BOOK CHAPTER

# Cyber Physical Systems

Cyber physical systems are a new, sophisticated computing technology. They integrate sensing, computation, control and networking into physical objects, connecting them to the internet and to each other. They efficiently bundle the physical and cyber worlds, and may be monitored by computer-based algorithms. Cyber-physical systems are transforming the way people interact with and use engineered systems. The efficacy of traditional physical systems is increased by utilizing the power of Computing, all this is done in a cost-effective manner.

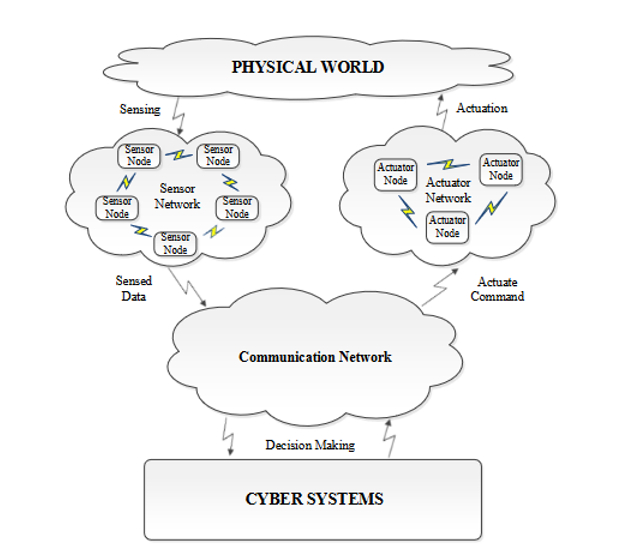
The term CPS was coined at the National Science Foundation (NSF) in the United States, 2006.

Cyber physical systems require three fundamental attributes; safety, security and sustainability - also known as the three Ss. It is important to understand the functionality and cost apart from design and analysis of these systems in depth and also have appropriate knowledge of the subsystems involved in their making.

Cyber physical systems are being researched in an attempt to integrate computational and engineering disciplines such as software, artificial intelligence, smart grids for power generation and distribution, etc. with electrical, mechanical, chemical, radiation, material science, networking and related disciplines. In fact, IoT or internet of things is a network of cyber physical systems and cyber physical systems with network connections is internet of things. Advancement in technologies, use of sensors and actuators, multicore processors and wireless networking, etc. will help in future automation and further integration of the cyber physical based models. Such advances re-shape our world and day to day life with more responsive, precise, reliable and efficient systems, enabling a revolution of "smart" devices and systems from smart cars to smart grids, collectively giving rise to smart cities. These will become a way of life just as how smart phones have taken over traditional dialling phones.

# Major Building Blocks of Cyber Physical Systems (CPS)

Cyber-Physical Systems (CPS) are a confluence of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. The technology builds on the discipline of embedded systems, computers and software embedded in devices whose principle mission is not computation. CPS integrates the dynamics of the physical processes with those of the software and networking and in the whole process add value to the efficiency of the process and quality of service delivery.

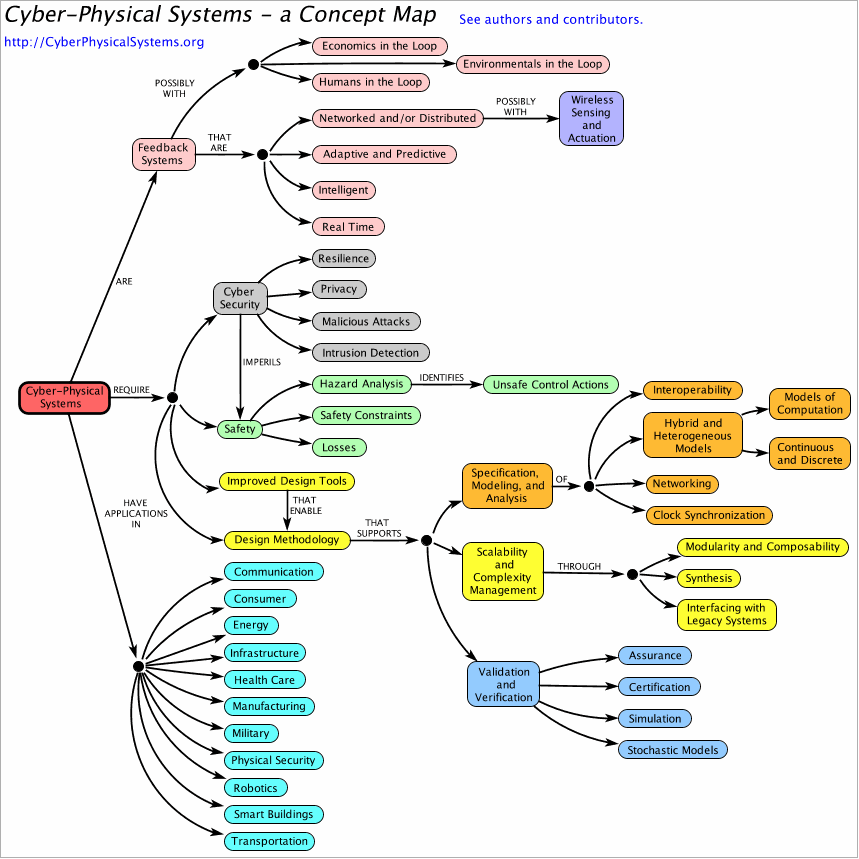


# Cyber Physical Systems – A concept map

Cyber Physical Systems -

***ARE***

* feedback systems that are networked / distributed with wireless sensors and actuators
  + CPS does not follow the routine practice of the controller continually or periodically observing the ``plant'' to provide actuation. In a typical CPS architecture, the signalling is mediated by software and networks that do not have continuous or periodic behaviour.
  + Low-power wireless sensors and actuators enable better measurement and control of physical processes but need to address the issues like
    - data models for distributed sensor data
    - spacing and positioning of sensors and actuators
    - time synchronization and global time-stamping of sensor and
    - data analysis.
* are intelligent and real-time
  + the opportunities and challenges associated with controlling or predicting the behaviour of such systems makes them intelligent which is achieved by the sensing, analysing and feedback process
  + include software that has timing constraints, including tasks that must be executed periodically, deadline constraints, or latency constraints
* are adaptive and predictive
  + Sensors make measurements of physical processes, the measurements are processed in the cyber subsystems, which then drive actuators that affect the physical processes. They are adaptive since they respond to changing conditions. The intelligence makes them predictive – anticipate changes in the physical processes.



***REQUIRE***

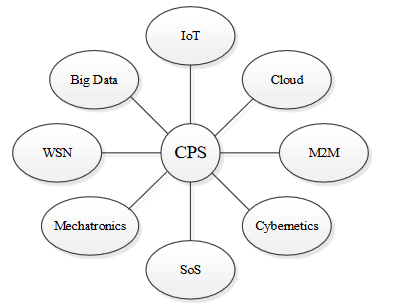
* Cyber Security which should take care of
  + *Resilience*: The ability of a system to continue operating satisfactorily when stressed by unexpected inputs, subsystem failures, or environmental conditions or inputs that are unexpected in normal working conditions / operating range. Necessary fault tolerance, fault detection, and adaptation are to be incorporated
  + *Privacy:* The technique of protecting confidential information from unauthorized access.
  + *Malicious attacks :* CPS have to be protected against possibility of accidental introduction of malicious code, back doors, DoS (Denial of service), DDoS (Distributed Denial of service) attacks, trojan horses and viruses
  + *Intrusion / Detection:* Systems have to protected against physical and cyber intrusions. Technologies that can be incorporated include:
    - embedded vision: motion detection and tracking, human detection, face recognition, iris detection etc..
    - timing models: enable detection of timing anomalies.
* Cyber Safety
  + Safety is the process of avoiding a hazard. An unsafe control action leads to a hazard. It is a situation arrived at by
    - not providing the control action
    - providing a safe control action too early, too late, or in the wrong order.
    - providing a control action lasts too long or is stopped too soon
  + Safety can be ensured by providing the right controls at the right time.

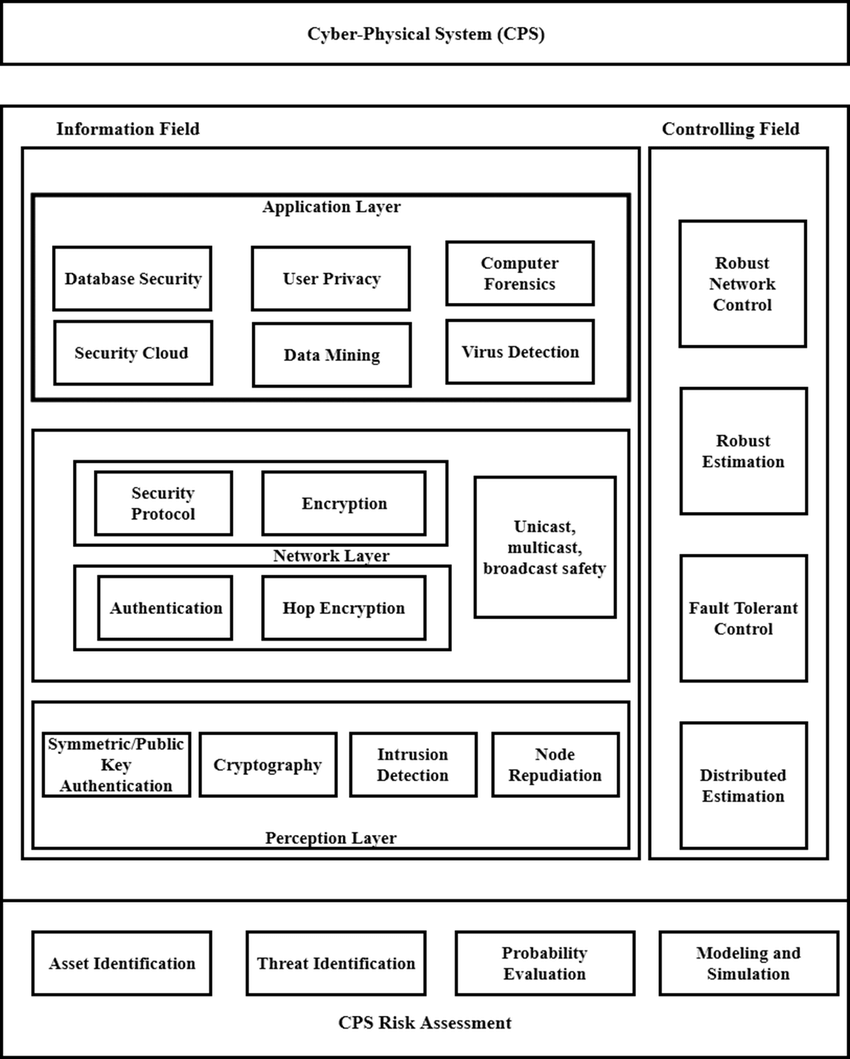
***HAVE APPLICATIONS IN***

* Communication
  + Cellular backhaul
  + Sensor networks
  + Wireless
* Consumer
  + Audio systems
  + Interactive games
  + Video systems
* Energy
  + Production
  + Distribution, and
  + Optimization
* Smart buildings
  + integrate wireless sensors into control systems for lighting,
  + HVAC (heating, ventilation, and air conditioning), and
  + Safety (fire monitoring and evacuation).
* Infrastructure(electric power, water, roadways, etc.)
  + Disaster recovery
  + Structural health monitoring
  + Water distribution optimization and
  + Water safety monitoring.
  + Critical infrastructure for distribution of water, oil, electricity etc.,
* Health Care
  + Information from sources like bedside monitors, lab results, and practitioner observations are combined to perform informed interventions.
  + Improve medical workflows and patient safety.
  + Smart medical treatments and services. Sensors in the home will detect changing health conditions and enable remote health monitoring.
  + Embedding sensors in chips which can be used to detect blood pressure, blood glucose levels, pulse rate, etc. with minimal human interference.
  + Developing and deploying new operating systems which can make personalized medical devices interoperable.
  + Adopting robotic surgery and bionic limbs which will help heal and restore movement to the injured and disabled.
* Manufacturing
  + Robotic machinery, embedded vision, or computer-controlled machinery
* Military
  + Almost all are cyber-physical systems.
  + Emergency response, such as handling large scale threats, protecting nature and important infrastructure.
* Physical Security
  + Electronic physical security systems like card access control systems, biometric readers like fingerprint scanner, iris scanner or face scanner
  + Networked video surveillance cameras to detect motion and recognize objects and people.
  + Point-of-Sale systems to help detect fraud at the cash register.
  + Airport video surveillance software to track abandoned luggages
* Robotics
  + Intellectual systems from motion control to artificial intelligence.
  + Robots for performing sensitive operations and necessary services.
* Smart Buildings
  + Automate and improve building systems management.
  + Daylight sensors to adjust room lighting.
  + HVAC (Heating ventilation and AC) systems utilize temperature, air quality and occupancy information to optimize heating, cooling and ventilation.
  + Elevator control systems to optimize elevator response, reduce congestion and improve convenience
  + Office hoteling — dynamically schedule or select their use of workspaces
* Transportation
  + Automotive systems eg. Autonomus cars on smart roads with drone assisted disaster zones
  + Elevators, escalators and moving sidewalks
  + Railroads and traffic management.
  + Intelligent transportation, automated traffic signals, improving real-time safety and coordination of traffic.
* Avionics and aerospace
  + Air transport, traffic management of aircrafts and their operation.
  + next gen flight test instrumentation
  + pilot crew communications
  + in-flight test & entertainment
  + wireless cabins
  + flight landing
  + space vehicles

Future cyber-physical systems will require hardware and software components that are certifiable and trustworthy, to the system level, highly dependable and reconfigurable in many applications.

# CPS Domains





# Need for CPS research

Cyber-physical systems research aims to integrate knowledge and engineering principles across the computational and engineering disciplines (networking, control, software, human interaction, learning theory, as well as electrical, mechanical, chemical, biomedical, material science, and other engineering disciplines) to develop new CPS science and supporting technology. CPS research is a growing field, it may be called ever changing because of the infinite possibilities of datasets and the task of finding their solutions. Even though the diversity of models and formalisms supports a component-based divide and conquer approach to the CPS’ development, it might pose an issue when it comes to accuracy and safety of the said designs on a large scale

Theory and tools are needed for developing cost-effective methods to:

1. design, analyze, and verify components at various levels of abstraction, including the system and software architecture levels, subject to constraints from other levels;
2. analyze and understand interactions between the control systems and other subsystems
3. ensure safety, stability, and performance while minimizing cost to the consumer

The major challenge in CPS research:

CPS research is still in its infancy. Research is partitioned into isolated subdisciplines such as sensors, communications and networking, control theory, mathematics, software engineering, and computer science. Either cyber or physical process may be well designed, analysed and represented in research not both. Although the diversity of models and formalisms supports a component based “divide and conquer” approach to CPS development, there exists a serious problem of verifying the overall correctness and safety of designs at the system level.

Research needs in CPS fall into three broad categories

1. Abstraction and Architectures

Innovative approaches to abstraction and architectures that enable seamless integration of control, communication, and computation must be developed for rapid design and deployment of CPS. It helps in easy deployment of cyber physical systems via interfaces or special developments in layers between networks or the internet. The existing engineering methods are not sufficient for rapid development of Cyber physical systems, hence solid abstractions are necessary for this purpose and hence innovations. The overall design allows heterogeneous systems to be composed in plug-and-play fashion. Standardized abstractions and architectures are required to fully support integration and interoperability and spur innovations in CPS.

1. Distributed Computations and Networked Control

The design and implementation of networked control systems pose several challenges related to time and event-driven computing, software, variable time delays, failures, reconfiguration, and distributed decision support systems. Design and application of the computational control systems or networks pose real time challenges- time delays, failures, dynamic reconfiguration, etc. They can be elaborated as accuracy of outcome, robustness or being stable, adaptability over ever changing and evolving circumstances, self-healing, proper functioning, correctness of information, privacy, availability in case of denial of service, incorporating operating components, keeping the heterogenous data secure, safety and quality of data over wireless networks, scalability in size or throughput, to name a few. Hence various tools, algorithms are needed to cater to the high security requirements and framework of CPS.

1. Verification and Validation

Hardware and software components, middleware, and operating systems need to be developed that go beyond existing technologies. The hardware and software must be highly dependable, reconfigurable, from components to fully integrated systems. Such complex systems must be trustworthy too. New models, algorithms, methods, and tools are needed that will incorporate verification and validation of software and systems at the control design stage.

Domains with CPS Research Potential

## **Biomedical systems**: CPS has tremendous potential in the medical or biomedical field. Including physical and neural prostheses, sensors for monitoring blood or body fluid flow, oxygen delivery machines, automated surgery and therapy, etc. to fulfil the needs of patients in complex environments or circumstances who require these devices. They must not only function without fault, but must be safe and reliable as fault in them might lead to mishaps.

Research goals could be

* Interoperable and open medical systems
* Distributed monitoring, distributed control, and real-time wireless networks for hospital ICU facilities
* Certification methods for medical device software and systems and networked patient monitoring and assistance
* Model-based frameworks that support patient-specific models.

## **Next Generation air transport Systems**

## Cyber-physical systems research is likely to have an impact on the design of future aircraft and air traffic management systems, as well as on aviation safety.

## Specific research areas include

## new functionality to achieve higher capacity, greater safety, and more efficiency, as well as the interplay and trade-offs among these performance goals

## integrated flight deck systems, moving from displays and concepts for pilots to future (semi)autonomous systems

## vehicle health monitoring and vehicle health management and

## safety research relative to aircraft control systems.

## One of the key technical challenges to realizing NextGen involves verification and validation of complex flight-critical systems with a focus on promoting reliable, secure, and safe use for NextGen operations also ensuring cost effectiveness.

## Some of the control engineering challenges include:

## Large-scale, real-time robust optimization algorithms

## Multiple-objective, multiple-stakeholder optimization frameworks

## Safety diagnosis/health monitoring methods

## System architectures that facilitate distributed decision making

## Data fusion from heterogeneous sensors and assessment of the value of the derived information.

## **Smart grid and renewable energy:** One of the most prominent recent research and development fields for CPS is Smart Grid and Renewable Energy. The main goal is to invest in modernization of energy infrastructure thereby improving energy efficiency.

Some factors to keep in mind regarding smart grids:

1. Cost of generating 1kwh is four times the cost of saving it.
2. Generation of electricity contributes to more than 40% of the greenhouse gas emissions,
3. Electricity demand is expected to increase by 75% or more in the next decade.

Smart meters will be put to use in households and business installations. The demand, distribution, generation would be monitored and analysed in substations or offices with the help of and information technology. The goal is to increase energy efficiency by distributed automation, significantly reducing peak load and optimization of demand.

The hardware or software involved must be dependable and go beyond traditional or existing technology. New tools, methods and algorithms are needed in multiple domains for verification and validation of systems/ software, etc. and certification of implementation, not the model (as it may be very costly) may prove that they are indeed trustworthy, unlike many of the available infrastructures today.

# Cyber security in general and for CPS

Cyber security or information technology security is the protocol to defend mobile phones, servers, clusters, networks, compute other handheld or electronic devices and data from malicious attacks or security breaches. Cyber threats are rampant and are ever increasing. Financial, medical, customer data and corporate espionage are some of the main areas of focus of cyber-attacks. Hence, there are various kinds of security practices:

* *Information security* maintains integrity of data and protects it. This may be when the data is being stored or transferred across devices.
* *Network security* protects computer networks from malware or other attackers.
* *Operational security* involves decisions regarding protection of data.
* *Application security* keeps data and devices free of threats. Data must be secured in the design stage itself, before the relevant program is deployed.

Disaster recovery is important in preventing loss of data in case of calamities, and in case of loss, restoring or backing up the data is very important. Some organizations prefer operating without all the previous resources but a sufficient amount of data. End users must be taught about the importance of security, such as deleting suspicious emails, not using unidentified USB drives, etc. Cyber crimes are becoming more common these days.

## **Types of cyber attacks**

1. *Malware:* Malicious software may be called malware. It is a very common cyber threat and may be spread through unwanted email attachments or file downloads. The various types of malware are:

* Viruses: make the device malfunction or reduces latency, replicates itself, thus infecting the system.
* Worms: are different from viruses, they are self-contained programs that are installed through emails, replicate themselves and overloads the server.
* Spyware: used by cybercriminals or hackers to spy on and record what some users do, to get confidential information such as credit card details or political information.
* Ransomware: locks data until a set amount of ransom is paid, to get it back.
* Botnets: infected computers are used by hackers to perform operations without the owner’s knowledge.
* Trojans: are malware disguised as legitimate software. They damage software and collect data and go undetected by many antivirus.
* Adware: malware spread through advertisements.

1. *Phishing* is in the form of fraudulent emails disguised as emails from legitimate sources, used to fool people into giving credit card or other information. They can also take place via social or online networks like Instagram, twitter, discord, etc. in the form of direct messages. Some kinds of phishing are whaling: aims at certain personnel within an organization and spear phishing: directed at some firms or individuals. There is also voice phishing and phishing via text messages.
2. *SQL injections* occur when malicious code is inserted into a server or search engine using SQL, server query language and extracts confidential information forcefully. Hence parametric queries must be used to avoid such injections.
3. *Man in the middle attacks* occur when an attacker gets in the middle of two parties exchanging important information and steals the data by exploiting the vulnerabilities in the system. In this process they also interrupt traffic. They are hard to detect; hence the parties must be careful and minimize or have zero faults in the transaction.
4. *DoS or Denial of service attacks* happen by flooding the server or networks with traffic, making them shut down responses or overloading them. TCP-SYN attacks, botnets, teardrop and smurf attacks are some types of DoS attacks.
5. *Password attacks* happen when hackers gain access to a user’s password and henceforth get confidential data and may also manipulate it as and when required. It includes “brute force attacks” where all possible combinations are tried to guess the password and user credentials are compromised. Two factor authentication or 2FA is used to counter this type of attack.
6. *Zero-day exploit* refers to exploiting vulnerabilities in a network when it has just been announced before it is patched up. Proactive security measures must be taken regarding zero-day attacks.
7. *Rootkits* are hidden and can gain remote control over a computer or host system, when installed inside it. It can steal passwords, credentials and other important data. It needs to be triggered through the persistence mechanism. They are also spread through suspicious websites.
8. *Cross-site scripting* has an attacker, website and victim involved. Attacker sends script-injected links to the victim in the form of scam emails, etc. then victim clicks on the link and requests legitimate websites, now the website loads the legitimate site along with execution of the malicious script, which sends the victim’s private data back to the attacker. It may be JavaScript, Flash, HTML, etc.
9. *IoT or internet of things attacks* interconnectivity of network makes it easy for attackers to breach an entry point and hack it or use it as a medium to exploit other connected devices within the network. They are becoming more popular because of the increasing number of IoT devices, especially those with low security. E.g. The Vegas casino attack, which was made by a breach through a fish tank. The O.S. used for these IoT devices along with their passwords must be changed and strengthened periodically.

Hence, we must protect ourselves against cyber crimes or criminals by:

* Using strong passwords.
* Using certified anti-virus software.
* Not using unknown Wi-Fis provided by public places “for free”.
* Update the operating system regularly.
* Not clicking on suspicious links sent via emails from unknown senders, as they may contain malicious software.

Every component and layer of the cyber physical system should be protected against all possible types of cyber attacks and also the system in its entirety has to be secure too in physical and logical space.

# Deep Learning and the ways in which it can be used to protect CPS

Recently, there have been attempts to leverage AI (artificial intelligence) techniques in a broad range of cyber security applications. Cyber security and Artificial intelligence have a wide range of interdisciplinary intersections. One such AI technology is termed as deep learning.

Deep learning is machine learning based on artificial neural networks with three or more layers, neural networks are an integral part of our brains. They make learning algorithms easier to use, enabling further progress in machine learning and AI.

Deep learning gets its name because it uses deeper networks compared to other AI methods like ML. The number of layers within an ANN defines the depth of the network. It is superior to ML because of its layered setting and effective algorithm for extracting useful information from training data.

There are various functions of deep learning, like creating smart models for implementing malware classification, intrusion detection and intelligent sensing of threats. Ai models often face many cyber threats, disturbing their sample, learning and decisions. Hence, they need specific cyber security defence and protection, and privacy in machine learning must be preserved.

Also, many CPS lack cybersecurity mechanisms like message authentication, making it difficult to detect false data injections or eavesdropping attacks. Research methodology for DL driven CPS security include CPS scenario analysis, cyber-attack identification, DL problem formulation, DL model construction, data acquisition and performance evaluation. Auto Encoder (AE) serves as a reliable regressor to predict energy load on the system.

Normal operations of CPS rely on dependability, real time operation, fault tolerance, cybersecurity, etc. Primary categories of CPS intrusion detection include physical process monitoring, closed control loops, attack sophistication and legacy technology. Denial of service and replay attacks are most prevalent.

Auto encoders are good at translating input data. They collect data through simulation. VAE (Variational Auto Encoder) transforms raw data into an encoded format for preventing interference attacks. It is a free forward model used for encoding an input in new data codes using a set of weighted parameters. Auto Encoders are a powerful and efficient model. ECU (Electronic control units) can control and monitor a vehicle’s status.

Deep neural networks or DNN have good potential; 0.978 accuracy, 0.016 for false positive rate, 0.028 for false negative rate. Cyber security of an electric power grid largely depends on state estimation, underpinning critical control processes for the grid. The DNN model with three hidden layers, 150 neurons on each layer without L1 regularization outperformed generalized linear models, gradient boosting machines, etc. and had 0.980 precision.

Divide and conquer strategy was used for secure water treatment by separating sets of sensors and actuators into functionality-wise groups. But due to its inefficiency DNN has limited use for real world applications. CNN, one of the most common kinds of ANN is used for computer vision tasks or Cyber security pattern recognition with convolutional neural networks achieved 0.912 for precision; it is a promising technique for detecting false message injection attacks to vehicular networks.

DeepFed or Federated Deep Learning is used to detect eavesdropping attacks, with a detection range of 98.86%. RNN based model detects cyber attacks in smart grids, like DoS (Denial of service) and data infiltration. Time decay indicates when the model must be restrained. Many deep learning frameworks, such as PyTorch and TensorFlow, allow you to create your own deep learning models and run deep learning experiments.

To summarize it, the following steps are done:

1. Inspecting CPS scenarios
2. Identifying cyber threats
3. Taken to ML/DL domain
4. DL model is created
5. Datasets are obtained and evaluated.

Applications of DL in cybersecurity

## Intrusion Detection and Prevention Systems (IDS/IPS) : These systems prevent intruders from accessing the systems, detect malicious network activities and also alert the user. They are recognized by known signatures and generic attack forms. This avoids threats like data breaches. Deep learning, convolutional neural networks CNN and RNNs; Recurrent Neural Networks can be applied to create smart ID/IP systems by reducing the number of false alerts and managing traffic. E.g. Web Application Firewall (WAF) and Next-Generation Firewall (NGFW).

## Spam and Social Engineering Detection : Natural Language Processing (NLP), a deep learning technique, can help in dealing with spam and the like and learns normal forms of communication and language patterns. It uses various statistical models to detect and block spam.

## Dealing with Malware: Deep learning algorithms are capable of detecting more advanced threats and do not rely on remembering known signatures or common attack patterns. They learn the system and recognize suspicious activities that may involve malware.

## Network Traffic Analysis : Deep learning ANNs are great in analysing HTTPS network traffic to look for malicious activity. This can easily deal with cyber threats such as SQL injections and DOS attacks.

## User Behavior Analytics : Tracking and analysing user activities and behaviours is an important security practice for any organization. For example, when insider threats occur and employees use their legitimate access in malicious intent, they are not infiltrating the system from the outside, hence rendering cyber defense tools useless against such attacks. User and Entity Behavior Analytics (UEBA) is a great tool against such attacks. It can detect suspicious activities by picking up normal employee behavioural patterns; like accessing the system during unusual hours, which indicates a possible insider attack and raises alerts.

### Footnotes

Cyber security mechanisms based on Artificial intelligence can protect cyber physical systems from attacks like zero-day attacks. Machine learning is used in this context to manage huge amount of heterogenous data from different sources of information with a goal of automatic attack pattern generation and hence predicting the future attackers’ attacks.

It also gives an overview of some state-of-the-art advanced AI Network security techniques, about what the foreseeable future of applications of artificial intelligence to network security is.

References:

<https://www.researchgate.net/profile/Mohamed-Mourad-Lafifi/post/What_is_the_difference_between_Cyber_Physical_Systems_and_Networked_Control_Systems/attachment/59d6407379197b807799caa6/AS%3A431158354812928%401479807570298/download/IoCT-Part3-02CyberphysicalSystems.pdf>

<https://www.researchgate.net/profile/Nasser-Jazdi/publication/269294836_Cyber_physical_systems_in_the_context_of_Industry_40/links/604d262392851c2b23c90841/Cyber-physical-systems-in-the-context-of-Industry-40.pdf>

<https://ptolemy.berkeley.edu/projects/cps/>

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4435108/>

<https://koreascience.kr/article/JAKO201403760397435.pdf>

<https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security>

<https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks>

A. Rajhans, S.W. Cheng, B. Schmerl, B.H. Krogh, C. Aghi, and A. Bhave, “An Architectural Approach to the Design and Analysis of Cyber-Physical Systems,” Third International Workshop on Multi-Paradigm Modeling, Denver, CO, October 2009.

<https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=e8eb154d3c&attid=0.1&permmsgid=msg-f:1738882612374970943&th=1821c085e0b6a23f&view=att&disp=safe&realattid=1821c059bba5989fd2b1&saddbat=ANGjdJ9VXEntlL3ccSRl4s7ksGIqCewWqcTlhg5VckTZt8D9EVbjHVdnf129tA81UfBxZU74900lKKhYrLoBwlD0JFVBvxiQRsXTO90Su8eb0F0vBCdpTMVZfKGBoja-16GyU9FeWreU4kjVYvo6nDx4EVsGLsrBYOHiBz_WBOoFvV5pB7zBnEWv7G7aw2nckroCADQAv2FRYNHuHHMHgubHvn7HRRdKXlt_W8HEnKInkA45OaFu7E9ImbsSr5b06boBVGBMfvc4oQ3i8uMO235BNkXSvKe5CPQNMBoQWESPMROKK7yxh6pOEaIg1FYmi11Fd9N9jRh2OqDiLYK0CbikuXvbItVroWkVwfu8Zfj1jt_LOU8tvuw24QZRgy8qdprPbbUaF3wjmgRIfWRewqhi4SBVtEKID_ptXxV2nC99DzzklHx1zqu2IwMfNNdedRfo3dIK57a1-ZP0frU8utEQqJmSgYGZOrCofsiF7VLqrrDL9xx7MxX6ywIeOKtk_7RkpciKMT4jgniQ8pHeKGl4a5AShaG8_Yj3h31Wv2hlesvkqy5A_GgJjtPRsx2tCU9TxgrzVu9xNH9TlQolS9otZ8OgXc1TjFVyr_ntpm6YsQ_wunPvu8xpzE2iFe_MK5W0qg19d5BjQ1elyvFbQqy3Qrc3R9z_35rq2rKs3ILpvM3P2giKXrY0TTogo2HgXELuj8Mab9g2yLaKqzouMsa_57nVG-2cIHiCOhwOToFP5j-omGFRm3ZIWOSrC1I>

<https://munin.uit.no/bitstream/handle/10037/14790/article.pdf?sequence=4&isAllowed=y>

<https://www.datto.com/blog/5-amazing-applications-of-deep-learning-in-cybersecurity>