Security Management Process in Distributed, Large Scale High Performance Systems

Article

1 author:

K. Kraus
KiwiSecurity Software GmbH
8 PUBLICATIONS **41** CITATIONS

SEE PROFILE

Security Management Process in Distributed, Large Scale High Performance Systems

K. Kraus
KiwiSecurity Software Gmbh, Vienna, Austria

Abstract- **This paper envisions the performance side of large-scale distributed systems. Security is the biggest performance hurdle; accordingly the most efficient technique to maintain or enhance system performance is to provide a reliable Integrated Security Management Process capable to support large-scale high performance distributed systems. A framework describing information security management core components of the security management process: ISO/IEC 27001 is presented.**

Subsequently, an advanced security management process for an enterprise is introduced. A general structural overview of the security management process, the enterprise point of view and an election process for large scale distributed systems was analyzed and adapted.

Finally, a concept for the architecture of an integrated security management process as an overlay for sub-security management processes in complex distributed systems is presented. This concept was analyzed for Smart Grids and the concept of the overlaid integrated security management process seems to be indispensible from the economic and performance point of view.

Keywords- **Security Management Process, Distributed Systems, Information Security Management, Smart Grids, SmartCam, Process Lifesycle.**

I. INTRODUCTION

This paper reports on part of a doctoral dissertation research project on Security Management Process together with the Department of Information Processing Science, Oulu University, Finland. One of the aims of the project is to develop an architectural framework and a process model, with supporting methodology that could enable integration of security management with the life cycle processes of large-scale, distributed systems in an enterprise environment.

Over the years, the focus of information security as well as physical security evolved from physical security of computer centers to securing information technology systems and networks, to securing business information systems [1].

From one side, with the unstoppable progress of communication networks [2], it is just common that computers communicate and share information with other computers outside the organization's networks, utilizing the high-speed broadband whether fixed or mobile, giving a big chance for cyber crime. This means that the existing security models are still inadequate to meet the threats and challenges in this new technology.

From the other side, according to the current economical situation and according to the boiling political situation in some regions, an increasing tendency of organized criminality on critical infrastructure worldwide is taking place. Hence a new approach to information and physical security management process is required to meet those security challenges [3].

A meta model for the information security and security management process was developed in this research, taking into consideration various principles such as business strategy and mission, security management goals and objectives, security management systems, security management programs, information security frameworks, security process improvement models with supporting methodology, enterprise business systems and finally high performance large scale projects for protecting critical infrastructure.

Challenges:

For a large scale, distributed system the main challenges are:

- heterogeneity of the systems
- different hardware & software components
- different manufactures and
- different operating systems

Those components must be operated, administrated and maintained simultaneously. Furthermore, those components are networked; most probably via heterogeneous network technologies. Their communication networks provide an optimal medium for security attacks.

Moreover, a large-scale system might comprise different subsystems or complex components, which use different security systems.

From the other side, the components of a high performance system must react in real time, must be self organized and must be available and reliable 24/7.

This reflects the need of an overarching security management process, controlling all security management processes of the different system components.

This work will begin with the high level analysis of the requirements of an information security management system, followed by security management process of a singular system together with an example for a large-scale enterprise. Based on this information, the architecture of a global security management process for a large scale high performance distributed system will be designed and

presented. Finally, different field applied use cases are presented and analyzed.

In this paper we report on parts of the results of our analytical study. This publication is divided into the following chapters:

- Information security management, the basic requirements: the CIA triad
- Frameworks describing information security management
- Core components of the security management process: ISO/IEC 27001
- Synchronization of processes for large scale distributed systems
- Election process for large scale distributed systems
- General structural overview of the security management process, the enterprise point of view
- Integrated security management process
- SMP and security control for a large scale enterprise: An illustrative example
- Smart grids, the applied study case of the integrated security management process concept

Thus a framework for Security Management Process in distributed, large scale high performance systems is presented.

II. INFORMATION SECURITY MANAGEMENT: THE BASIC REQUIREMENTS, THE CIA TRIAD

IT systems and procedures play the huge role in information security management (ISM). The ISM process is driven by three main factors: Availability, Confidentiality and Integrity, see Figure (1).

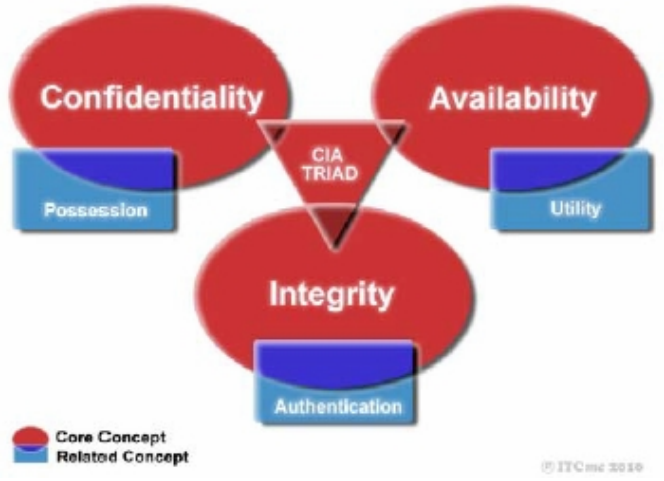

Figure (1): Core Information Security Management Concept, the CIA Triad

Availability:

Availability ensures reliability and timely access to data and resources to authorized individuals. Most information needs to be accessible and available to users when it is requested so that they can carry out tasks and fulfill their responsibilities. Accessing information does not seem that important until it is inaccessible, thus fault tolerance and recovery mechanisms are put into place to ensure the continuity of the availability of resources. User productivity can be greatly affected if requested data is not readily available. Thus Availability is the assurance that information is available to authorized users or systems at the times they are authorized to access it. An example of a security failure concerning availability might be the prevention of authorized persons accessing corporate data because of an internet-based denial of service (DoS) attack. Another might be the inability to run a payroll program because of accidental deletion of a staff data file.

One further example: It may be extremely important for a stockbroker to have information that is accurate and timely, so that he can buy and sell stocks at the right times at the right prices. The stockbroker may not necessarily care about the privacy of this information, only that it is readily available.

Confidentiality:

Confidentiality is upheld when the assurance of accuracy and reliability of information and systems is provided and unauthorized modification is prevented. Some information is more sensitive and requires a higher level of confidentiality. Control mechanisms need to be in place to dictate who can access data and what the user can do with it once they have accessed it. These activities need to be controlled, audited, and monitored.

Examples: Health records, financial account information, criminal records, source code, trade secrets and military tactical plans can be termed confidential. Some security mechanisms that would provide confidentiality are encryption, logical and physical access controls, transmission protocols, database views and controlled traffic flow. Confidentiality can also counteract identity theft where one individual misrepresents himself as another, usually for fraudulent financial gain.

Integrity:

Integrity is the assurance that information has not been changed or modified in storage or transmission except by authorized personnel or processes. It covers any form of unauthorized change, deliberate or otherwise. An example might be modification of data stored on a computer by the action of a computer virus. When a security mechanism provides integrity, it protects data or a resource from being altered in an unauthorized fashion. If some type of illegitimate modification does occur, the security mechanism must alert the user in some fashion.

An Example: A user sends a request to her online bank account to pay her $24.56 water utility bill. The bank needs to be sure that the integrity of that transaction was not altered during transmission, so the user does not end up paying the utility company $240.56 instead. It must be noted that different security mechanisms can supply different degrees of availability, integrity and confidentiality.

The environment, the classification of the data that is to be protected and the security goals need to be evaluated to ensure that the proper security mechanisms are bought and put into place. In the context of distributed systems, the task of securing both the services and the infrastructure can be arbitrarily complex.

Figure (1) also presents the related concepts to Integrity, Availability and Confidentiality, which are authentication (Identity verifying), utility (usefulness of data) and Possession (control of information) respectively.

III. FRAMEWORKS DESCRIBING INFORMATION SECURITY MANAGEMENT

This chapter discusses the contents and purposes of, and relationships between global standards [4], best practice guidance and organizational policies and procedures in the creation of an effective Information Management System. In May 2009, an analytical report white paper was released [5] discussing the Information Security and its important role in the Information Security Management.

Accordingly, in order to design a global architecture for a large-scale distributed system, we have to analyze the current published ISO standards as well as the ongoing trends. Those standards are used as a framework for our architecture design.

Currently, there is an ever-growing list of global standards in ISM resembling the ISO/IEC 27000 family. This series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS).

It has a broad scope, covering more than just privacy, confidentiality and IT or technical security issues. It is intended for organizations of all shapes and sizes. They are encouraged to assess their information security risks and then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant.

Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities [6] or impacts of information security incidents. Figure (2) presents the recent status (2010) overview of Information Security Management (ISM) / Information Technology Security Management (ITSM) standards.

The different standards can be summarized as follows:

Already published:

- ISO/IEC 27000: presents an introduction and overview for the ISMS Family of Standards, plus a glossary of common terms.
- ISO/IEC 27001 at the moment its best known representative, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). Its full name is "ISO/IEC 27001:2005 - Information technology -Security techniques -- Information security management systems - Requirements" but it is commonly known as "ISO 27001".

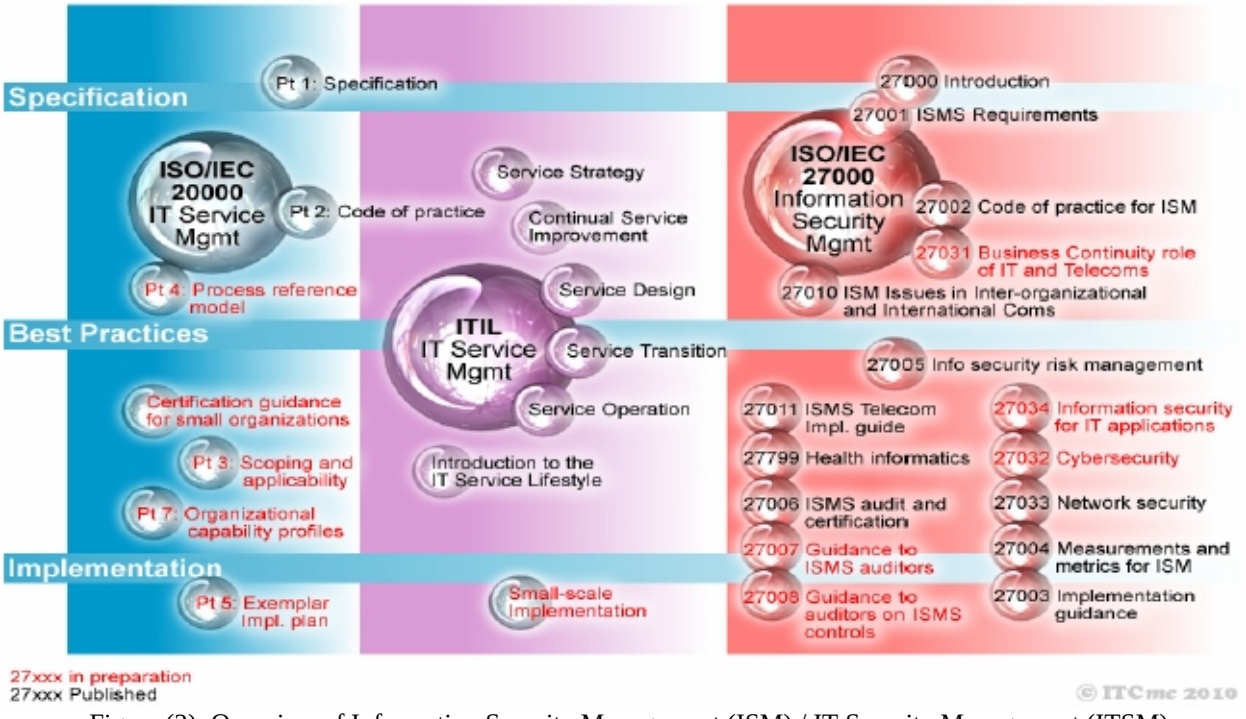

Figure (2): Overview of Information Security Management (ISM) / IT Security Management (ITSM) Status Sept. 2010

The recommendation ISO/IEC 27002, is usually used in conjunction with ISO/IEC 27001, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMS in accordance with the best practice advice in ISO/IEC 27002 are likely to simultaneously meet the requirements of ISO/IEC 27001 but certification is entirely optional (unless mandated by the organization's stakeholders).

- ISO/IEC 27003, the third of the ISO/IEC ISMS standards, has been published 2008 as "Information technology, Security techniques, and Information security management system implementation guidance". The purpose of this standard is to provide practical guidance for implementing an information security management system (ISMS) based on ISO/IEC 27001. ISO/IEC 27001 represents a business outlook for managing information security within an organization.
- ISO/IEC 27004 - a standard for information security management measurements
- ISO/IEC 27005 - a standard for information security risk management
- ISO/IEC 27006, the fifth of the ISO/IEC ISMS standards, has been published 2007 as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".
- ISO/IEC 27031 - an ISMS implementation guideline for the telecommunications industry (also known as X.1051)
- ISO/IEC 27033-part 1: - IT network security, a multi-part standard currently known as ISO/IEC 18028:2006

Still under preparation:

- ISO/IEC 27007: a guideline for ISMS auditing (focusing on the management system)
- ISO/IEC 27008: a guideline for Information Security Management auditing (focusing on the security controls)
- ISO/IEC 27031: a specification for ICT readiness for business continuity
- ISO/IEC 27032: a guideline for cyber security (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27034: a guideline for application security

From the above discussion, ISO/IEC 27001 requires that

- Management systematically examines the organization's information security risks, taking into account the threats, vulnerabilities and impacts.
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable.
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis. The core components of this group is discussed and analyzed in the following section.

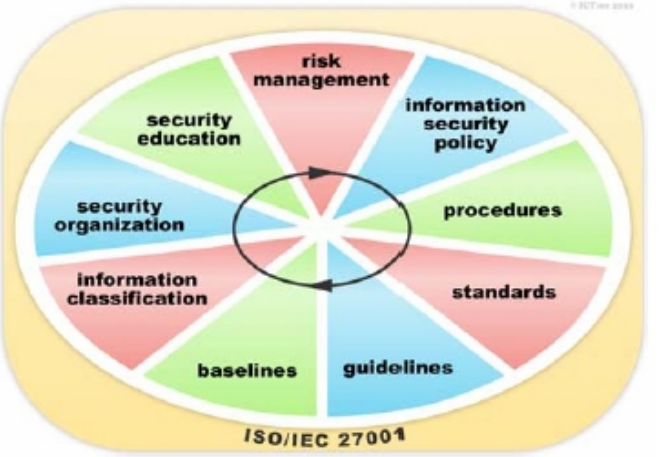

Figure (3): The Security Management Process according to ISO/IEC 27001

IV. CORE COMPONENTS OF THE SECURITY MANAGEMENT PROCESS, ISO/IEC 27001

As the main Information Security Management Systems Standards, the 27001 has the following core components as seen in Figure (3).

The core components can be summarized as follows:

Risk management:

First assets have to be identified. The actual risk management is then concerned with identifying and assessing risks to those assets, reducing them to an acceptable level and implementing the right mechanism to maintain that level.

Consequently, possible mitigation scenarios are discussed and also listed. An evaluation of cost versus benefit of each of the suggested measures allows the selection of the controls best suited to meet the identified risks.

Information security policy:

This step gives a general, implementation agnostic framework of what the security measures should look like. In addition to the results of the risk analysis, the Legal Constraints of the organization / large scale enterprise provides additional important input for the development of the policy.

Moreover, every relevant area e.g. access control, business continuity, application security, physical security, incident handling, human resources security, compliance and IS acquisition, development and maintenance have to be analyzed carefully. Much more fine grained information is needed to guide the realization of the policy and this happens with the use of procedures, standards, and guidelines.

Procedures:

Procedures represent detailed step-by-step tasks describing how to achieve a certain goal. These steps can apply to the

authorized personnel/users, e.g. IT staff, operations staff and security members. Procedures are to be followed as they spell out how the policy, standards and guidelines will actually be implemented in an operating environment.

Example: A general network security policy could be: "According to a certain event, every network node has to be locked down".

A procedure would then detail how this should be achieved. One part could be: "The installation of the operating system shall only contain programs necessary for the realization of the required functionality within the project under consideration."

Standards:

There may be mandatory activities, actions, rules or regulations issued either by the customer organization or from some external entity or authority, which the customer organization has decided to embrace. Standards can give a policy its support and reinforcement in direction. Standards could be internal or externally mandated (government laws and regulations).

Example: For the Identity Management aspects of the User Management part of the project in question the European Directive 95/46/CE about data protection could be applicable with all its consequences.

Guidelines:

There have to be recommended actions and operational guides to users, IT staff, operations staff and others when a specific standard does not apply or is not explicit enough. Guidelines can deal with the methodologies of technology, personnel or physical security.

Example: A general policy concerning Access Control could be that access to the identified assets must be audited. A supporting guideline would then have to explain how audits could contain sufficient information to allow for reconciliation with prior reviews. In addition procedures outlining the necessary steps to configure, implement and maintain this type of auditing will have to supplement the guideline.

Baselines:

The end result of the steps described above yields a picture of what needs to be done for the desired level of security. This is then a baseline for the planned security activities.

There are two types of definitions for a baseline:

- Consistent reference point: A baseline can refer to a point in time, when risks have been mitigated, and security put in place. All further comparisons and development are measured against this status.
- Minimum level of protection: Mostly, specific baselines have to be defined per system type, indicating the necessary settings and the level of protection provided.

Information classification:

During the risk analysis phase values were assigned to the identified assets in order to enable ESA to provide adequate funds and resources for the protection of each type of data. In the course of the development of the security baseline data also need to be organized according to its sensitivity to

- Loss
- Disclosure or
- Unavailability

This forms part of the basis of knowing, which security controls have to be applied to these assets (as put down in the security baseline). The classification also forms an important part of the input for the security organization, which needs to be put into place.

Security organization:

Depending on the organization, security needs, and size of the environment, organizational structures may be introduced as part of the security controls.

Example: A separate security administrator might be necessary to administer and maintain restricted parts of the network (e.g. IDS) and the database (e.g. user identities).

Security education:

Individuals of an organization need to be trained according to the roles in their security organization so that the identified threats are mitigated as planned. Different roles require different types of training (e.g. firewall administration, risk management, policy development, IDSs ...) to arrive at the proper levels of security education.

System Security requirements:

Large-scale distributed computing environments include a combination of computer resources from multiple administrative domains to reach the common goal of high performance, in spite of the fact that the processing components are heterogeneous and geographically dispersed.

Such systems and applications may require all or some of the standard security functions including authentication, access control, integrity, privacy and non-repudiation. In this example, we consider the issues of authentication and access control on the system level which is a representing example.

The Policy of the Security Management Process in this case is summarized as follows:

- The environment consists of multiple administrative domains.
- Local operations (i.e. carried out within one domain only) are subject to local security policies only: It is assumed that each domain has a local security policy, which cannot be changed when the domain participates in the whole system (i.e. the global policy of Globus cannot override the local security policy). Consequently a security policy in Globus will restrict itself when operations involve multiple domains.

- Global operations (i.e. involving several domains) require the initiator to be known in each domain where operations are carried out: Requests for operations can be initiated both globally and locally. The initiator (user or process) needs to be known locally within each domain, where that operation is carried out.
- Operations between entities in different domains require mutual authentication: If a user of one domain wants to make use of a service in another domain his identity will have to be verified as well as the service identity (to be sure that he is using the right one).
- Global authentication replaces local authentication: This is a combination of point 3 and 4: If the identity of a user has been verified and the user is also known locally in a domain, he can act as if authenticated in the local domain.
- Controlling access to resources is subject to local security only: After authentication of a user, his exact privileges still have to be verified (authorization check).
- Users can delegate rights to processes: processes in different domains in order to execute/complete a certain task, it makes sense to allow authenticating an agent and subsequently enable this agent to initiate operations without having to contact the agent's owner.
- A group of processes in the same domain can share credentials: as credentials needed for authentication, this statement allows keeping the number of necessary credentials scalable.

This security policy allows designers to concentrate on security threats involving multiple domains and thus deliver an overall solution for security taking into account the representation of a user in a remote domain and the allocation of resources from a remote domain to a user or his representative.

Two types of representatives are defined:

- User proxy: process given permission to act on behalf of user for a certain limited time period.
- Resource proxy: process running within a specific domain translating global operations on a resource into local operations complying to the local security policy.

Thus the security architecture mainly consists of the entities "user", "user proxy", "resource proxy" and general processes as seen in Figure (4).

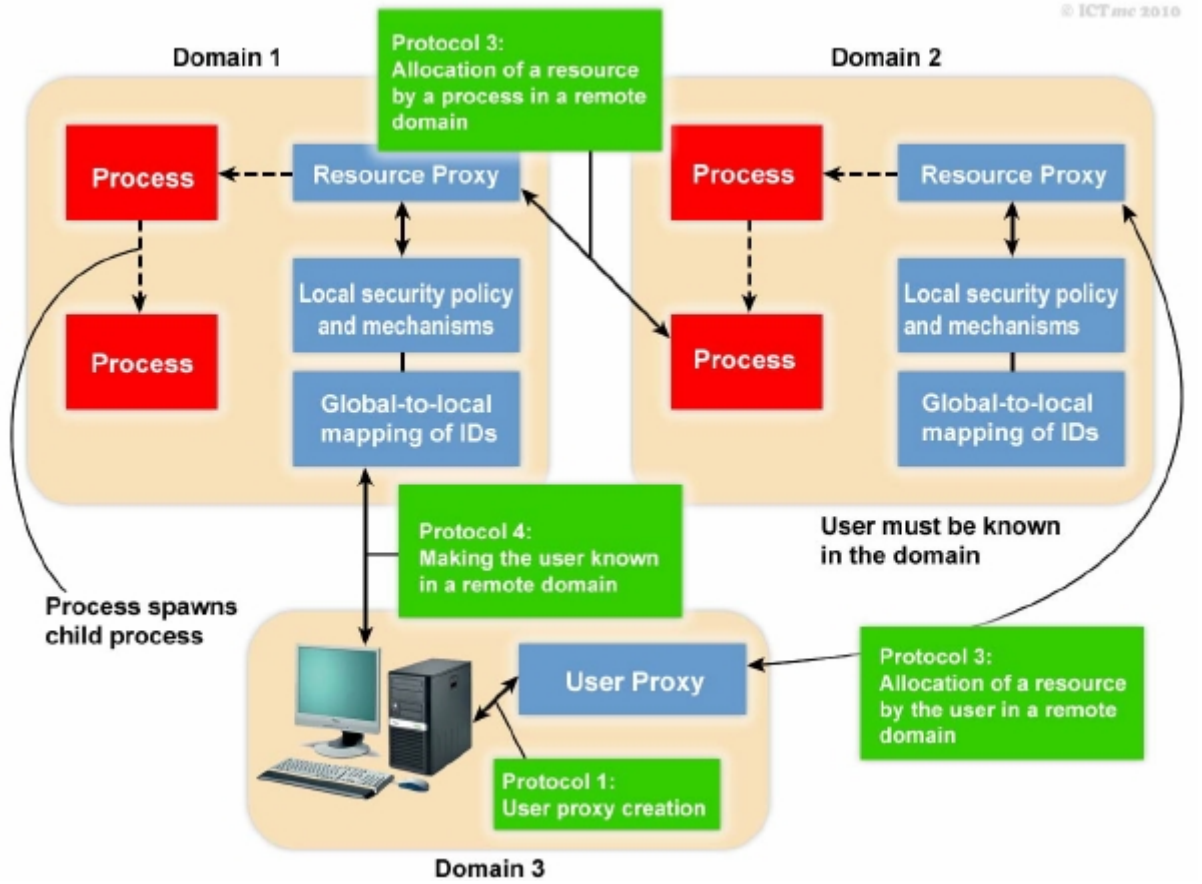

Figure (4): Security Architecture for the Distributed System

V. SYNCHRONIZATION OF PROCESSES FOR LARGE SCALE DISTRIBUTED SYSTEMS

Taking into consideration large scale distributed systems with heterogeneous components and heterogeneous operating systems we have to look at processes and communication between processes. How processes cooperate (e.g. by means of naming, which allows processes to at least share resources or entities in general) and how processes synchronize with one another. It is important that multiple processes do not access a shared resource simultaneously, such as a security node, Smart Cameras or local memory, but instead cooperate in granting each other temporary exclusive access. Multiple processes may sometimes need to agree on the ordering of events, such as whether message m_1 from process P was sent before or after message m_2 from process Q, as this might trigger different reactions.

Clock Synchronization:

In a centralized system, time is unambiguous. When a certain process requires the time, it makes a system call to the kernel to get the exact time. If process *A* asks for the time and a little later process *B* asks for the time, the value that *B* gets will be higher than the value *A* got (never lower). In distributed system, synchronizing and achieving agreement on time is not easy. In addition application areas of distributed systems, in all our day-to-day life, like communications, financial brokerage or collaborative sensing makes it clear that accurate timing is indispensible.

Physical Clocks:

Every modern computer or processor has a circuit for keeping track of time. This is achieved via precisely machined quartz crystal, which oscillates at a well-defined frequency when kept under tension. Associated with each crystal are two registers, a counter and a holding register- every oscillation of the crystal decrements the counter by one. When the counter gets to zero, an interrupt is generated and the counter is reloaded from the holding register. In this way, it is possible to program a timer to generate an interrupt 60 times a second, or at any other desired frequency. Each interrupt is called one clock tick.

When the system kernel (the central coordination processing unit) is booted, it usually asks the user to enter the date and time, which is then converted to the number of ticks after some known starting date and stored in memory. In a distributed system, every computer has a special battery backed up CMOS RAM so that the date and exact time need not be entered on subsequent boots. At every clock tick, the interrupt service procedure adds one to the time stored in memory. In this way, the (software) clock is kept up to date.

The situation changes when multiple CPUs are introduced, each with its own clock. Although the frequency at which a crystal oscillator runs is usually fairly stable, it is impossible to guarantee that the crystals in different computers all run at exactly the same frequency. In practice, when a system has *n* computers, all *n* crystals will run at slightly different rates, causing the software clocks a gradually to get out of synch and give different values when read out. This difference in time values is called clock skew. As a consequence of this clock skew, programs that expect the time associated with a file, object, process or message to be correct and independent of the machine on which it was generated, can fail.

Synchronization Algorithms:

If one machine has a WWV receiver (WWV: radio call sign for National Institute of Standards and Technology/Time & Frequency shortwave radio station), the goal becomes keeping all the other machines synchronized to it. If no machines have WWV receivers, each machine keeps track of its own time and the goal is to keep all the machines together as well as possible.

All the algorithms proposed in this area have the same underlying model of the system. Each machine is assumed to have a timer that causes an interrupt H times a second. When this timer goes off, the interrupt handler one to a software clock that keeps track of the number of ticks since some agreed upon time in the past. Let us call the value of this clock C. More specifically, when the UTC (Universal Coordinated Time) time is t, the value of the clock on machine p is $C_{p(t)}$. In a perfect world

$$C_{p(t)} = t \quad \text{for all } p \text{ and all } t \tag{1}$$

This is equal to the fact

$$C'_{p(t)} = \frac{dC_{p(t)}}{d_t} = 1. \tag{2}$$

$C'_{p(t)}$ is called the frequency of p'_s clock at time t. The skew of the clock is defined as $C_{p(t)} - 1$ and denotes the extent to which the frequency differs from that of a perfect clock. The offset relative to a specific time t is $C_{p(t)} - t$.

Real timers do not interrupt exactly H times a second. Theoretically, a timer with $H = 60$ should generate 216,000 ticks per hour. In practice, the relative error obtainable with modern timer chips is about 10-5, meaning that a particular machine can get a valuable in the range 215,998 to 216,002 ticks per hour. More precisely, if there exists some constant ρ such that

$$1 - \rho \le \frac{dC}{dt} \le 1 + \rho. \tag{3}$$

The timer can be said to be working within its specification. The constant is specified by the manufacturer and is known as the maximum drift rate. It specifies to what extent the clock's skew is allowed to fluctuate. The relation between clock time and UTC is shown in Figure (5).

A common approach in many protocols is to let clients contact a time server. There latter can accurately provide the current time, for example, because it is equipped with a WWV receiver or an accurate clock. The problem is that when contacting the server, message delays will have outdated the reported time. So, one has to find a good

estimation for these delays. Consider the situation shown in Figure (6).

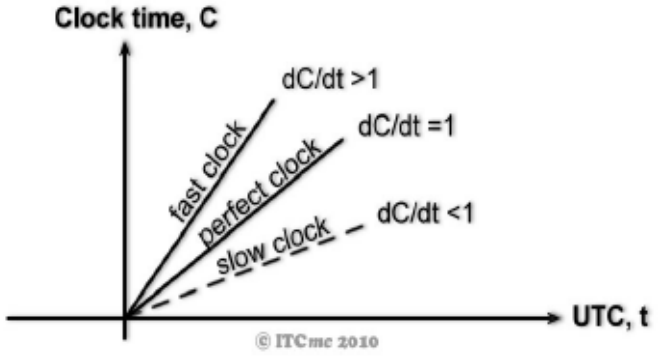

Figure (5): Relation between clock time and UTC
Network Time Protocol

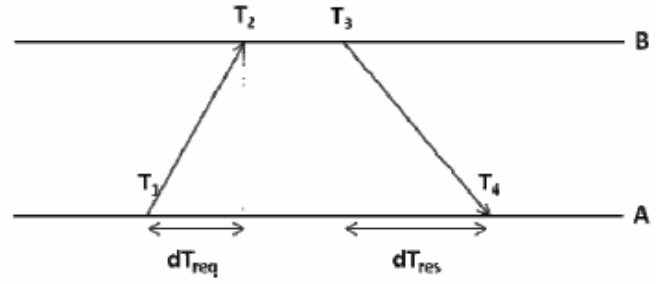

Figure (6): Getting the current time from a time server

In this case, *A* will send a request to *B*, time stamped with value T_1. *B*, in turn, will record the time of receipt T_2 (taken from its own local clock) and returns a response time stamped with value T_3 and piggybacking the previously recorded value T_2. Finally, *A* records the time of the response's arrival, T_4.

Assume that the propagation delays from *A* to *B* are about the same as from *B* to *A*, meaning that $T_2 - T_1 \approx T_4 - T_3$. In that case, A can estimate its offset relative to B as

$$offset[p.q](t) = \alpha t + \beta. \tag{4}$$

Of course, time is not allowed to run backward. If *A*'s clock is fast, $\theta < 0$, meaning that *A* should, in principle, set its clock backward. This is not allowed as it could cause serious problems as shown in the introductory example seen in Figure (7). Such a change must be introduced gradually. One way is as follows: Suppose that the timer is set to generate hundred interrupts per second. Normally, each interrupt would add 10 milliseconds to the time. When slowing down, the interrupt routine adds only 9 milliseconds each time until the correction has been made. A similar mechanism can be used in the clock is slow.

In the case of the network time protocol (NTP) this protocol is set up pair wise between servers. In other words, *B* will also probe *A* for its current time. The offset θ is computed as given above, along with the estimation δ for the delay:

$$\delta = \frac{(T_2 - T_1) + (T_4 - T_3)}{2} \tag{5}$$

Eight pairs of (θ,δ) values are buffered, finally taking the minimal value found for δ as the best estimation for the delay between the two servers, and subsequently the associated value as the most reliable estimation of offset.

Applying NTP symmetrically should, in principle, also let *B* adjust its clock to that of *A*. However, if *B*'s clock is known to be more accurate, this adjustment does not make sense. To solve this problem, NTP divides servers into stratum. A server with a reference clock such as a WWV receiver or an atomic clock is known to be a stratum-1 server (the clock itself is said to operate at stratum 0). When *A* contacts *B*, it will only adjust its time, if its own stratum level is higher than that of *B*.

In manly algorithms such as NTP, the timeserver is passive. Other machines periodically ask it for the time. All it does is respond to their queries. In Berkley UNIX, exactly the opposite approach is taken. Here the timeserver is active, polling every machine from time to time to ask what time it is there. Based on the answers, it computes an average time and tells all the other machines to advance their clocks to the new time or slow them down until some specified reduction has been achieved. This method is suitable for a system in which no machine has a WWV receiver.

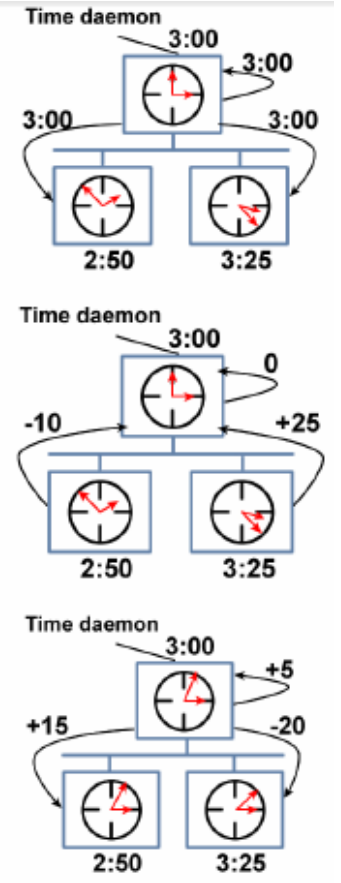

Figure (7): Berkeley Algorithm of clock synchronization in distributed computing

At 3:00, the time daemon tells the other machines its time and asks for theirs. They respond with how far ahead or behind the time daemon they are. Armed with these numbers, the time daemon computes the average and tells each machine how to adjust its clock. Note that for many purposes, it is sufficient that all machines agree on the same time. It is not important that this time also agrees with the real time as announced on the radio.

Clock Synchronization in wireless networks:

Most of large scale distributed systems, especially security oriented ones have many wireless hardware components, which in turn must be synchronized. An important advantage of more traditional distributed systems is that we can easily and efficiently deploy timeservers. Moreover, most machines can contact each other, allowing for are relatively simple dissemination of information. These assumptions are no longer valid in many wireless networks, notably sensor networks [7]. Nodes are resource constrained, and multi-hop routing is expensive. In addition, it is often important to optimize algorithms for energy consumption. These and other observations have led to the design of very different clock synchronization algorithms for wireless networks.

Reference broadcast synchronization:

Reference broadcast synchronization (RBS) is such a clock synchronization protocol. This protocol does not assume that there is a single node with an accurate account of the actual time available. It aims at internally synchronizing the clocks, similar to the Berkeley algorithm. The algorithm lets only the receivers synchronize, keeping the sender out of the loop.

The sender broadcasts a reference message that will allow its receivers to adjust their clocks. The key observation is that in a sensor network the time to propagate a signal to other nodes is roughly constant, provided no multi-hop routing is assumed. Propagation time in this case is measured from the moment a message leaves the network interface of the sender. As a consequence, two important sources for variation in message transfer no longer play a role in estimating delays:

- the time spent to construct a message
- the time spent to access the network as seen in Figure (8).

It must be noted that as wireless networks are based on a contention protocol, there is generally no saying how long it will take you for a message can actually be transmitted. These factors of non-determinism are eliminated in RBS. What remains is the delivery time at receiver side, but this time varies considerably less than the network access time.

The idea underlying RBS is simple: when are nodes broadcasts were a reference message *m*, each node *p* simply records the time $T_{p,m}$ that it received *m*. Note that $T_{p,m}$ is read from *p*'s local clock. Ignoring clock skew, two nodes *p* and *q* can exchange each other's delivery times in order to estimate their mutual, relative offset:

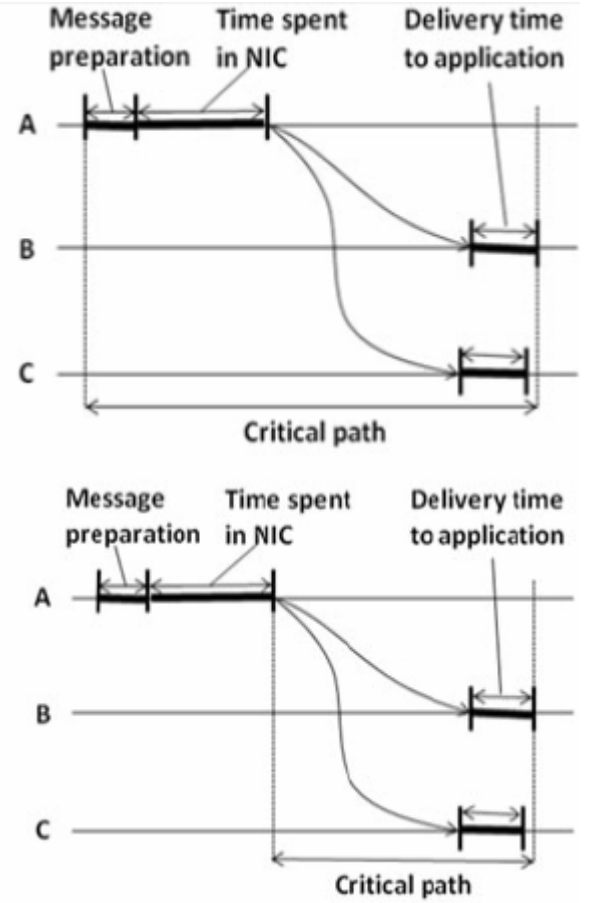

Figure (8): the usual critical path versus the critical path in the case of RBS

$$offset[p.q] = \frac{\sum_{k=1}^{M} \left(T_{p,k} - T_{q,k}\right)}{M} \quad (6)$$

where *M* is the total number of reference messages sent. This information is important: *p* will know the value of *q*'s clock relative to its own value. Moreover, if it simply stores these offsets, there is no need to adjust its own clock, which saves energy.

Unfortunately, clocks can drift apart. The effect is that simply computing the average offset as done above will not work. The last values sent are simply less accurate than the first ones. Moreover, as time goes by, the offset will presumably increase. One can compensate for this by applying standard linear regression to compute the offset:

$$offset[p.q](t) = \alpha t + \beta \quad (7)$$

The constants *a* and *b* are computed from the pairs ($T_{p,k}$, $T_{q,k}$).

Thus it is possible to keep the time synchronized in every single component of the distributed system. Now, solving the problem of synchronization, the next challenge of finding an election algorithm is to be dealt with.

VI. ELECTION PROCESS FOR LARGE SCALE DISTRIBUTED SYSTEM

When services are provided using a distributed system, they are most probably realized as a set of processes, which need a coordinator of some form.

In general it does not matter which process takes on this responsibility, but one of them has got to do it. The following section deals with an algorithm for electing a coordinator especially in the complex case of a wireless ad-hoc system.

If all processes are exactly the same, with no distinguishing characteristics, there is no way to select one of them to be special. Consequently we will assume that each process has a unique number, for example, its network address. In general, an election algorithms attempt to locate the process with the highest process number and designate it as coordinator. The algorithms differ in the way they do the location.

Furthermore we assume that every process knows the process number of every other process. What the processes do not know is which processes are currently up and which ones are currently down. The goal of an election algorithm is to ensure that when an election starts, it concludes with all processes agreeing on who the new coordinator is.

Traditional election algorithms are generally based on assumptions that are not realistic in wireless environments. For example, they assume that message passing is reliable and that the topology of the network does not change, which is not true for wireless networks, especially in the case of mobile ad-hoc networks.

Only few protocols have been developed that work in adhoc networks (e.g. the wireless mobile parts of video surveillance systems). The solution presented is able to handle failing nodes (cameras and their local wireless processing units) and network partitioning. An important property of this solution is that the best leader can be elected rather than just a random as before. The following discussion only deals with the ad-hoc property of the network and not the mobile part of the wireless network.

To elect a leader, any local wireless processing unit in the network (a wireless node), called the source, can initiate an election by sending an *ELECTION* message to its immediate neighbors. When a node receives an *ELECTION* for the first time, it designates the sender as its parent, and subsequently sends out an election message to all its immediate neighbors, except for the parents. When a local wireless processing unit receives an *ELECTION* form another node than its parent, it just acknowledges the receipt.

When node *R* has designated node *Q* as its parent, it forwards the *ELECTION* message to its immediate neighbors with the exception of *Q* and waits for acknowledgements. In this waiting phase all local wireless processing units that have already selected a parent will respond to *R* immediately. If all nodes already have a parent, *R* can quickly report back to *Q* also including information about e.g. battery lifetime and other resource capacities.

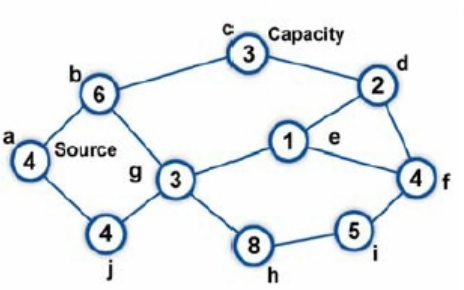

Figure (9.1)

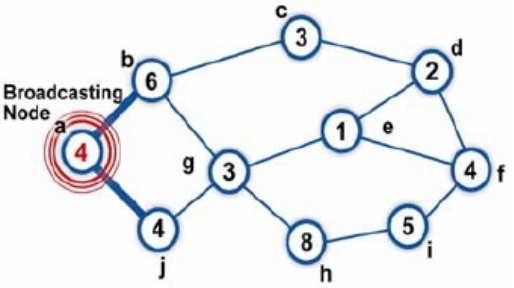

Figure (9.2)

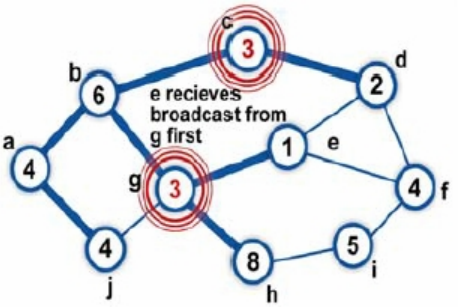

Figure (9.3)

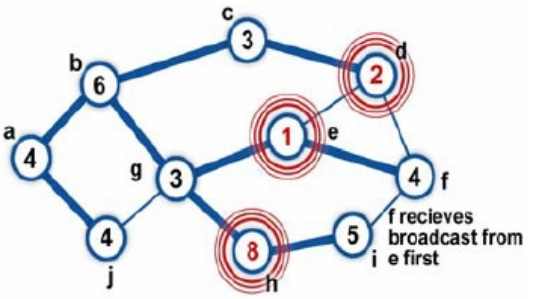

Figure (9.4)

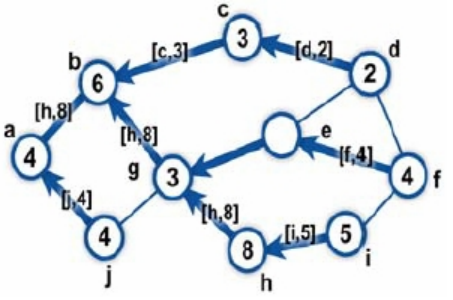

Figure (9.5)

This information will allow *Q* to compare *R*'s capacities to the ones of other downstream nodes and select the best eligible local wireless processing unit for leadership. *Q* sent the *ELECTION* message, because it was triggered by an *ELECTION* message from its parent. When *Q* acknowledges the *ELECTION* message it will also send the info of the most eligible node to *P* as well. In this way the source will eventually know, which local wireless processing unit best to select and broadcast this information to all other nodes.

This process is illustrated in the Figure (9). Local wireless processing unit have been labeled *a-j*, along with their capacity. Node *a* initiates an election by broadcasting an *ELECTION* message to nodes *b* and *j*. After that step, *ELECTION* messages are propagated to all nodes. From there on every node reports to its parent the node with the best capacity. In the end the source will recognize *h* as the best leader and will broadcast this information to all other nodes.

When multiple elections are initiated, each local wireless processing unit will decide to join only one election. To this end the source tags the *ELECTION* message with a unique identifier. Nodes will only participate in the election with the highest identifier, stopping any running participation in other elections.

VII. GENERAL STRUCTURAL OVERVIEW OF THE SECURITY MANAGEMENT PROCESS, THE ENTERPRISE POINT OF VIEW

The security management process was analyzed carefully in [3]. Subsequently an architecture for Security Management Process for CCTV / Video Surveillance Systems was presented. This concept was applied in the field in several cases. The goal of most of those cases was to protect and monitor the security activities of critical infrastructure. This was done in assignment of high level security authorities and governments. All field trials showed remarkable success. However, there arose a number of minor failures during the stress test phase. Those failures were corrected and further tested till a steady state was achieved.

This manifold success of the Security Management Process for Video Surveillance System encouraged us to generalize and extend this process architecture to involve all aspects of the security related activities of an enterprise.

Security Dilemma:

Though the enormous progress of security technology, it is still difficult for many security authorities as well as global industry player to realize the simple fact that "Security is not a product". For several systems, security splits into a number of standalone security islands, e.g. physical access control, surveillance system for the enterprise, network security, firewalls and security against natural disaster.

Moreover, it happens that the responsibilities of those security sectors are devoted to different departments. The result is what we see every day in the press about success of organized crime and collapse of the corresponding security system.

General Security Management Process for an Enterprise:

In order to avoid those disasters, and to minimize the probability of a security breakdown, a generalized Security Management Process Architecture is proposed, based on the success achieved in the case of Video Surveillance.

In this case, the security management authority is concentrated on the highest management level, and is responsible for the whole security management process in every aspect of the enterprise business as seen in Figure (10).

The main components of the Global Security Management Process are:

Physical security:

Physical security contains the administrative, technical and physical controls which range from design tasks of deciding the facility location and the construction process to the planning of counter measures against possible physical security risks and threats. This entails the planning process, deployment, monitoring and continuous improvement of physical countermeasures against infrastructure including the safeguarding of electric power as well as fire prevention, detection and suppression.

Network security:

Network security is responsible for securing the network against threats on all layers of the OSI model without hampering the normal communication. This pertains to securing the network elements as well as securing the network as a whole. In the planning stage of the security management process communication policies are defined for all areas of security. For network element security, these policies will be implemented by appropriate hardening measures like closing unused ports, deleting compilers, shutting down unneeded services or uninstalling games which might be part of the original operating system. For network security these policies will be implemented by using well known measures like firewalls, routers and higher level access controls to suppress or minimize communication from insecure networks to the secure infrastructure.

Access control:

Access control deals with the well-defined and controlled access to data, information, locations or other resources like tapes, printouts and the like. For any data in connection with identities of human beings policies and enforcement of identification and authentication of users of the system are defined in the course of Identity Management and Access Control. Discretionary, mandatory and nondiscretionary models are defined and their status controlled by well defined monitoring and auditing practices.

For software running on a computer access control means the definition of mathematical and information models, which make sure that processes will not try to manipulate data they should not or using resources (e.g. memory) they should not. In addition intrusion detection policies and countermeasures are also placed into this topic.

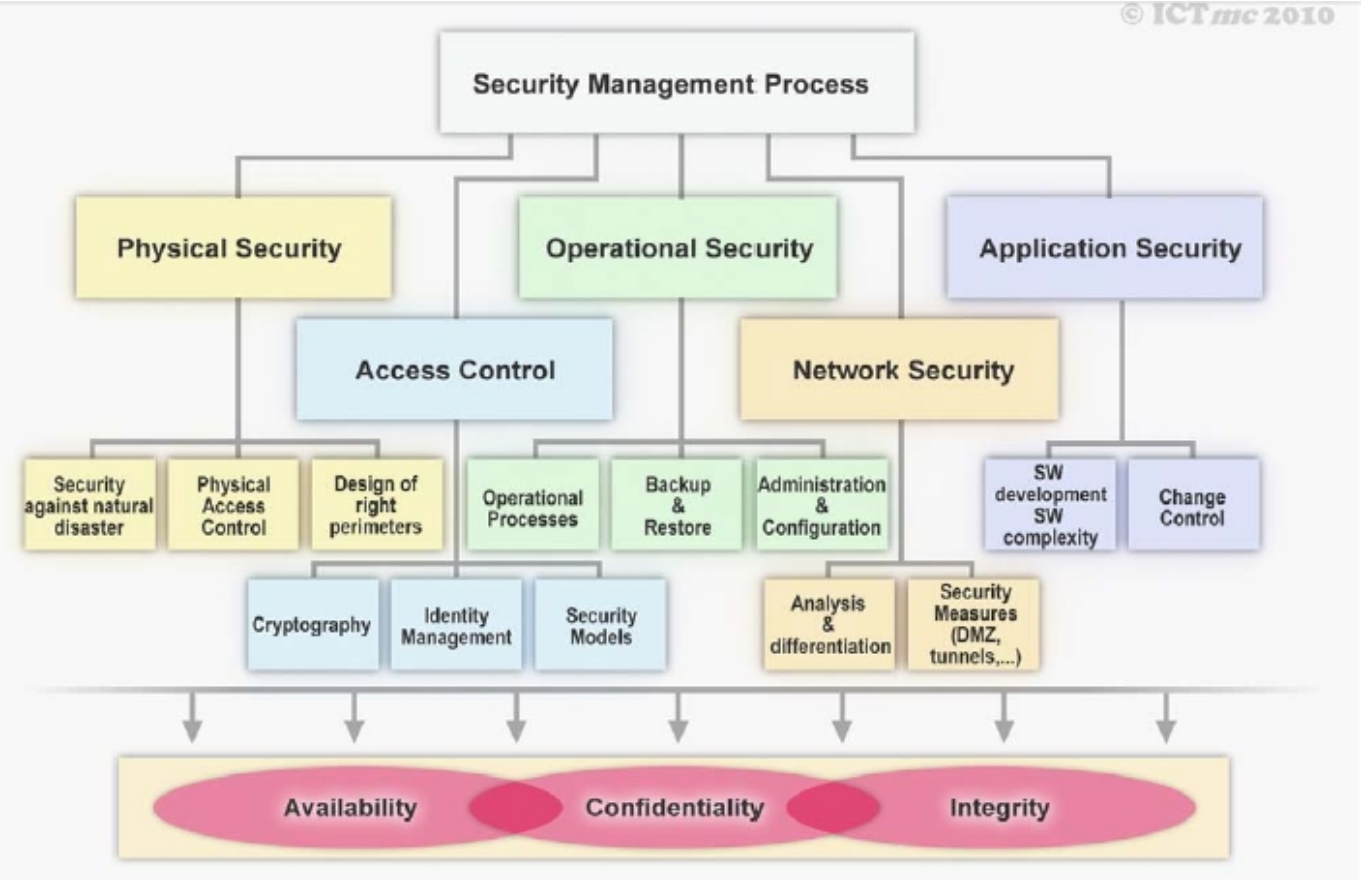

Figure (10): General Architecture of the Security Management Process for an Enterprise.

Security models contain the policies of which computer hardware architecture to use and the security configuration and protection mechanisms of the operating system.

The security model of the data contained within the system has to be defined in the planning phase of the security management process as well as the relevance of the integrity and confidentiality of the data. For example models like Biba take preference on the integrity whereas in the Bell-LaPadula model confidentiality is paramount. Moreover the process of certification and accreditation and the corresponding attack types fall within this topic.

Cryptographic security models govern the cryptographic components, technologies and encryption policies and their integration into the system. In the requirement phase the cryptographic policies are inquired which leads to the selection of the necessary technologies like symmetric and asymmetric key algorithms, hashing algorithms and certification infrastructure. Research of possible attack vectors on the infrastructure are also part of the cryptographic security model and must be present throughout the whole management process.

Business Continuity:

Business continuity is concerned with keeping the business processes of the organization in question up and running with as little interruption as possible. Prominent topics in this area are the planning of continuity using perhaps redundancy concepts of different types and of recovery requirements, which can range from backup strategies to hot stand-by sites all based upon a business impact analysis. Disaster management which includes analysis, selection and developing of recovery plans are also evaluated in business continuity.

Law, investigation and ethics presents the following: Ethics pertaining to the professionals working with information contained within the system which can include personal data of both worker and guests; the operator must impose policies on how the data can be accessed and used and introduce measures to detect unethical or unlawful data usage. Legal policies are defined on how to handle computer crimes and computer related laws as well as procedures to enable computer crime investigation and evidence collection in case of criminal activity.

The topic of application security contains plans on how to develop or choose various types of software and components. It defines security standards that all components of the system

must comply to, as well as procedures to manage the software implementation process, the corresponding life-cycle management and the versioning tools and their configuration. In addition best practices in regard of programming and quality assurance are defined in application security.

Operation security:

Operation security deals with administrative management and their responsibilities. This includes product evaluation and configuration management e.g. by defining trusted recovery states of the system or how to handle component failure both in redundant and non redundant systems and data management workflows.

VIII. INTEGRATED SECURITY MANAGEMENT PROCESS

During the last few years, the newspapers and press surprised the whole world several times with news about dreadful incidences; this chapter presents information about the most major security disasters.

Bank Robberies:

Value	Date	Disaster	Location
$65m	06.08.09	Graff Diamonds robbery 2	London/UK
$92.5m	21.02.06	Securitas depot cash robbery	Kent/UK
$41.5m	20.12.04	Northern Bank robbery	Belfast/ Ireland
$6.7m	16.03.06	Agricultural Bank of China robbery	Hebei/ China
$94.3m	07.08.05	Banco Central burglary	Fortalezo/ Brazil
$1.8m	30.12.07	Chelembra bank robbery	Kerala/ India

Art Crimes:

Value	Date	Disaster	Location
$123m	20.05.10	Pablo Picasso painting stolen	Paris/ France
$163m	11.02.08	Monet, Degas, Van Gogh, Cezanne stolen	Zurich/ Switzerland
$55m	20.12.07	Picasso, Portinari stolen	Sao Paulo/ Brazil
$47m	21.01.06	Saliera stolen	Vienna/ Austria
$612m	12.06.08	Picasso et al stolen	Sao Paulo/ Brazil
$133m	27.08.03	Da Vinci Painting stolen	Drumlanrig Castle/ Scotland

Cyber / Software Security:

As the market for selling exclusive information on software vulnerabilities grows, independent press revealed how the hackers gain is your loss when it comes to PC security.

It is even expected that in the short range, computer users will be more exposed to cyber-criminals than ever before. It's not just because online crime is so attractive for organized identity theft but ironically, because the computer security industry that is supposed to protect users was undermined from a private expert who shared everything about newly discovered weaknesses, which is currently a new challenge for the "protection racket".

Global Players of the security computing industry are now paying hackers for exclusive access to newly discovered vulnerabilities. This ensures their customers are protected while the software vendor works out a solution and rolls out a patch, a process which can take weeks.

This is not only wrong, because it protects only one company's customers; it also gives a lucrative market for hackers. They don't have to run the risk of going to jail any more by actually using vulnerabilities, they can just threaten you with it which is extortion.

Growing weaknesses: The number of flaws that can be exploited in software is growing fast: for example, last year the US National Vulnerability Database (nvd.nist.gov) alone, a clearing house noted 6,680 new vulnerabilities across a huge range of products and operating systems. A forecast by analysts Gartner suggested that the security industry would be worth $11 Bn. in 2010, up by 10 per cent from 2009.

The Confidential Report:

Just few months ago, in June 2010, a confidential report from the “European Security and Trust Experts Alliance ESTEAlliance, http://www.estealliance.com” went to one of the security authorities in Europe. Here is an amazing statement from the non-confidential part: Analyzing all those security disaster cases, we came to the following conclusion:

- In most of the cases, advanced high-tech equipment was used, e.g. intelligent video surveillance or advanced Smartcams [8]
- In most of the cases, state-of-the-art software components were used
- In most of the cases of art crimes, the object was in a high security sector, with several guards around the clock
- All standard security precautions were fulfilled

A simple analysis of those facts, just from the published press, reveals the facts that:

- There were high-tech components, state-of-the-art elements, resembling a modern security process
- However, there was a missing link between those different security islands

This means, an overlying Security Management Process is required. From the above discussion, for a high performance security system, those isolated “security islands” must be interconnected, in order to minimize the vulnerabilities of the system, see Figure (11).

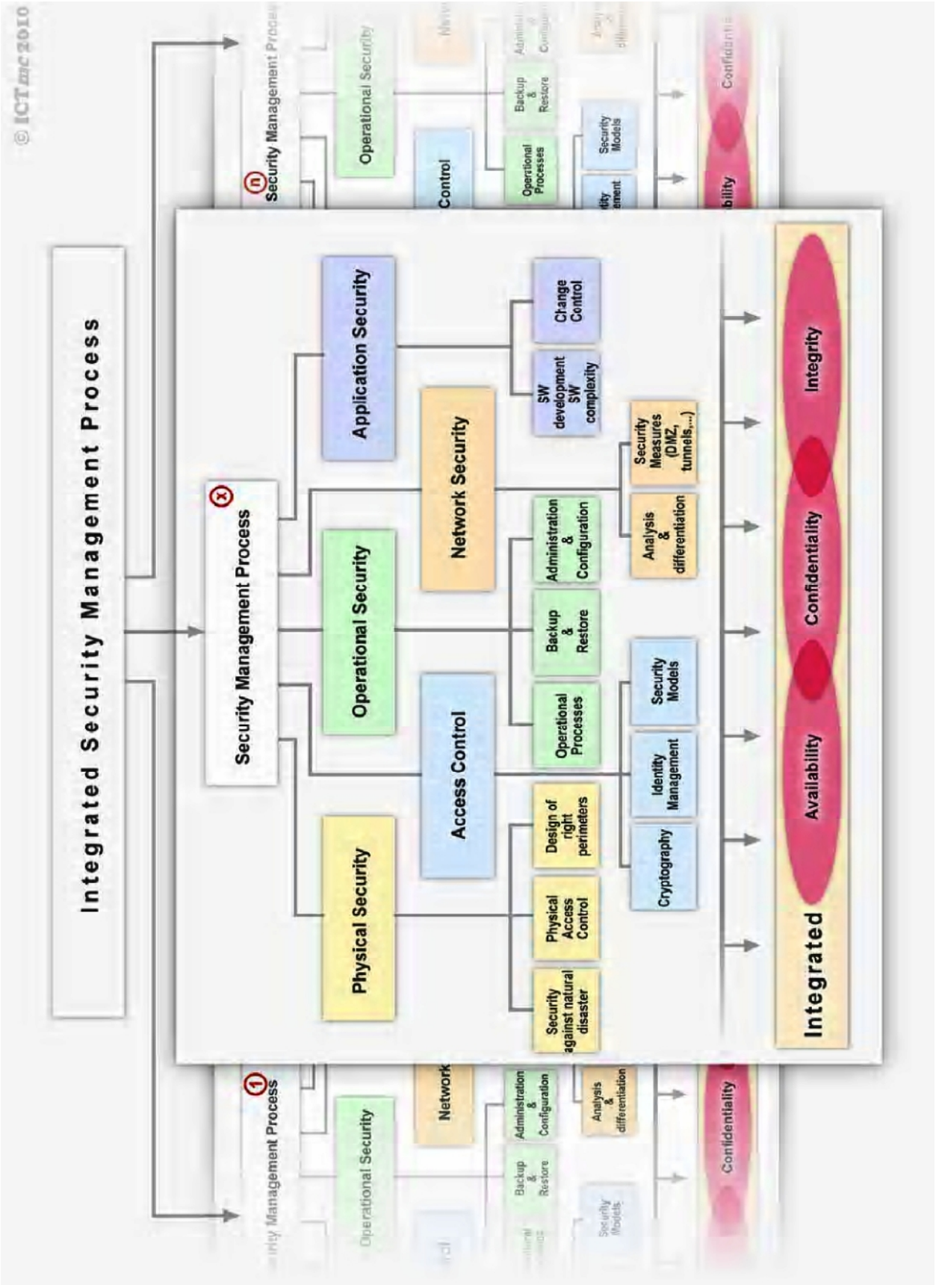

Figure (11): Integrated Security Management Process

An Integrated Security Management Process is to be assigned as an Overlay Process for all different Security Management Processes of the system, e.g. Video Surveillance, Alarming, Access Control, Cyber Security System, Security Sensors, … etc.

IIX. SMP AND SECURITY CONTROL FOR A LARGE SCALE ENTERPRISE AN ILLUSTRATIVE EXAMPLE

This chapter presents an illustrative example and overview of the security management process which must be in place to implement security control within a large scale enterprise, authority or distributed project.

An effective security management process comprises six sub-processes [9]

- Policy: to establish a framework for the development of organizational standards with respect to security
- Awareness: to educate those affected by security policy on their roles and responsibilities
- Access: to limit dissemination and modification of customer data and other sensitive information
- Monitoring: to detect policy violations and other security vulnerabilities
- Compliance: to track security issues and help ensure that resources facilitate the resolution of security issues
- Strategy: to meet the security challenges presented by new information technologies

Thus, security management relies on policy to dictate organizational standards with respect to security. Once a security incident has been recognized, a security management process requires methods to ensure that known security vulnerabilities are closed and open security issues are resolved. As representative examples, we discuss two of those six sub-processes.

The Policy Sub-Process:

A security policy is needed to establish a framework for the development of security procedures and practices. It also provides a vehicle with which to communicate roles and responsibilities with respect to securing information. A policy framework should specify the minimum security standards to be applied to all information systems, and more stringent standards for systems which contain highly sensitive or proprietary data.

A security policy should address the following:

- Scope of the policy, including the facilities, systems, and personnel to which it applies
- Objectives of the security management process and descriptions of sub-processes
- Accountability and responsibility for sub-processes at all levels of the organization
- Minimum requirements for the secure configuration of all systems within the scope
- Definition of violations and consequences of noncompliance
- A user statement of responsibility with respect to the information to which he or she is granted access

A security policy is a dynamic process. Its design should be flexible to allow frequent and updates as technology and/or management changes require.

Security policy development is not a project with a beginning and an end. A security policy coordinator should have responsibility for maintaining a policy team which is knowledgeable in both security techniques and the target information systems operating environment. The team leader must maintain open communications channels between the policy team, the management team who approves the policy and those to which the policy applies. An example security policy process is depicted in Figure (12).

The Compliance Sub-Process:

The extent to which there exists a formal compliance process is the extent to which security management efforts are effective in establishing a uniform level of security controls. Because compliance activities must be distributed among those who are responsible for the secure operation of information systems, departmental management must manage with reference to policies established by Information Security.

However, there will be instances of non-compliance for many reasons, including:

- The technical architecture of a system does not support a required security function
- Resources required to maintain compliance are unavailable
- A security incident reveals a security vulnerability which is not yet addressed by policy
- Routine security audits or security reviews reveal previously unnoticed risks

In any case, the instance of noncompliance must be:

- Reported to the Information Security
- Assigned to appropriate management
- Supported by a risk acceptance until resolved

The security compliance process must track all such security issues to ensure that steady progress is made toward their resolution. An example of a compliance process is displayed in Figure (13).

IX. SMART GRIDS, THE APPLIED STUDY CASE OF THE INTEGRATED SECURITY MANAGEMENT PROCESS CONCEPT

Smart Grids offered a representative example of a large scale, high performance distributed system, and it includes an

Figure (12): Example of a policy sub-process

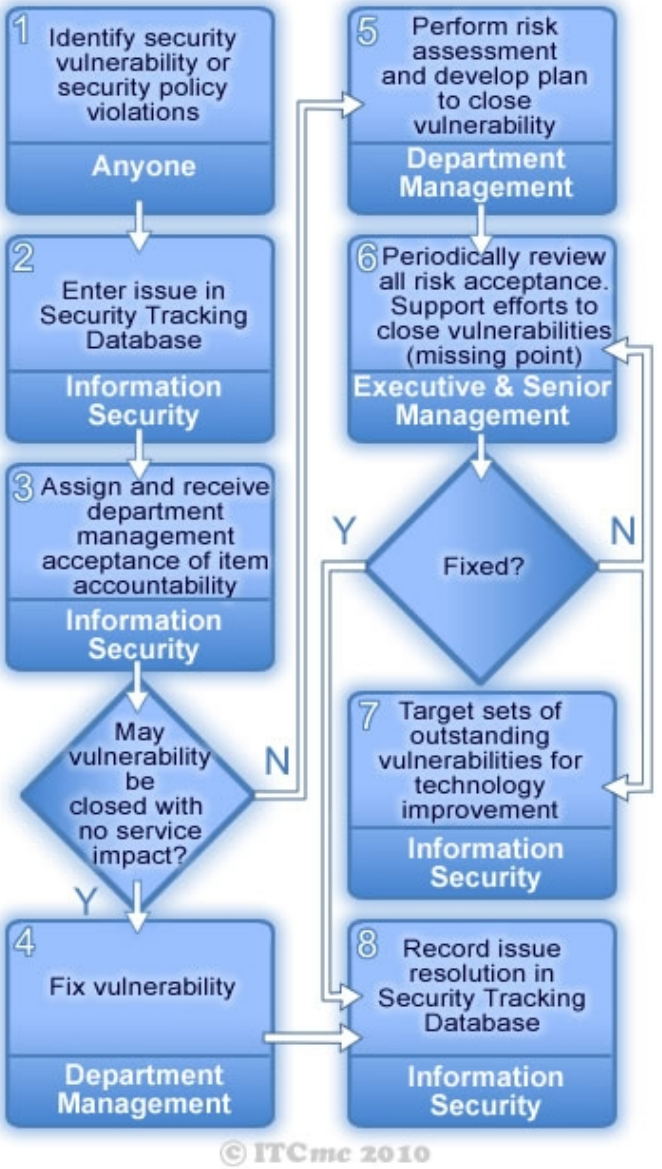

Figure (13): A further example of a policy sub-process

especially large number of critical infrastructures. In order to design a reliable security system for such a giant system, we have to analyze its structure, functionality and subsequently its vulnerabilities.

Smart Grid is traditionally defined as a combination of equipment, communications and processes that devices use to provide enhanced operations. Smart Grid includes smart meters, distribution system automation, demand response and other features that provide information for customers to lower meters, distribution system automation, demand response and other features that provide information for customers to lower their energy use. An important building stone of the Smart Grid is the Advanced Metering Infrastructure (AMI) or simply "smart meters" [10]. AMI has turned out to be synonymous with Smart Grid. Within the last two years (2008-2010), a number of huge multinational companies started research and development of a cooperative Smart Grid project. That project includes smart meters, but also switches, monitors, analysis software and other communication equipment running between the basic infrastructure and the customers. An important Smart Grid R&D focus is to add monitoring, analysis, control and communication capabilities to the national electrical delivery system to maximize its

capabilities while simultaneously helping consumers to reduce energy consumption.

Thus, considering the smart grid life cycle, it will provide electricity from suppliers to consumers using advanced technology, which will allow suppliers to remotely monitor consumer usage as well as implement variable rates that increase and decrease during peak energy use times. Additionally, consumers will be able to monitor their energy use in real time, which could allow them to save money by conserving energy during peak energy use times. The major goals of the smart grid initiative are to increase efficiency, reliability and safety of the electricity critical infrastructure. However, a crucial part of the Smart Grid [11], Security, did not gain big attention.

Smart Grids Architecture:

The smart grid architecture is predicted to cause convergence of three industries/sectors namely Electric Power (Energy), Telecommunication Infrastructure and Information Technology.

Each industry's expertise is needed to provide one of three high-level layers of a complete end-to-end Smart Grid and/or Intelligent Utility Network: The Physical Power Layer (transmission and distribution), the Data Transport and Control Layer (communications and control) and the Application Layer (applications and services)

Each of those three structural levels again compromise three fundamental sectors: Utilities, Infrastructure and End Users.

Integrated Security Management Process Concept for Smart Grids:

As discussed, Smart Grid consists of a collection of heterogeneous computers and resources spread across multiple administrative domains with the intent of providing users uniform access to these resources. There are many ways to access the resources of the Grid, each with unique security requirements and implications for both the resource user and the resource provider.

Accordingly, a three layered integrated security management processes is proposed to execute the following functions:

Functional Requirements:

An effective security strategy for smart grids needs to be end to end. This means that security capabilities need to be layered such that defense mechanisms have multiple points to detect and mitigate breaches. These capabilities also need to be integral to all segments of the grid infrastructure and address the full set of logical functional requirements, including:

- Physical security
- Identity and access control policies
- Hardened network devices and systems
- Threat defense
- Data protection for transmission and storage
- Real-time monitoring, management, and correlation

Therefore, we propose three Security Management Sub-Processes as seen in Figure (14).

Power–Security Management Process:

This sub-process is responsible for managing the Power Layer, this includes:

- Power Utilities, which represents electrical power generation, independent of the energy source or type, e.g. Nuclear, Coal, Gas, Wind or Concentrating Solar Power (CSP)
- Power Infrastructure including:
  - Transmission, e.g.: Flexible AC Transmission Systems (FACTS) and High Voltage DC.
  - Substations, e.g. automatic correction voltage plants and Dynamic Thermal Rating
  - Distribution, as Phase Measurement Units (PMU), Optical Sensors (OS) and Dynamic Sag Reducers (DSR)
- Power End User, including:
  - Building: Smart Meters, e.g.: Automation of Home/Building Systems, Next Generation Applications:.
  - Distribution Generation and Storage (DGS)

Communication–Security Management Process:

This sub-process is responsible for managing the Communication & Control Layer and includes:

- Communication & Control Utilities, This is the utility enterprise networks, like Local Area Networks (LAN)
- Communication & Control Infrastructure, including:
  - Wireless Access Networks (WAN), which resemble the backhaul network between utilities and Field Area Network (FAN).
  - The missing link in End to End Network, i.e. Advanced Metering [12] Infrastructure (AMI) and Field Area Network
- Communication & Control End User, including local network nodes, e.g. the Smart Home Access Networks SHAN.

Applications–Security Management Process:

This sub-process is responsible for managing the Application Layer. From the market point of view, this is the predominant layer includes advanced metering infrastructure, demand response, grid optimization, distributed generation, energy storage, PHEVs (including smart charging and V2G), advanced utility control systems and smart homes/networks.

Smart Grid Application Layer again splits down into three segments:

- Application Utilities, this includes
  - Outage Detection
  - Demand & Respond Applications, e.g. Load Measurement and Control, Grid Optimization Applications

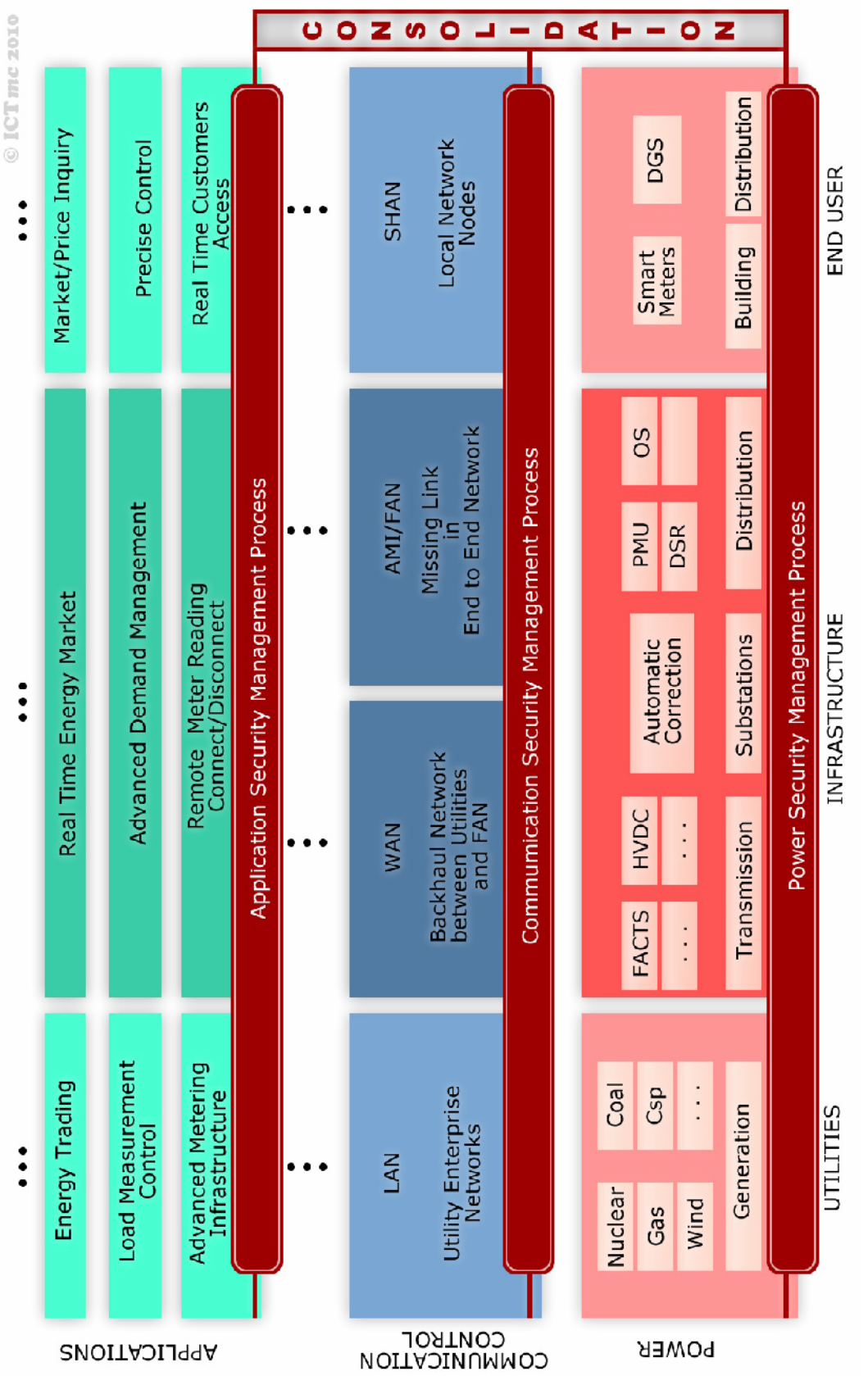

Figure (14): Integrated Security Management Process for Smart Grids

  - Smart Charging or utility control
  - Load monitoring and measurement applications
  - Future Oriented Apps and Services, e.g. Energy Trading Applications
- Application Infrastructure, including the following application segments
  - Remote Meter Reading, Connect/Disconnect, Tamper and Theft Detection, Customer pre pay.
  - Load Measurement & Control Apps. e.g. Advanced Demand Maintenance & Load Forecasting.
  - Application Data Flow for Plug-in Hybrid Electric Vehicles (PHEV).
  - Advanced Demand Management
  - Real Time Energy Market:
- Applications End User which includes Market and Price Inquiry applications, Precise Control and Real Time Customer Access in addition to Future Oriented Apps e.g. Bid / Ask Market Data necessary for buying and selling power.

Integration of the Sub- Security Management Processes:

Finally, the three Sub-security Management Processes are inter-connected. Every local action or process will be consolidated; a priority will be assigned and released to the system or the considered components as described in the first section.

X. CONCLUSION

This work presented an analytical study of Security Management Process for high performance, large scale distribute systems. During the last few years, the newspapers and press surprised the whole world several times with news about dreadful incidences. Analyzing those security disasters revealed the importance and necessity of an overlaying reliable security management system. The basic requirements for distributed systems, the CIA triad information security management is presented, introducing the core concepts as well as the related concepts for these systems.

As the system is supposed to be heterogeneous, we studied and analyzed the current and ongoing standardization activities related to security management. Subsequently a framework describing information security management, core component of the security management process: ISO/IEC 27001 is presented. A proposal for synchronization of processes for large-scale distributed systems is presented to extend the synchronization process to the heterogeneous distributed systems.

As next step, we introduced an advanced security management process for an enterprise. A concept for the integrated security management process as an overlay for sub- security management processes in a complex distributed system is presented. Subsequently, this concept of the overlay integrated security management process was applied for the case of Smart Grid. This concept of the overlay integrated security management process from the economic and performance point of view seems to be indispensible.

Future work:

A field application for the proposed Integrated Security Management Process in an airport is going to be implemented. These activities involve cyber- as well as physical security systems. This is an on-going work for one of the European main airports. A large scale security management process, taking into account privacy aspects, in assignment of a government in the Middle East is on the way. From the research point of view, the concept of Integrated Security Management Process will be studied for possible process optimizations.

ACKNOWLEDGMENT

Discussions with Prof. O. Martikainen, Department of Information Processing Science, Oulu University, Finland are highly acknowledged.

This work was supported by Austria Economic Service "Austrian Wirtschaftsservice" www.awsg.at, Austrian Research Promotion Agency "Österreichische Forschungsförderungs-gesellschaft" www.ffg.at and the Academic Business Incubator INiTS www.inits.at. This work will be partially included in a PhD thesis at the Pierre & Marie Curie University (UPMC).

REFERENCES

[1] S. Sutor, O. Martikainen and R. Reda, *ICT Security and Physical Security in High Performance Systems: Emerging Technologies, Future Trends and The Market Place* Proceedings of the 7th. International Conference on Informatics and Systems, INFOS2010, 28-30 March 2010, Cairo, Egypt

[2] R. Reda & H- Leopold, *Keynotes: "Telecommunications of the new Era, Future Technology Trends and Business Paradigm Transformation, the Industry Point of View"*, Proceedings of the 7th. International Conference on Informatics and Systems, INFOS2010, Cairo, Egypt 28-30 March 2010

[3] K. Kraus, F. Matusek, O. Martikainen and R. Reda, "*High Performance Security Management Processing in Advanced Intelligent Video Surveillance"*, Proceedings of the 7th. International Conference on Informatics and Systems, INFOS2010, Cairo, Egypt, 28-30 March 2010

[4] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management.*

[5] J. Clinch, Clinch Consulting, *"ITIL V3 and Information Security"* White Paper, Published by Clinch Consulting, 2009

[6] Andy Greenberg. *"Congress Alarmed At Cyber-Vulnerability Of Power Grid."* 22 May 2008

[7] Traynor,Raju, Choi, Cao, Zhu, La Porta, *Efficient Hybrid Security Mechanisms for Heterogenous Sensor*

Networks: Mobile Computing, IEEE Transactions on Volume 6, Issue 6, 2007

[8] A. N. Belbachir, *Smart Cameras*, ISBN 978-1-4419-0952-7, Springer Science+Business Media, 2010

[9] J. L. Bayuk, Enterprise Security for the Executive: *Setting the Tone from the Top*, Praeger Publishing, ISBN: 0313376603, Nov. 2009

[10] Linda Stuntz, *"Smart Grid, the Enabler of the New Energy Econom"*, Report of the Electricity Advisory Committee, USA, 2008

[11] T. Flich, J. Morehouse *"Securing the Smart Grid: Next Generation Power Grid Security"* Publisher: Syngress ISBN-10: 1597495700, 2010

[12] Mike Davis. *"Black Hat USA 2009 Briefings Speaker List."* Recoverable Advanced Metering Infrastructure <http://blackhat.com/html/bh-usa-09/bh-usa-09-speakers.html#Davis>, 25 Jun 2009