and process orientation ensure improved coordination of flows in the supply chain. There are various domains of resource allocation in real world such as river water sharing among various states or countries, bandwidth allocation in communication sector, energy flow in a smart grid, budget allocation and typical supply chain management in manufacturing and retail industry. Let us explore how to extend the aforesaid concept of supply chain management to river water sharing between upstream and downstream states. In case of river water sharing, a lack of coordination and disputes occur if information is distorted as it moves across the supply chain or if different stages of the supply chain focus on optimizing their local objectives of demand and capacity utilization. For example, an upstream state may be reluctant to share water with the downstream state.

Collaborative intelligence is an emerging field of artificial intelligence which is focused on human computer collaboration [5]. It is the basic building block of the proposed resource sharing mechanism. Let us first define collaborative intelligence. It supports supply chain collaboration. Collaborative planning, forecasting and replenishment (CPFR) is a strategic tool for comprehensive value chain management of an organization; this is an initiative among all the stakeholders of the supply chain in order to improve their relationship through jointly managed planning, process and shared information [4]. The ultimate goal is to improve a firm's position in the competitive market and the optimization of its own value chain in terms of optimal inventory, improved sales, higher precision of forecast, reduced cost and improved reaction time to customer demands. Information technology allows supply chain partners to interconnect, but trust is also important. The interplay between trust and technology encourages the commitment of collaboration among the organizations. The partners of a supply chain are often reluctant to share their private information. What has remained the open issue is how privacy can be ensured in exchange of strategic information for collaborative supply chain planning. In case of river water sharing, supply chain collaboration is essential for efficient demand and supply management.

Collaborative intelligence is achieved through multi-party negotiation. *Negotiation* is a means for a group of decision-making agents to reach mutually beneficial agreements through communication and compromise. It is an important conflict management and group decision-making technique by which a joint decision is made by the agents who cannot achieve their objectives through unilateral actions. They exchange information in the form of offers, counter-offers and arguments and search for a consensus. A wise agreement resolves the conflicting interests of the community fairly and is durable. Negotiation methodology has two key components – *negotiation process and negotiation protocol*. Multi-party negotiation is a group decision-making process having five distinct phases. The negotiation process starts with the planning phase. The agents initiate several joint activities by specifying their objectives, preference, aspiration and reservation levels and communication mode. Next, they set various agenda such as negotiation protocol, the timing of exchange, deadline, priorities and constraints. Then, they exchange

offers and arguments; learn about the limitations of other agents; identify the areas of agreement and disagreement and modify negotiation strategies. Next, they develop joint proposals by relaxing their individual limitations and reach an agreement. Finally, the agents analyze the compromise proposals at conclusion phase and may explore the scope of possible improvements.

The *negotiation protocol* is a formal model which defines a set of rules to govern the processing of a *negotiation support system* and related communication and specifies permissible inputs, assumptions, actions and constraints. A protocol can be evaluated on the basis of different perspectives such as computational efficiency, communication efficiency, individual rationality, distribution of computation and pareto efficiency. Distribution of computation is necessary to avoid the problem of a single point of failure. An efficient negotiation mechanism enables the agents to reach a pareto optimal solution by decreasing the cost of negotiation.

Negotiators are the decision-making agents involved in the negotiation process; the other interveners are mediator, arbitrator, facilitator and rules manipulatos. The mediator acts as an impartial agent and guides the negotiators to reach an agreement. The arbitrator may generate a solution on the basis of facts and arguments; the rules manipulator can alter the rules of the negotiation.

Collaborative intelligence in resource allocation is associated with efficient collaborative supply chain planning. Planning is defined as a rational, structured decision making process which aims to find the best choice of objectives and measures to a decision situation and its environmental setting. The coordination of operations along the supply chain requires well structured planning processes. In case of collaborative supply chain planning, two or more local planning domains collaborate through sharing of relevant information in order to create a common and mutually agreed upon plan. It has five strategic moves - domain planning, data exchange, negotiation & exception handling, execution and performance measurement.

Collaborative intelligence is associated with efficient and intelligent supply chain contract such as swing option. *Swing option* is a specific type of supply contract in trading of stochastic demand of a resource. It gives the owner of the swing option the right to change the required delivery of resources through short time notice. It gives the owner of the swing option multiple exercise rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, $i \in [1,2,..,n]$, $1 \leq t_1 < t_2 < \ldots < t_n \leq T$ at which a fixed volume of d_0 units of computational resources may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where $g \leq n$ is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0. There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function ρ for violating local or global constraints. The next section outlines Resource Sharing Mechanism (RSM) based on collaborative intelligence and then applies the concept to a test case of river water sharing dispute.

6. STAFF-RESOURCES

This section outlines the sixth element of deep analytics i.e. staff-resources in terms of 5M – man, machine, material, method and money. The technological innovation related to artificial rainfall demands the commitment of creative talent from the domains of earth science, cloud physics, space research organization and ministry of water resource management. It is crucial to analyze dynamics of the technological innovation in terms of sources of innovation and roles of organizations, government and collaborative networks; fair and correct resources allocation for effective technological evolution and diffusion, dominant design factors and commitment of creative people. Section 6.1 highlights the resource sharing mechanism in details.

6.1 Water Sharing Mechanism (WSM) [Appendix 1]

++

Agents: Country or state - B and S; /* There may be multiple parties i.e. countries or states involved in water treaties*/

Input:

- ♦ Analytics for exception handling: Real-time online data on rainfall, inflow and outflow of water in a river;
- ♦ Availability of water in the reservoirs;
- ♦ Demand plan of water for agriculture, drinking and other purposes;

Output : Collaborative water resource sharing plan or delivery plan (P^d);

AI Moves :

- ✓ collaborative intelligence through domain planning, data exchange among planning domains, multi-party negotiation, exception handling, delivery execution and performance measurement.
- ✓ The agents negotiate a swing option contract in terms of
  - fixed base demand (d), local constraints : up-swing (α) and down-swing limits (β);
  - global constraints : maximum total demand (γ) and minimum total demand (λ);
  - penalty (ρ) for violating local or global constraints and
  - swing number constraint (g)
- ✓ Intelligent and rational resource capacity utilization [Reference : section 2.3]

Protocol:

- Develop front end agreement by forming association.
- Define joint water sharing plan.

  Negotiation issues:
  - primary : delivery plan;
  - secondary : swing option ($d,\alpha,\beta,\gamma,\lambda,\rho,g$);

  S bids its optimal delivery plan P_o to B.

  Set i = 0. Reference plan = P_o;

  Repeat until the stopping criteria is satisfied:

  Set i = i + 1;

  B counter bids P_i^B to S or S counter bids P_i^S to B;

  $N^s(t, P^t_{i,B\rightarrow S})$ = quit if $t > T^S$ or

  accept offer if $u^S(t,P^t_{i,B\rightarrow S}) \geq u^S(t', P^{t'}_{i,S\rightarrow B})$ or

  counter offer $P^{t'}_{i,S\rightarrow B}$;

  If both parties agree, output plan $P_f = P_i$.

  B and S jointly settle the compensation plan to be given to the victim or losing party through negotiation based on final plan P_f in terms of artificial rainfall, cloud seeding, glaciogenic seeding, hygroscopic seeding, rain enhancement, weather modification and water transportation by rail or truck / tanker
- Create demand forecast plan.
- Identify exceptions for demand forecast of water. Call analytics for exception handling [refer section 2.4).
  - demand plan of water
  - supply plan of water
- Collaborate and resolve demand forecast exception items.
- Create the replenishment of order forecast.
- Identify exceptions to the order replenishment forecast.
- Collaborate and resolve exceptions to the order replenishment forecast.
- Create the replenishment order.
- Execute delivery plan : allocate and share water.

Verification principle:

- verify *security intelligence* of water allocation and sharing system of the association in terms of
  - rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, commitment, reliability and consistency;
  - Revelation principle :
    - authentication, authorization, correct identification, non-repudiation and integrity,
    - audit quality, pollution level and volume of shared water;

- verify *machine intelligence* (M_p) in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy.

Payment function: verify *business intelligence* (B_p) in terms of cost sharing, incentive and compensation policy.

++

Let us explain the water sharing mechanism. Three different classes of agents are involved in the resource sharing mechanism: B, S and mediator (M). B and S have well-defined objective function and a set of constraints that represent their preferences over the possible outputs of the mechanism. These agents act rationally to optimize their objective functions and follow the coordination mechanisms correctly. B and S disclose their negotiated data to M. The primary responsibility of M is to ensure fairness and correctness of resource allocation and sharing.

Planning domains (Local and Global)**:** In case of water sharing, it is hard to define a planning domain based on single or multi-objective optimization; it may be based on a valuation model. Here, B and S hold individual planning domains which are derived from their optimization models; B has a budget constraint and S has a capacity constraint. The agents try to minimize the cost of transaction. The *local planning domain* of B is defined through the constrained optimization problem: max $(o^B)^T\mathbf{x}^B$, s.t. $M^B\mathbf{x}^B \leq b^B$ where $\mathbf{x}^B$, o^B, b^B and M^B are the vector of decision variables, the cost vector, the constraint lower bound vector and the constraint matrix for B, respectively (T: matrix transpose operation). Similarly, the lpd of S is: max $(o^S)^T\mathbf{x}^S$, s.t. $M^S\mathbf{x}^S \leq b^S$. Combining these two one can obtain the joint optimization problem: max $o^T\mathbf{x}$, s.t. $M\mathbf{x} \leq b$ where $\mathbf{x} = \mathbf{x}^B \oplus \mathbf{x}^S$, $o = o^B \oplus o^S$, $M=M^B \oplus M^S$ and $b = b^B \oplus b^S$ for the entire system referred as the *global planning domain.* Here, **x**, o, M and b represent the set of decision variables, the cost or objective function vector, the constraint matrix and constraint upper bound vector for the global plan.

Plan: The plan in water sharing is basically a delivery plan of river water. It is a multi-issue negotiation. The bi-party negotiation starts with B bidding a plan P to S. S evaluates P and counter bids an alternative plan P'. B in turn evaluates P' and counter proposes yet another P" and so on. Finally, if the negotiation ends successfully, B and S accept the commonly accepted agreed plan. The negotiation for a plan consists of successive bidding cycles. In each bidding round, a plan P is bid by either B or S. A successful negotiation process consists of an initial plan followed by a series of compromise plans which culminates in a finally accepted plan.

Plan utility: For any plan P, the utility components of B and S are denoted by $u^B(P)$ and $u^S(P)$ respectively. These are private to the agents and will not be disclosed to the opponent, i.e. what is revealed in the negotiation process is the proposal for B and the proposal for S without any utility implications. The total utility for a plan P, $u(P) = u^B(P) + u^S(P)$, is also not revealed to either agent. The concept of utility is also used as plan cost or revenue in artificial intelligence and operations research literature.

Local and global utility effects: Since P_0 is optimal for B, $u^S(P_0) < u^S(P_i)$ for all $i \geq 1$, i.e. the *utility effect* for B(S) for P_i, $\Delta u^B(P_i) = u^B(P_0) - u^B(P_i)$. $\Delta u^S(P_i) = u^S(P_i) - u^S(P_0)$. Utility effect of B or S is also referred as *local utility effect*, whereas the *global utility effect* or total utility effect for P_i is sum of the local utility effects of all the agents. This is because the objective of the coordination process is to increase the total utility, not the individual utility. However, B is entitled to ask for suitable compensation from S to compensate for the reduced utility it has to incur in P_i. Individual utility effects are treated as private information.

Compensation and utility sharing: The losing party will always ask for a compensation amount, which is at least the utility effect. The compensation negotiation has basically two purposes: i) to determine whether the current plan P_i is a feasible one, i.e. whether total utility of P_i has increased over the previous plan P_{i-1} (or any other past plan P_j, $j<i-1$); and ii) to determine how the increased utility to be shared between B and S. This is known as *utility sharing*.

Utility implication: *Utility Implication* of B for a plan P denoted $u'^B(P)$ is the utility component of P, $u^B(P)$ plus the compensation settled $u_m(P)$. Similarly, the utility implication for S agent $u'^S(P)$ is determined. The total of utility implications for B and S is same as the total utility for the plan, u(P). Thus, $u'^B(P) = u^B(P) + u_m(P)$; $u'^S(P) = u^S(P) - u_m(P)$; $u(P) = u^B(P) + u^S(P) = u'^B(P) + u'^S(P)$.

Compensation negotiation and rational behaviors of the agents : Incentive or compensation negotiations are realistic. The agents behave rationally. If the total utility increases, compensation will always be settled such that no agent loses compared to the previous round. In other words, the utility implications for both parties improve. Further, if the compensation negotiation fails, it only means that the total utility for the

current bid is less than that for the previous bid. When the negotiation ends successfully in the final plan P_f, the total utility achieved is nothing but $u(P_f)$. The total improvement of utility through the negotiation will be $u(P_f) – u(P_0) > 0$, which is apportioned as $u_m(P_f)$ for B and $u(P_f) – u(P_0) – u_m(P_f)$ for S. Both B and S are assumed to be rational in exchange of truthful communication and are interested in reducing total plan utility. If none of parties respond then there will be a deadlock. That means that neither B nor S is interested in utility improvement, which violates our assumption. Privacy preservation of individual agents is an important concern for this cooperative game. For this purpose, the utility effects are compared privately. Because the utility effects are kept secret from the respective opponents, the compensation negotiation becomes relevant and the parties feel encouraged to participate in this negotiation. It may be a single or multi-issue negotiation.

Payment: The buying and selling agents disclose the pricing, compensation and delivery plans to the mediator. The mediator checks the authenticity of the identities of the agents and regulatory constraints such as ceiling, consent and sustainability clauses; verifies fairness and correctness of valuation and announces penalty clauses against malafide behavior. The mediator computes payment based on disclosed data; collects payment. S collects payment from B.

Stopping criteria: Stopping the mechanism is possible on various counts such as stable preference matching, total negotiation time deadline, total number of plan bidding rounds and number of successive failed biddings. If any agent withdraws prematurely the mechanism ends unsuccessfully.

Compensation : The agents may settle compensation in various ways such as financial budget allocation or incentive sharing or unconventional ways. Let us consider the case of water sharing between two countries or states. B and S jointly settle the compensation plan to be given to the victim or losing party through negotiation based on final plan in terms of artificial rainfall, cloud seeding, glaciogenic seeding, hygroscopic seeding, rain enhancement, weather modification and water transportation by rail or truck / tanker. The upstream state requires additional amount of water for the growth and development in agriculture, industries, power plants and urban and rural planning. Its demand for water has increased and so the inflow of river water to the downstream state has reduced significantly. On the other side, the downstream state requires more water for the growth and development of urban and rural zones, agriculture and industries. The problem is severe during drought in the summer. So, how is it possible to supply more water to the downstream state – the option is artificial rainfall through cloud seeding. In this case, the compensation may not be directly related to fund allocation or financial support from the upstream to the downstream state. Actually, it is expected to be technological support for artificial rainfall. Can we think of cloud computing in the context of artificial rainfall and cloud seeding – how to control the generation and movement of cloud as per the demand of water of a specific zone?

There are several critical factors associated with fair, correct and rational resource sharing mechanism like river water: good governance, trust, positive mindset, commitment, political will, power play, corporate social responsibilities, cancer of mind, selfish ego, identity crisis and conspiracy for war. Malicious agents always try to sustain the conflict of resource sharing among multiple entities to gain political mileage, incentives from enhanced defense budget and other financial opportunities. War or terrorism may start due to conflict in water sharing. The Supreme Court is expected to act as a Trusted Third Party. A supervisory panel should be set up to decide quantum of water release after studying online data of rainfall and flow in the river. Central Water Commission (CWC) should define a new protocol of online collection of data related to rainfall and flow of water on real-time basis. The meteorological department's rainfall data and flow into reservoirs of upstream state should match with inspected or verified data. The inflow may be artificially reduced due to unauthorized diversions by a state through various lift irrigation schemes in violation of the final order of the tribunal. It is the duty of the state government to maintain law and order.

7. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforces involved in this technological innovation are expected to develop different types of skills in technical, management and system administration. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of top technology innovation requires the support of great leadership style; they are not only industry leaders but also political one. The

style is basically the quality of leadership; the great leaders must have passion, motivation and commitment. The leaders must be able to share a rational vision, mission and values related to the innovation among all the stakeholders honestly and appropriately in time. A traditional functionally centered organization model may not be suitable for supporting end-to-end water resource management process. The technology needs the support of a collaborative enterprise model. The stakeholders are expected to develop skills in collaborative planning, forecasting and replenishment (CPFR) practice as follows.

- **Develop front end agreement**

Process steps:

- Develop mission statement.
- Determine goals and objectives.
- Discuss competencies, resources and systems.
- Define collaboration points and responsible business functions.
- Determine information sharing needs (what information, frequency, technology).
- Determine service and order commitments.
- Determine resource involvement and commitments.
- Define conflict resolution process.
- Determine process for reviewing the collaborative arrangement.
- Publish front-end arrangement.

Objectives : Establish rules and guidelines for a collaborative relationship.

- **Joint Resource Sharing Plan**

Process steps:

- Identify partner strategies.
- Develop category roles, objectives and goals.
- Develop joint category strategies and tactics.
- Develop item management profiles.
- Develop joint resource sharing plans.
- Agree to joint resource sharing plans.

Objectives: Understand each partner needs and capabilities in creating and influencing demand, manufacturing and replenishment.

- **Demand forecast creation**

Process steps:

- Analyze joint resource sharing plan.
- Analyze causal factors (e.g. seasonality) on demand.
- Collect and analyze point of history or time series data.
- Identify planned events.
- Identify exceptions or forecast disagreements.
- Generate the demand forecast.

Objectives: Create a demand forecast that will lead to the creation of the replenishment order.

- **Identify exceptions for forecast.**

Process steps:

- Understand and retrieve exception criteria.
- Identify changes and updates.
- Update the system with constrained demand forecast.
- Compare item values to exception criteria.
- Identify exceptions for collaborations.

Objectives : Using predefined tolerances and metrics, identify exceptions in the demand forecast for collaborative resolutions

- **Collaborate and resolve demand forecast exception items.**

Process steps:

- Identify desired adjustments to the demand forecast.

- Recommend forecast adjustments.
- Agree on the forecast adjustments.

Objectives: Resolve exceptions to the demand forecast through collaboration.

- **Create the replenishment of order forecast.**

Process steps :

- Communicate the demand forecast.
- Consider inventory strategies and current inventory levels.
- Analyze manufacturer's historical replenishment performance.
- Analyze and communicate manufacturing capacity limitations.
- Evaluate factors affecting replenishment planning decisions.
- Review execution performance.
- Create order replenishment forecast.

Objectives: Develop and communicate a time-phased projection of replenishment orders based on demand forecast.

- **Identify exceptions to the order replenishment forecast.**

Process steps :

- Understand and retrieve exception criteria.
- Utilize the replenishment order forecast in the sales and operational planning processes.
- Compare the proposed replenishment order forecasts to supply and capacity.
- Apply constraints and capacity optimization factors to the order replenishment forecast.
- Identify exceptions items based on predefined tolerances.

Objectives: Identify replenishment orders based on predefined tolerances and criteria.

- **Collaborate and resolve exceptions to the order replenishment forecast.**

Process steps :

- Identify and communicate exceptions.
- Recommend order replenishment forecast adjustments.
- Agree on the forecasts.

- **Create the replenishment order.**
  - Utilize the planning system to generate and communicate replenishment orders internally and to the trading partners.
  - The final output is the replenishment orders that are in synchronization with the demand forecast and are aligned with the joint resource sharing plan.
- **Delivery Execution**
  1. Start sharing resources.

8. CONCLUSION

This work outlines an interesting project for critical resources (e.g. river water) sharing among multiple entities rationally with fairness, correctness, transparency and accountability. It is also essential to control heavy rainfall which often results flood, landslide and soil erosion in urban and rural zone. Such type of project requires the support of deep analytics of river and irrigation engineering, water resource management and cloud physics. Rational resource sharing is basically the problem of real-time supply chain optimization.

It is also a critical research agenda to explore efficient risk mitigation strategies against heavy rainfall and flood. How can we fight against natural calamities like flood due to heavy rainfall? We need an optimal mix of proactive and reactive approaches. Intelligent urban and rural development planning is essential in terms of reliable infrastructures (e.g. houses, roads, bridges, flyover, drainage system etc.). Can we explore the concept of a '*smart water grid'* to divert surplus water through pipelines, canals, rivers and drains to neighboring districts or states from flooded zone? It is rational to monitor timely release of water from various dams sequentially during rainy season; simultaneous release of water from all the dams of a state may aggravate the flood situation; it may be a conspiracy to draw flood relief fund by creating chaos

through malicious artificial intelligence. Sufficient number of water storage or harvesting systems (e.g. dams) is required.
Modern, well designed networks of drainage systems should be built along with filters. Regular cleaning of drains is essential to remove mud, sand, plastic goods, polythene packets, haggis and pads to avoid congestion or jamming in rainy season. It is also required to open manholes during rain carefully monitored by municipal and cleaning staff so that there should not be water logging problems on the roads and streets. It is an interesting and feasible option to increase level of residential plots at low land using soil and bricks. Intelligent evacuation plan should be ready during natural disaster. Migration of human civilization from risky zone and fair rehabilitation is also essential. The problem should be tackled scientifically; there may be threats of false data injection attacks and rumors such as superstitions, narrow prejudices and religious curses through various broadcast communication channels. The system administrators should be alert of the readiness of natural disaster relief workforce (NDRF) and army with helicopters, choppers, life-boats and other relief equipments during rainy season. It is rational to exercise capital budgeting based on fair and correct valuation by the experts, surveys, audit and demand plan of reliable infrastructure (e.g. road, bridges, flyovers and nano-housing scheme). How can we tackle cloudbursts artificially applying the concept of cloud physics? It is an open research agenda.

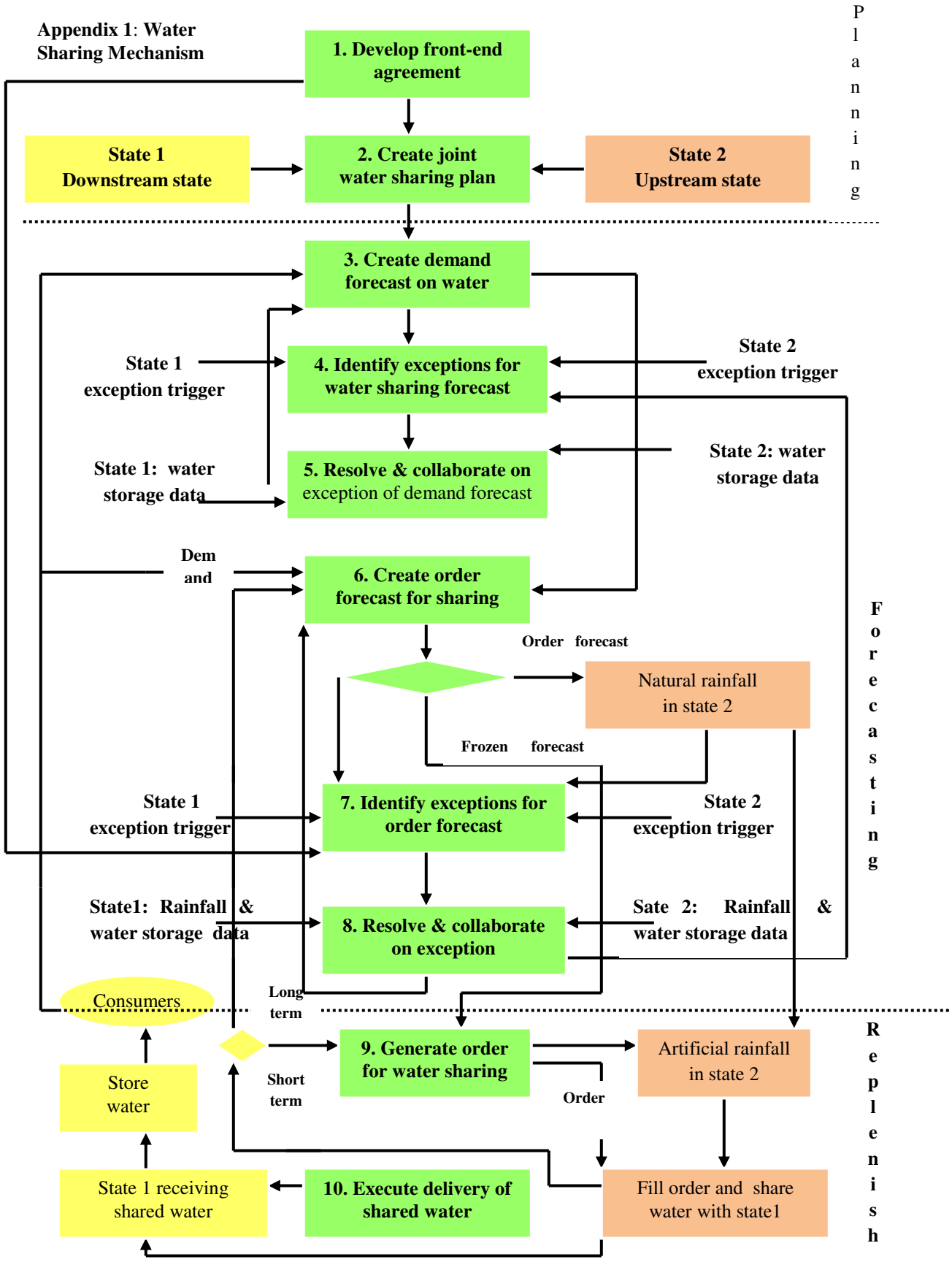
REFERENCES

[1] S.Chakraborty. 2007. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Thesis, Fellow Programme, Indian Institute of Management Calcutta.
[2] S.Chakraborty and S.K.Sharma. 2007. Enterprise Resource Planning: an integrated strategic framework. International Journal Management and Enterprise Development, vol. 4, no. 5.
[3] G.Dudek and H. Stadtler 2005. Negotiation-based collaborative planning between supply chain partners. European Journal of Operational Research, 163, 668-687.
[4] D.Seifert. 2002. Collaborative planning, forecasting and replenishment. Galliers Business.
[5]. S.L.Epstein. 2015. Wanted: Collaborative Intelligence. Artificial Intelligence, 221, 36-45.
[6] R.T.Bruintjes. 1999: A review of cloud seeding experiments to enhance precipitation and some new prospects. Bulletin of the American Meteorological Society: Vol. 80, No. 5, pp. 805-820.
[7] W.A.Cotton and R. A. Pielke. 1995. Human Impacts on Weather and Climate. Cambridge University Press.
[7] R.T. Bruintjes, D. W. Breed, V. Salazar, M. Dixon, T. Kane, G. B. Foote and B. Brown. 2001: Overview and results from the Mexican hygroscopic seeding experiment. Preprints, AMS Symposium on Planned and Inadvertent Weather Modification, Albuquerque NM.
[8] A.C.Cooper, R. T. Bruintjes and G. K. Mather. 1997: Calculation Pertaining to Hygroscopic Seeding with Flares. Journal of Applied Meteorology: Vol. 36, No. 3, pp. 1449-1469.
[9] G.K.Mather, D. E. Terblanche, F. E. Steffens and L. Fletcher. 1997. Results of the South African cloud-seeding experiments using hygroscopic flares. Journal of Applied Meteorology: vol. 36, No. 11, pp. 1433-1447.
[10] B.A.Silverman and W. Sukarnjanaset. 2000. Results of the Thailand warm-cloud hygroscopic seeding experiment. J. Appl. Meteor., 39, 1160-1175.
[11] K. Shivshankar, K.R. Chopkar, A. Gangakhedkar and B.Dhone. 2014. Cloud formation and atmospheric rain making by endothermic reaction due to plasma laser & UV radiation in the atmosphere. International Journal of Information Technology and Business Management, vol.21 No.1.

Exercise

1. **Explain the technology of artificial rainfall? Justify it as a technology for humanity. What is the scope of this technology for the protection against drought and flood?**
2. **What is the dominant design of the technology? Is it possible to adopt laser induced rainfall?**
3. **What are the basic elements of the system architecture? How to represent the structure correctly?**
4. **What do you mean by technology security? How to verify the security intelligence?**
5. **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**

6. **How to manage resource sharing rationally for this innovation project? Develop a collaborative resource sharing mechanism to resolve the conflicts of water distribution among two neighboring states or countries.**
7. **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently?**
9. **What should be the shared vision, common goals and communication protocols?**
10. **How can you ensure a perfect fit among '7-S' elements?**


Appendix 1: Water Sharing Mechanism
1. Develop front-end agreement
State 1 Downstream state
2. Create joint water sharing plan
State 2 Upstream state
Planning
3. Create demand forecast on water
State 1 exception trigger
4. Identify exceptions for water sharing forecast
State 2 exception trigger
State 1: water storage data
5. Resolve & collaborate on exception of demand forecast
State 2: water storage data
Dem and
6. Create order forecast for sharing
Order forecast
Natural rainfall in state 2
Frozen forecast
Forecasting
State 1 exception trigger
7. Identify exceptions for order forecast
State 2 exception trigger
State1: Rainfall & water storage data
8. Resolve & collaborate on exception
Sate 2: Rainfall & water storage data
Consumers
Long term
Short term
9. Generate order for water sharing
Order
Artificial rainfall in state 2
Store water
State 1 receiving shared water
10. Execute delivery of shared water
Fill order and share water with state1
Replenish

CHAPTER 10: REAL-TIME MOVING TARGET SEARCH FOR DETECTION OF ASTRONOMICAL HAZARDS : ADAPTIVE SECURITY & DDM

Abstract: The basic objective of a search is to identify an object and the position of the target. The target's position may be uncertain or there may be complete or incomplete information about its location in terms of a probability distribution. The target may be stationary or in motion. The target distribution is associated with discrete or continuous search space. The problem of optimal search is to maximize the probability of detecting a target subject to the constraints of resources, effort and time. Adaptive security and dynamic data management (DDM) is an essential part of space technology that can monitor the space in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. This work presents Real-time Probabilistic Search Mechanism (RPSM). The probabilistic search approach addresses the incomplete information on the target location by location probability. The problem is probabilistic from the perspectives of the location, size, distance and timing of the moving target(s) and distribution of the search efforts. The effectiveness of probabilistic search procedure can be verified on the basis of various properties of adaptive secure multiparty computation such as correctness, privacy, transparency, reliability and consistency. The search space can be divided into a set of private blocks; adequate number of sensors should be assigned to each private block; each block is monitored independently. This work highlights the complexity analysis of RPSM from the perspectives of computational cost and security intelligence. It also exercises case based reasoning on a test case of astronomical hazards and explores the scope of RPSM to assess and mitigate those threats. The universe is basically a computer, its history is being computed continuously. The astronomical hazards may be really dangerous threats against the sustainability of today's human civilization and the existence of a safe earth. This type of probabilistic search problem is really hard to solve, it is not a trivial problem. It is also challenging to deploy automated real-time search in reality and seeks extensive support, coordination, planning and corporate social responsibilities from various space research organizations and earth science institutes globally. Today, we have been dreaming of the moon and Mars voyage in space research. It may be a hard target. But, the sustainability of our earth from the dangerous astronomical hazards should be a top priority in space research globally : isn't it rational?

Keywords: Artificial intelligence, Probabilistic Light Beam Search, Predictive threat analytics, Astronomical hazards, Reactive and proactive security, Private search, Adaptive security, Dynamic data management

1. SCOPE

The basic objective of a search is to identify an object and the position of the target. The target's position may be uncertain or there may be complete or incomplete information about its location in terms of a probability distribution. The target may be stationary or in motion. The target distribution is associated with discrete or continuous search space. Search is conducted with various types of sensors such as CCTVs, cameras, telescopes, satellites and eyes of human agents. A detection function gives the probability of detection for a search as a function of effort (e.g. swept area, time). The detection function evaluates the effectiveness of search efforts in terms of probability of detecting the target object. The problem of optimal search is to maximize the probability of detecting a target subject to the constraints of resources, effort and time. The search space can be divided into a set of private blocks; adequate number of resources (sensors) can be assigned to each private block; each block is monitored independently.

In a search problem, a searching agent tries to find a hidden object by screening a certain defined area. The search space may be either discrete or continuous. In a continuous space, the target may move in various ways such as random, Markovian or Brownian moves. If the location of the target is known, then it may be complete-information tractable search problem and it may detect the target with a minimal number of search moves. The exact location of the target is generally unknown to the searching agent in incomplete

information search and the problem is addressed using the concepts of fuzzy logic or probability theory. The probabilistic search approach addresses the incomplete information on the target location by location probability. The problem is probabilistic from the perspectives of the location of the target and distribution of the search efforts. The effectiveness of probabilistic search procedure can be verified on the basis of various properties of secure multiparty computation: correctness (i.e. correct identification of the targets), privacy, transparency, reliability and consistency.

The problem of optimal search for a moving target in both discrete and continuous space has been investigated extensively in various research articles on operations research and artificial intelligence [1-9]. This work is an attempt to extend the study on the basis of related literature review and case based reasoning. This work is organized as follows. Section 1 is focused on scope; it defines the problem of probabilistic search of moving targets in discrete and continuous space. Section 2 is focused on system and structure and presents real-time probabilistic search mechanism (RPSM); the strategic moves include real-time light beam projection on the search space, automated data stream mining and adaptive secure multi-party computation. It defines the private search with a broad outlook of adaptive SMC. Sections 3, 4, 5 and 6 analyze security, strategy, staff-resources and skill-style-support respectively. Section 7 concludes the work.

2. SYSTEM & STRUCTURE

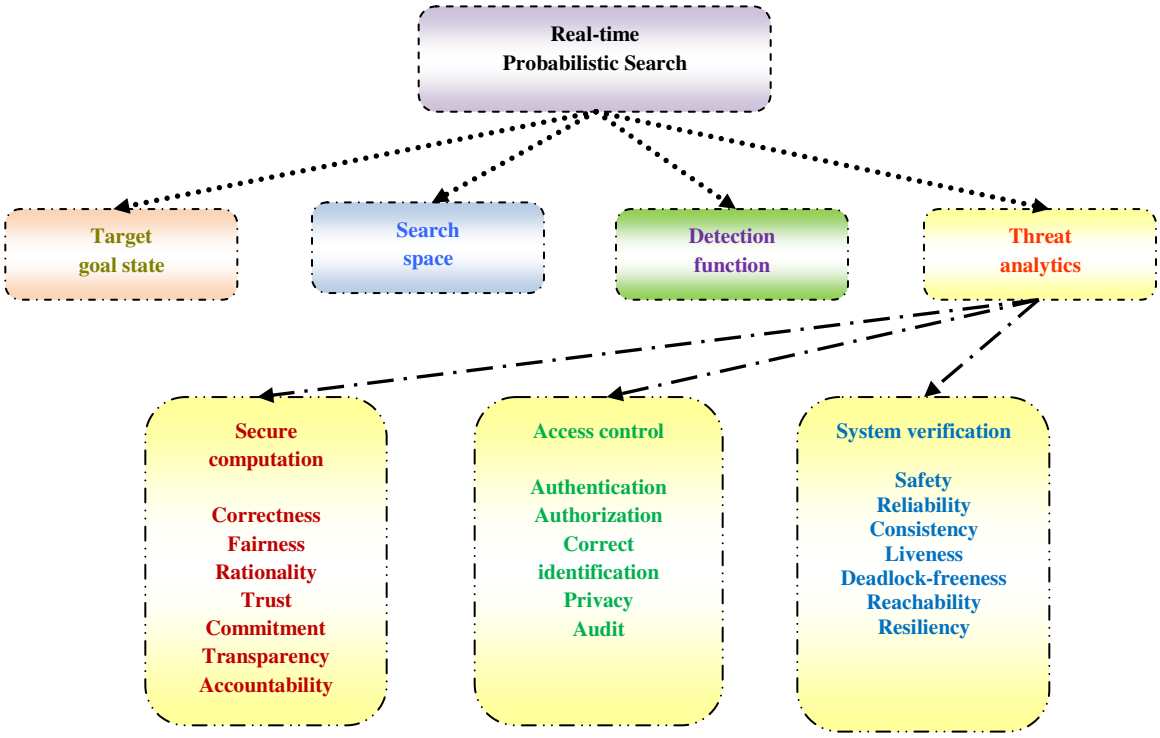


Figure 11.1 : Real-time Probabilistic Search Mechanism (RPSM)

REAL-TIME PROBABILISTIC SEARCH MECHANISM (RPSM)

++

Input: Search space, Goal state, Target distribution, Detection function;

Output: Identify objects (e.g. moving targets);

Moves:

- Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities;
- Real-time search;
- Automated data stream mining by intelligent threat analytics,
- Adaptive secure multi-party computation;.

Procedure (Probabilistic Search):

Divide the search space into a set of private blocks;
Assign resources to each private block;
Project light beam on private search space → move forward and backward;
Search discrete or continuous search space → sense data stream → filter data stream;
Detect target → verify correctness → give alert.

Security measures : (a) Proactive (b) Reactive.

++

The aforesaid mechanism (RPSM) is defined by a set of elements: system, searching agents, a finite set of inputs, a finite set of outcomes as defined by output function, a set of objective functions and constraints, an optimal set of moves, revelation principle, security measures and search procedure. It evaluates a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations. The mechanism seeks the support of an intelligent reasoning system i.e. threat analytics.

RPSM defines private search based on adaptive secure multi-party computation. Let us first discuss the traditional concept of secure multi-party computation. Two or more agents want to conduct a computation based on their private inputs but neither of them wants to share its proprietary data set to other. The objective of secure multiparty computation (SMC) is to compute with each party's private input such that in the end only the output is known and the private inputs are not disclosed except those which can be logically or mathematically derived from the output [13,15]. In case of secure multi-party computation, a single building block may not be sufficient to do a task; a series of steps should be executed to solve the given problem. Such a well-defined series of steps is called a SMC protocol.

In the study of SMC problems, two models are commonly assumed : semi-honest model and malicious model [12]. A semi-honest party follows the protocol properly with correct input. But after the execution of the protocol, it is free to use all its intermediate computations to compromise privacy. A malicious party does not need to follow the protocol properly with correct input; it can enter the protocol with an incorrect input. Adaptive secure multi-party computation deals with adaptive adversaries that may choose the corrupted parties during the course of computation in a setting of insecure communication channels [14]. In case of Non-adaptive secure multi-party computation, the set of corrupted parties is arbitrary but fixed before the computation starts.

A search protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. Secure multi-party computation preserves privacy of data in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to a DMA through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. Security and privacy of critical data is an important concern in any search procedure. Existing literature on private search is highly focused on the construction of various types of cryptographic tools (e.g. encryption and decryption, signcryption) and query processing on encrypted data as per the needs of revelation principle, information disclosure and privacy policy and risks of corruption of a mechanism. But it is not the only serious concern in a probabilistic search procedure. Let us define the private search on the basis of adaptive secure multi-party computation from a new outlook.

The security intelligence of the private probabilistic search procedure is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy. The search procedure addresses the issues of authentication, authorization, correct identification, privacy and audit through cryptographic solutions. For private search, the system should ask the identity and *authentication* of one or more agents involved in the mechanism. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, the procedure should address the issue of *authorization*. The system should be configured in such a way that an unauthorized agent cannot perform any searching task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. *Privacy* is another important issue; a searching agent can view only the

information according to authorized access rights. The search procedure preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication. Privacy is the primary concern of the revelation principle of a private search; the issue can be addressed through the concept of cryptography to provide confidentiality, data integrity, authentication and non-repudiation.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. But there are other different types of cryptographic concerns since the security intelligence is evaluated in terms of fairness, correctness, transparency, accountability, confidentiality and trust. The search mechanism is expected to ensures *correctness* in correct detection of target objects through adaptive real-time data mining and secure communication among the searching agents free from any false data injection attack; each recipient must receive the same correct data in time without any change and modification done by any malicious agent. *Fairness* is associated with the commitment, honesty and rational reasoning and trust. Fairness ensures that something will or will not occur infinitely often under certain conditions; it is important from the perspective of fair resource allocation in a search procedure. The search procedure must ensure the *accountability* and responsibility of the searching agents in access control and data mining. In fact, accountability is associated with collective intelligence. The *transparency* of the procedure is associated with communication protocols, revelation principle and automated system verification procedures (e.g. group testing). For example, a procedure should clearly state its goal state.

The performance and quality of search is expected to be consistent and reliable; it should be validated through *audit* of probabilistic search procedure. *Reachability* ensures that some particular state or situation can be reached. *Safety* indicates that under certain conditions, an event never occurs. *Liveness* ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. The effectiveness of probabilistic search procedure is expected to be verified adaptively on the basis of correctness, privacy, transparency, reliability and consistency. *Adaptability* is about responding to change effectively and decisively through real-time search: the ability to identify the change in search space for the moving targets, understanding the probable impacts of the hit by the targets, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The aforesaid discussion gives a complete definition of 'private search' based on adaptive secure multiparty-computation.

The cost of computation of probabilistic search depends on light beam projection on private search space.

Let us show an illustration of private search. The basic steps of an interactive search algorithm which operates between a decision making agent (DMA) and the mediator agent (MA) are as follows: (a) MA computes an initial feasible solution. (b) MA interacts with the DMA and (c) MA obtains a (or a set of) new solution. If the new solution or one of the previous solutions is acceptable to the DMA, stop. Otherwise, go to step 2. The design of interactive search methods depends on various issues: (a) The form through which DMA gives information, (b) The approach by which a multi-objective problem is transformed into a single objective problem, (c) The type of data used for interaction with DMA, (d) Number of non-dominated points to be presented to the DMA (a single point or a sample of points) and (e) How the DMA evaluates a set of alternatives?

Let us consider a specific interactive search procedure called *Light Beam Search* (LBS) method [10]. The idea of light beam search is analogous to projecting a focused beam of light from the aspiration point onto the search space. The lighted part of the frontier changes if the *aspiration point* or the point of interest in the non-dominated set is changed. This interactive search occurs between a DMA and the MA. The mediator asks the DMA to specify its preference in the form of aspiration and reservation point and various types of preferential thresholds. At each iteration of LBS procedure, MA generates a sample of non-dominated points using this preferential information. The sample is composed of a middle point and a set of non-dominated points from its neighborhood. MA shows these points to the decision-making agent.

Private Light Beam Search

Agents : A decision-making agent (DMA) and the mediator agent (MA).

Input : The mediator holds the deterministic problem; The DMA holds its aspiration point, reservation point, indifferent threshold, strong and weak preference threshold and veto threshold.

Output: DMA knows a set of solutions; MA can not know the output.

1. MA requests the DMA to specify its preferential parameters (P_A,P_R,I_{th}, P_{th}, S_{th}, W_{th}, V_{th}).
2.The DMA generates (n-1) random set of preferential parameters and appends its desired set of preferential parameters at a random position. The DMA sends to MA the list H = (H_1,…,H_n) where for a secret index $1 \le j \le n$, H_j = (P_A, P_R, I_{th}, P_{th}, S_{th}, W_{th}, V_{th}).
3. Repeat until the DMA is satisfied with a solution or concludes that no compromise point exists for the present constraints
a. MA computes a middle point (MP) alongwith characteristic neighbors for each set of preferential parameters.
b. The DMA gets back the results of k middle points alongwith characteristic neighbors using k-out-of-n oblivious transfer protocol where k<<n.; DMA scans the inner area of the current neighborhood and stores its preferred solutions in a private list L_1; it stores the invalid middle points in a private list L_2.
c. Case
(i) *The DMA wants to define a new aspiration and/or reservation point and/or updates preferential thresholds:*

- The DMA adds a set of new aspiration and/or reservation points and/or new preferential thresholds to the list H and sends H to MA.
- MA projects the aspiration points onto the non-dominated set and generates middle points with characteristic neighborhood.
- The DMA gets back the result of desired middle point alongwith characteristics neighbors using 1-out-of-n oblivious transfer protocol.

(ii) *The DMA wants a point from the current neighborhood to be the new middle point or wants to return to one of the stored points of L_1:*

- The DMA adds the desired middle point to the list L_2 and sends L_2 to MA;
- MA generates neighborhood of the middle points.
- The DMA gets back the result of desired middle point alongwith characteristics neighbors using 1-out-of-n oblivious transfer protocol.

The private light beam search procedure preserves the privacy of individual preferential parameters of the decision making agents about the target in terms of aspiration point (P_A), reservation point (P_R), indifferent threshold (I_{th}), strong preference threshold (S_{th}), weak preference threshold (W_{th}), veto threshold (V_{th}), middle point (MP) and preferred solutions resulted from the search process. The mediator agent preserves the privacy of the search problem.

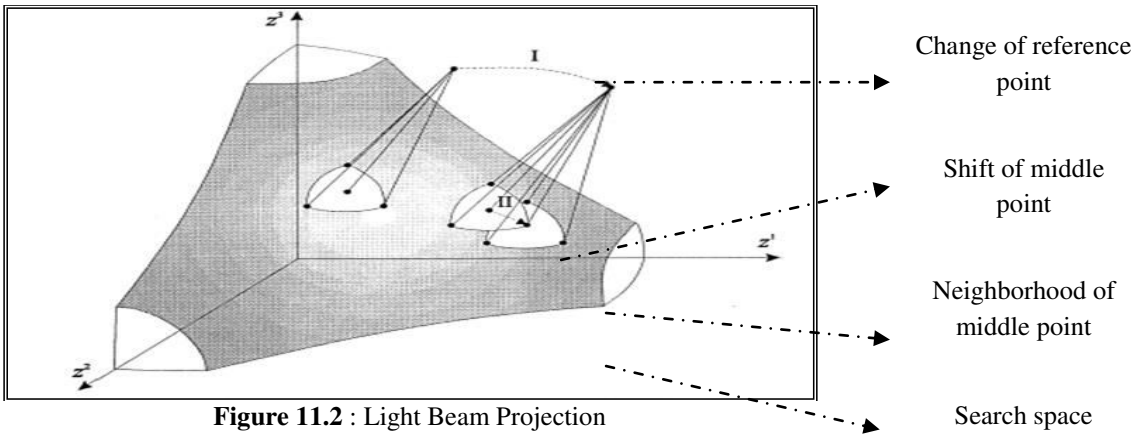


Figure 11.2 : Light Beam Projection

The value of an objective function which is desirable or satisfactory to the decision maker . *aspiration point*. The value of an objective function that the decision maker wants to avoid is called *reservation point*. A decision vector $x^* \in S$ is pareto optimal if there does not exist another decision vector $x \in S$ such that $f_i(x) \le f_i(x^*)$ for all i =1,…,k and $f_j(x) < f_j(x^*)$ for at least one index j; f_i is objective function and S is feasible space. An objective vector $z^* \in Z$ is pareto optimal if there does not exist another objective vector $z \in Z$ such that $z_i \le z_i^*$ for all i =1,…,k and $z_j < z_j^*$ for at least one index j. The decision maker should inform the mediator various *preference thresholds* in order to compare alternatives and to define outranking relations. There is an interval of preference wherein it is not possible for the decision-making agent to

distinguish between different alternatives due to imprecision and uncertainty of measurements and this corresponds to *indifference threshold*. *Strict preference threshold* is defined as minimal increase/decrease of any objective that makes the new alternative strictly preferred with respect to this objective. There exists an intermediate region between indifference and strict preference threshold where the decision-making agent hesitates to compare alternatives. This corresponds to *weak preference threshold*. *Veto threshold* It indicates that what is the minimal increase/decrease of any objective that makes the new alternative unacceptable regardless of the value of other objectives. In each computation phase of search, a finite sample of non-dominated points is generated by the mediator agent. The sample is composed of a middle point and a set of points within its *neighborhood*. The starting middle point is obtained by projecting aspiration point on the non-dominated set in the direction of reservation point. For a middle point, the neighborhood is defined as a set of non-dominated points that are not worse than the middle point. The neighborhood points from the sample indicate to what extent the values of particular objectives can be improved in relation to the *middle point*.

3. SECURITY

Astronomical Hazards

Figure 11.3: Deep Barringer Crater, Winslow, Arizona; Meteriotes

Figure 11.4: Asteroids, Comets

This section exercises reasoning on a test case of astronomical hazards and explores the scope of the aforesaid probabilistic search mechanism (RPSM) to assess and mitigate those threats. The universe is basically a computer, its history is being computed continuously (Zuse,1967). It is not possible to restrict the occurrence of astronomical hazards; but we have try to protect our earth from total destruction. The astronomical hazards may be really dangerous threats against the sustainability of today's human civilization and the existence of a safe earth. This type of probabilistic search problem is really hard to solve, it is not a trivial problem. Let us discuss the motivation of this threat in details based on the information and images given in figure 11.3 and 11.4 [11].

Asteroids are the largest of space rocks; most of them circle the Sun in the asteroid belt. Many of 3000 known asteroids are only a few miles across and all of them together would weigh much less than the Moon. Ceres, the largest asteroid, is about 600 miles across; Pallas and Vesta are about 350 miles in diameter. Bright *comets* are visible in the sky only once or twice in a century and stay for many days or weeks. *Meteors* flash in the sky every night or day. Meteor flashes are known as *shooting stars*. But meteors are not stars. Meteors begin as meteoroids in the form of rock or metal that orbit around the Sun. But, sometimes meteoroids plunge into Earth's atmosphere at speeds faster than a bullet. The friction with air particles makes them glow red hot and are called *meteors*. The bright flash is seen for only a few seconds. Perhaps as many as 100 million meteoroids enter the Earth's atmosphere every day. Most are just

small pieces of rock and burn in an instant; some become dazzling fireballs and fall to the earth surface called *meteorite*.

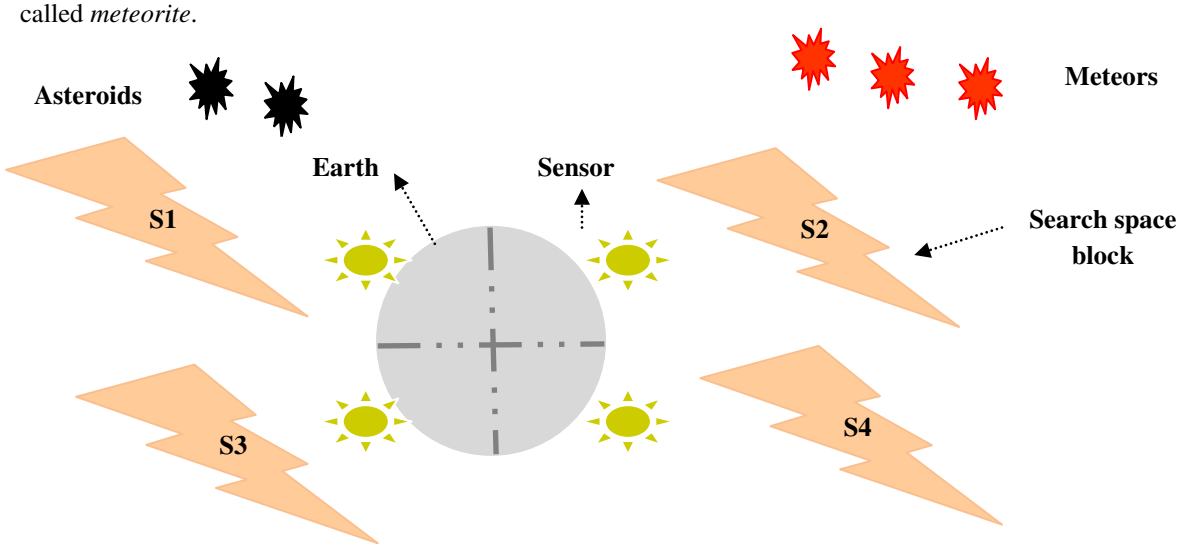


Figure 11.5: Structure - Astronomical Hazards Detection System

The problem of astronomical hazards : Will an or large number of asteroids or a large meteorites ever hit Earth? Many large objects had hit our earth in the past and resulted huge hollows in the ground known as *impact craters*. The largest is the 4150 foot wide and 600 foot deep Barringer Crater near Winslow, Arizona. Is there any probability of mass destruction of human civilization and the earth due to the strike of a comet or the shower of numerous large meteorite or asteroids in future? How to protect our earth from the threat of such type of astronomical hazards? One possible solution may be the real-time probabilistic search. The basic objective of the search is to detect the motion of the asteroids, meteors and comet moving dangerously towards the earth in terms of distance, time and size of the objects. The target's position may be uncertain or there may be incomplete information about its size and location. The automated light beam search is expected to be conducted with various types of sensors such as telescopes and satellites. The detection function gives the probability of detection for a search as a function of effort (e.g. search area, distance, time) and evaluates the effectiveness of search efforts in terms of probability of detecting the incoming objects.

Real-time Probabilistic Search Mechanism ($RPSM_{ah}$) :

++

Agents : System administrator (Space Research Organization), Human agents;
Input: Data stream sensed by the sensors, Rough definition of target, Detection function;
Output: Identify objects or moving targets such as asteroids and meteors coming very near to the earth within threshold distance;
Moves: Real-time search, group testing, adaptive secure multi-party computation, automated data stream mining by intelligent threat analytics;
Procedure:
Divide the search space into a set of private blocks;
Assign resources (sensors, satellites, earth station) to each private block; each block is monitored independently; /* the resources of different blocks interact with each other through coordination mechanism and secure broadcast communication protocol (Internet) */;
Project light beam from the sensors on private search space → move forward and backward repeatedly;
Filter data stream;
Detect target → verify correctness to avoid false alarm → call threat analytics → give alert.
***Risk Mitigation Strategies*:**

- ***Proactive security* (Before astronomical hazards):**

- Learn drop-cover-hold
- Have an emergency kit ready and always carry (if possible).
- Build a disaster proof house as per the advice of structural or civil engineering consultant; repair deep cracks on ceilings and walls of the house; fix shelves securely to the walls, avoid heavy loading of the rooms.
- *Safe shelter* : (a) build artificial caves at critical locations in urban and rural zone; (b) build robust shed on the roof made of steel (Fe) / Al / Tin (Sn) structure;
- Wear robust helmets and jackets
- Give alert through broadcast communication -→ take safe shelter in time;

- ***Adaptive security*:**
  - *Laser beam projection* for *object decomposition* after detection of incoming objects through probabilistic real-time search;
  - Artificial *collision* of asteroids and meteors, network *traffic congestion* or *traffic diversion* in space
  - Activate *Antenna* for blocking and throttling (i.e. slowing speed) of incoming objects entered into the earth based on the principle of electromagnetic induction;
  - Divert the traffic to the desert or remote zone to minimize the negative impact of astronomical hazards.
  - During astronomical hazard
    - Remain calm and do not panic.
    - Take shelter under a table, cover head with hands and hold the table till the hazards last;
    - If you are outside, move towards buildings, trees, walls and poles and take shelter;
    - I you are inside a vehicle; pull over in a covered place and remain inside.
  - After astronomical hazards
    - Avoid entering damaged civil infrastructure (residential flats, office buildings, industrial plants).
    - Use stairs instead of lifts and elevators..
    - If trapped in rubble or damaged infrastructure, sound whistle, clap or shout, avoid lighting matchstick, turn on search lights of mobile phones, tap on a pipe or a wall safely.

++

5.1 ADAPTIVE SECURITY & DYNAMIC DATA MANAGEMENT

Our earth may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of intelligent security policies, protocols and mechanisms. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the space in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of the space to protect against and adapt to specific threats before the occurrence of known or unknown types of astronomical hazards. Adaptive security monitors the space in real time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventative capabilities allow to create infrastructure, products, processes and policies that can mitigate the astronomical hazards . The detective capabilities should identify those threats in time at minimum impact and not detected by preventative capabilties. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.

Let us consider the technology associated with adaptive security and dynamic data management for the protection of our earth. Today, it is essential to deploy adaptive security architecture for real-time moving target search. A smart grid demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent astronomical hazards. Adaptive security is an essential part of solar computing. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous,

contextual and coordinated approach. For example, prevention and detection are traditional approaches to the security of our earth. In today's universe of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques for the protection against astronomical hazards.

Dynamic data management is an effective way to move towards adaptive security architecture. DDM surfaces anomalies and adjusts security controls proactively in near real-time to protect our earth. Adaptive Security with dynamic data management is expected to offer many benefits over traditional security platforms : real-time monitoring of events and traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of the system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of the security of our earth with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

4. STRATEGY

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovations are closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of this innovation today.

This technological innovation is closely associated with R&D policy and organizational learning strategies in new product development and process innovation. There are various strategies of learning such as learning by doing and learning before doing. learning before doing is possible through various methods such as prototype testing, computer simulations, pilot production run and laboratory experiments. It is effective where deep practical and theoretical knowledge can be achieved through laboratory experiments that model future commercial production experience.

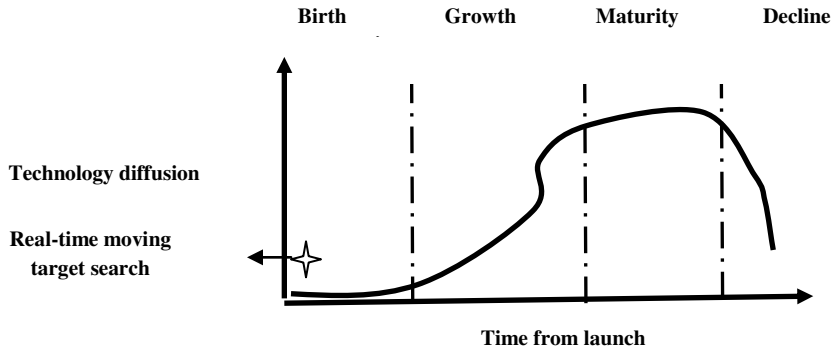


Figure 10.6 : Technology life–cycle analysis

Deep analytics can evaluate and explore this technological innovation in terms of technology life cycle, technology trajectory, S-curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, each technology emerges, grows to some level of maturity and then declines and eventually expires. It is essential to evaluate the status of each technological innovation through TLC analysis. At present, this technology is at emergence phase of S-curve.. Emergence of new technologies follows a complex nonlinear process. All technologies evolve from their parents; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early

phases, it adapts and forwards to its intended environment. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. Let us consider the analysis of the performance of a new technology vs. effort; it is basically an S-curve. Initially, it is difficult and costly to improve the performance of a new technology. The performance begins to improve with better understanding of the fundamental principles and system architecture. Next, let us analyze the adoption of a new technology over time which is also an S curve. Initially, a new technology is costly for the adopters due to various uncertainties and risks. Gradually, this new technology is adopted by large segments of the society due to reduced cost and risks. Gradually, the diffusion of new technology slows with the saturation of market or due to the threats imposed by other new technologies.

The evolution of this technology passes through a phase of turbulence and uncertainty; various stakeholders of the design chain explore different competing design options of the new technology and a dominant design emerges alongwih a consensus and convergence of structure. The dominant design considers an optimal set of most advanced technological features which meet the demand of the customer, supply and design chain in the best possible way.

Technology trajectory is the path that a technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of this innovations today. How to manage evolution of this technological innovation? The nature of innovation shifts markedly after a dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow an S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by technologies. Technology diffusion indicates how new technologies spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards.

5. STAFF-RESOURCES

This section outlines the sixth element of deep analytics i.e. staff-resources in terms of 5M – man, machine, material, method and money. The technological innovation demands the commitment of creative talent from the domains of earth science, space research organization and ministry of science and technology. It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion, dominant design factors, effects of timing and mode of entry. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment.

It is important to analyze this element in terms of 5M – man, machine, material, method and money. ‘Man’ analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive and performance evaluation. ‘Machine’ analyzes the basic aspects of tools and automated / semi-automated / manual machines. ‘Method’ explores various aspects of process innovation, intelligent mechanism and procedure. Finally, ‘money’ highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. The universities should define sound research mission and vision and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators). Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms.

This is not a trivial problem; it needs useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. It is difficult to conclude that

moderate knowledge is adequate for creativity. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routines, incentive policy, social processes and contextual factors.

6. SKILL-STYLE-SUPPORT

The seventh element of deep analytics is skill-style-support. The workforces involved in this technological innovation are expected to develop different types of skills in technical, management and system administration. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of top technology innovation requires the support of great leadership style. The style is basically the quality of leadership; the great leaders must have passion, motivation and commitment. The leaders must be able to share a rational vision, mission and values related to the innovation among all the stakeholders honestly and appropriately in time.
What should be the ideal organization model for this technological innovations? A traditional functionally centered organization model may not be suitable for supporting end-to-end business processes. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common, customer oriented goal. The business models of top technological innovations require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement. The process enterprise requires a collaborative and cooperative work culture. Top innovations need proactive, reactive and preventive support for proper technology management. The technology needs the support of a collaborative enterprise model.

7. CONCLUSION

It is possible to construct similar type of search mechanism like $RPSM_{ah}$ and risk mitigation strategies against the threats of geological hazards such as earthquake. For example, the risk mitigation strategies should include rational approaches in urban and rural development planning, public policy making, cautious approach and regulatory compliance on mining of earth's soil (e.g. coal, minerals, sand, gas pipeline) and construction activities (e.g. saturation in metropolitan cities, building high storied buildings without soil testing, tunnels, metro rails, irrigation projects, dams etc.), monitoring of volcanoes and landslides in hilly zones. The aforesaid type of probabilistic search problem is really hard to solve and it is also challenging to deploy RPSM in reality and seeks extensive support, coordination, planning and corporate social responsibilities from various space research organizations and earth science institutes globally. The most critical challenges involve the innovation of automated real-time search algorithm, intelligent sensors and predictive analytics, resource planning and deployment, system administration and coordination both locally and globally. Artificial intelligence is basically simulation of human intelligence. A rational reasoning system often needs the support of an intelligent analytics. An intelligent reasoning system demands new solution methodology beyond traditional knowledge base with imagination, envision, perception and proper assessment of a hard problem like the aforesaid probabilistic search.

REFERENCES

1. S.S.Brown. 1980. Optimal search for a moving target in discrete time space. Operations Research, volume 28, no. 6, pp. 1275-1289.
2. T.Ishida. 1992. Moving target search with intelligence. AAAI-92, pp. 525-532.
3. E. Kagan and I. Ben-Gal. 2013. Moving Target Search Algorithm with Informational Distance Measures. Entropy.
4. P. J. Schweitzer. 1971. Threshold Probabilities when Searching for a Moving Target. Operations Research, 19(3), 707–709.
5. J. N. Eagle. 1984. The Optimal Search for a Moving Target when the Search Path is Constrained. Operations Research, 32, 1107–1115.
6. L. C. Tomas and J. N. Eagle. 1995. Criteria and Approximate Methods for Path-Constrained Moving-Target Search Problems. Naval Research Logistics, 42, 27–38.
7. D. A. Grundel. 2005. Searching for a Moving Target: Optimal Path Planning. IEEE Conference on Networking, Sensing and Control, 19–22 March, 2005, 867–872.
8. I. M. MacPhee and B. P. Jordan. 1995. Optimal Search for a Moving Target.
9. A. Stenz. 1994. Optimal and Efficient Path Planning for Partially-Known Environments. IEEE International Conference on Robotics and Automation, San Diego, CA, USA, vol. 4, 3310–3317.
10. A.Jaszkiewicz and R.Slowinski. 1999. The light beam search approach an overview of methodology and applications. European Journal of Operational Research, 113, 300-314.
11. S.Simon. 1998. Comets, meteors and asteroids. Scholastic Inc.
12. W.Du and M. J. Atallah. 2001. Secure multi-party computation problems and their applications: a review and open problems. In 2001 workshop on new security paradigms (pp. 13 - 22). ACM Press.
13. Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.
14. R.Canetti, U.Feige, O.Goldreich and M.Naor. 1996. Adaptively secure multi-party computation.
15. S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. IIMC.

Exercise

1. **Explain the problem of real-time moving target search? Justify it as a technology for humanity. What is the scope of this technology for the protection of our earth against astronomical hazards?**
2. **What is the dominant design of the technology?**
3. **What are the basic elements of the system architecture? How to represent the structure correctly?**
4. **What do you mean by technology security for real-time moving target search? How to verify the security intelligence? What is the role of adaptive security and dynamic data management in this context? Design an adaptive security architecture.**
5. **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**
6. **How to manage resources in this innovation project? What should be the talent management strategy?**
7. **What are the skills, leadership style and support demanded by the technological innovation?**
8. **How to manage technology innovation project efficiently?**
9. **What should be the shared vision, common goals and communication protocols?**
10. **How can you ensure a perfect fit among '7-S' elements?**

CHAPTER 11 : CONCLUSION

The central message of this book is that the success of technology innovation projects depends on several factors: strength, weakness, opportunities, threats, technology life-cycle, understanding the needs of consumers, competitive environment, blind spots and the ability to recognize and align the partners associated with the value chain and innovation ecosystem. Deep analytics is essential to coordinate, integrate and synchronize '7-S' elements: scope, system, structure, staff-resources, skill-style-support, security and strategy. Even the most brilliant innovation cannot succeed when its value creation depends on innovation of other technologies. This draft is the summary of the extended deep business analytics of top seven technology innovation. Most of these technology innovations are at emergence stage, some others are at maturity stage. The extended draft reasons ten technology innovation projects deeply from the perspective of numerical, statistical, quantitative and qualitative analysis based on up-to-date data. In fact, there is no end of this intelligent deep analysis. Hopefully, deep analytics should be able to accelerate the pace of emerging technological innovations associated with solar power, electrical and hybrid vehicles, Railtech, digital technology, solar computing for a smart grid, IIOT enabled ICS & SCADA, bio-medical instrumentation, cancer prediction and prevention, artificial rainfall and real-time search for astronomical hazards: ***let us try to save the world.***

Sumit Chakraborty is one of the authors of this book. He had done his graduation in Electrical Engineering from Jadavpur University and attended Fellow programme at IIM Calcutta. His major area was Management Information Systems (MIS) and minor area was Strategic Management. He worked in power project management, power transmission and distribution and global supply chain management and ERP for a manufacturing plant and business consulting such as process mapping and requirements management. He has also made modest efforts to carry out research in MIS, Information Security and business analytics. He has taught courses at various management institutes in India. Suryashis Chakraborty is the co-author. The authors have interest in business analytics, data science and technology for humanity.

FREE eBooks

WHOEVER
WHENEVER
WHEREVER
YOU ARE

INSTANTLY DOWNLOAD THESE MASSIVE BOOK BUNDLES

CLICK ANY BELOW TO ENJOY NOW

3 AUDIOBOOK COLLECTIONS

Classic AudioBooks Vol 1 ▪ Classic AudioBooks Vol 2 ▪ Classic AudioBooks Kids

6 BOOK COLLECTIONS

Sci-Fi ▪ Romance ▪ Mystery ▪ Academic ▪ Classics ▪ Business