UiT The Arctic University of Norway

Department of Computer Science and Computational Engineering

Cyber-security of Cyber-Physical Systems (CPS)

Faraz Safarpour Kanafi

Master's Thesis in Applied Computer Science...DTE3900...May 2021

Acknowledgments

I would like to thank Bernt Arild Bremdal and Halldor Arnarson for their consultancies and guidance through the project and Mohammad Rahnamafard for sharing his insight and introducing me to Cisco SAFE and study materials. My gratitude would also extend to all who have assisted me during the project.

Contents

List of Figures

List of Tables

Executive Summary

This master's thesis reports on security of a Cyber-Physical System (CPS) in the department of industrial engineering at UiT campus Narvik. The CPS targets connecting distinctive robots in the laboratory in the department of industrial engineering. The ultimate objective of the department is to propose such a system for the industry.

The thesis focuses on the network architecture of the CPS and the availability principle of security. This report states three research questions that are aimed to be answered. The questions are: what a secure CPS architecture for the purpose of the existing system is, how far the current state of system is from the defined secure architecture, and how to reach the proposed architecture. Among the three question, the first questions has absorbed the most attention of this project. The reason is that a secure and robust architecture would provide a touchstone that makes answering the second and third questions easier.

In order to answer the questions, Cisco SAFE for IoT threat defense for manufacturing [1] approach is chosen. The architectural approach of Cisco SAFE for IoT, with similarities to the Cisco SAFE for secure campus networks [2], provides a secure network architecture based on business flows/use cases and defining related security capabilities. This approach supplies examples of scenarios, business flows, and security capabilities that encouraged selecting it. It should be noted that Cisco suggests its proprietary technologies for security capabilities. According to the need of the project owners and the fact that allocating funds are not favorable for them, all the suggested security capabilities are intended to be open-source, replacing the costly Cisco-proprietary suggestions. Utilizing the approach and the computer networking fundamentals resulted in the proposed secure network architecture. The proposed architecture is used as a touchstone to evaluate the existing state of the CPS in the department of industrial engineering. Following that, the required security measures are presented to approach the system to the proposed architecture.

Attempting to apply the method of Cisco SAFE, the identities using the system and their specific activities are presented as the business flow. Based on the defined business flow, the required security capabilities are selected. Finally, utilizing the provided examples of Cisco SAFE documentations, a complete network architecture is generated. The architecture consists of five zones that include the main components, security capabilities, and networking devices (such as switches and access points). Investigating the current state of the CPS and evaluating it by the proposed architecture and the computer networking fundamentals, helped identifying six important shortcomings. Developing on the noted shortcomings, and identification of open-source alternatives for the Cisco-proprietary technologies, nine security measures are proposed. The goal is to perform all the security measures. Thus, the implementations and solutions for each security measure is noted at the end of the presented results.

The security measures that require purchasing a device were not considered in this project. The reasons for this decision are the time-consuming process of selecting an option among different alternatives, and the prior need for grasping the features of the network with the proposed security capabilities; features such as amount and type of traffic inside the network, and possible incidents detected using an Intrusion Detection Prevention System.

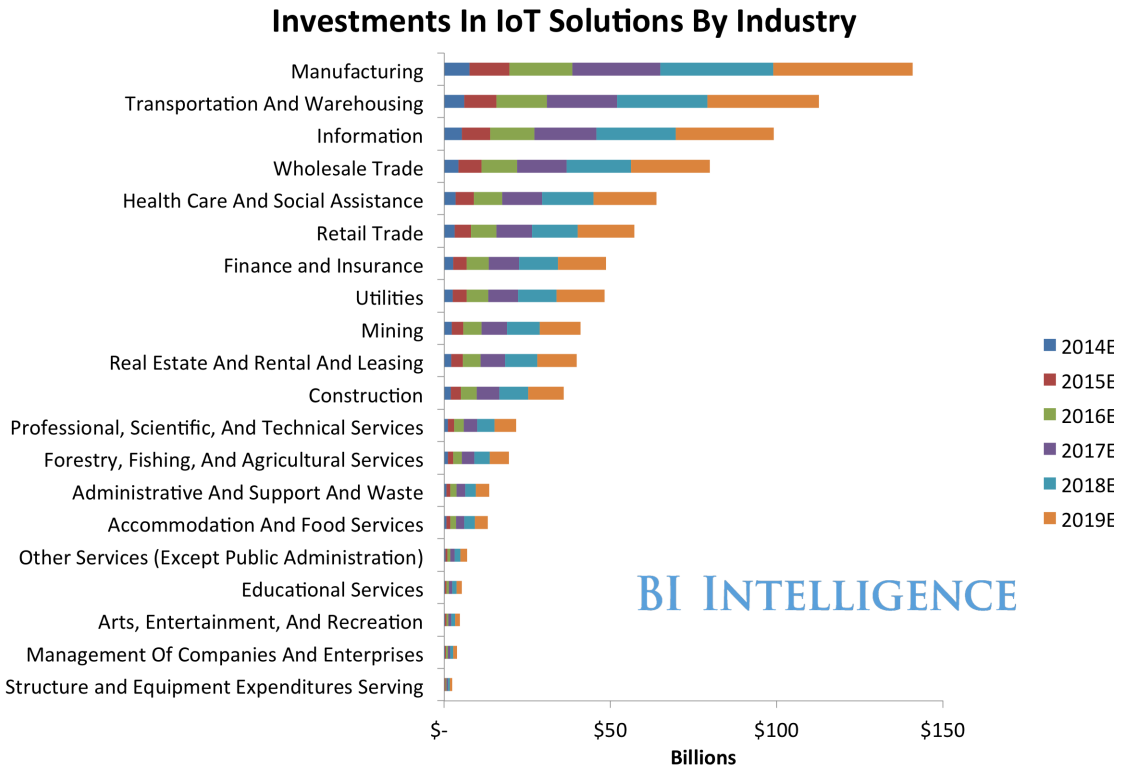
The attempts to construct a secure cyber-physical system is an everlasting procedure. New threats, best practices, guidelines, and standards are introduced on a daily basis. Moreover, business needs could vary from time to time. Therefore, the selected security life-cycle is required and encouraged to be used in order to supply a robust lasting cyber-physical system.

1 Introduction

Industry is the part of an economy that produces material goods which are highly mechanized and automatized. As yet, there have been four technological leaps that led to paradigm shifts (industrial revolutions): in the field of mechanization, of the intensive use of electrical energy, of the widespread digitalization, and the present combination of Internet technologies and future-oriented technologies in the field of smart objects (machines and products). The fourth paradigm shift was established as Industry 4.0, the term being a reminiscence of software versioning [3].

Industry 4.0 is the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things and cloud computing, creating what has been also called as a smart factory. All the technologies which Industry 4.0 includes, indicates the fact of high connectivity between the components and to the Internet.

As it could be seen in figure 1.1[1], manufacturing was the most invested industry in Internet of Things (IoT) solutions in 2016. The predictions even indicate a growth in the near future. For instance, Meticulous Research[2] has reported about an increase in the expected investment and forecasts 263.4 billion dollars market size by 2027[4].



Source: BI Intelligence Estimates

Figure 1.1: Investments in IoT solutions by industry

[1] https://www.businessinsider.com/the-enterprise-internet-of-things-market-2015-7?r=US&IR=T
[2] https://www.meticulousresearch.com/

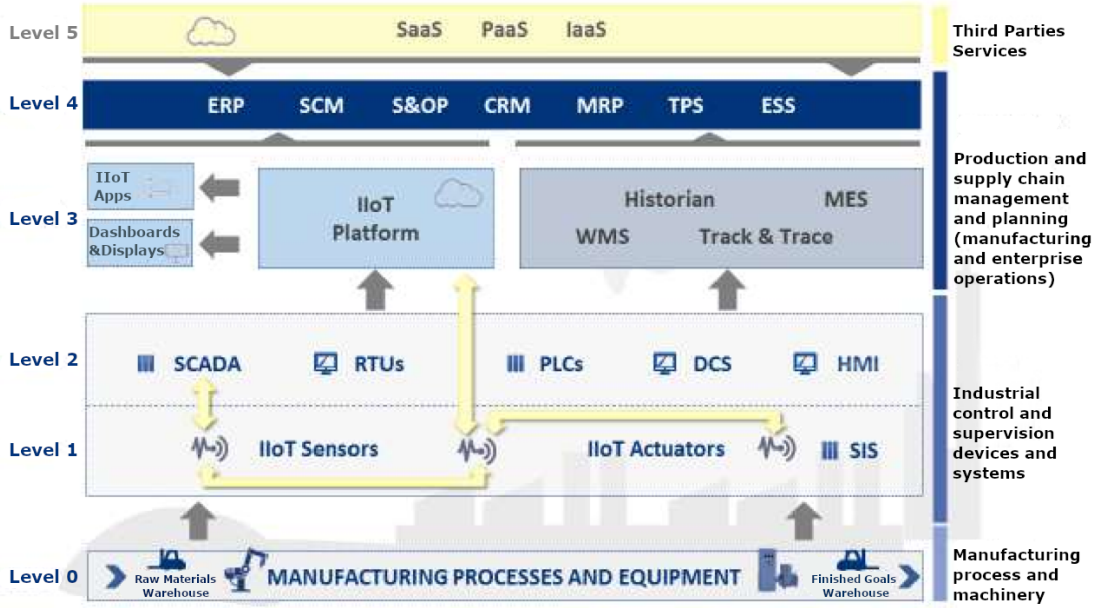


Figure 1.2: High-level reference model adapted from [7]

Industry 4.0[3] takes a great interest from manufacturing companies. It facilitates dealing with huge data volumes, developing human-machine interactive systems and improving communication between the digital and physical environments [5]. To provide a better explanation of this concept, a high-level reference model based on the Purdue Model [6] tailored to the scope of this project has been proposed in figure 1.2 [7]. The first layer indicates the manufacturing process (level 0). Level 1 and 2 represent OT layers, including Supervisory control and data acquisition (SCADA), Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), Distributed Control System (DCS), and Human Machine Interface (HMI). Layer 3 is an intermediate layer with system classified in-between IT and OT, while layer 4 corresponds to the IT part of a corporation. The highest layer (layer 5), not appeared in the original Purdue model, is specific for smart manufacturing, where external services are commonly used (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)). It should be noted that new communication paths introduced by Industry 4.0 and enabled by the incorporation of IIoT devices into the network, are added with yellow arrows to emphasize their criticality in terms of security and privacy.

Industry 4.0 includes three essential stages. Firstly, gathering digital records through sensors that attached to industrial assets, which collect data by closely imitating human feelings and thoughts, also knows as sensor fusion. Secondly, analyzing and visualizing step which includes an implementation of analytical abilities on the captured data (From signal processing to optimization, visualization, cognitive and high-performance computation, etc). Many different operations are performed with background operations. Thirdly, the stage of translating insight to actions involves converting the aggregated data into meaningful outputs, such as additive manufacturing, autonomous robots and digital design and simulation [5].

According to European Union Agency for Cybersecurity (ENISA) Industry 4.0/Smart manufacturing assets are classified into key groups depicted in figure 1.3 [7]. ENISA, also, suggests a short

description of each components [7]. The figure expands on different types of components involved in Industry 4.0/smart manufacturing.

Cybersecurity is one of the main technological pillars to fully implement Industry 4.0, shown in figure 1.4 [8]. Moreover, the large investment, connectivity of components, and use of the Internet, as mentioned earlier, would be some of the other reasons to consider the cybersecurity as a core concern.

1.1 Research questions

This master's thesis aims for the security of Cyber-Physical Systems (CPS) in general, and establishing a more secure system for the existing CPS in the department of industrial Engineering at Arctic University of Norway (UiT) campus Narvik. The scope of security and security in cyber-physical systems is vast. It covers from the most tangible facts, such as physical security of components of a network, to the security of processes inside the Central Process Unit (CPU). The focus of this project is on the network and architecture. An architecture provides the required logical orientation of security capabilities[3] that must be considered when selecting products to ensure that the documented business flow, threats, and requirements are met. An architecture could provide many designs based on performance, redundancy, scale, and other factors [2, p.22]. In this section the main questions that this thesis emphasizes on is presented.

Research Question 1: What is a secure Cyber-Physical System for the purpose of the existing system in the department of industrial engineering at UiT campus Narvik?
If there is no clear definition for a secure cyber-physical system for the purpose of the project owner, no security measures could be accomplished. Therefore, in the first place, a secure cyber-physical system which addresses the stakeholder's need (the department of industrial engineering at UiT campus Narvik) is to be sketched. This sketch would assist measuring the security level of the current system and the required steps for enhancing it. This question draws the majority of the attention of the thesis.
In order to answer the question, Cisco SAFE [11], i.e. SAFE for IoT Threat Defense for Manufacturing [1] and SAFE for campus networks [2], are enabled. Other standards and guidelines, such as NIST 800-82 [12] and SANS[13] were also utilized. The fundamental concepts of routing and switching [14, 15, 16] (in line with the background of the author) were also considered to depict a secure network architecture. Moreover, studying the security of OPC Unified architecture as the most critical element of the network (expanded in section 2.10) assisted the process.

Research Question 2: How secure is the current Cyber-Physical System?
A detailed analysis of the current level of security brings attention to both threats and possible solutions. This question indicates the standing position of the system and how far it is from being relatively secure.
Sketching a secure CPS architecture for the case would ease grasping the security level of the existing CPS. A robust and trustworthy architecture would provide a goal and measurement scale for the security of a cyber-physical system. Thus, the shortcomings of the existing CPS is presented by comparing the proposed secure system and the current system as the next step of the thesis.

Research Question 3: How to approach the defined secure Cyber-Physical System?

[3] A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). [9, 10]

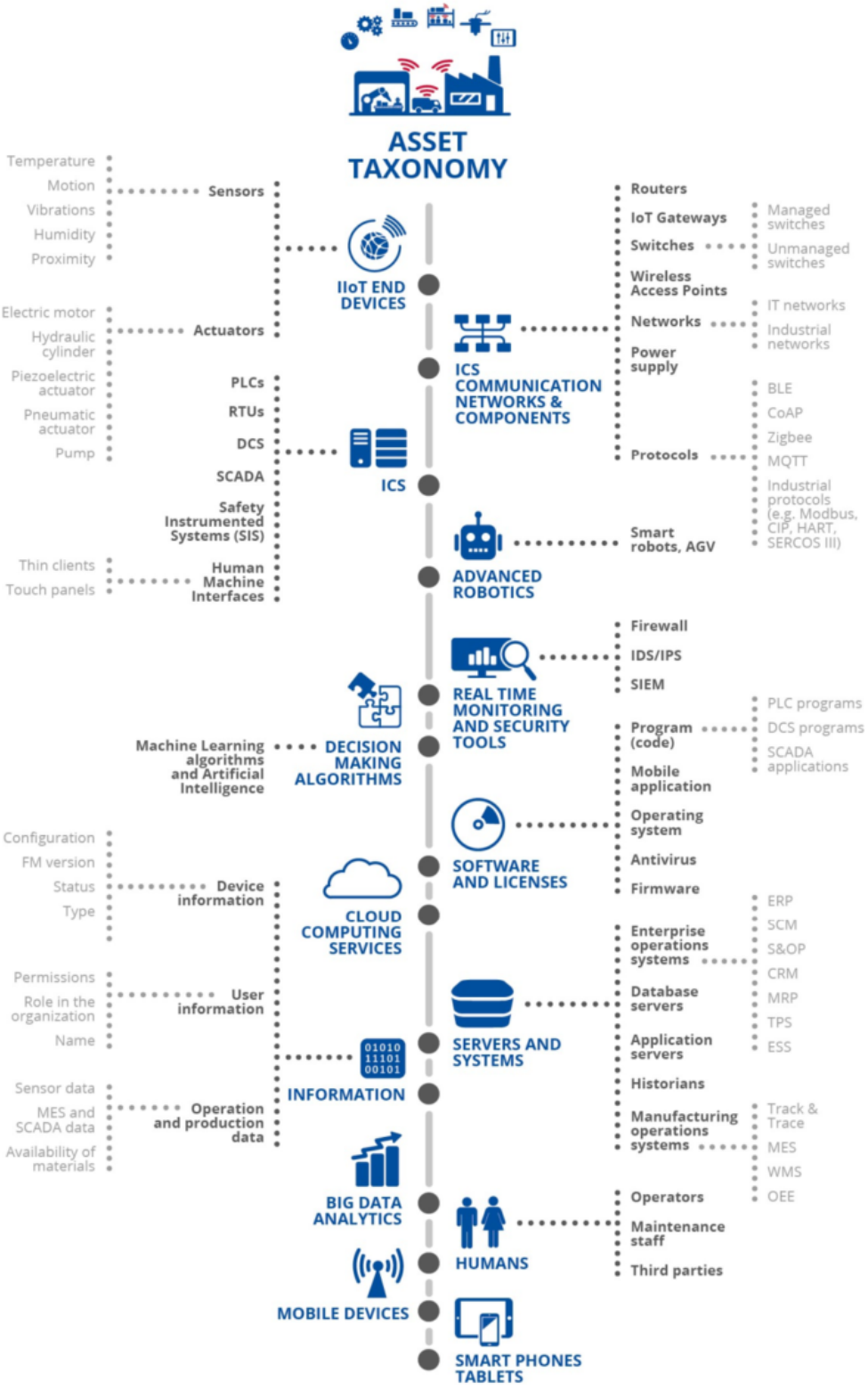


Figure 1.3: Industry 4.0 asset taxonomy [7]

Figure 1.4: Technological pillars of Industry 4.0, adapted from [8]

Lastly, some security measures have been undertaken in order to proceed toward a more secure cyber-physical system. These actions intend to bring the system to the proposed architecture and a more secure state.
There are a number of alternatives for the proposed security capabilities (provided as an answer to the first research question). Since Cisco SAFE suggests Cisco-proprietary security capabilities, in this project, the commonly used open-source alternatives are suggested and implemented, provided by security experts and benchmarks.

The details about the approaches toward answering the questions are found in section 3.

1.2 Outcomes

A secure network architecture for the purpose of the stakeholder (department of industrial engineering) is presented as the first expected outcome. Afterwards, based on the defined secured architecture and network computing fundamentals, six important shortcomings of the current system are noted. Subsequently, nine measures for enhancing the security level of the system is provided.

1.3 Road map

In this section, the steps and challenges which were encountered throughout the project are stated. This statement would assist in clarifying the road map undertaken during the thesis. Table 1 presents an overview of the challenges.

In the first place, the main question is the definition of security. Is it only a concept, a component like Firewall, or a product? The well-known security materials, such as Convery's book [17], help to perceive the concept.

Step No.	Challenge description
1	Definition of security
2	Relation of guidelines, standards, risk assessments, and best practices to security system
3	Finding the related guidelines, standards, risk assessments, and best practices
4	Generating a security system based on the selected materials (standards, ...)
5	Selecting alternatives for Cisco-proprietary security capabilities

Table 1: Challenges encountered throughout the project

When searching for security and security of CPS through articles, a number of articles introduce attacks and distinct categorization. Numerous best practices and guidelines will be also encountered when reading through different standards, such as NIST and ISO. Being lost in an amount of security threats with different categorization for them, some solutions, and a number of best practices could be the consequence of this extent and variety.

Another challenge is grasping whether applying the best practices and the guidelines make a system safe and secured or not. What if there is a new best practice announced? Should everything be started over? Therefore, a system or a life-cycle containing all concepts and leading to a routine is craved. This is where Cisco Security Life-cycle, figure 3.6, assists with connecting all best practices, guidelines, standards and risk assessments together and understand their roles for a security system.

Once a life-cycle for security is selected, the challenging point would be finding the proper policies, guidelines, standards, best practices and risk assessments related to Cyber-Physical Systems.

The next case would be generating a security system based on the selected materials. Here is where Cisco SAFE approach for IoT aids. Cisco SAFE proposes an architecture-based approach, in which four fonts (Segmentation, Visibility and Analysis, Remote Access, and Secure Services) are considered to overcome any threats and further secure the system. The proposed solution of Cisco (Cisco SAFE for IoT Threat Defense for Manufacturing) gathers different standards and existing models, including ones for classic computer networks that Cisco has been focused on for long, and yields a business-flow-centered mechanism. Cisco recommends different security capabilities, such as network management and firewall, regarding the mentioned four fonts. The recommended architecture and security capabilities have valued the thesis as a starting point for understanding the application of different standards and guidelines, plus a foundation that the suggested security system of this project is built upon and intended to be improved over the time.

After designing the network architecture and identifying the required security capabilities, implementing the designed network ensues. The key challenge during the implementation phase is identifying open-source alternatives for the security capabilities proposed in Cisco SAFE. The proposed security capabilities are mostly Cisco proprietary and costly.

1.4 Structure of the thesis

A short introduction about Industry 4.0 and the importance of cybersecurity, the questions, expected outcomes, and challenges of this thesis were discussed as yet. In this section a brief description of the following sections and their contribution within the thesis are offered.

Section 2 covers the state-of-the-art, the necessary concepts (or references to materials) for grasping the article, and a description of the existing CPS in the department of industrial engineering. Section 3 expresses the chosen methods for generating the results. Afterwards, the provided answers to the stated research questions are presented in three different subsection respectively (since there are three different research questions), section 4. In section 5 the opinions related to the results, and further works are discussed. Eventually, conclusion of the thesis are supplied in section 6.

2 Background and Literature Review

This section provides the state-of-the-art in this field of study, and a summarized background of the required knowledge for clarifying the provided methods and results. After presenting the state-of-the-art, a summarized description of cyber-physical systems and OPC unified architecture is expressed in section 2.2 and 2.3. Thereupon, definition of security (section 2.4), the utilized security capabilities, and services (section 2.5-2.9) are mentioned. Next, the security threats related to cyber-physical systems and dynamic host configuration protocol are introduced. Eventually, the existing CPS at UiT campus Narvik is introduced.

2.1 State-of-the-art

A number of articles in this field of study focus on different cyber attacks, their effects on the systems and classify them. Ding [18] presents an overview of recent advances on security control and attack detection of industrial CPSs. Amin [19] focuses on the risks that arise from interdependent reliability failures (faults) and security failures (attacks). Alguliyev [20] includes the main types of attacks against cyber-physical systems and a analyzes them. His categorization was also adapted in this paper.

Several articles cover the physical aspect of Cyber-Physical Systems. Cheh's article [21] proposes to protect critical infrastructure systems by assessing the safety of the system and using models that integrate they cyber, physical, and human domains for detecting malicious physical threats on the system. Niu [22] considers an optimal controller by using Q-learning for the physical system with uncertain dynamics, since the cyber system under attack will affect the physical system. He models the linear discrete-time system with dynamics that is unknown and altered by the cyber state vector, including packet losses and time delays as two important metrics for the network that may cause deterioration or potential instability of the system [23]. Then the optimal control gain is introduced and the system stability only when the cyber state vector satisfies a certain criterion is shown. If the state vector of the cyber system fails to satisfy the criterion, the appropriate defense is launched. Niu adapts the Q-function update law and development of the system dynamics from Xu et al [24]. The performance of the strategy is evaluated for the cases that there is a degradation of performance for physical systems.

Furthermore, there are some articles focusing on introducing new approaches for evaluating security of different systems. For instance, Shreshta focuses on an approach of security classification; in which, generally systems (IoT systems), based on their impact and exposure are divided into classes [25, 26, 27]. Garitano provides a methodology together with a Multi-metrics [4] approach

[4]Multi-Metrics is a simple process which evaluates the repercussion of each metrics component or sub-system, based on its importance within the system [28, p.1371]

to evaluate the system security, privacy and dependability (SPD) level during both the design and running processes [28]. National Institute of Standard and Technology (NIST) [29] has also suggested a framework. The framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs, without replacing additional regulatory requirement on business.

2.2 Cyber-Physical Systems

The Cyber-Physical Systems (CPS) term was proposed by Helen Gill at the National Science Foundation (NSF) CPS workshop conducted by the US NSF in 2006. From computer science point of view, CPS are the integration of computing and physical process [30]. They include embedded computers, network monitors and controllers, usually with feedback, where physical processes affect computations and vice versa [20]. According to Alguliyev [20], some of the most important and distinctive characteristics of a CPS are:

- Input and possible feedback from the physical environment
- Distributed management and control
- Uncertainty regarding reading, status and trust
- Real-time performance requirements
- Wide-distribution geographically, with components in locations that lack physical security
- Multi-scale and systems of systems control characteristics (systems-of-systems).

In general, the CPS process could be divided into four stages. The stages are as follows:

1. Monitoring
2. Networking
3. Computational processing
4. Actuation

The current state of the CPS includes variables that present data obtained by sensors and control variables representing control signals. The normal value of a certain parameter, called a set point, is considered and the distance between the values of the process variables and corresponding control point is calculated by the controllers. After calculating this offset, the controllers, using a complex set of equations, develop a local actuation, and compute new actuation and control variables. The received control value is sent to the corresponding actuator to keep the process closer to a specific point; PID controllers could be named as an example.

It should be noted that the controllers also send the received measurements to the main control servers and execute the selected commands from them. In CPS, system operators should be aware of the current status of the controlled objects. Thus, the graphical interface (GUI), called the human-machine interface (HMI), provides the current state of controlled object to the human operator [20]. Figure 2.1 presents the role of human in CPSs and how human decisions effects the system.

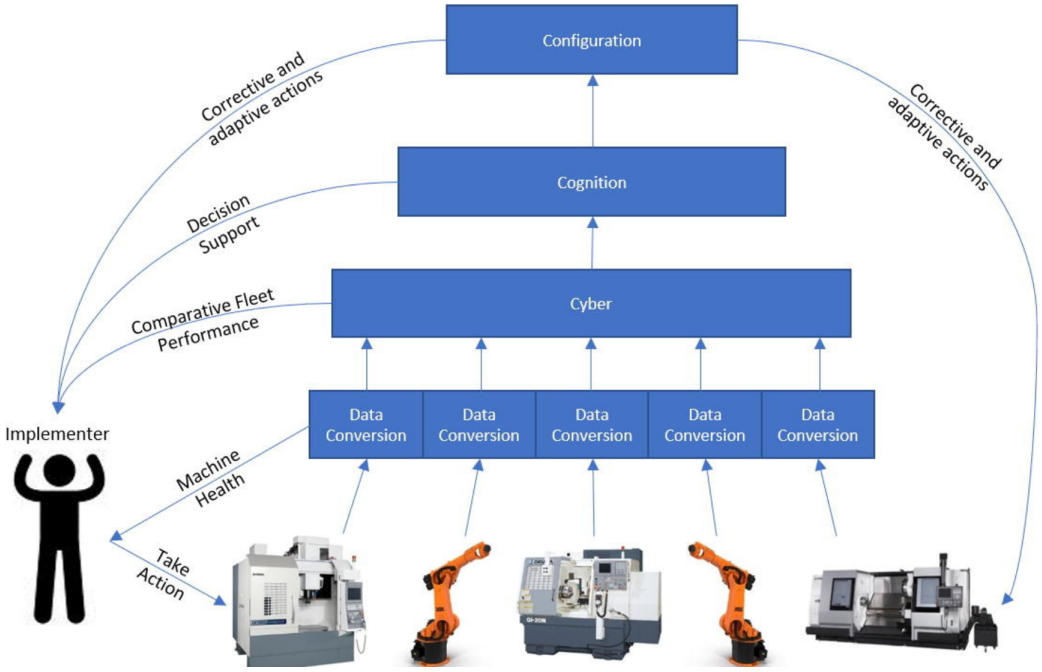


Figure 2.1: Illustrating the human role and interaction with cyber-physical systems, adapted from [31]

2.3 OPC Unified Architecture

The OPC Unified Architecture (UA), released in 2008, is a platform independent service-oriented architecture [5]. It is in the common area of IoT, Industry 4.0, and Machine-to-machine communication (M2M), figure 2.2 [32]. OPC UA is built on the success of OPC classic and was designed to enhance and surpass the capabilities of its classic version.

OPC UA, as an International Electrotechnical Commission (IEC) standard (IEC 62541), enables connecting machines together, exchanging data, and communication between different manufacturing products [34, 35]. Being flexible, suitable for different embedded systems, and different Operation Systems (Windows, macOS, and Linux), forms it to be a popular option. It operates with a client-server model [36]; the server fetches and shares data.

Woopsa[6] and RT-Middleware [37] are two open-source alternatives for OPC UA. Since they are not supported by manufacturing simulation software, such as Visual components [7] and RoboDK [8], they were not utilized as a part of the CPS of the department of industrial engineering [38].

2.4 Security

In this subsection a correct definition of security with the axioms are introduced.

[5] `https://opcfoundation.org/about/opc-technologies/opc-ua/`
[6] `http://www.woopsa.org/`
[7] //www.visualcomponents.com/
[8] https://robodk.com/

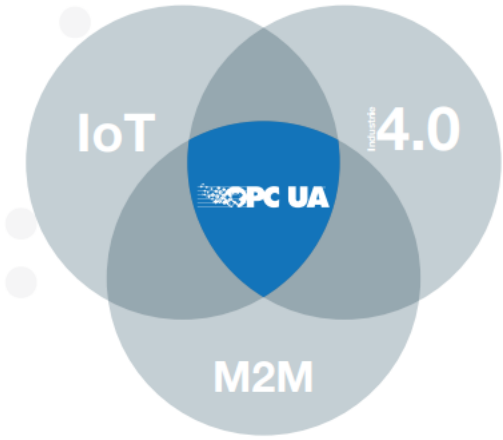


Figure 2.2: The common data connectivity and collaboration standard for local and remote device access in IoT, M2M, and Industry4.0 adapted from [33]

The fundamental question in the first place is "What is security?". According to Convery's book [17], security could become subjective and complementary in cases (this book is also an important source because it is a base for Cisco SAFE approach which is the method of ours). He defines some axioms as follows:

> "When I say "axiom" in this book, I am referring to overarching design principles, considerations, or guidelines that are broad enough to apply to all areas of secure network design. Axioms are similar to design principles but are subtly different. A design principle is smaller in scope and often involves only a single technology or affects only a limited area of the network. For example, that the intrusion-detection system (IDS) should be installed as close as possible to the hosts you are trying to protect is a design principle."

The axioms are:

- **Network Security is a System**: Security is not a firewall, IDS, VPN, Authentication, Authorization and Accounting (AAA). Security is not anything that Cisco System or any of its competitors can sell. Network security system is a collection of network-connected devices, technologies, and best practices that work in complementary ways to provide security to information assets. The key word in that definition is complementary. A complementary technology that applies to a specific threat pattern is needed, which some refer to as "defense-in-depth". In the book it is referred to as a practical method of determining the quality of your system, breaking down the quantity, and makeup of the various deployed threat mitigation techniques (protect, detect, deter, recover and transfer), similar to NIST Framework [29].
- **Business priorities must come first**: It is necessary to ensure that businesses are able to continue to evolve.

- **Network Security promotes good network design**: The most effective way to improve pre-exisitng network security is to logically divide the network into functional modules. A network design provides the infrastructure and serves the matter of segmenting the network into smaller modules as one of its most important services.
- **Everything is a target**: Any components of a network could be a target for attacks. Although there is no doubt that Internet-reachable servers (such as web servers and proxy servers) are one of the highest-profile targets, focusing on protecting only those systems will leave a design lacking in many areas.
- **Everything is a weapon**: One of the biggest reasons that everything is a target is because nearly everything (computers, routers, ...) could be used as a weapon. An attacker is motivated to acquire weapons to wield against future targets. Therefore, nearly every successful attack has not only a direct result for the attacker, but also an indirect gain for using against new targets. The notion of using your own systems as weapons against you is critical for the attacker's success.
- **Strive for operational simplicity**: In layman's terms, achieving operational simplicity means the difference between a security system that works for you and a security system that you work for.
- **Good network security is predictable**: Predictability is required to implement a successful security system. in other words:
  - Assuring that the activity and events the system might experience is understood, including attack vectors.
  - Considering how to construct a system that mitigates these attacks.
  - Considering failure conditions that might arise within your own system to ensure the design is layered.

  the work does not stop with the security design, operational processes must be considered to ensure the ability to deal with a security incident properly.
- **Avoid security through obscurity**: Security through obscurity is not security. This does not mean that obscurity mechanisms are never meant to be used. It means you should never rely on them.
- **Confidentiality and security are not the same**: Security is the protection of systems, resources, and information from unintended and unauthorized access or misuse. While confidentiality is the protection of information to ensure that it is not disclosed to unauthorized audience. Here we can refer to the famous CIA (Confidentiality, Integrity, Availability) triad, figure 2.3, which has been expended during the time (mentioned in section 2.10).

2.5 Firewalls

Firewalls are the principal element in many secure network designs. As NIST has expressed [39], firewalls are devices or programs that control the flow of the network traffic between networks or hosts that employ differing security postures. While firewalls are often discussed in the context of

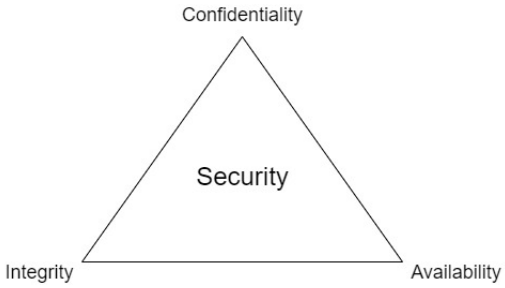


Figure 2.3: The classic CIA Triad

Internet connectivity, like the focus in the early days of its existence [40], they also have applicability in other network environments. For example, many enterprise networks employ firewalls to restrict connectivity to and from the internal networks used to service more sensitive functions, such as accounting and personnel. By employing firewalls to control connectivity, an organization is able to prevent unauthorized access to its systems and resources. It could be said that inclusion of a proper firewall provides an additional layer of security.

Several types of firewall technologies exist. One way of comparing their capabilities is to look at the TCP/IP protocol suite layers that each is able to examine. Basic firewalls operate on one or a few layers (typically the lower layers) while more advanced ones investigate all of the layers. The ones which investigate more layers are able to perform more thorough examinations. The application layer firewalls, potentially, accommodate advanced application and protocol and provide services that are user-oriented. As an example, it could enforce user authentication and log events to specific users. A notable point is that firewalling is often combined with other technologies - most notably routing and Network Address Translation (NAT) [41] (which is actually a routing technology). Moreover, some firewalls include Intrusion Prevention System (IPS) technologies too.

Firewalls are often placed at the perimeter of a network. Such firewalls have one or many internal and external interfaces with the external interface being on the outside of the network. They are also sometime referred as unprotected and protected. Since the firewall's policies could operate in both directions we would avoid "protected" and "unprotected" terms and will use internal and external for such firewalls. Generally, as NIST [39] mentions, ten firewall technologies could be arranged in the following sub-sections:

2.5.1 Packet Filtering

The most basic feature of firewalls is packet filtering. The old firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and sessions. The devices with only such functionality are also knows as stateless inspection firewalls which do not keep track of the state of each flow of traffic that passes through them. For example, they are not able to associate multiple requests within a single session to each other. Packet filtering is the core of most modern firewalls, but, nowadays, there are a few firewalls sold that are only capable of stateless packet filtering. Their access control functionality is based on a set of directives (rule-set). Packet filtering capabilities are built into most operation systems (OS) and devices capable of routing, such as routers and Access Control Lists (ACL). The access control could

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.1	1032	192.168.3.2	433	Established
192.168.1.5	1030	192.168.3.2	433	Initiated
192.168.3.6	1033	192.168.2.6	80	Established

Table 2: Example of the State table of a stateful firewall

be done based on: source IP, destination IP, network or transport protocol, ports and interfaces. Packet filters own some drawbacks. Stateless packet filters are generally vulnerable to attacks and exploits which take advantage of problems within TCP/IP specification and protocol stack. For instance, they are unable to detect spoofed or altered network layer addressing information. On the other hand, firewalls that operate at higher layers (TCP/IP layers) are able to detect some spoofing attacks by verifying the establishment of a session or authenticating users before allowing traffic to pass. Moreover, packet fragmentation has been used for attacking; in which, some network-based attacks have used packets that should not exist in normal communication, such as sending fragments of a malicious packet but not the first fragment, or packet fragments that overlap each other. To prevent such use of fragmentation, fragmented packets could be blocked that could also cause interoperability issues of Virtual Private Networks (VPN). Some firewalls could reassemble fragments before passing them, although it requires additional resources, particularly memory. They should be configured carefully, since a denial-of-service attack could be mounted too. Choosing whether to block, reassemble, or pass fragmented packets is a trade-off between overall network interoperability and full system security. Nevertheless, automatic blocking of fragmented packets is not recommended according to NIST guidelines on firewalls and firewalls policy [39], because of applicability of fragmentation on the Internet.

2.5.2 Stateful Inspection

It improves on the functionality of packet filters by tracking the state of connections and blocking packets that differ from the expected state. Incorporating greater awareness of the transport layer enables this feature. The tracking is done inside a table called state table and the table contents varies between firewall products. Although, the contents of the table, typically include source IP, Destination IP, port number, and connection state information.

Three major states exist for TCP traffic (establishment, usage, termination). Each new packet is verified by state of the connection listed in the state table. For example, if an attacker claims the packet to belong to an established connection while the state table expressed a different state of connection, the packet is filtered. Stateful firewalls could also consider the TCP sequence numbers and NAT information. Regarding connection-less protocols such as UDP, stateful firewalls are only able to track the source and destination IP addresses and ports and the packets must still match an entry in the state table. For example, a Domain Name System (DNS) [42] response from an external source must match a corresponding DNS query. An instance of a state table is presented in table 2.

2.5.3 Application Firewalls

A newer trend in stateful inspection is the addition of a stateful protocol analysis capability, also called deep packet inspection. It improves upon standard stateful inspection by adding basic intrusion detection technology. Intrusion detection technology analyzes application layer protocols

to compare vendor-developed profiles of harmless protocol activity against the observed events, for example, identifying denied attachment types of emails, blocking connections over which specific actions are being performed, or inspecting contents of web pages.

Application firewalls could also identify unexpected sequence of command which would cause buffer overflow, DoS, Malware and HTTP attacks. More importantly, they could validate input of individual commands, such as minimum and maximum lengths for arguments which is a great capability against buffer overflow threats.

Furthermore, another useful feature of some of application firewalls is enforcing compliance checking. Many products implement protocols in ways that match the specification. It is therefore usually necessary to let such implementations communicate across the firewall.

Firewalls with both stateful inspection and stateful protocol analysis capabilities are not full-fledged intrusion detection and prevention systems (IDPS). IDSPs offer more extensive attack detection and prevention capabilities, such as, signature-based and/or anomaly-based analysis to detect [43].

2.5.4 Application-proxy gateways

It is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. The firewall reacts as a proxy and never allows a direct connection between two hosts that wish to communicate. In fact, each successful connection results in the creation of two separate connections (one between the client and the proxy server, another between the proxy server and the true destination. The connection would seem transparent but the internal IP addresses are not visible to the outside world.

In addition to the usual rule-set, some proxy agents are able to mandate authentication of each individual network user, in the forms of user ID and password, hardware or software token, and biometrics.

Although application-proxy gateways resemble to application firewalls and have the ability of operating at the application and transport layer, they are quite different. First, the application-proxy gateways offer higher level of security for some applications since it prevents direct connections and inspects the traffic content. Second, application-proxy servers have the ability to decrypt packets (e.g., SSL-protected payloads), examine them and re-encrypt them before sending them to the destination.

Like any devices, firewalls with application-proxy gateways contain some disadvantages. Because of the full packet awareness in some of the application-proxy gateways, they are poorly suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server could be used to secure less time-sensitive services. Another disadvantage is the tendency of application-proxy gateways to limit the terms of support for new network application and protocols and simply allow unsupported traffic to tunnel through the firewall. Therefore, it is essential to investigate the support of an application-proxy gateway for a specific protocol, before purchasing it.

2.5.5 Dedicated Proxy Servers

They differ from application-proxy gateways and retain dedicated proxy control of traffic and limited firewalling capabilities. They are only mentioned here because of their close relationship to application-proxy gateway firewalls. Many of them are application-specific and some perform analysis and validation of common application protocols such as HTTP. It should be noted that due

to their limited firewalling capabilities, they are typically deployed behind traditional firewall platforms.

2.5.6 Virtual Private Networking

A common requirement for the firewalls at the edge of a network is encrypting and decrypting specific network traffic flows between the protected network and external networks. This is nearly always involves Virtual Private Networks (VPN) [44], which use additional protocols to encrypt traffic, authenticate users and check integrity.

VPNs are most often used to provide secure network communication across untrusted networks, such as extending the protected network to a multi-site organization , and providing secure remote access to the internal network across the Internet. According to NIST [39] two common choices for secure VPNs are IPSec [45] and Secure Socket Layer (SSL) / Transport Layer Security (TLS)[46] and the two common VPN architectures are gateway-to-gateway and host-to-gateway. VPNs generally rely on authentication protocols, such as Remote Authentication Dial In User Service (RADIUS) [47] and Lightweight Directory Access Protocol (LDAP) [48]. The VPN functionality upon firewalls requires additional capacity planning and resources which many firewalls include hardware acceleration for encryption to minimize the impact of VPN services.

2.5.7 Network Access Control

Another common feature for firewalls at the edge of a network is to perform client check for incoming connections from remote users, commonly called Network Access Control (NAC) or Network Access Protection (NAP). This feature allows for access based on the user's credentials and performing health check on the user's computer. The health checking consists of verifying one or more of the following items:

- Latest updates to anti-malware and firewall software
- Configuration settings for anti-malware and personal firewall software
- Elapsed time since the previous malware scan
- Patch level of the operation system and selected applications
- Security configuration of the operation system and selected applications

It should be noted that these health checks require a software on the user's system that is controlled by the firewall.

2.5.8 Unified Threat Management (UTM)

Many firewalls combine multiple features into a single system to set and maintain policy easier. A typical Unified Threat Management (UTM) system has a firewall, malware detection and eradictation, sensing and blocking of suspicious network probes (IDPS functionality) and etc. There are positive and negative sides for such firewalls. It reduces the complexity but it should have all the desired features for security objectives too. Moreover, another trade-off is performance, the system handling multiple tasks. Some organizations might find UTM useful, while others would prefer to have multiple firewalls at the same location in their network.

2.5.9 Web Application Firewalls

One of the most prone components of a network is the HTTP protocol used in web servers that has been exploited by attackers in many ways, such as placing malicious software on someones computer who is browsing the web, or tricking identities to reveal their private information. Many of these exploits could be detected by this type of firewalls which reside in front of the web server (these firewalls are a relatively new technology).

2.5.10 Firewalls for Virtual Infrastructure

Considering virtual systems (a quite popular solution of having multiple virtual systems on one real computer), most of them include virtualized networking. Virtualized networking permits the multiple operating systems communicate as if they were on a standard Ethernet, even though there is no actual networking hardware.

As a relatively new area of firewall technology, since network activities that passes directly between virtualized operation systems within a host cannot be monitored by an external firewall, some virtualization systems offer built-in firewalls or permit third-party software firewalls to be added as plug-ins.

2.5.11 Topology options of Firewalls

Convery [17] suggests five firewall placement options which move from less to more secure solutions:

- Basic filtering router: this implementation is easy to implement and does not impact surrounding network. The drawbacks of this topology are the existence of public servers on the internal side of router and enabling attacking internal systems, a single point of access control failure, and lack of stateful filtering.
- Classic dual-router demilitarized zone (DMZ): The separation of public servers from the internal network and reducing the chance of attacks against internal network, in case of having a compromised public server, are the main benefits of this design. But absence of stateful inspection endangers the internal systems to attacks.
- Stateful firewall DMZ design: This design is an improvement upon the classic dual-router DMZ and suits the situations which the performance capability of the existing firewall cannot match the throughput requirements of the public servers.
- Modern three-interface firewall design: This design, according to Convery [17], is a gold standard in firewall edge deployment which is the best balance of security, cost, and management. The most important benefit of such design is requiring all traffic flow to pass through the firewall, including traffic from the internet to the public servers, which in all previous designs were only protected by basic ACLs. This design could be modified by adding more segments allowing public servers to be separated from one another.
- Multifirewall design: A number of variation of this design exist. But it is, primarily, used for e-commerce or any other sensitive transactions which generally require multiple trust levels.

An illustration of each placement (topology) is presented in figure 2.4, 2.5, 2.6, 2.7, and 2.8, adapted from [17].

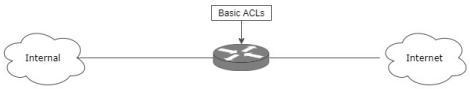


Figure 2.4: Basic filtering router topology

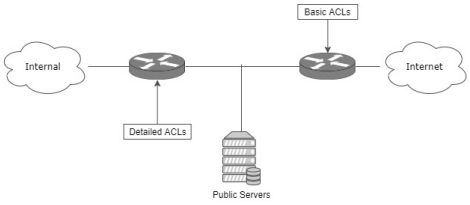


Figure 2.5: Classic dual-router demilitarized zone (DMZ) topology

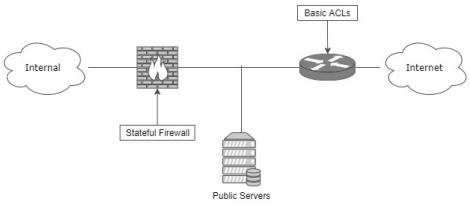


Figure 2.6: Stateful firewall DMZ topology

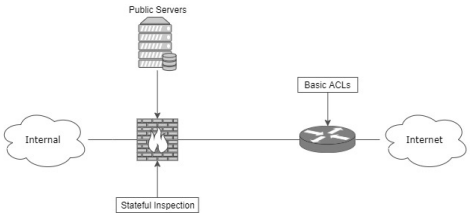


Figure 2.7: Three interface firewall topology

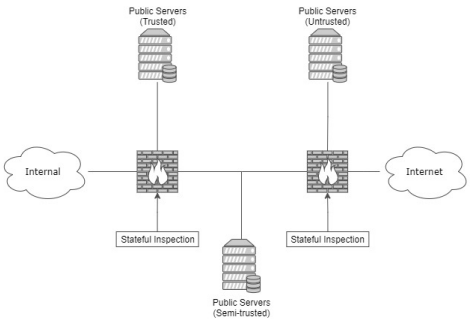


Figure 2.8: Modern firewall topology

2.6 Intrusion Detection Prevention Systems

As NIST mentions [43],

> "Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring

individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization."

There a number of types of IDPS technologies differing, primarily, based on the types of events they are able to recognize and the methodologies they use to identify possible incidents. Four types of IDPS technologies which are also mentioned in NIST Guideline [43] are as follows:

- Network-Based: It monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity.
- Wireless: as the name implies, this type of technology monitors and analyzes wireless network traffic and protocols.
- Network Behavior Analysis (NBA): Examining network network traffic and identifying threats generating unusual traffic flows, such as DDoS attacks and scanning is the functionality of this type of technology
- Host-based: it is commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information. This technology monitors the characteristics and events of a single host.

Their typical components are:

- Sensor or agent: Monitoring and analyzing activities are done by them. The term *sensor* refers to network-based, wireless, and NBA technologies. The term *agent* refers to host-based IDPS technologies.
- Management Server: It is a centralized device receiving information from the sensors or agents and manages them (some types of IDPS sensors and agents could be deployed standalone, and managed and monitored directly by administrators). Management server perform analysis on the event information that sensors or agents provide and identify events that individual sensors or agents are not able to. Matching event information from different sensors and agents, which is known as correlation. Appliances and software-only products of management servers are available. Zero, one, and multiple management servers could exist based on different use-cases.
- Database Server: It is a repository for the recorded event information by sensors, agents, and management servers, which is supported by many IDPSs.
- Console: It is a program that provides an interface for the IDPS's users and administrators, that is, typically, installed onto standard desktop or laptop computers. IDPS administration - such as configuring sensors or agents, and applying software updates - and IDPS monitoring/analysis could be done using separated or integrated consoles.

It should be noted that the IDPS components could have two network architectures: using the organizations' standard networks or a separate network strictly designed for security software management, known as a *management network*. In management networks, each sensor or agent contains an additional network interface known as *management interface* that connects to the management network. In case a management network is not deployed, a virtual management network using a virtual local area network (VLAN) [49] withing the standard networks is recommended by NIST [43].

Generally, most IDPS provide information gathering, logging, detection and prevention security capabilities.

2.7 Authentication, Authorization, and Accounting

Authentication, Authorization, and Auditing (AAA) essentially defines a framework for coordinating discipline across multiple network technologies and platforms. In practice, an AAA Server with a database of user profiles and configuration data communicates with AAA clients residing on network components, such as Network-Attached Storage (NAS) and router, provide distributed Authentication, Authorization, and Accounting services [50].

As it is mentioned in section 2.10, authentication involves validating the end users' identity prior to permitting them network access, authorization defines what rights and services an authenticated user is allowed, and accounting provides the methodology for collecting information about the end users' resource consumption, used for billing, auditing, and capacity planning. One or more AAA server serves a central repository for storing and distributing AAA information.

2.8 Network Management

Hagering [51] defines network management as all measures ensuring the effective and efficient operation of a system within its resources in accordance with corporate goals. Boutaba and Xiao [52] state the objectives of network management as follows:

- Managing network resources and services: including the control, monitor, update, and report of network states, device configuration, and network services
- Simplify network management complexity: extrapolating network management information into human manageable form and interpreting high-level management objectives.
- Reliable services: providing network high quality of service, minimizing downtime, detecting and fixing network faults and errors, and safeguard against security threats.
- Cost conscious: keeping track of network resources and users. All network resources and service usages are to be kept track of and reported.

A more general categorization of network management functions is provided by OSI reference model [51, p.82-94]. The OSI model breaks network management functions into five functional areas:

- Fault Management: detection, recovery, and documentation of network anomalies and failures
- Configuration Management: recording and maintaining network configuration, and updating configuration parameters to ensure normal network operations
- Accounting Management: user management, user administration, and billing on usage of network resources and services.
- Performance Management: providing reliable and high quality network performance, including quality of service
- Security Management: providing protection against security threats to network resources, services, and data, in addition to ensuring user privacy and access rights.

It should be noted that in the recent years many other features have been added to the network management servers but the mentioned features are the basis of majority of them.

2.9 Time synchronization

The Network Time Protocol (NTP) [53] is one of the oldest protocols on the Internet and has been widely used since its initial publication. NTP is widely used to synchronize computer clocks to some time reference. The client software continuously runs a background task that periodically gets updates from one or more servers. The client software ignores responses from servers that appear to be sending the wrong time, and averages the results from those that appear to be correct.

Many of the available NTP software clients, for personal computers, do not average at all. Instead, they send a single timing request to a signal server and then use this information to set their computer's clock, called Simple Network Time Protocol (SNTP) [54]. The best current practices has been published as RFC 8633 [55].

2.10 Security threats

Generally, apart from any type of system, security is preservation of the following concepts [20]:

- **Confidentiality**: to maintain the security of user's personal data in the CPS and prevent an attacker from attempting change of the state of the physical system by "eavesdropping" communication channel between the sensors and the controller, and between the controller and actuator.
- **Integrity**: to maintain the data or resources unchanged without permission.
- **Availability**: to prevent any failure in computer technology, management, communication and equipment
- **Authenticity**: to identify a subject or resource as it claims.
- **Accountability**: to trace the actions of an entity uniquely to the entity
- **Non-repudiation**: to prove nonexistence of any replication of actions or events.
- **Reliability**: to confirm that both parties involved are really ones they pretend to be

There could be some confusion about the difference between reliability and authenticity. Reliability means that the entity is capable of standing for the facts to which it attests, while authenticity means that a record is what it claims to be.

Cyber-physical threats are threats that originate in cyberspace but have an impact on physical space of the system. In other words, they emerge from cyberspace and affect the physical space [20].

Based on [20] work which is owed to [56], a tree of attacks and threats based on the functional model of CPS is proposed, figure 2.9. The branches of the tree include the following types of attack:

(a) Attacks on sensor devices (Sensing)

(b) Attacks on actuators (Actuation)

(c) Attacks on computing components (Computing)

(d) Attacks on communications (Communications)

(e) Attacks on feedback (Feedback)

Figure 2.9: A tree diagram of attacks and threats on cyber-physical systems, adapted from [20]

It should be noted that threats are not necessary external and deliberate. Threats may be deliberate, accidental or environmental.

Meanwhile, attacks in the published literature can be roughly divided into three categories too [18]:

- **Denial of Service(DoS)**: which mostly aims to disrupt the availability principle of security.
- **Replay attacks**: a replay attack is a natural strategy, in which a valid data transmission is maliciously or fraudulently repeated or delayed.
- **Deception attacks**: in which the data integrity is modified for transmitted packets among different cyber-parts. In different scenarios, it could also be called as false data-injection attacks, malicious attacks, to just name a few.

ENISA have evaluated the criticality of each assets of Industry 4.0, figure 1.3, by interviewing experts. It involved a structured questionnaire and resulted in a figure correspond to the percentage of experts who selected a given option, figure 2.10. The figure indicates that stake holders consider ICS, i.e. Programmable Logic Controller (PLCs), Remote Terminal Unit (RTUs), Distributed Control Systems (DCS), Supervisory Control And Data Acquisition (SCADA), and in our case OPC UA systems, to be the most critical assets for Smart Manufacturing and Industry 4.0.

Figure 2.10: Asset criticality [7]

2.10.1 Dynamic Host Configuration Protocol attacks

Since the current system is benefiting from the ease of using Dynamic Host Configuration Protocols (DHCP) server [57] in the network, it is noteworthy to mention different attacks and threats which could a DHCP server suffers from.

The number of IP-based network nodes is continuously, such as mobile devices, IP telephony, sensors and IoT devices. These newly connected devices must have a correctly configured Internet Protocol (IP) settings, to be able to communicate over a data network. Configuring all these options manually, would require considerable amount of time and labor. Therefore, usually, these devices receive such settings automatically, requesting from a DHCP Server.

DHCP was developed from Bootstrap protocl (BOOTP) for dynamically assigning binding information, which includes an IP address and other related network configuration, such as subnet mask and default gateway, to any node on the network. DHCP service uses a User Datagram Protocol (UDP) [58]. It utilizes UDP port number 67 for DHCP server originated traffic and port 68 for client originated traffic, mentioned in the related RFC [57]. The main fields and the process could be found in the RFC[57] and Aldaoud's article [59]. Grasping the functionality and the packet structure of DHCP matters, but since it is not in line with the purpose of the project, the more important part of the concept and DHCP attacks are focused on, i.e. DHCP attacks.

DHCP is considered a vulnerable and insecure service since the protocol does not mandate authentication from the DHCP clients and it could be attacked in various ways, according to

Aladoud [59]. Apart from exploiting DHCP configuration to provide incorrect settings for the DHCP clients or exploiting bugs to crash the service, there are three more popular attacks which put the server in danger [60]. As Bhaiji [60] provides some details, the attacks in addition to a brief description of them are as follows:

- DHCP flood attack: It occurs when the attacker, continuously sends forged DHCP client messages to the DHCP service. It is done in order to downgrade the performance and capabilities which, normally, is due to the extra amount of incoming packers. This type of attacks may lease or reserve pool's available IP addresses [61].
- DHCP starvation attack: it is a specific kind of flood attack where an attacker continuously sends forged DHCP client messages in order to exhaust the available IP addresses of the server's pool. This will cause the legitimate DHCP clients to lease their IP addresses and lose their connection.
- DHCP spoofing attack: which is done by introducing a DHCP Rouge server, also known as spurious DHCP server. This will lead to a race condition in replying to client DHCP messages and the DHCP client will use the first arrived message to configure its binding information. In other words, the DHCP rouge server creates a man-in-the-middle (MITM) attack [62] (details regarding the MITM attack could be found in Mallik's article [63].

Aldaoud has also investigated different DHCP attacking tools and two relevant packet crafting libraries, which is noted in the related article [59].

2.11 The existing Cyber-Physical System at UiT campus Narvik

Cooperation among manufacturing systems could be named as one of the visions behind industry 4.0 which focuses on smart manufacturing facilities. Department of Industrial Engineering (DIE), which operates a robotic laboratory, encompasses a Cyber-Physical System (CPS) setup as shown in figure 2.11. This department has discussed the use of OPC Unified Architecture (OPC UA) standard for communication between hardware and software components in a typical manufacturing system and developed a digital twin which presents a demonstration of the digital laboratory [38] [64].

The OPC UA [9] server, shown in figure 2.11, is running the server version of OPC UA and all the first-layer components are running client version of OPC UA. Running a OPC UA client on any workstation being involved in the network and adding the server and other components based on their URL, would enable controlling the components and administrating the system.

In a bigger picture, considering the mentioned three essential stages of Industry 4.0 (section 2.10.1), in our case, the first step is done by integrating Systems on a Chip (SoC), like Raspberry Pi, and the functionality of OPC UA clients. All the OPC UA clients are connected to the OPC UA server. The second step, which is related to analyzing data, is handled by an OPC UA server. A commanding system using OPC UA and simulation of the existing components using Visual Components [10] would be named as the third essential stage of Industry 4.0.

[9] `https://opcfoundation.org/`

[10] `https://www.visualcomponents.com/`

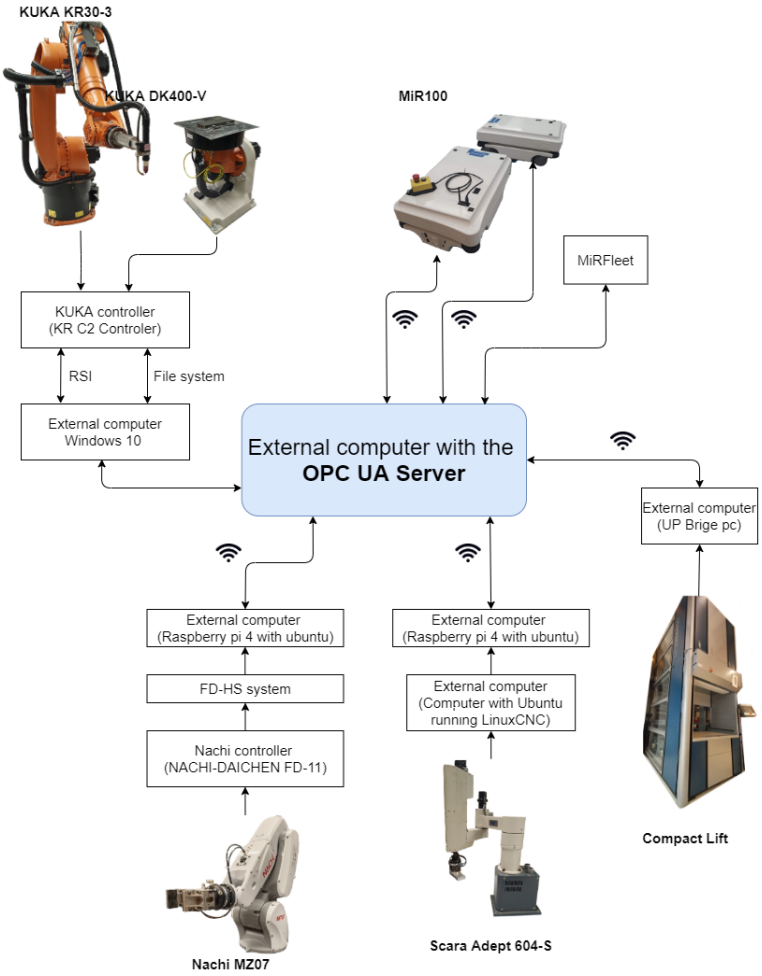


Figure 2.11: The existing system of Industrial engineering department

Figure 2.12: The Visual Components model of the laboratory

New functionality and features, such as Machine Learning for the robot arms, are being developed and added upon the system in a fast pace. Nevertheless, the main objective of this system is to bring all components with different brands, rather new or old, together and build a command center that also simulates the laboratory using Visual Components software, figure 2.12. The ultimate

objective of the laboratory is to provide such a system for the industry.

3 Method

This section states the methodology for answering the research questions (section 1.1). Emphasizing on the first question as the most important part of this thesis, a method is selected to institute a secure architecture for the purpose of the department of industrial engineering. The architecture would be the ground for answering the second and third question.

As it was mentioned in the prior section (section 2.1), there are a number of frameworks and approaches to evaluate and consider security for a system, such as NIST [29], Security classification [27], and Multi-metric approach [28]. Although NIST Framework is one of the most popular approaches toward security, not having different examples and use-cases, which NIST Framework has been applied on, found, resulted in looking for an approach that has a more clarified concept.

Investigating the security approach of Cisco Systems[11], as one of the leading companies in manufacturing and selling networking hardware, software, telecommunications equipment and other high-technology services and products, is a valid choice. Cisco has already been first in introducing new proprietary protocols that were improved and standardized later, like NetFlow [65], Enhanced Interior Gateway Protocol (EIGRP) [66] and etc. Moreover, during a talk with a security expert, Cisco, i.e. Cisco SAFE, was suggested.

After reading through different materials that Cisco has published, Cisco's approach and the vision of visibility for security have piqued my interest. Moreover, different use-cases, detailed explanations and clear road maps are introduced inside the documentations. These clarifications are a great help for a non-expert to grasp the concept. Therefore, Cisco's approach, referred to as Cisco SAFE, is the method chosen for approaching security (i.e. Cisco SAFE for IoT Threat Defense for Manufacturing [1] and Cisco SAFE secure Campus [2]).

Cisco SAFE is a quiet ripe and mature concept. The first blueprints[17] found about Cisco SAFE, return to 2004. Convery's book[17] is named as the main force behind the original SAFE Blueprints, from concept to consolidating considerations, to builds outs to authoring the first pivotal white papers that Cisco posted. The official revised reference guide [67] was published in 2010. SAFE is a security model and method used to secure business [11]. It provides the design and implementation guidelines for building secure and reliable network infrastructures that are resilient to both well-known and new forms of attacks. It takes a defense-in-depth approach, where multiple layers of protection are strategically located throughout the network, but under a unified strategy [67, p. 1].

SAFE supplies an approach for IoT and manufacturing networks quiet different from Cloud and classic computer networks. In Cloud and classic computer networks, SAFE proposes the key to simplify cybersecurity into secure Places In the Network (PINs) for infrastructure, and Secure Domains for operational guidance. While for Iot threat defense for manufacturing, it tackles the challenge the threats pose to IoT, on four critical fonts. In the following two sections more details regarding both concepts are expressed.

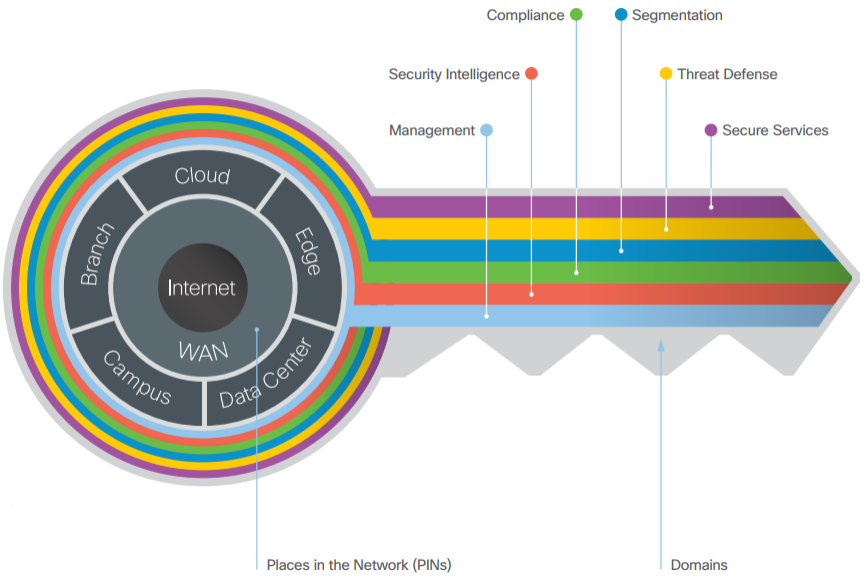


Figure 3.1: Key to SAFE, the approach of SAFE for classic computer networks

3.1 Cisco SAFE for networks

SAFE simplifies network security by providing solution guidance using the Places In the Network (PINs). PINs are locations that are commonly found in networks and conceptually represent the infrastructure deployed in these locations. PINs are as follows:

- Branch
- Campus
- WAN
- Data Center
- Edge
- Cloud

Cisco has published articles for each PIN [2, 68, 69, 70, 71, 72] and the further information could be found on the Cisco website[12].

The Secure Domains represent the operational side of the key. Operational security is divided by function and the people in the organization that are responsible for them. The domains are:

- Management: coordinates policies, objects and alerting.

[11] https://www.cisco.com/

[12] https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html#~tab-architecture

- Security Intelligence: provides global detection and aggregation of emerging malware and threats.
- Compliance: addresses internal and external policies.
- Segmentation: establishes boundaries for data and users.
- Threat Defense: provides visibility into the most evasive and dangerous threats.
- Secure Services: provides technologies such as access control, virtual private networks, and encryption

Figure 3.2 represents different capabilities regarding each secure domain.

It is noteworthy to attend to the Cisco SAFE approach for campus networks [2]. This approach is integrated inside the Cisco SAFE for IoT threat defense for manufacturing, which is the main approach of this thesis toward generating a secure architecture.

3.2 Cisco SAFE for IoT Threat Defense for Manufacturing

Cisco's IoT threat defense solution takes an architectural approach to protect IoT using the SAFE model for security. Cisco SAFE starts with the business flow/use cases. This design guide specifies the components and configurations used to validate this architecture, protecting manufacturer as they embark on their transformation journey to achieve Industry 4.0 or realize the Industrial IoT (IIoT) [1]. Cisco SAFE for IoT Threat Defense for Manufacturing tackles the threats to IoT on four critical fonts, which is presented in figure 3.3.

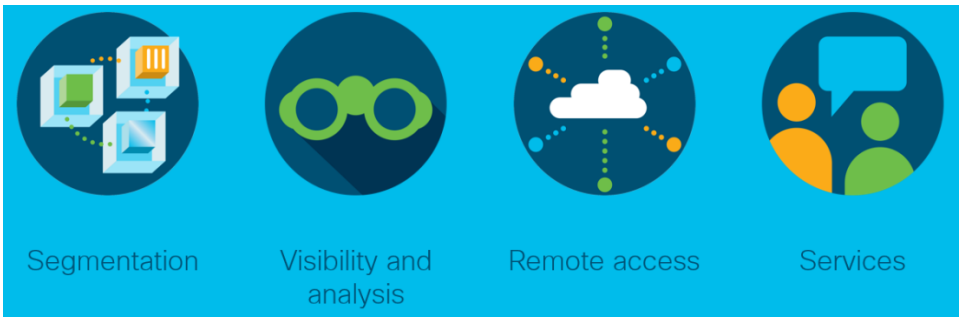
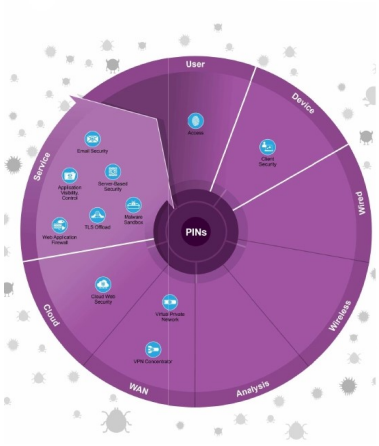


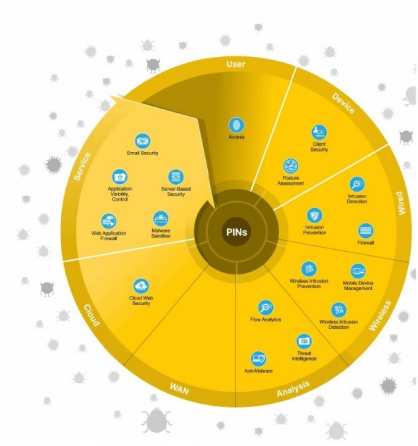
Figure 3.3: Four critical fronts of IoT threat defense for manufacturing, adapted from [1]

This approach suggests an architecture for IoT. International Society of Automation ISA-99 Committee for Manufacturing and Control System Security (IACS) bases itself on the Purdue Model Hierarchy [73], a common well-known model in the manufacturing industry, and identifies the levels and logical framework zones as the Plant Logical Framework, figure 3.4. Cisco adapts IACS, adjusts it based on its own background, and proposes a more complicated architecture. As it is mentioned in the documentation [1],

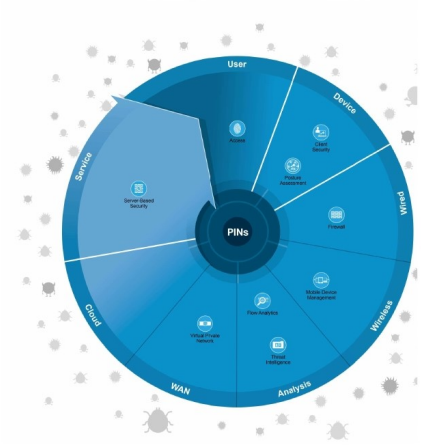
> "The Purdue model and ISA-99 have identified levels of operations and key zones for the IACS logical framework. In addition to the levels and zones, Cisco and Rockwell



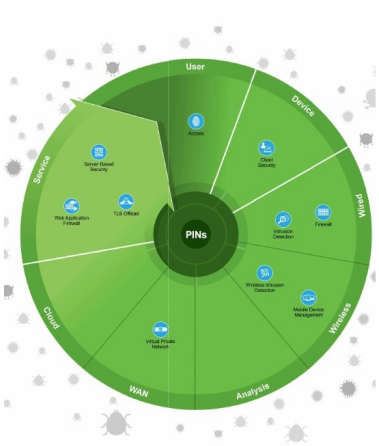
Secure Services Capabilities



Threat Defense Capabilities

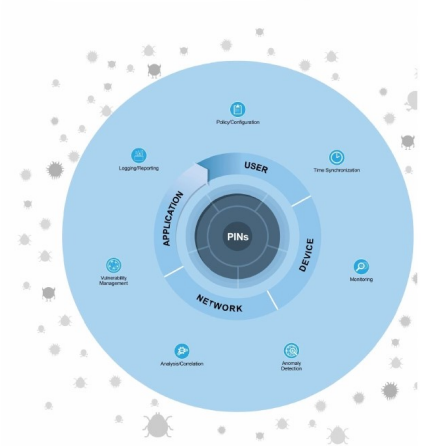


Segmentation Capabilities



Compliance Capabilities

Security Intelligence Capabilities



Management Domain Capabilities

Figure 3.2: Secure Domains capabilities, adopted from [11]

Automation include a demilitarized zone (DMZ) between the enterprise and manufacturing zones as part of Converged Plantwide Ethernet (CPwE) architecture. Emerging IACS security standards such as ISA-99, NIST 800-82, and Department of Homeland Security INL/EXT-06-11478 also include a DMZ as part of a defense-in-depth strategy. the purpose of the DMZ is to provide a buffer zone where data and services can be shared between the enterprise and manufacturing zones. The DMZ is critical in maintaining availability, addressing security vulnerabilities, and abiding by regulatory compliance mandates (e.g., Sarbanes-Oxely). In addition, the DMZ allows for segmentation of organizational control; for example, between the IT organization and manufacturing. This segmentation allows different policies to be applied and contained. for example, the manufacturing organization may apply security and quality-of-service (QoS) policies that are different from the IT organization. The DMZ is where the policies and organizational control can be divided."

The importance of a Demilitarized Zone (DMZ), as a buffer zone, in order to maintain availability is a key point. Availability, is the most important principle of security for cyber-physical systems [12]. Therefore, throughout the project, availability is considered as the most important principle of security.

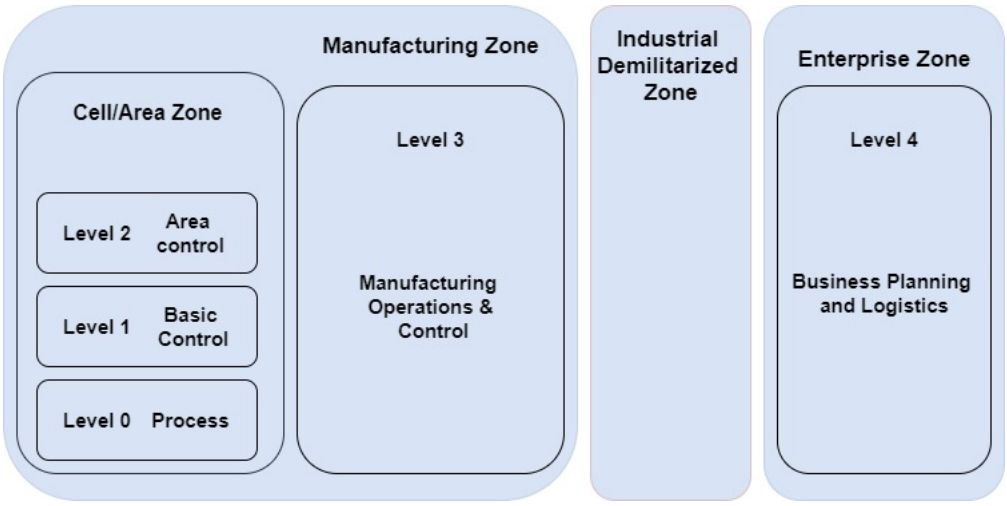


Figure 3.4: Plant Logical Framework, adapted from [1]

Using the SAFE Campus reference architecture [2] and IoT Threat Defense business flows, it could easily be shown that how the end-to-end architecture, as shown in figure 3.5 (given example by Cisco), could include both IT and OT models, and the deployment of the capabilities protecting the flow. This example and the general plant logical framework were adopted for this project. The proposed case of this project is presented in the proposed architecture section (section 4.1.4).

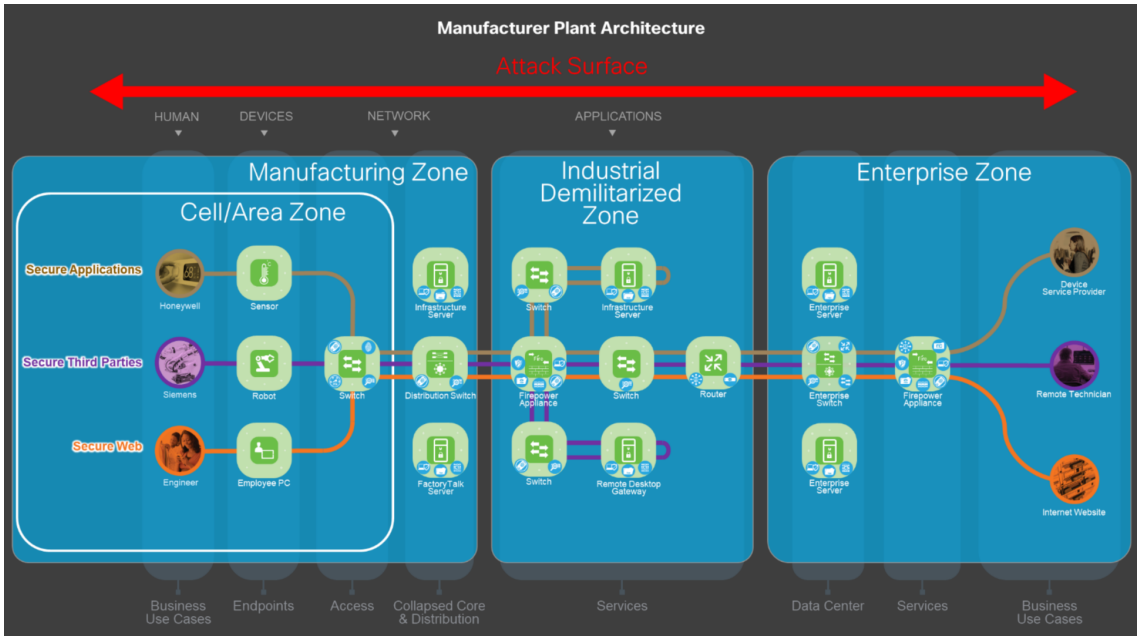


Figure 3.5: CPwE reference architecture in SAFE Format with business flows, adapted from [1]

Details related to the mentioned four fonts of Cisco SAFE for treating the threats of IoT for manufacturing is presented in the following four subsections.

3.2.1 Segmentation

Security starts with visibility [1]. But for the IoT systems, segmentation comes first. There are varied techniques of attacking and gaining access to IoT devices [74]. Therefore, segmentation could limit the effect of a potentially compromised device to a limited area of the network. In other words, Segmentation is about:

- restricting network access
- diving the network based on role and function

Cisco suggests its Identity Services Engine (Cisco ISE) [13] plus TrustSec [14] for the purpose of segmentation. The practical deployment of Cisco ISE is provided by Richer and Wood [75].

3.2.2 Visibility and Analysis

After applying segmentation for devices and users, visibility and analytic enables identification of devices on the network. As soon as all devices are identified, detecting and remediation of threats

[13] https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
[14] https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

that bypass existing controls is done with ease. Cisco ISE, Stealthwatch [15], Firepower [16] and Umbrella [17] are the advised technologies from Cisco to provide visibility and analysis.

3.2.3 Remote Access

Secure remote access replaces the legacy modems and other connectivity methods vendors used in the past, eliminating the back doors to a digitally connected network. The security capabilities related to this font enable and ensure secure remote connectivity to the system. Identity capability (AAA server), VPNs, and Anti-malwares for the client devices are the capabilities regarding having a secure remote access.

Cisco ISE, AnyConnect VPN [18], and Advanced Malware Protection (AMP) [19] are proposed by Cisco for this purpose.

3.2.4 Services

The former fonts and the related capabilities help to create a secure network. And as it was mentioned earlier, a secure network is the foundation for a secure system. Services such as security network penetration assessment, and automation & control system risk assessment could help understanding the facts of the situation. Services which Cisco provides for IoT could be found on their website [20].

3.3 Security Life-cycle

Security is a system (section 2.4). The security threats evolve; hackers will continue to evolve new and sophisticated methods to get around even the tightest security [76]. Therefore, as the threats evolve, the security system should also develop. The new standards, guidelines, risk assessments, best practices, and the feedback from the existing security system should be utilized to improve the system. Moreover, business needs could alter over time. Absence of a procedure in which all the new concepts and necessary changes are applied, would result in a fragile system.

After establishing the system according to the Cisco SAFE method, the security life-cycle, presented in figure 3.6, is selected to improve the security system over the time. This life-cycle, considers business needs, guidelines, standards, risk analysis, industry best practices, and the feedback from the current security operations, to enhance a security system. Therefore, if there are some other materials, such as new risks and best practices, the security system could be improved based on this life-cycle. The security life-cycle is adapted from the blueprint of Cisco SAFE, Convery's book [17].

3.4 Vulnerability detection

Intrusion Detection Prevention Systems could be used to document the existing threats in the system, although it is not their main purpose of existence inside a network (stated in section 2.6). Nevertheless, vulnerability assessment tools are dedicated implementations for such purposes. They

[15] https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
[16] https://www.cisco.com/c/en/us/products/security/firepower-management-center/index.html
[17] https://umbrella.cisco.com/
[18] https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html
[19] //www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
[20] https://www.cisco.com/c/m/en_us/customer-experience/architectures/iot.html

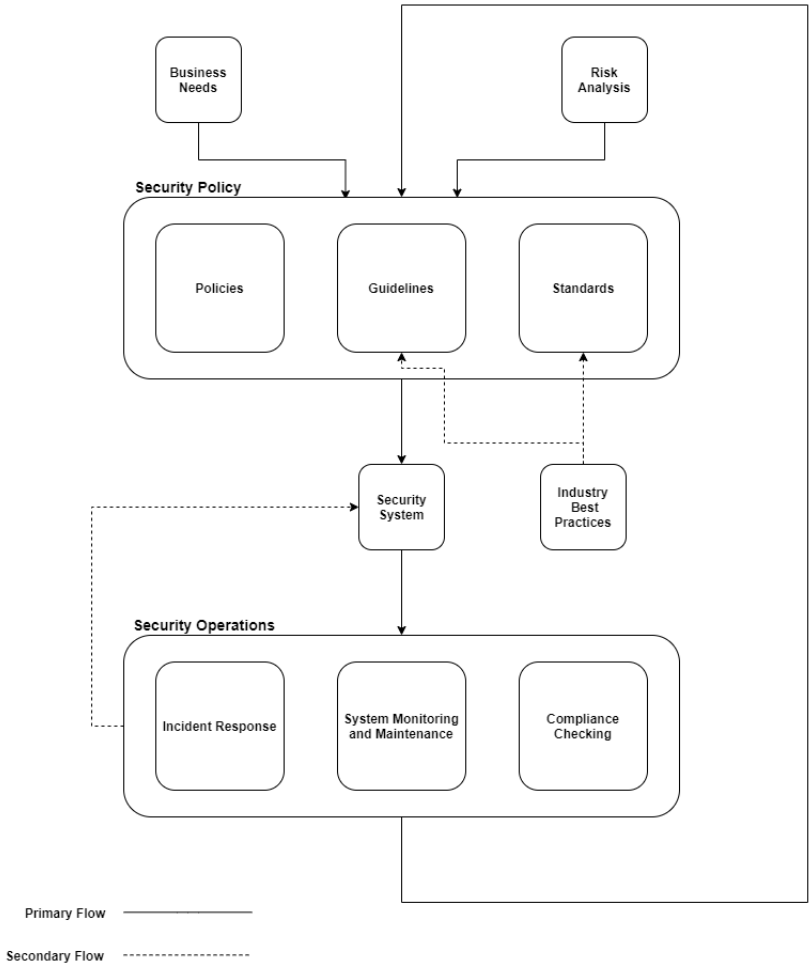


Figure 3.6: Security Life Cycle Overview adapted from [17]

assist administrators to detect the vulnerabilities of networks and receive recommendations for the remediation.

There are a number of vulnerability assessment tools for networks and cyber-physical systems. In order to choose one, several benchmarks exist to provide a number of best choices, such as G2 which uses user satisfaction in order to rate the softwares [21]. McMahon [77] has also benchmarked vulnerability assessment tools for enhanced CPS resiliency. He provides knowledge on how to improve the resiliency by evaluating and comparing the accuracy, and scalability of two popular vulnerability assessment tools, Nessus and OpenVAS.

After investigating different vulnerability scanner tools (Nessus, OpenVAS and Zenmap) Nessus has been selected for this project. Nessus is one the most popular tools, user-friendly, powerful, and easy-to-use. Nonetheless, OpenVAS and Zenmap (A graphical front end for Nmap) are handy and open-source which form them as valid alternatives.

[21] `https://www.g2.com/categories/vulnerability-scanner`

Subsection Number	Title	The answering question
4.1	Secure Architecture	Research Question 1
4.2	Current State	Research Question 2
4.3	Protective Measures	Research Question 3

Table 3: Relativity of subsection with the research questions

3.5 Evaluation of the current CPS

In order to evaluate the current system, in its current state, the architecture of the system has been assessed. Cyber-Physical Systems same as a normal computer network, enables the existing networking infrastructure concepts to establish a network architecture. Therefore, Cisco routing and switching materials [14, 15, 16, 78], which are related to the background of the author, in addition to Cisco SAFE for IoT [1] were used to assess the system.

The idea for the method of assessment is to propose a secure architecture for the system firstly and compare the current architecture of the system with it. There are a number of factors constructing a secure architecture. Considering all the distinct factors separately and evaluating the existing CPS with each factor individually, would be a tiresome and complex procedure. Therefore, all the factors were firstly utilized to yield a complete secure architecture that satisfies the need of the department of industrial engineering. Following that, the existing system is compared to the proposed touchstone. The touchstone is the answer to the first research question (section 1.1).

4 Results

In this section, the effort for answering the three main questions of this research (section 1.1) eis respectively mentioned. Section 4.1 pertains to introducing a secure architecture for the project proprietor (the department of industrial engineering at UiT campus Narvik). Section 4.2, as an answer to the second question of this research, investigates the current state of the CPS and discusses the related shortcomings. Ultimately, section 4.3 covers the security measures that should be done, or are already done, to enhance the security level of the system. Table 3 supplies an overview of the relation of each following sections to the research questions (the research questions are already mentioned in section 1.1.)

4.1 Secure Architecture

As Neuman [79] mentions, security experts (and the victims of cyber-attacks) calling for designing applications for security rather than adding it later. This call is often misunderstood, or perhaps it is misstated. What does it mean to design an application for security? To many it means including security requirements during design, so that necessary data and interfaces up form the application to use myriad security mechanism such as encryption, authentication, etc. As he believes, it, unfortunately, misses the point. "Yes, Providing the ability to use such mechanisms is important; but, true security requires an even more fundamental integration of security in a way that permeate the basic design and structure of application itself." [79]. The security level of a system is as strong as the weakest security point of your system. In other words, no matter how secure the majority of a network is, if there is a small part which is vulnerable, the whole network is vulnerable.

In order to answer the first question of this research about defining a secure CPS for the purpose of the existing system in the depart of industrial engineering (Research Question 1 in section 1.1), Cisco CAFE IoT threat defense for manufacturing approach [1] was mainly utilized. Moreover, an study of the OPC UA security enabled a better perception of the existing system and aided proposing a better architecture, section 4.1.3.

4.1.1 Business Flow

Cisco SAFE [11] uses business flow as a basis and contemplates it for applying security capabilities. Moreover, the visibility of the users and how they use the system, provides clarity inside the network which assists any developer to have a better perspective of the system.

According to the department of industrial engineering, currently, there are only three characters (identities) defined to use the system:

- Engineer: who has the full access to all devices (including the OPC UA clients and servers and other components).
- CEO and clients of the CPS products: who has only a limited access to the reporting device that reports the current status of the CPS.
- Third-parties: who tend to access specific devices for maintenance purposes.

Apart from automatic and periodic activities, such as Address Resolution Protocol (ARP) [80] requests, which is done independent from real identities, fetching updates and information from servers and repositories is independent from any engineer seeking them and they should be scheduled. The security analysis of Kaspersky Lab [81] regarding OPC UA implies the necessity of keeping the system updated too. Therefore, devices were considered inside the defined business flow as separate entities.

A more exact illustration of the business flow is presented in figure 4.1. The effort is to provide an overview of the flow and emphasize the most important features which identities would use the system for. Therefore, the details about the exact servers and devices as the destination of the users has been generalized (i.e., devices and how they fetch services and updates from the servers). Therefore, this figure provides an overview of the business flow rather than a detailed one. Visualizing the precise business flow of a system, requires an analytic system registering flows, which the network lacks at the current state.

4.1.2 Business Flow and Security Capabilities

Cisco SAFE for IoT Threat Defense for Manufacturing [1] provides an example of business flows and the related security capabilities. The security capabilities are categorized based on the four critical fonts that tackles the challenges pose to IoT (Segmentation, Visibility and analysis, Remote access, and Services), figure 4.2.

If the business flow of this project, figure 4.1, is contemplated, security capabilities which fit the flow should be proposed. Based on the example that Cisco provides, figure 4.2, the business flow and related capabilities are presented in figure 4.3. In the background section (section 2.5-2.9) a brief description of each capability is supplied.

The first layer of a good defense-in-depth strategy is appropriate access control strategies [82]. For the segmentation feature, mentioned in section 3.2.1, the identity security capability (using a

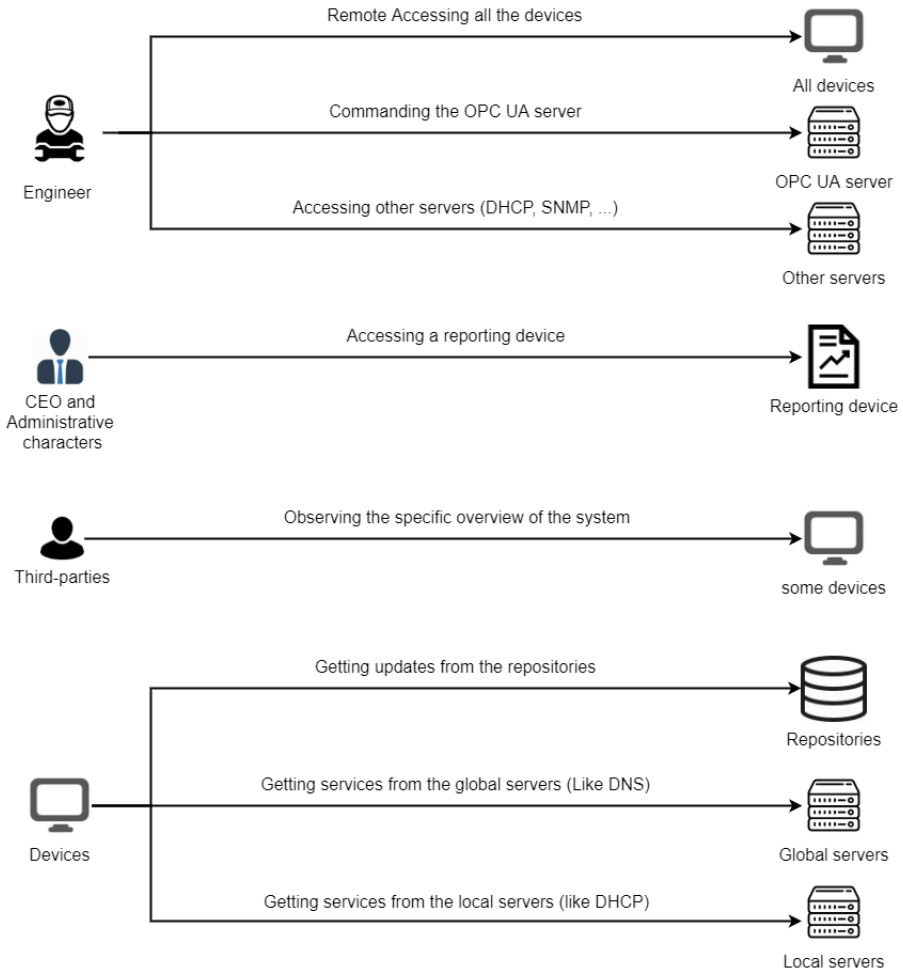


Figure 4.1: Business flow defined based on the need of the department of industrial engineering

AAA server) and firewalling, limiting network traffics based on set of rules, have been proposed. It should be noted that the segments in the network architecture also is a part of segmentation feature which is not shown in the figure 4.3.

The visibility and analytic feature is done by using IDPS, network analytic and threat intelligence systems. These named feature could all be integrated into one component but since the functionality, in this case, matters the most, they were named as separate entities. The ideal situation for the research purposes, is considering a threat intelligence system independent from any other components. The independent component would enable a deep investigation of the flow and traffic of the network, and defining the norms inside the network.

Virtual Private Network (VPN) access and the fact of using an anti-malware software on the connecting client device would respect the feature of remote access of Cisco SAFE for IoT.

It should be noted that the mentioned capabilities are not dedicated to only one of the four fonts. But in order to clarify the main purpose of each of them, they are mentioned in only one of the fonts. For every mentioned capability, Cisco provides a Cisco-proprietary technology (noted in

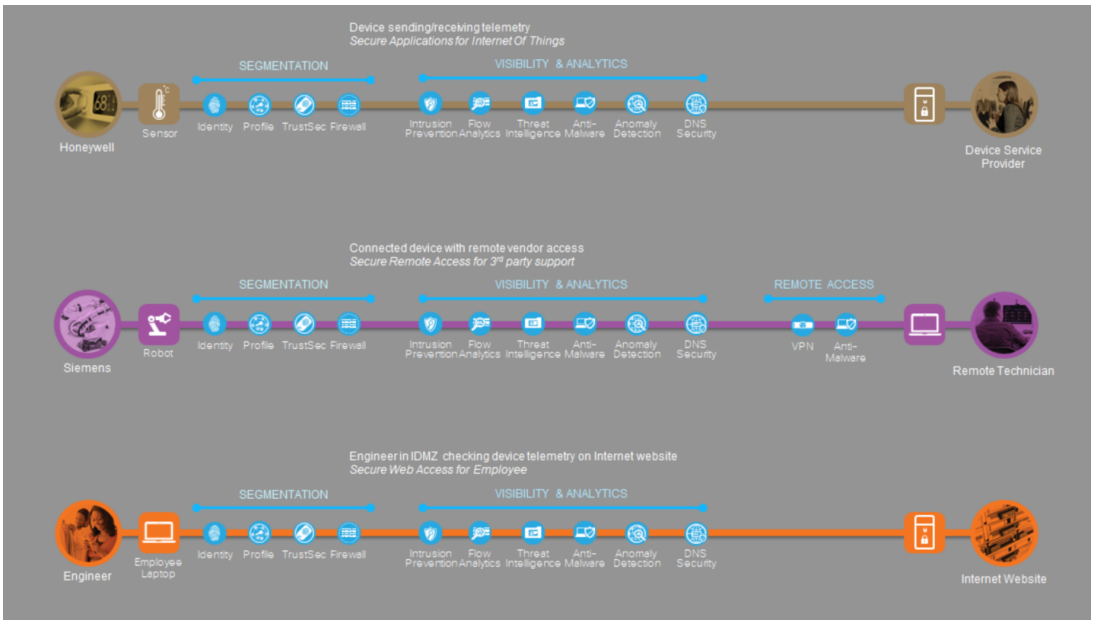


Figure 4.2: Example of SAFE Business Flows and Capabilities, adapted from [1]

section 3.2). Most of the proposed technologies are costly and well-performed using Cisco devices (Switch, Router, Access point, and etc.). Since the objective of the department is to have the lowest possible expense for the project, the technologies should be replaced by the open-source alternatives. The open-source alternatives for the mentioned capabilities are discussed in section 4.3.

4.1.3 OPC UA security study

Section 2.10 denoted the ICS (in our case OPC UA) as the most critical component of Cyber-Physical Systems. In this section, a security study of OPC UA is discussed. The study would help perceiving the system and the main service of the CPS better and affect the proposing architecture.

OPC Foundation has published an article by the title of "Practical Security recommendations for building OPC UA application" [32]. The article is the most recent publication of the company in the field of security, until March 2021. Within the article, the following points were outstanding.

The OPC Foundation claims OPC UA as a system which in contrast to many other industrial protocols, provides a high level of security. This claim is backed up by the analysis of the Federal Office for information security (BSI). BSI is the first and foremost the central IT security service provider and national cyber security authority for the federal government in Germany. Moreover, the company tries to introduce a security model for the concept and some best practices which were described for two different use cases, one for a low level of implementation of OPC UA inside a network ,and another one for a higher contribution of OPC UA inside a network (the second use case is a more similar system to our existing system). The proposed security architecture considers:

- Trusted Information (CIA triad)

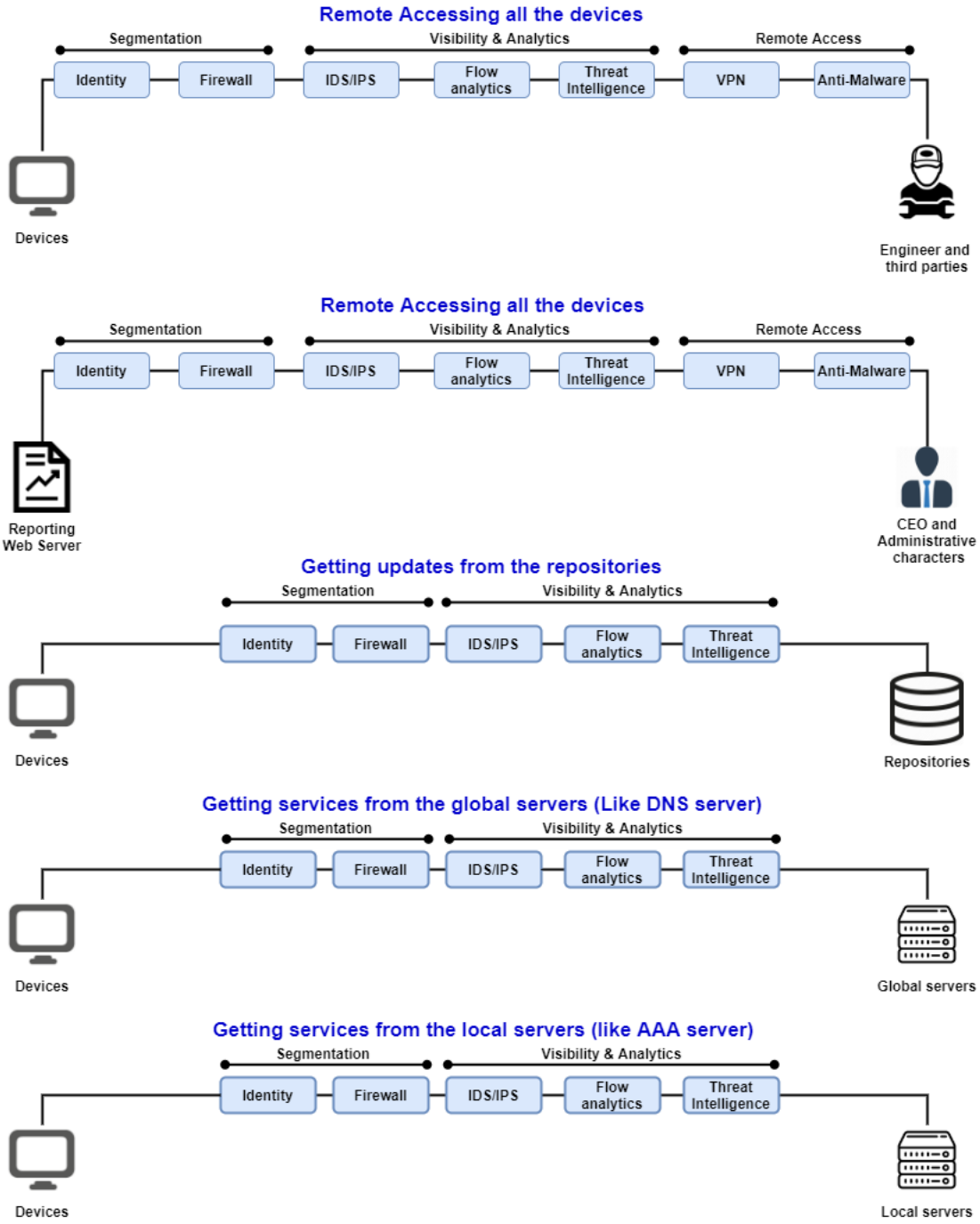


Figure 4.3: The business flow and the required security capabilities, which are categorized based on the four fonts of overcoming threats

  - confidentiality in transport layer,
  - integrity in transport layer
  - availability by restricting the message size and returning no security related codes,
- Access Control (AAA Framework)
  - Authentication by username and password or X.509 certificate on the application layer
  - Authorization by access rights of the users or the user's role
  - Accountability by generating audit events for security related operations

Moreover, the security aspect of OPC UA uses defense/security in depth, certificate management, and storage of private keys are the two key points that are discussed within the publication.

Most importantly, OPC Foundation is not considering the following concepts and refers them to Information Security Management System (ISMS) that the ISO 27001 defines:

- Security training of personnel
- Security life cycles
- Security Policies
- Handling physical access

Because of the popularity of OPC UA in the industry and being a member of the OPC Foundation consortium, Kaspersky Lab has also analyzed the security of OPC UA [81]. Despite the seventeen zero-day vulnerabilities in the OPC Foundation's products and several vulnerabilities in the commercial applications that use these products, Kaspersky Lab has identified a number of insecure data structures and lack of documentation. The poor documentation makes errors more likely to be introduced in the process of using and modifying OPC UA. The reported vulnerabilities were reviewed and fixed by OPC Foundation, the formal response of OPC Foundation is accessible on the Kaspersky website [22]. Nevertheless, being prone to errors (i.e., stack overflow) and the necessity of keeping the system up-to-date is concluded from the study.

4.1.4 Proposed Architecture

OPC Foundation [33] and Cisco SAFE [1] have emphasized on the concept of defense/security in depth. As McGuiness mentions [83], defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. The strategy considers the fact of variety of attack methods and absence of a single method to protect a network from all the variations of attacks.

As many articles, such as [84], broach defense in depth at each layer of the TCP/IP protocol suite, it is essential to consider the security from the lowest layer. Moreover, if security of the lower layers of the protocol suite is not taken into consideration, the higher layer security approaches are precarious. In other words, if the concept of security is not applied on first layer of TCP/IP (Network interface layer), the security of the third layer (Network layer) is not in its highest effectiveness. NIST in one of its Guidelines related to IPsec VPNs [85] mentions:

[22] `https://ics-cert.kaspersky.com/reports/2018/05/10/opc-ua-security-analysis/`

"Data is passed from the highest to the lowest layer, with each layer adding more information. Because of this, a security control at a higher layer cannot provide full protection for lower layers, because the lower layers perform functions of which the higher layers are not aware".

Therefore, importance of security in all layers and starting form the lowest layer is an acceptable concept.

The proposed architecture is based on Cisco SAFE approach, discussed in section 3.2. It is presented in figure 3.5. In general, four different zones are assumed, Enterprise Zone, Industrial Demilitarized Zone (DMZ), Manufacturing Zone which includes Cell/Area Zone. Every traffic is either generated or terminated in the DMZ. Since functionality of some servers differs from others, segmenting the Industrial Demilitarized Zone (DMZ) into two different subnets (Infrastructure servers and directly accessed servers) is considered. Elements of each zone are explained as follows:

- **Cell/Area Zone**:

  The Cell/Area zone contains the robots (KUKA, MiR100, ...) that are connected to the network through two access points. In order to increase the availability of the robots, two access points are assumed. In case one of the access points encounters failures, the other one would compensate for the loss of the other, until the faulty device is up and running again. This functionality requires a third entity that controls the status of the two access points.

- **Manufacturing Zone**:

  In the Manufacturing zone which contains the Cell/Area zone, a wireless Local Area Network (LAN) controller, as its main functionality, handles the redundancy of the access points and detects rogue access points [23]. The OPC UA server is placed apart from the Cell/Area zone to be available apart from other robots. In other words, disconnection in the Cell/Area zone would not effect the OPC UA server. A switch connects all the mentioned elements together and to the DMZ.

- **DMZ 1**: The first DMZ, tagged as Infrastructure servers in figure 4.4, contains all the mentioned security capabilities mentioned in section 4.1.2. The servers are all brought together and connected to the other zone through a switch.

- **DMZ 2**:

  The second DMZ, tagged as Directly accessed servers in figure 4.4, contains the proxy/VPN server that handles remote accesses, and the reporting server that aims to present general information regarding the system and its products, mentioned in figure 4.1 and figure 4.3. The reporting device (a web server) has not been implemented by the project owners yet, but according to the need of the project owners this element is mentioned. As it is mentioned in the network architecture book by Cisco press [17], proxy server functionality could be merged with stateful firewall functionality, although separating the two functions generally provides superior security, greater flexibility, and less-complex configurations (mentioned in section 2.5.)

[23] A rogue access point (RAP) is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack [86]

Network Address	Usable Host Range	Broadcast Address	Subnet Mask	Usable Hosts
192.168.1.0	192.168.1.1-14	192.168.1.15	255.255.255.240	14

Table 4: Example of a /28 IP subnet

The reason for segmenting this zone from the former zone is the different functionality the components own. None of the components in DMZ 1 is accessed directly through the Internet, while all the components in DMZ 2 are accessed from the Internet. Nevertheless, the servers in DMZ 1 need to be connected to DMZ 2 to fetch the necessary data for their functionality. Same as all the former zones, a switch handles the connectivity in this zone.

- **Enterprise Zone**: This zone connects the network to the Internet or the other possible networks. A stateless firewall could enable a basic packet filtering and bring another layer of defense, while the other firewall performs a deeper packet inspection.

Each subnet should be assigned based on the maximum number of possible clients in that subnet. For example, if the maximum number of clients in the manufacturing zone is assumed to be 10, the IP subnet should have a chunk of 14 assignable IP addresses available. The presented IP addresses in figure 4.4 are only examples . Table 4 provides an example of such IP subnet. The communication of different subnets is enabled using routers and firewalls (firewalling is often combined with routing, mentioned in section 2.5).

4.2 Current state

The current cyber-physical system functions as the users expect it. Nonetheless, the presented figures (section 2.11) suffers from the lack of documentation of the exact topology of the system. The topology would assist anyone who is interested in the exact functionality of the system, to grasp it better. Therefore, firstly, an investigation of the network topology of the system has been executed. Figure 4.5 indicates the components of the system in which an ASUS wireless router carries the connectivity of the components to each other and to the Internet.

The existing system is designed based on functionality, neither efficiency nor security. The measurements for the designing phase has only aimed functionality of the system. In other words, only the services, functionality of OPC UA, and capabilities that enable connectivity of the components is taken into consideration.

The previously described approach toward evaluation of the system, section 3.5, indicates the need for a robust network architecture for further security analysis of the system. Considering the proposed secure architecture (section 4.1.4), and the fundamentals of computer networks, the following notable problems for the existing system are as follows:

- Lack of a Demilitarized Zone
- The single point of failure
- Uncertainty in the identities using the system
- Uncertainty about the IP address of critical components (IP Planning)
- Unsynchronized time of the system

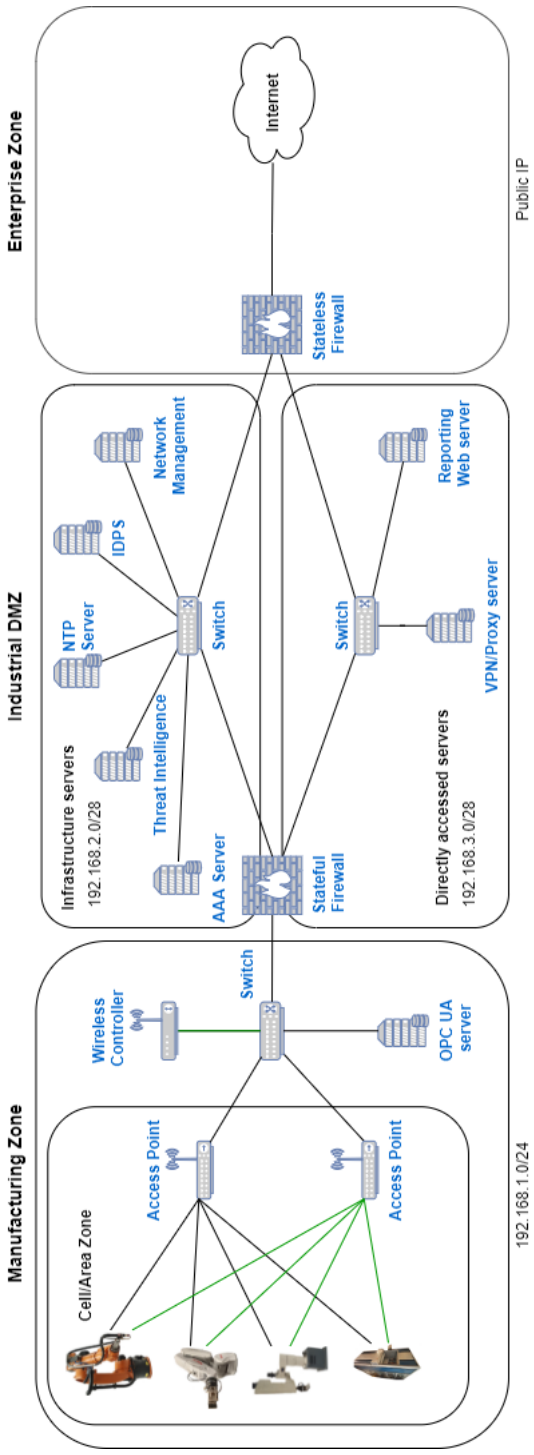


Figure 4.4: A sketch of the final design of the CPS network

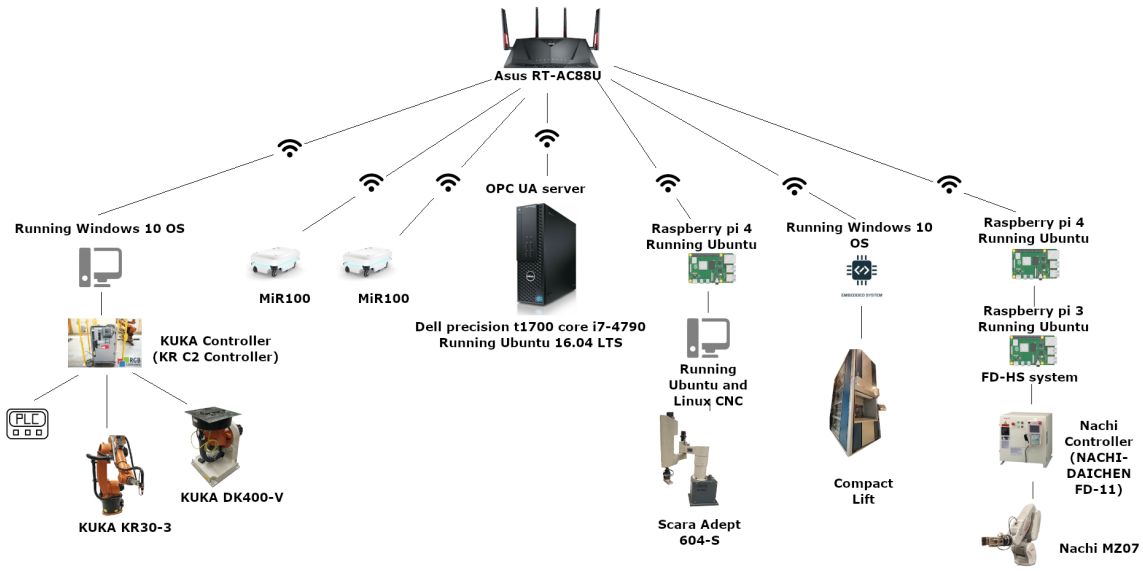


Figure 4.5: Topology of the system

- Absence of any security capabilities

In the following section the details regarding the difficulties of the existing system are delivered.

4.2.1 Shortcomings of the current design

Considering the reviewed materials (NIST Guidelines, such as 800-82, Cisco SAFE, and computer networking fundamentals, and comparing the proposed architecture with the existing architecture, would assist pinpointing the shortcoming of the current design. This section would provide the details regarding the most important detected flows of the existing design of the the robotic laboratory.

The shortcomings are as follows:

- **Absence of Demilitarized Zone**

  NIST 800-82, Cisco SAFE [1], and SANS [13] emphasize on restricting logical access to the local network and network activity by using a demilitarized zone (DMZ). This zone will force all the network traffics to either generate or terminate in this zone. Therefore, absence on such critical zone in the network would endanger the system.

- **Single Point of Failure**

  Cisco in its networking design materials (CCNP Routing and Switching [15, p.13]) mentions the importance of redundancy and resilience for high availability. Previously mentioned importance of availability in CPS (NIST 800-82 [12]), and the Cisco's emphasize on redundancy,

would criticize the usage of one device as the communication hub (ASUS wireless router, presented in figure 4.5). Santra [87] also mentions the problem of single point of failure [24] in star topology, which is the current topology of the system (figure 4.5).

In case there is a failure in the ASUS device, all the communication between the components are terminated. The proposed design (figure 4.4) offers a redundancy in the number of access points of the network. In case the main access point faces failure, the other access point would compensate for the absence of it, until the faulty access point functions properly. This compensation requires a third component called wireless controller, or as Cisco mentions it as Wireless LAN Controller (WLC), managing different access points.

Moreover, the device is functioning as three different components, access point, switch and router. Although this integration of critical functionality in one device reduces the complexity of the network, it would cause a single point of failure for all the three functionality. The proposed design first of all divides the three functionality into three different devices, access points for connecting the wireless components to the network, a switch for connecting the wired/wireless components to each other and the firewall. The firewall would have the functionality of a router contained. This design would make the system flexible and expandable in case there is a need for a bigger area of wireless coverage or adding more components to the network.

- **IP planning**

  In the existing system a DHCP server, running on the ASUS device, assigns binding information, mentioned in section 2.10.1. Although clients normally request their old IP addresses when they ask the DHCP server for the binding information, there is uncertainty in being assigned the same IP address all the time. Therefore, in the existing system the IP address of all components could alter. This change of IP would bring uncertainty, problems with logging, or loss of connection with the devices that are always accessed through a certain IP address.

- **Time synchronization**

  Time synchronization in the existing state is handled automatically by the operation systems with the global clock provided by the default options of the different operation systems. Lee [88] notes the devastating consequences of attack on a global clock synchronization and believes synchronized clocks offer new mechanisms for improving security, primarily because of key property that they enable coordination without communication. For example, with synchronized clocks, the absence of a message conveys information. Moreover, many smart grid testbeds, as an example of Cyber-Physical Systems, in local substation protection schemes use the Simple Network Time Protocol (SNTP) to synchronize time in the network of intelligent electronic devices [89].

  It was observed during investigating the existing system that the time of the devices are not synchronized. Some devices are behind/ahead of the correct global clock. Therefore, it is favorable to have a point in the local network which all devices are synchronized with. That point could be synchronized with the exact global clocks. As it was mentioned in section 2.9, a very simple system of SNTP could be starting point for the components which would have

[24] A single point of failure (SPOF) is a system component which, upon failure, renders an entire system unavailable or unreliable, adapter from `https://docs.oracle.com/cd/E20295_01/html/821-1217/fjdch.html#:~:text=A%20single%20point%20of%20failure,these%20SPOFs%20can%20be%20mitigated`

a local server to have their time synchronized with. This local time synchronization would also enable accuracy for the logs generated by different devices and value them more. With a synchronized time accurate scheduled time would also be facilitated.

- **Lack of Authentication, Authorization, and Accounting**

  The current system does not differentiate between any of the identities using the system. For example, all the connected devices or people are able to access the OPC UA server or any other component. Moreover, there is no functionality for storing, managing, and supplying events and configuration information. No information about who, how, and when the users used the system is stored in the current system.

  The proposed architecture, in the first place, considers the type of identities and how they use the system, figure 4.1 - the figure regarding business flows. Afterwards, it establishes the security capabilities based on the business flows. The proposed architecture with an Authentication, Authorization, and Accounting (AAA) server, facilitates a better segmentation of access to the system (respecting the different identities which were defined in section 4.1.1), limiting the privileges of different users, and tracking the activities. Following that, visibility of the people who are using the system is also enabled. All the remote accesses should also be validated by the AAA server. The other security services, such as IDPS, would have access to the gathered data by AAA server and the security services themselves are validated by the server too.

- **Unknown status of the devices**

  No status of the components, whether they are on or off, having a high CPU usage, and etc., is being collected or known in the present system. For example, if one of the SoCs (Raspberry Pi), faces a problem or is turned off due to a high temperature of the CPU, no one would notice it, unless the engineer is unable to remote access the system and checks the component physically. A network management server would handle such performance.

- **Absence of network traffic controlling**

  The existing network provides no control over the types of traffic that enter, exists, and lives inside the system. Any types of traffic including the malicous one could enter the network and no information regarding them would be provided inside the network. It was mentioned earlier (section 2.5) that how firewalls with its different features enable a control over the network. Therefore, absence of such critical concept inside the network is one of the shortcoming of the existing system.

- **Want of intrusion detection and prevention**

  Detecting abnormalities and possible incidents inside a system requires a dedicated security capability. Intrusion Detection and Prevention Systems (IDPS), mentioned in section 2.6, are responsible for such concern. Thus, absence of such component would disable detecting possible incidents.

- **Third-parties remote access software**

  On February 8th 2021, an attacker attempted hacking of the city of Oldsmar's water treatment system in Florida, USA. The attacker tried to increase the levels of sodium hydroxide [25].

[25] `https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV`

The hacker gained access to a control panel that was password protected accessible using TeamViewer, a remote control software, according to local authorities.

In a Motherboard report [26], several well-known security experts criticized companies and workers who often use TeamViewer for sensitive resources. In the article, according to Cynthia Brumfield [27] TeamViewer has years of acknowledgment of being a fairly insecure application. Carhat, also, describes her ideal as setting up a secure VPN to the organization's internal network, then a secured login with mandatory multi-factor authentication to an intermediate host and another secure login inside the network that controls the critical infrastructure. Cisco SAFE for IoT also considers ta local VPN server (AnyConnect) for enabling remote access. NIST also provides some guidelines for remote access and Bring Your Own Device (BYOD) Security [90] too.

In the present state of the laboratory, TeamViewer is used for accessing all the devices, rather critical ones or normal ones. According to the mentioned notes, using TeamViewer is one of the shortcomings of the system. Replace such functionality with a local VPN/Proxy server would disable remote accessing through a third-part software and enable a more secure solution.

Alleviating the mentioned threats and shortcomings would approach the system to a more secure one. The following section as a response to the third question of this research, mentioned in section 1.1, would provide security measures and open-source alternatives for the proposed security architecture, figure 4.3 and 4.4.

4.3 Protective Measures

In this section, firstly, the concept of IP planning and assigning IPs based on the requirements of the system, as one of the mentioned shortcomings, are discussed. Following that, the experimented/suggested tools and services, and options for the open-source alternatives of Cisco proprietary security capabilities (Cisco ISE, TrustSec, Stealthwatch, Umbrealla, Advanced Malware Protection (AMP), cisco cyber Vision Assessment Services, and Anyconnect) are presented. The hardware alternatives for the proposed design, figure 4.4, are not considered as a part of this project. The discussed alternatives are the ones that were claimed to be commonly used in the industry, and implemented without a lot of complexity.

Table 5 provides an overview of the following sections and how the proposed alternatives are related to the four fonts of security proposed by Cisco SAFE [1] (Segmentation, Visibility and Analysis, Remote Access, and Services). The provided options in the following sections are meant to replace the Cisco-proprietary security capabilities, which are costly and mostly well-performed alongside the Cisco products (switches, routers, ...).

4.3.1 IP Planning

Since the number of connected people to the network, varies and different people need to gain access to the network, a DHCP has been already implemented inside the system. According to the need of the laboratory for having the highest estimate of 30 clients connected to the network, an IP subnet

[26] https://www.vice.com/en/article/akdqxk/why-cybersecurity-experts-hate-teamviewer-the-software"%2D"-used-to-tamper-with-florida-water-supply

[27] https://www.csoonline.com/article/3606714/oldsmar-cyberattack-raises-importance-of-water-utility"%2D"assessments-training.html?utm_campaign=organic&utm_content=content&utm_medium=social&utm_source=twitter

Subsection Number	Alternatives for	Purpose	Cisco-proprietary Capability
4.3.2	AAA Server	Segmentation	Cisco ISE
4.3.3	Management Server	Visibility and Analysis	Cisco Stealthwatch
4.3.4	NTP Server	Visibility and Analysis	-
4.3.5	IDPS	Visibility and Analysis	Cisco Stealthwatch
4.3.6	DNS Response Policy Zones	Visibility and Analysis	Cisco Umbrella
4.3.7	Secure Remote Access	Remote Access	Cisco AnyConnect
4.3.8	Endpoint protection	Remote Access	Advanced Malware Protection (AMP)
4.3.9	Vulnerability Detection	Services	Cisco Cyber Vision Assessment Services

Table 5: Overview of considered security capabilities with their subsection number and the equal Cisco-proprietary options

of thirty available hosts was dedicated for the manufacturing zone. According to the predictions of the maximum connected devices to each segment, the IP planning and creating different subnets have been done for the entire network and examples of them have been presented in figure 4.4 (due to security reasons the exact IP addresses are not provided in the figure.)

DHCP reservation - assigning specific IP addresses to specific MAC addresses, for the sensitive components, such as the OPC UA server and Kuka Controller, that are know for the components based on their IP addresses, is also applied. This would assist the consistency and availability of the network and those IP addresses would never be offered by the DHCP server to any other client, except the defined ones. DHCP reservation, alleviates the consequences of DHCP flood and starvation attack, mentioned in section 2.10.1 (the spoofing attacks are treated by a wireless LAN controller, discussed in section 4.1.4.)

4.3.2 Alternatives for AAA Server

The OPC Foundation and CISCO SAFE emphasize on the fact of Authentication, Authorization, and Accounting. Instead of Using Cisco ISE as one of the most expensive products in the market, open-source alternatives were tried to be investigated. During the investigation FreeRADIUS has shown a lot of attention in the market. As the developers point it out [28], FreeRadius is the main Open source RADIUS server and the world's most popular one. As jumpcloud [29] compares FreeRADIUS and Cisco ISE, both solutions technically enable RADIUS protocol. There are multiple choices as a FreeRADIUS GUI and daloRADIUS [30] is one of the easiest solutions [31].

[28] https://networkradius.com/technology/overview/
[29] https://jumpcloud.com/blog/freeradius-vs-cisco-ise
[30] https://github.com/lirantal/daloradius
[31] https://www.cloudradius.com/is-there-a-freeradius-gui/

4.3.3 Alternatives for Management Server

Cisco Stealthwatch which has integrated a number of features, such as IDPS, inside one server is Cisco's solution as a network management technology. There are a number of management servers in the market. Zabbix [32] has been installed in many networks and has become an important player on a market [91]. There is a comparison between Cisco Stealthwatch and Zabbix available by IT Central Station [33], in which obviously number of available features by Cisco stands out. It is also noted that Zabbix is easy to install and manage, stable, and scalable. There has been an effort to initiate it as an appliance (on a VMware platform) that proved the ease of initialization.

4.3.4 Alternatives for Network Time Protocol

The current system suffers from unsynchronized time. The clients have difference in their times not only by seconds, but by some minutes. As a starting point for time synchronization, an NTP server could be implemented on the existing server. The clients could have the address of the NTP server either being set manually or provided by the DHCP server. A DHCP server provides a number of options to the clients. The option 42 [34] would enable providing an IP address as the NTP Server. The NTP server, itself, could have its time synchronized with the NTP Pool [35] available in Norway [36]. Since there are not many components within the system, it is preferable to have the address of the NTP server set manually on the clients and provide the option on the DHCP server for whoever is being introduced to the system newly and temporarily.

4.3.5 Alternatives for IDPS

Studying different open-source options for Intrusion Detection systems, Isa and his colleagues have published a comprehensive performance assessment on open source intrusion detection system [92], referring to three different articles [93, 94], name two major products in the open source area. Of these, Snort [37] has the most dominant market share, and Suricata [38] is one of its rivals. According to a talk to security expert Snort was highly recommended as an open-source solution of IDPS. Therefore, a preliminary testing, installing and initializing of it has been done.

4.3.6 DNS Response Policy Zones

Cisco Umbrella, formerly named as OpenDNS Enterprise service, facilitates the content filtering service. The devices are configured to use Umbrella as their DNS Servers. Umbrella operates as intermediate identity for the DNS requests, Cisco explain the functionality in more details [1, p.100-102].

Domain Name Service Response Policy Zones (DNS RPZ) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide responses to

[32] https://www.zabbix.com/

[33] https://www.itcentralstation.com/products/comparisons/cisco-stealthwatch_vs_zabbix

[34] http://networksorcery.com/enp/protocol/bootp/option042.htm

[35] A big virtual cluster of timeservers providing reliable easy to use NTP server for millions of clients, adapted from https://www.ntppool.org/en/

[36] https://www.pool.ntp.org/zone/no

[37] https://www.snort.org/

[38] https://suricata-ids.org/

queries [39]. RPZ could be set up in BIND Resolver on Debian/Ubuntu. Xiao Guoan has provided an implementation guide [40].

4.3.7 Alternatives for Secure Remote Access

Cisco offers AnyConnect VPN service to supply a secure remote access (VPN connection). An investigation of alternatives for such service is conducted. OpenVPN [95] has been used in different solutions [96, 97, 98]. It has also shown a solid and portable implementation, where clients can use standard sotware to connect to the real-time simulation system [96]. OpenNAC [41] has been attempted to be initiated inside the system. Since the latest update for it was in 2015, there were some problems with initiating it in the newer Operating systems (CentOS 8.3). On the other hand, OpenVPN has been initiated quiet easily and finely which eases the further investigation of it.

4.3.8 Client-based Anti-malware and Firewalls

In case of endpoint protection, SAFE for IoT [1] only mentions Anti-malware technologies. While in SAFE for campus networks [2], as a foundation of SAFE for IoT, it is expanded as client-based security. The client-based security includes Anti-malware, Anti-virus, cloud security, and personal firewall [2, p.10]. It is preferable to consider all the mentioned technologies, except the cloud security which is not a part of the current and desired architecture. There are already some consideration taken by the project owners. Thus, this part of security measures is not emphasized on. Nonetheless, assuring the healthy performance of personal firewall and anti-virus of all client devices is noteworthy.

4.3.9 Detected Vulnerabilities

As it was mentioned in section 3.2.4, services such as Penetration testing and vulnerability assessment provide a better perspective of the system. After scanning all the clients of the network using Nessus basic network scan, severity base CVSS v3.0 [99], 57 vulnerabilities were found. It should be noted that there are some devices connected to the network, as a temporary user. The severity of the founded vulnerabilities is presented in figure 4.6.

[39] https://dnsrpz.info/

[40] `https://www.linuxbabe.com/ubuntu/set-up-response-policy-zone-rpz-in-bind-resolver-on-debian-ubuntu`

[41] `https://sourceforge.net/projects/opennac/`

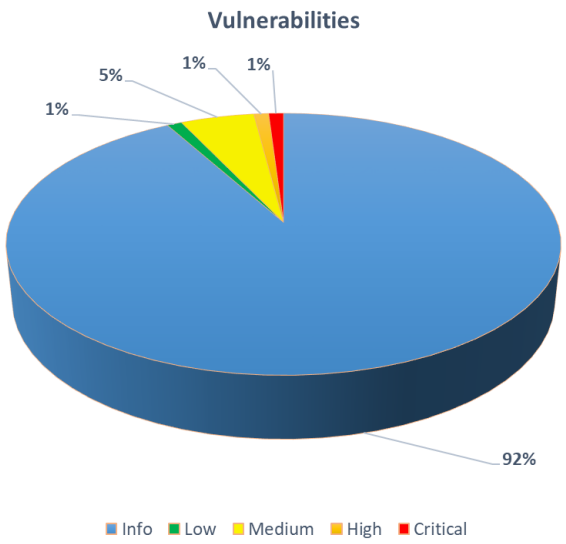


Figure 4.6: The percentage of criticality of detected vulnerabilities using Nessus basic network scan

Due to security reasons the details about the detected vulnerabilities are not noted here. Nonetheless, the details and solutions, which Nessus itself provides, are accorded to the project owners.

5 Discussion

This section presents the discussions about the the project. The significance of network architecture and a secure one is discussed firstly. Thereupon, the open-source alternatives of security capabilities, required devices, and how to improve the overall system is debated.

5.1 A secure network architecture

Cisco SAFE approach focuses on defense-in-depth approach for securing both the business flow and the TCP/IP protocol suite. Generally, network architecture is the bed of the TCP/IP protocol suite. In other words, a network architecture is required to have TCP/IP perform upon it. Cisco SAFE clears the fact that having a secure architecture priors securing TCP/IP protocol suite. To clarify this argument, assume the system as a car. In order to construct a safe (secured) car, building strong (secured) chassis is prior to strong functionality, like doors and ECU. Secondly, chassis are designed to contain the potential of having strong functionality (components), such as bullet-proof doors and glasses, mounted on them. In other words, the relation between the functionality and chassis is mutual. Therefore, no strong functionality without a strong chassis is useful and efficient and the chassis itself should contain the potential of holding strong components.

In the sense of network architecture and TCP/IP protocol suite, a secured and efficient network architecture which considers security of TCP/IP is prior to securing TCP/IP. If a network architecture itself is not well-designed and secured, then no security capability (firewall, IDS/IPS, Encryption, Integrity service, ...) is efficient and functional enough.

Therefore, the need for a well-established network architecture, the level of complexity and inter-connectivity of the networks is tangible. This issue is not newly discussed and for many years it has been faced and sought to be resolved. Thus, starting from the scratch trying to design a secure network architecture which results in a secure system in general, is time consuming and requires a vast area of knowledge which does not suit the scope of the project (approximately four months) and the knowledge of the author; alternatively stated, utilizing a number of standards, guidelines, policies, and risk assessments and building a secured system from the scratch. Furthermore, the defined project is meant to take actions and aid the client (The department of Industrial Engineering) in practice. Hence, the effort is going through the conceptual parts as early as possible and yield actions. For this purpose, Cisco SAFE was enabled to accelerate the process from analysis to implementation. Since security lives as a life-cycle, the next cycles would improve the establishments too.

Cisco SAFE has provided a generalized template, including a network architecture and security capabilities for general use-cases/business flows. Standing on the shoulder of giants and more importantly, the fact that building a system that is commonly acceptable and used in the Industry, brings us to the existing trend. This project would credit Cisco SAFE as a standing point. Utilizing Cisco SAFE method (architecture), adjusting it based on the need of the project provide, and applying computer networking backgrounds, established the proposed network architecture including proposed security capabilities.

5.2 Open-source security capabilities

The ongoing effort of establishing the suggested system is notable. Cisco has suggested its proprietary technologies for the mentioned four fonts of overcoming threats (segmentation, visibility and analysis, remote access, services). An investigation of open-source alternatives has been done, which could become enhanced and more extensive. Benchmarks of different alternatives provide constructive aid to select the best option. Nevertheless, it is required to implement and test the efficiency of such choices for the specific CPS of this project. Although all networks share common properties of data and data patterns, each network could have a specific type or pattern of data differentiate the network. New tools and options are introduced on a daily basis, and there could be alternatives that perform optimally for special scenarios.

Thus, a more extensive investigation of open-source security capabilities to enhance the security system would be named as a noteworthy further work.

5.3 Required Devices

In order to fully accomplish the implementation of the proposed design, there is a need for purchasing the proposed devices, the firewall(s), access points, wireless LAN controller and switches. The firewall(s) is required to improve the segmentation font of Cisco SAFE and alleviating the discussed shortcoming regarding the absence of network traffic controlling. Access points and switches are required for the connectivity of the devices and the wireless LAN controller enables handling multiple access points and rouge access point detection.

This scope of work due to its complexities was not covered during this project. The process requires a strong interaction with the department of industrial engineering. Moreover, the procedure is time-consuming in both sense of evaluation of alternatives, and receiving the purchased alternative. Furthermore, analyzing the network traffic and grasping the details of it would provide

insight on features that a firewall should own. Hence, enabling network analysis and management services before finalizing any alternative for firewalls is an asset.

As the result, a thorough assessment of options for each type of device would be required to approach the proposed network architecture excellently.

5.4 Security life-cycle

Last but not least, securing a system never ends. More cycles of the security life-cycle, as proposed in section 3.3 is essential to provide a more secure system at all time. New standards, best practices, and threats are introduced daily. Also, business needs could vary over time. The process of securing a system never ends and devoting time and effort to cybersecurity is an inevitable principle. It could be observed in CISSP [82], as one of most the valid security certificates, that a large scope of the book is dedicated to establishing teams and managing them.

6 Conclusion

This thesis emphasizes on a network architecture and states three questions to approach a secure cyber-physical system for the existing one in the department of industrial engineering at UiT campus Narvik. The questions are: what a secure CPS architecture is, how far the current state of system is from the defined secure architecture, and how to reach the proposed architecture. The emphasize of the project is on the first question and proposing a secure robust network architecture. Because, such architecture would ease identifying the security level of the current state and the required security measures to improve it.

There are already some device hardening and endpoint security measures have been performed in the network. Although device hardening or any security measures which are related to the application layer of TCP/IP protocol suite (the higher layers) is a positive step toward security, they would not be efficient and practical enough to make a system secure, unless the network architecture is secure. A network architecture is the bed of the TCP/IP protocol suite. Therefore, owning a secure network architecture priors to any other actions for securing the protocols or applications executing over it.

As a fundamental step, this project has suggested a secure architecture based on Cisco SAFE approach for IoT. Cisco SAFE is easy-to-use, intuitive, and includes examples and clear explanations. The whole of security for the system has been categorized in four fonts, segmentation, visibility and analysis, remote access, and services. In other words, all the security measures considered in this project are related to either one or more of the fonts. The result is a secure network architecture, focusing on the availability principle of security, containing security capabilities that are placed correctly in different segments of the network. Due to need of the project owner and the fact that spending money is not favorable for them, all the suggested security capabilities are intended to be open-source. Therefore, an investigation of the open-source alternatives for each security capability is performed and presented.

A secure network architecture establishes a base in which security is acceptable. Comparing the current architecture of the system with the proposed one besides utilizing the computer networking fundamentals, resulted in identifying the six notable shortcomings of the current architecture. Based on the identified flaws and computer networking fundamentals, the required technologies and changes to the architecture, in order to enhance the security of the system, have been discussed as the final part of this thesis. Precisely, nine distinguished security measures are noted.

The everlasting procedure of securing a system mandates considering a life-cycle. Business needs, threats, and solutions vary from time to time. Therefore, the selected security life-cycle of this project would aid in constructing a durable and robust cyber-physical system.

References

[1] Cisco, "Iot threat defense for manufacturing, safe design guide, security domain: Threat defense." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/iot-threat-defense-mfg-design-implementation-guide.pdf`, 2018.

[2] Cisco, "Safe architecture guide, places in the network: Secure campus." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-architecture-guide-secure-campus.pdf`, 2018.

[3] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & information systems engineering*, vol. 6, no. 4, pp. 239–242, 2014.

[4] M. Research, "Industrial iot (iiot) market by component, application (robotics, maintenance, monitoring, resource optimization, supply chain, management), industry (aerospace, automotive, energy, healthcare, manufacturing, retail), and geography - global forecast to 2027," Jun 2020.

[5] B. Ervural and B. Ervural, *Overview of Cyber Security in the Industry 4.0 Era*, pp. 267–284. 09 2018.

[6] T. J. Williams, "The purdue enterprise reference architecture," *Computers in Industry*, vol. 24, no. 2, pp. 141–158, 1994.

[7] ENISA, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*. 11 2018.

[8] M. Saturno, V. M. Pertel, F. Deschamps, and E. Loures, "Proposal of an automation solutions architecture for industry 4.0," in *24th International Conference on Production Research, Poznan, Poland*, 2017.

[9] N. NIST, "Special publication 800-53a revision 4," *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, 2014.

[10] K. Dempsey, P. Eavy, and G. Moore, "Automation support for security control assessments: Volume 1: Overview.(national institute of standards and technology, gaithersburg, md), nist interagency or internal report (ir) 8011," 2017.

[11] Cisco, "Safe overview guide - threats, capabilities, and the security reference architecture." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf`, 2018.

[12] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," 2015-06-03 2015.

[13] L. Obregon, "Secure architecture for industrial control systems," *SANS Institute InfoSec Reading Room*, 2015.

[14] B. Morgan and J. Ball, *CCNA Collaboration CIVND 210-065 Official Cert Guide: CCNA Col CIVND 210-06 OCG_c1*. Cisco Press, 2015.

[15] D. Hucaby, *CCNP Routing and Switching SWITCH 300-115 Official Cert Guide: Exam 38 Cert Guide*. Cisco Press, 2014.

[16] K. Wallace, *CCNP routing and switching ROUTE 300-101 official cert guide*. Cisco Press, 2015.

[17] S. Convery, *Network security architectures*. Cisco Press, 2004.

[18] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 01 2018.

[19] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," *IEEE Network*, vol. 27, no. 1, pp. 19–24, 2013.

[20] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212 – 223, 2018.

[21] C. Cheh, *Protecting critical infrastructure systems using cyber, physical, and socio-technical models*. PhD thesis, University of Illinois at Urbana-Champaign, 2019.

[22] H. Niu and S. Jagannathan, "Optimal defense and control of dynamic systems modeled as cyber-physical systems," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 423–438, 2015.

[23] H. Li, M.-Y. Chow, and Z. Sun, "Optimal stabilizing gain selection for networked control systems with time delays and packet losses," *IEEE Transactions on Control Systems Technology*, vol. 17, no. 5, pp. 1154–1162, 2009.

[24] H. Xu, S. Jagannathan, and F. L. Lewis, "Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses," *Automatica*, vol. 48, no. 6, pp. 1017–1030, 2012.

[25] M. Shrestha, C. Johansen, and J. Noll, "Criteria for security classification of smart home energy management systems," in *Advances in Smart Technologies Applications and Case Studies* (A. El Moussati, K. Kpalma, M. Ghaouth Belkasmi, M. Saber, and S. Guégan, eds.), (Cham), pp. 157–165, Springer International Publishing, 2020.

[26] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 28, p. 100342, 2020.

[27] M. Shrestha, C. Johansen, M. D. Moghadam, J. Johansen, and J. Noll, "Tool support for security classification for internet of things (long version)," *Research report http://urn. nb. no/URN: NBN: no-35645*, 2020.

[28] I. Garitano, S. Fayyad, and J. Noll, "Multi-metrics approach for security, privacy and dependability in embedded systems," *Wireless Personal Communications*, vol. 81, no. 4, pp. 1359–1376, 2015.

[29] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity version 1.1," 2018.

[30] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*, pp. 363–369, IEEE, 2008.

[31] M. Krugh and L. Mears, "A complementary cyber-human systems framework for industry 4.0 cyber-physical systems," *Manufacturing Letters*, vol. 15, pp. 89–92, 2018. Industry 4.0 and Smart Manufacturing.

[32] S. W. G. of OPC Foundation *OPC Foundation, Whitepapaer*, 2018.

[33] O. Foundation, "Practical security recommendations for building opc ua applications," 2018.

[34] V. Souza, R. Cruz, W. Silva, S. Lins, and V. Lucena, "A digital twin architecture based on the industrial internet of things technologies," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–2, IEEE, 2019.

[35] J. Imtiaz and J. Jasperneite, "Scalability of opc-ua down to the chip level enables "internet of things"," in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pp. 500–505, IEEE, 2013.

[36] H. S. Oluwatosin, "Client-server model," *IOSRJ Comput. Eng*, vol. 16, no. 1, pp. 2278–8727, 2014.

[37] N. Ando, T. Suehiro, K. Kitagaki, T. Kotoku, and W.-K. Yoon, "Rt-middleware: distributed component middleware for rt (robot technology)," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 3933–3938, IEEE, 2005.

[38] H. Arnarson, B. Solvang, and B. Shu, "The application of open access middleware for cooperation among heterogeneous manufacturing systems," in *2020 3rd International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*, pp. 1–6, 2020.

[39] J. Wack, K. Cutler, and J. Pole, "Guidelines on firewalls and firewall policy," tech. rep., BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2002.

[40] S. M. Bellovin and W. R. Cheswick, "Network firewalls," *IEEE communications magazine*, vol. 32, no. 9, pp. 50–57, 1994.

[41] G. Tsirtsis and P. Srisuresh, "Network address translation-protocol translation (nat-pt)," 2000.

[42] P. V. Mockapetris, "Rfc1035: Domain names-implementation and specification," 1987.

[43] K. A. Scarfone and P. M. Mell, "Sp 800-94. guide to intrusion detection and prevention systems (idps)," 2007.

[44] L. Andersson and T. Madsen, "Provider provisioned virtual private network (vpn) terminology," 2005.

[45] S. Cybersecurity, V. Clifton, and R. Hat, "Guide to ipsec vpns," *NIST Special Publication*, vol. 800, p. 77, 2020.

[46] K. McKay and D. Cooper, "Guidelines for the selection, configuration, and use of transport layer security (tls) implementations," 2019-08-29 2019.

[47] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Rfc2865: Remote authentication dial in user service (radius)," 2000.

[48] K. Zeilenga *et al.*, "Lightweight directory access protocol (ldap): Technical specification road map," tech. rep., RFC 4510, June, 2006.

[49] "Ieee standard for local and metropolitan area network–bridges and bridged networks," *IEEE Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014)*, pp. 1–1993, 2018.

[50] C. Metz, "Aaa protocols: authentication, authorization, and accounting for the internet," *IEEE Internet Computing*, vol. 3, no. 6, pp. 75–79, 1999.

[51] H.-G. Hegering, S. Abeck, and B. Neumair, *Integrated management of networked systems: concepts, architectures and their operational application*. Morgan Kaufmann, 1999.

[52] R. Boutaba and J. Xiao, "Network management: State of the art," in *IFIP World Computer Congress, TC 6*, pp. 127–145, Springer, 2002.

[53] D. Mills, J. Martin, J. Burbank, and W. Kasch, "Network time protocol version 4: Protocol and algorithms specification," 2010.

[54] D. Mills, "Simple network time protocol (sntp) version 4 for ipv4, ipv6 and osi," tech. rep., RFC 2030, October, 1996.

[55] D. Reilly, H. Stenn, and D. Sibold, "Network time protocol best current practices," *Work in Progress, draft-ietf-ntp-bcp-00*, 2017.

[56] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39 – 50, 2015.

[57] R. Droms *et al.*, "Dynamic host configuration protocol," 1997.

[58] J. Postel *et al.*, "User datagram protocol," 1980.

[59] M. Aldaoud, D. Al-Abri, A. Al Maashri, and F. Kausar, "Dhcp attacking tools: an analysis," *Journal of Computer Virology and Hacking Techniques*, pp. 1–11, 2021.

[60] Y. Bhaiji and C. Systems, "Layer 2 attacks and mitigation techniques.," 2006.

[61] E. Vyncke and C. Paggen, *Lan switch security: what hackers know about your switches*. Cisco Press, 2007.

[62] D. Al Abri, "Detection of mitm attack in lan environment using payload matching," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1857–1862, IEEE, 2015.

[63] U. Meyer and S. Wetzel, "A man-in-the-middle attack on umts," in *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 90–97, 2004.

[64] H. Arnarson, "Digital twin simulation with visual components," Master's thesis, UiT Norges arktiske universitet, 2019.

[65] B. Claise, G. Sadasivan, V. Valluri, and M. Djernaes, "Cisco systems netflow services export version 9," 2004.

[66] D. Savage, J. Ng, S. Moore, D. Slice, P. Paluch, and R. White, "Cisco's enhanced interior gateway routing protocol (eigrp)," in *RFC Editor*, 2016.

[67] A. Headquarters, "Cisco safe reference guide," 2009.

[68] Cisco, "Safe architecture guide, places in the network: Secure branch." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-branch-architecture-guide.pdf`, 2018.

[69] Cisco, "Safe architecture guide, places in the network: Secure data center." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-secure-dc-architecture-guide.pdf`, 2018.

[70] Cisco, "Safe architecture guide, places in the network: Secure internet edge." `https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-architecture-guide-pin-secure-internet-edge.pdf`, 2018.

[71] Cisco, "Safe architecture guide, places in the network: Secure cloud." `https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/safe-secure-cloud-architecture-guide.pdf`, 2019.

[72] Cisco, "Safe architecture guide, places in the network: Secure internet." `https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/safe-secure-cloud-architecture-guide.pdf`, 2019.

[73] T. J. Williams, "The purdue enterprise reference architecture," *Computers in industry*, vol. 24, no. 2-3, pp. 141–158, 1994.

[74] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial iot devices," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 519–524, IEEE, 2016.

[75] A. Richter and J. Wood, *Practical Deployment of Cisco Identity Services Engine (ISE): Real-world Examples of AAA Deployments*. Syngress, 2015.

[76] B. McKenna, "Measuring cyber-risk," *Network Security*, vol. 2018, no. 10, pp. 12–14, 2018.

[77] E. McMahon, M. Patton, and S. Samtani, "Benchmarking vulnerability assessment tools for enhanced cyber-physical system (cps) resiliency," pp. 100–105, 11 2018.

[78] R. Lacoste and K. Wallace, *CCNP Routing and Switching TSHOOT 300-135 Official Cert Guide: Exam 39 Cert Guide*. Cisco Press, 2014.

[79] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS workshop on future directions in cyber-physical systems security*, pp. 22–24, Citeseer, 2009.

[80] D. C. Plummer *et al.*, "Ethernet address resolution protocol: Or converting network protocol addresses to 48. bit ethernet address for transmission on ethernet hardware.," *RFC*, vol. 826, pp. 1–10, 1982.

[81] P. Cheremushkin and S. Temnikov *Kaspersky Lab ICS CERT*, 2018.

[82] R. Abernathy and T. McMillan, *CISSP Cert Guide (3rd Edition)*. Indianapolis, Indiana, USA: Pearson IT Certification, 3rd ed., 2018.

[83] T. McGuiness, "Defense in depth," *SANS Institute InfoSec Reading Room. SANS Institute*, 2001.

[84] J. A. Dominguez, "An overview of defense in depth at each layer of the tcp/ip model," *SANS Institute InfoSec Reading Room. SANS Institute and GIAC certifications*, 2002.

[85] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, and S. R. Sharma, "Guide to ipsec vpns:.," 2005.

[86] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," in *MILCOM 2007-IEEE Military Communications Conference*, pp. 1–7, IEEE, 2007.

[87] S. Santra and P. P. Acharjya, "A study and analysis on computer network topology for data communication," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 1, pp. 522–525, 2013.

[88] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[89] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[90] M. Souppaya and K. Scarfone, "Guide to enterprise telework, remote access, and bring your own device (byod) security," *NIST Special Publication*, vol. 800, p. 46, 2016.

[91] A. Shokhin, "Network monitoring with zabbix," 2015.

[92] F. M. Isa, S. Saad, A. F. A. Fadzil, and R. M. Saidi, "Comprehensive performance assessment on open source intrusion detection system," in *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)*, pp. 45–51, Springer, 2019.

[93] S. Chakrabarti, M. Chakraborty, and I. Mukhopadhyay, "Study of snort-based ids," in *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, pp. 43–47, 2010.

[94] A. Saboor, M. Akhlaq, and B. Aslam, "Experimental evaluation of snort against ddos attacks under different hardware configurations," in *2013 2nd National Conference on Information Assurance (NCIA)*, pp. 31–37, IEEE, 2013.

[95] J. Yonan, "Openvpn: An open source ssl vpn solution," *http://openvpn. net/*, 2008.

[96] J. Liu, Y. Li, N. Van Vorst, S. Mann, and K. Hellman, "A real-time network simulation infrastructure based on openvpn," *Journal of Systems and Software*, vol. 82, no. 3, pp. 473–485, 2009.

[97] P. Likhar, R. S. Yadav, *et al.*, "Securing ieee 802.11 g wlan using openvpn and its impact analysis," *arXiv preprint arXiv:1201.0428*, 2012.

[98] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Experimental performance comparison between tcp vs udp tunnel using openvpn," in *2015 International Conference on Computing, Communication and Security (ICCCS)*, pp. 1–5, 2015.

[99] C. Team, "Common vulnerability scoring system v3. 0: Specification document," *First. org*, 2015.