UNIVERSITY OF TURKU

Software-defined zero-trust network architecture

Evolution from Purdue model -based networking

Cyber Security / Faculty of Technology

Master's thesis

Author:

Patrik Svensberg

Supervisor(s):

D.Sc. (Tech) Antti Hakkala

Prof. Jouni Isoaho

7.5.2023

Turku

Master's thesis

Subject: Cyber Security
Author(s): Patrik Svensberg
Title: Software-defined zero-trust network architecture: Evolution from Purdue model -based networking
Supervisor(s): D.Sc. (Tech) Antti Hakkala, Prof. Jouni Isoaho
Number of pages: 71 pages
Date: 7.5.2023

Digitalization has brought many technological developments which improve the business operations on many industries. In recent years, the drive towards service-based solutions has superseded the locally managed solutions towards vendor-managed solutions that are managed through the Internet. Unfortunately, the architecture, and the infrastructure which it is based on, have not developed at the same pace. This has led to organizations undermining the architecture and policies designed for it. Therefore, a modern architecture is needed with the capability of supporting these uprising technologies. The objective of this thesis was to find out if Purdue model works as a valid reference architecture for building networks in today's standards, and if it needs to be replaced, what would be the alternatives.

To answer the research question, it was first investigated whether Purdue model can be used for modern network architecture. After that, a literacy review was performed to see what some of the current and modern recommendations are. The literacy review also included research on what some of the current threats to digital platforms are, and how cybersecurity is engineered.

It was discovered that zero-trust architecture and software-defined solutions enhance the overall security and management of the operating environments. The thesis concludes with a logical reference architecture for networks as a suggested solution. The suggested solution is a new network architecture that implements the elements of zero-trust and uses software-defined networking to manage the underlying infrastructure.

Key words: cyber security, zero-trust, architecture, network segmentation, software-defined networking, policy-based security, Purdue model

Table of contents

Table of Figures

Abbreviations

AAA	An authentication, authorization, and accounting framework used in computer networks to manage and monitor accesses according to applied policies. (Farris et al., 2019)
APBSA	Authorization Policy-based Security Architecture is a network architecture which aims to distinguish different network flows to create path and flow-based policies. (Karmakar et al., 2020)
API	Application Programming Interface is used to accomplish computer-to-computer generated communication. (Check Point, 2020)
BYOD	Bring-your-own-device is an operational model where employees can use their own devices within the corporate network to do their work-related tasks.
CIA	The confidentiality, integrity, and availability triad is commonly used as the foundation for developing cybersecurity. (Fruhlinger, 2020)
CSP	Cloud Service Provider is an entity that provides various cloud services.
DOS	Refers to Denial-of-Service type of attack where an attacker aims to deny access to a service.
DMZ	Demilitarized zone refers to a network segment that connects the managed and controlled network to the unmanaged network, such as the Internet.
IDS	Intrusion detection systems aim to detect malicious activities in the underlying network that is being monitored.
IOT	Internet of Things refers to network devices that are integrated into physical operations, such as mechanical valves and sensors.

ISA	Integrated Security Architecture is a network architecture which utilizes different network flows to create path and flow-based policies in a software-defined network environment. (Karmakar et al., 2020)
IT	Information Technology refers to the processing of information for developing and managing business operations. (Ross et al., 2021)
NFV	Network Function Virtualization refers to the decoupling of software from hardware. This means that network functions, such as routing or switching, are not dependent on any specific hardware. (Lina & Dongzhao, 2020)
OSI	The Open Systems Interconnection model sets computer systems into physical, data link, network, transport, session, presentation, and application layers. (Linthicum, 2020)
OT	Operational Technology refers to physical operations and production. (Ross et al., 2021)
SAAS	Software-as-a-Service type of solutions aim to simplify the operating environments by providing software that aims to centralize control and increase overall manageability.
SCADA	Supervisory Control and Data Acquisition systems provide a centralized monitoring and control system for various processes. SCADA systems collect, transfer, and present information for monitoring or controlling an entire system from a central location in near real time. (Stouffer et al, 2015)
SDN	Software-Defined Networking is a technology that separates the control logic from the network equipment by having a centralized controller that controls the state of the network equipment. (Kreutz et al., 2015)
SIEM	Security information and event management systems monitor and analyze security events in the organization. The purpose is to

	increase the capability to respond to security incidents. (Rose et al., 2020)
VLAN	Virtual Local Area Network refers to virtual subnets that are used to segment the underlying network for more clarity and manageability.
VPN	Virtual Private Network is a separate virtual network for connecting an end-device to a resource over the public network. This forms a private network that masquerades the ongoing network traffic.

1 Introduction

In recent years, there has been a great shift in many industries to move resources into cloud for increasing their availability and reducing the costs related to locally managed solutions. For a long time, traditional network solutions worked well for delivering and hosting a variety of applications and services. As a rule, companies managed their own infrastructure, devices, and the software running on them locally. Today, however, cloud-managed applications and solution are replacing on-premises solutions because they are not nearly as convenient for answering the business needs of the companies.

In addition, with the cloudification, employees are no longer forced to work on premises. Instead, companies are offering the possibility for their employees to choose where they want to work, be it remotely from home or somewhere else. This means that flexible network solutions are required to manage the security risks associated with the change.

This paradigm shift, from having locally managed resources to expanding the network perimeter with those resources being on the Internet and employees of the companies working from uncontrolled places, has posed significant security related challenges. With cloudification and network perimeter expanding, the companies are challenged with losing control over their infrastructure. The loss of control means that the risk factors are increasing because the security cannot be guaranteed to the same level as with on-premises solutions.

To answer these challenges, it is not sufficient to just implement solutions that try to solve singular problems. A new architecture is needed that supports modern solutions and answers to security related challenges brought up by trending technologies. The evolution of technologies that have expanded the network perimeter has been faster than organizations being able to adapt to the fundamental changes that those technologies have caused.

For the background of this thesis, a well-known enterprise architecture called the Purdue model is used as an example architecture. The Purdue model was developed in the 1990s and has been widely adopted as a reference architecture in many industries. For this reason, and also because the model being quite old already, it works as a great example architecture for this thesis, especially in a situation where the Purdue model is used as a solution for building network segments.

The purpose of this thesis is to research and identify whether a network architecture based on the Purdue model is still viable for modern day technologies, and what would be the

alternative that supports current trends. The aim is to design and present a solution that develops the network architecture from the Purdue model, moves away from straightforward and generic security domains and their implementations, and implements zero-trust principles. The end result will be a logical network architecture that answers the research questions.

The key questions, which this thesis aims to answer, are whether the Purdue model still works a reference architecture for building networks, what would be the alternative, what are some common security challenges with modern technologies, and what are recommended solutions for those challenges. When designing a new network architecture, it is important to understand the limitations of the existing architecture and what challenges it faces. If the architecture is deemed unviable, implementing a new one will be easier because then the integrity can be guaranteed. Compared with implementing solutions to an existing architecture, the issues will inflate in time since there are fundamental issues with it. Especially, if the security policies and such are formed to cohere with the architecture.

The thesis discusses how cybersecurity is engineered, and how the current cyber threat landscape looks to provide background and insight into the topics that will be later presented in this thesis. For the research question, the thesis lists the various cybersecurity challenges with the Purdue model and modern technologies. After that, solutions are represented for each of these challenges and those are embodied to develop a cohesive network architecture. Finally, a logical network architecture is presented which features to-be implemented components and the changes that need to be made to a network architecture based on the Purdue model.

2 Understanding cybersecurity

Digitalization has tremendously improved the daily lives of people by bringing convenience and new possibilities. The societal infrastructures are supported by digital products and services which have increased the efficiency, availability, and stability of social services. The downside of digitalization is that all these digital systems are more or less reachable from anywhere. This is a considerable risk because it necessitates the need to secure those systems from malicious entities.

The number of cybersecurity threats and attacks have increased significantly in the last two decades, and it can be assumed that they will continue to increase. Of course, cybersecurity has also developed but it has to play catch-up with all the systems that are being digitalized, and with the new security threats that occur. Hackers keep finding vulnerabilities to exploit in various devices that are connecting to the Internet. This has led to the increase of spectrum in required security.

Security, and more specifically information security, has been relevant for centuries. Back in the day, security was built with physical measures. For example, banks used to have locked vaults that housed their valuables, and even further back in time, kingdoms had walls surrounding them to keep away unwanted parties. Kingdoms also had vaults that contained all the riches, which meant that the security was layered.

Cybersecurity has become relevant because many of the different valuable assets have been digitalized. For example, no longer do banks have physical vaults that house every customer's money. Instead, banks circulate money and are responsible for ensuring that they have a certain level of liquidity in case customers want to make withdrawals. Therefore, most of the money that is seen in bank accounts is digital and does not directly correlate to physical valuables.

Besides just these various social and financial services, among others, being digitalized, in most cases, these systems and services are also accessible via the Internet. The benefit of digitalizing these types of services is the efficiency and availability it provides, but this also means that the attack surface has become significantly bigger. With digitalized systems that are accessible from the Internet, there is a concern with the various vulnerabilities and malware. Therefore, in terms of cybersecurity, it is important to understand how these

vulnerabilities are exploited and how malware works. This is a crucial part in order to create security and protect from these threats.

2.1 Security engineering

One aspect of understanding cybersecurity fundamentals is to define security engineering. Security engineering is the process of designing various systems and applications to operate securely (Anderson, 2018). The desired outcome is to have these systems and applications be able to withstand different variables. To achieve this, there needs to be several assurance factors that guarantee the operational continuity in case an incident would occur.

Cybersecurity is one form of security engineering because it aims to secure the processes that involve various systems and applications. Whereas some security engineering aspects focus on physical security, cybersecurity is the digital equivalent. It aims to secure these systems and applications from malicious software, entities, and access, among other things.

Nowadays, security engineering is needed to keep social services and infrastructure safe, and in working order. As mentioned previously, societies, and more specifically social services, are built upon digital or digitally supported systems and applications. In recent years, this has increased more and more, which has made those systems quite critical and essential. With all these systems that handle personal information, medical records, finances, et cetera, they could be, and are, targeted by hackers to exploit and profit from them.

Targeted cyberattacks happen regularly nowadays. It is quite apparent because there are often articles on the news about data breaches, or a good example of this is the different service providers having warnings on their websites about scam emails targeting their customers. Wikipedia has a list of data breaches that have become public, and it shows how the number of breaches has increased over the years (List of data breaches, 2023). For a visual presentation of the amount of data breaches having increased, the blog post from Logan Strain has a picture showing how the data breaches increased steadily year-over-year (Strain, 2018).

Security engineering focuses on securing the processes which need to be secured, not just certain parts of it. Where cybersecurity is more related to digital assets and systems, there also needs to be security surrounding them. For example, a digital system with an access control will not guarantee security if there is no access policy. Then again, an access policy will not guarantee security if users do not understand the nature of resources they are accessing. So, on top of securing digital systems and applications, security engineering also applies to the

people using them. By providing security education, the users can be engineered to avoid and respond appropriately when an incident occurs.

When engineering cybersecurity, the typical security measures for digital systems include authentication, transaction integrity and accountability, fault tolerance, and message security and covertness. These can also be described as confidentiality(C), integrity(I), and availability(A). The CIA triad is commonly used as the foundation for developing cybersecurity (Fruhlinger, 2020).

From the CIA triad, confidentiality could be considered the most important. Many infrastructure-critical systems need to communicate with different endpoints to ensure and complete their operations. These communications need to be secured in a way that the information stays integral, and that it is only accessed by authenticated and authorized individuals. On top of that, because of the sensitive nature of the communication, it also needs to be kept secret from external entities. In other words, communications need to be encrypted.

The CIA triad is great as a basis for security, but when designing and implementing cybersecurity, it is crucial to understand all the various variables that are needed for securing a system. The level of required security is often defined by the purpose of the system and its criticality. Defining the purpose helps with assessing what type of access control is needed. The access control can be physical or digital, and in most scenarios, there is mix of both. The criticality of the system defines whether a high availability solution is required or not. With high availability systems and solutions, there are typically requirements for more fault-tolerant measures.

2.1.1 Security Layers

There is not a single solution or methodology that guarantees safety. When considering an enterprise, it includes various different assets which need to be secured. There are confidential information, facilities, business operations, employees, and many other things. Each of these variables serve different functions which have different security threats. For example, confidential information must be kept secret, facilities must keep unwanted individuals away, and employees need to understand how to operate securely. This means that each variable needs appropriate security measures to ensure business continuity.

Cybersecurity also does not have a single solution for every cyber threat, and each threat is different depending on what is being targeted. Therefore, cybersecurity is built upon layers.

By having layers in cybersecurity, it is easier and more manageable to implement different security solutions and mitigate different attack vectors.

The Open Systems Interconnection (OSI) model layers computer systems into the following layers: physical, data link, network, transport, session, presentation, and application (Linthicum, 2020). Each layer has its own purpose, and a way of creating security. The physical layer refers to physical components which require physical security measures such as fences and locks. The data link layer refers to the data and information being transmitted across the physical layer, and security measures here are for example firewalls and VPNs (Mullins, 2021).

The aim of these two layers is to deter intrusions. It is less likely that a security breach will occur when the initial requirements for it are increased. For example, a building with a fence is less likely to be robbed than a building without one.

The network and transport layers ensure that data and information get exchanged (Mullins, 2021). The network and transport layers typically have preventative measures of some sort, such as intrusion prevention systems and antivirus software. The session, presentation, and application layers aim to ensure accountability and integrity of the environment. In these layers, various sessions are managed, data is made presentable, and applications utilize that data (Mullins, 2021). For security, these layers typically include technologies such as SSL certificates and data encryption.

All the security measures that were mentioned above can be called security protocols. Security protocols are used to securely unify various systems that are commonly used. The purpose of these commonly used, or standardized, security protocols is to assure the confidentiality, integrity, and availability of communication between systems. By having standardized security protocols, it becomes easier to implement solutions that retain security while still guaranteeing interoperability.

Referring to the previously mentioned CIA triad, and how authentication could be considered the most important aspect, one can say that access control is one of the most important security protocols. Access control, whether it is physical or digital, is meant to manage who can and cannot access a resource that has limited accessibility. Physical access controls include things such as fences and locks whereas digital access controls refer to accounting, authentication, and authorization.

When discussing security protocols, it is important to mention distributed systems. A distributed system refers to the group of computers or systems that operate by sharing data between each other. A distributed system might be more efficient in data processing since it can allocate processing activities to other nodes in the system. This means that it is not reliant on a single node or entity to handle the processing. A good example would be an office environment. The network in the office forms one system that enables connectivity between resources. A workstation connected to that network is another system that needs to be authenticated in order to access other resources. The authentication of workstation is accomplished via a database that holds authorization details, and this is also another system. This means that an office environment could be considered as a distributed system. A centralized system in this example would be a single workstation with local credentials and a straight connection to the internet.

These distributed systems are very common and can be found in various forms. One of the most tangible examples would be how social services are supported by digital solutions in a society. People use their personal computers to visit websites where they can manage their banking or healthcare related things. That alone makes two different systems. In addition, there is the backend of the bank or healthcare provider which is formed by various systems, and each of those have security measures of some sort in place. Therefore, it is crucial to acknowledge what distributed systems are because they iterate the importance of security protocols and how security is layered.

2.1.2 Information and Operational Technologies

In security engineering, it is crucial to understand the nature of things being secured. Some systems might be more prone to certain types of threats than others. For example, a website has a higher risk of being targeted by a Denial-of-Service type of attack compared with some internal company resources. As mentioned previously, security layers aim to simplify cybersecurity by categorizing different variables in a way that they can be subjected to appropriate security measures.

One of the major categorizations, in terms of cybersecurity, is having assets and resources divided into information and operational technologies. The main difference between the two is that operational technology (OT) usually refers to physical operations and production, whereas information technology (IT) refers to the processing of information for developing

and managing business operations (Ross et al., 2021). Usually, the OT environments are more sensitive and mission critical for companies, and therefore require stricter security measures.

When talking about IT and OT, it is important to acknowledge the role of Internet of Things -devices in modern operational solutions. The usage of IoT devices has grown exponentially in recent years. Without mentioning all the consumer IoT devices, such as TVs, stereos, lights, even cars, many industries are using various IoT devices to support their business operations. However, the issue with IoT devices is that they are quite limited in their processing capabilities. IoT devices are usually designed for only performing certain tasks and operations which means that they cannot be programmed to do other things, such as encryption or antivirus operations.

The adaptation of IoT devices is a relatively new occurrence, and therefore the risks related to those are still quite unknown. One of the most significant risk factors, however, is the bridging of IT and OT that IoT devices bring. IoT devices do not operate standalone and more often are related to some service that is hosted and managed in the IT environment. This poses a risk from the operational perspective because usually OT environments contain business critical assets that need to be continuously operational, and any outage can cause serious monetary loss.

In the past, OT has been kept separate from IT because of its critical and sensitive nature. However, recently there has been a surge of desire to integrate IT and OT more and more together which has posed a security concern for OT environments. With all the rising technologies, ensuring business continuity by keeping IT separate from OT has become more challenging.

2.2 Modern cybersecurity

Part of understanding cybersecurity is to know what the most common threats and current industry standards are. Cybersecurity is constantly changing and being capable of protecting from security threats requires being up to date with modern security standards. Ransomware and crypto miners are just a couple of examples of how cyber threats have evolved. A few years ago, these threats were not that common, but as more and more services have digitalized, the more these threats have occurred and been perceived. It is not a surprise that most of these threats relate to money since cybercrime is often done for financial gain.

2.2.1 Current security threats

Cybersecurity measures and tools are built based on the threats that have previously occurred and that are currently observed, while also trying to be proactive. The most challenging part of this is to handle current and upcoming threats. This is because current threats might easily evolve based on their popularity, and responding to unknown attacks and threat vectors is difficult.

Fortunately, cyberattacks usually conform to certain types. There are limited possibilities for how cyberattacks would happen and operate. In most cases, they try to infect a target machine, and there are only a limited number of ways to achieve that. To infect a target machine, there needs to be some type of access to the machine and some type of infection method. These infection methods can vary but are often similar on a fundamental level.

Looking at cyber threat maps is a good way to find out what the most common infection methods are. Various cybersecurity vendors have cyber threat maps that show the number of threat events they have monitored. The counters of monitored events usually reset daily, so it shows the number of events for each day.

Based on Kaspersky's cyber threat map, the most common activities detected are on-access and on-demand scans which refer to basic antivirus malware scanning operations (Kaspersky, n.d.). The next most common are mail and web antivirus scans. All of these events have millions of hits which gives a good understanding of what the most common security threats are.

Based on Kaspersky's (n.d.) cyber threat map, it could be assumed that the most common threats are phishing attacks and adware. Even though Kaspersky (n.d.) lists on-access and on-demand scans as the highest monitored security event, these do not necessarily translate to malicious activity since there are many false positives. Phishing attacks and adware are more recognized instead because they do not have many different forms. Malicious domains are more easily recognized when compared with malicious file signatures.

Where Kaspersky's cyber threat map focuses on specific attack vectors and methods, FireEye and Check Point give more generic information (FireEye, n.d.; Check Point, n.d.). This information includes which industries are being targeted and what type of malware is being detected. According to Check Point (n.d.), the most targeted industries are education, government, and healthcare, and the most detected malware types are related to phishing and

backdoors. Of course, these can change but it is quite common that these types of malware are trending, and that these industries are being targeted, since the targets include sensitive information and attacks usually aim to gain financial benefits. FireEye (n.d.) also reports the most targeted industries and for them those include financial services, telecom, and insurance, among others, which reiterates the financial aspects of cybercrime.

When cybercrime is covered in the media, it usually relates to some sort of data breach, and how victim's data is held for a ransom or sold on the web. Data breaches are a result of a cyberattack where a malicious actor has gained unauthorized access to a system or a network, and has stolen private, sensitive, or confidential data. Data breaches are usually a result of systems being out of date with updates, insufficient access controls, the system getting infected with malware, or the system is directly targeted. There is a possibility that a data breach happens accidentally but usually there is malicious intent behind.

Data breach is an umbrella term in regard to security threats since it does not translate to any specific threat or an attack method. However, data breaches have increased in recent years because cybercriminals aim to gain monetary benefits by stealing the data and selling it or holding it for ransom. So, when it comes to modern cybersecurity, it is good to keep in mind that when security incidents happen, most often the target is the data.

Regarding current security threats, one of the most essential resources is the OWASP Top 10. OWASP Top 10 is a document of the most critical risks in cybersecurity gathered by a group of security experts. According to the document, in 2021, the most critical security risks were broken access control, cryptographic failures, injection, design failure, misconfiguration, outdated components, authentication issues, software integrity violations, and server-side request forgery (OWASP Top 10 team. 2021).

2.2.2 Trends

Some trends in cybersecurity were already briefly mentioned. The adaptation of IoT devices, the increase in data breaches because of cybercriminals seeking to gain monetary benefits, and ransomware becoming one of the most common types of malware are just a few examples of trends happening in the cyber space. Of course, when accounting cybersecurity as well, there are trending aspects on both sides of the spectrum.

On the cyber threat side, as earlier mentioned, ransomware has become one of the most common types of malware. Ransomware is a type of malware that will encrypt or block

access to files and data in an infected system and holds those for ransom. Ransomware can also spy on the activities happening in the system to steal or find incriminating information which could be used to extort the victim. Fundamentally, ransomware aim to hold some piece of information for a ransom to make the victim pay a fee to free that information.

Ransomware became quite notorious a few years back. In 2017, there was a ransomware called WannaCry which gained media attention because of it affecting many people (Fruhlinger, 2022). Because of its impact, it gave popularity for other ransomware to show up. However, due to the attention it received, antivirus methods were quick to develop solutions to counter them. Nowadays, antivirus vendors might even have specific solutions to keep certain file-storages unencryptable.

Besides antivirus solutions trying to answer popular security threats, there are also trends in the security side of things. Among other things, one of the major trends and buzzwords in security is the zero-trust model, which aims to create security by removing trust between subjects. Another trend in security, and in digitalization in general, are the Software-as-a-Service (SaaS) and software-defined solutions which have become quite popular. These solutions aim to simplify operating environments by centralizing control and increasing manageability.

One of the examples of SaaS and software-defined approaches is the adaptation of mobile solutions. These include the usage and integration of IoT devices, smartphones, personal computers, wearable technologies, and many others in business operations. Mobile platforms have become one of the most, if not the most, popular Internet-connected devices. Mobile platforms are so popular that they have impacted the way the Internet is used. The most tangible example of this is the many websites and applications that are designed to be mobile-friendly, or straight up designed mobile-first.

Considering the amount mobile services and devices that have gained popularity, one could assume that mobile malware will increase in the future. Especially with the surge of social media and banking applications, among multiple others, mobile devices have become quite essential for people in their daily lives. This unfortunately means that these mobile devices have become a so-called single point of failure. If people become too reliant on their mobile devices, it creates a significant security risk.

Lastly, considering that cybercrime is heavily related to money, the importance of malware and data breaches staying undetected is increasing. After all, the longer the attacker has access to an infected machine or environment, the more they are able to steal information from it. Based on this, one could assume that malware will develop to be more difficult to detect. Because cybercriminals often aim to gain monetary benefits, the malware needs to operate in a way that is undetectable, and in a way that will achieve them maximum profits.

3 Purdue model

As part of this thesis, the aim is to find out whether a network infrastructure based on the Purdue model is still viable. Therefore, in this chapter, an overview of the Purdue model and how it relates to networking is presented. This provides a basic understanding of what the background to the thesis is, and lays the foundation for highlighting the issues, and for finding possible solutions for those issues.

3.1 What is Purdue model?

The Purdue model is an enterprise reference architecture model that was developed in the 1990s by Theodore J. Williams with the members of the Purdue University Consortium. The Purdue Enterprise Reference Architecture, or PERA in short, is a structural model for Computer-Integrated Manufacturing, or in other words, a structural model for production processes that are controlled by computers (Check Point, 2021).

The Purdue model divides different enterprise functions and applications into six layers which define the criticality and control of the production infrastructure and how it should be secured. The Purdue model is specifically designed for industrial control system (ICS) security which includes physical processes, sensors, supervisory controls, operations, and logistics (Zscaler, n.d.).

3.2 How does Purdue model relate to networking?

Even though the Purdue model was originally created as an enterprise architecture reference model, it was adopted by ISA99 which is a standards committee for industrial automation and control systems security conspired of cybersecurity experts (International Society of Automation, n.d.). ISA99 used the Purdue model as a template to create a concept model for network segmentation in ICS environments. The purpose of the concept model is to show the interconnections and dependencies between different components and functions (Check Point, 2021).

ISA99 divides the ICS architecture into two zones, Information Technology (IT) and Operational Technology (OT). These two zones are then subdivided into six layers or levels from 0 to 5. The layers follow the Purdue model by having the most critical systems at layer 0 and the least controlled at layer 5. Typically, in the Purdue model, OT falls into the lower layers because it consists of critical infrastructure for controlling and monitoring the

operational processes, and IT is on the top layers. These layers are separated by a DMZ (demilitarized zone) which aims to increase security by separating the control and access of IT and OT (Check Point, 2021). The following Figure 1 shows how a typical environment in a Purdue model is structured.

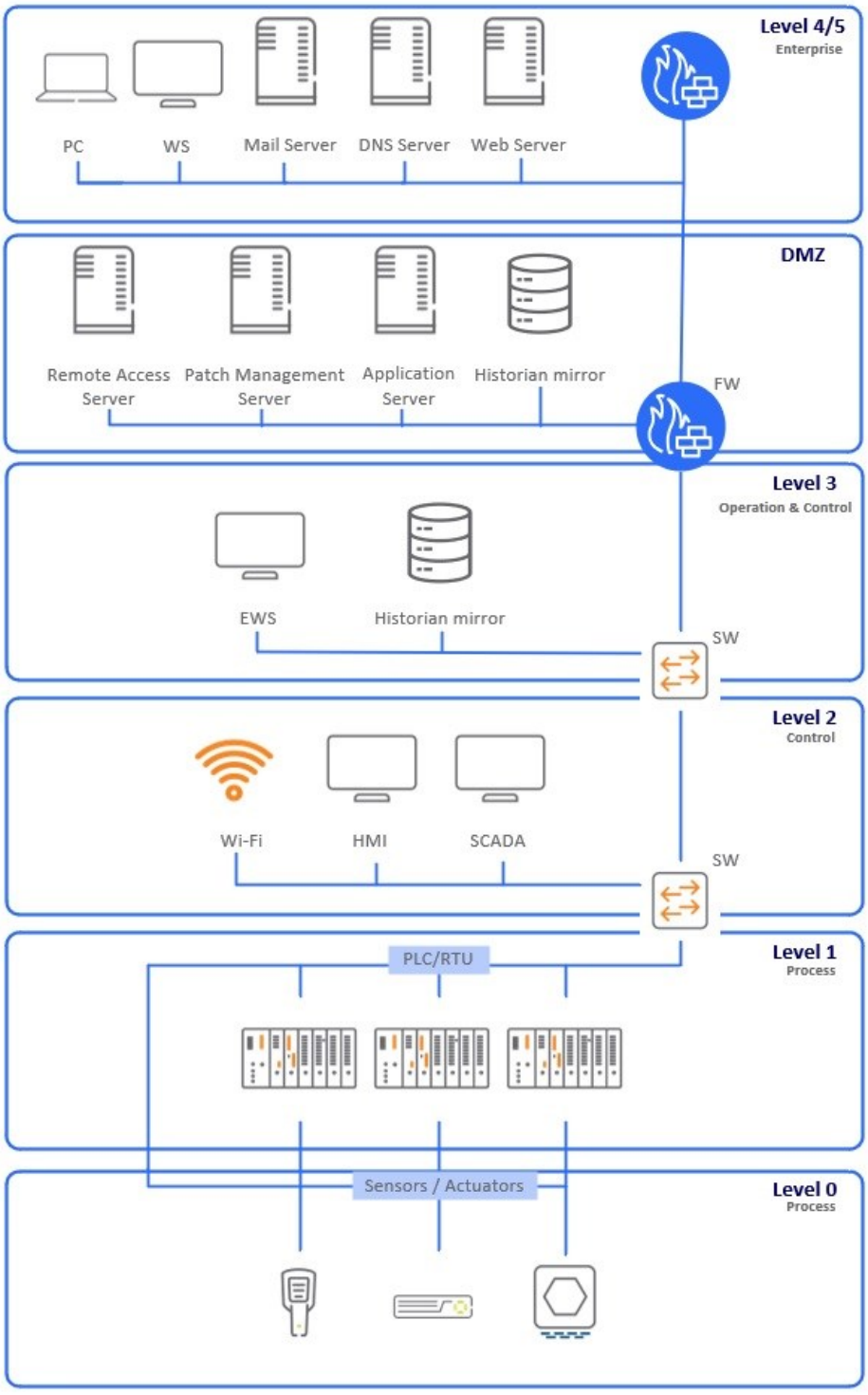

Figure 1 A basic render of the Purdue model (Zscaler. n.d.)

To further understand the structure of Purdue model's layering, here are the typical explanations for each layer:

Level 0: The physical process layer where the actual production happens. The physical process includes hardware, such as motors, pumps, sensors, valves, etc.

Level 1: Devices that monitor and send commands to the devices at Level 0. These include, for example, programmable logic controllers and remote terminal units.

Level 2: The process management layer where systems that control the whole process are located. For example, software and systems, such as supervisory control and data acquisition (SCADA), that allow human management and of the physical process.

Level 3: Management of the production workflow. Collects data from lower levels that can then be stored or forwarded to higher levels for IT operations. This is also the level where databases and domain controllers can be found.

Layer 3.5 (DMZ): This level creates a barrier between the IT and OT networks. Even though level 3 might have some parts of IT, generally, the DMZ is meant to separate OT from IT. The aim is to keep the environments separate so that it is less likely for IT, which is seen as less secure, to cause any disturbance for operations happening in OT.

Level 4: This level is solely for IT. In here, there are more databases, email servers, and other systems. Systems and devices at this level have some level controllability but because they are most likely connected to the Internet, it means that the controllability has decreased, and it makes them less secure.

Level 5: This level is called the enterprise network. In here, the data is collected from the IT and OT operations which is then used for making business decisions. From a network point of view, this level has the least control, and in some implementations, the company's cloud infrastructure, which is accessed via the Internet, belongs here.

(Check Point, 2021)

4 Challenges with Purdue model and modern technologies

Before trying to find a replacement model, it is important to understand the challenges with Purdue model and how it works with modern and trending technologies. More specifically, the focus is the challenges of using Purdue model as reference for network architecture, and the challenges posed by modern technologies, such as IoT and cloud, among others. First, it needs to be established that is Purdue model viable at all before proceeding to discuss challenges with modern technologies.

4.1 Is Purdue model still viable as a network architecture?

The Purdue model was developed in the 1990s when the capabilities of the Internet were largely unknown and undiscovered. There were of course some early signs which indicated its usefulness but such technological advancements as cloud, IoT, and X-as-a-Service were unobtainable.

Despite being over two decades old, the Purdue model is still widely used. The main reason is likely the hierarchy it creates in the environment and the lack of realizing the need for an overhaul. By having a hierarchical system that categorizes systems from least secure and the most critical to the least control over, it is possible to easily create an infrastructure that supports them. An infrastructure with separate levels for different components achieves a logical architecture which seemingly enables an easy scaling of operations. Moreover, creating access control based on network segmentation sets clear boundaries (Check Point, 2021).

Unfortunately, the Purdue model is starting to show age. Even though hierarchy creates logic in the architecture, it does not meet the expectations of some modern solutions. As mentioned above, technologies such as cloud, IoT, and X-as-a-Service have emerged since the development of the Purdue model, and they have become quite prevalent in modern business operations. More and more services are offered as a service.

When looking at the breakdown of the levels in the Purdue model, nowadays there are solutions such as the monitoring and control of components in the physical processes offered as a service. In these cases, the vendor is responsible for delivering the agreed solution but in order to do that, they will need access to the OT environment through the Internet because

they do not operate on the company premises or infrastructure. This creates a situation where devices from levels 0 and 1 need to be connected to the Internet.

Whereas the Purdue model aims to create security by setting clear boundaries for each layer by categorizing assets into a hierarchical system, another aspect of securing an enterprise architecture is to focus on the actual functions. The Purdue model is not strictly a security reference architecture. It works well to display how information travels within an organization, but when it comes to security, the Purdue model does not apply security to the actual processes. Because of the hierarchical design of the Purdue model, the model applies security more to the system and not to the thing that the system aims to do. For example, when looking at the Purdue model, there are the hierarchical levels from 0 to 5. The lower levels contain critical and sensitive assets, and therefore are more heavily secured and isolated in comparison with the higher levels. When these levels are secured up to a certain standard, it does not take into consideration the whole process where information can travel all the way from level 0 to level 5 (S4 Events, 2019).

Another challenge for an architecture based on Purdue model is the ever-expanding network edge. This includes IoT devices and technologies which aim to provide modern solutions for traditional OT environments. However, whereas Purdue model has six layers, IoT solutions usually break those environments and make them seem closer to three layers. Gartner, a technological research and consulting company, categorizes these layers as edge, platform, and enterprise.

In this three-layer approach, the edge layer consists of the actual devices that are used for the physical processes and includes a gateway for these devices so that the data can be further transferred. The gateway also handles device management and works as an access control in the network. The platform layer stores, aggregates, and analyzes data, processes and orchestrates event data, and manages network communication. Lastly, the enterprise layer supports backend applications which include things, such as databases and applications services (Mission Secure, 2021).

Considering the abilities of the Purdue model in this three-layered approach, the edge could be considered as layers 0 to 2, the platform layer would be similar in operations with layers 3 to 4, and the enterprise layer would be layers 4 to 5. This highlights the issue with Purdue model not being able to provide appropriate foundation for security, since the boundaries with

IoT solutions get blurrier. Instead, there should be a foundation for securing the actual functions because that way, the security is not determined by static boundaries.

One of the big security concerns regarding this three-layered streamline architecture is that it sets a lot of weight on to the IoT gateway. The IoT gateway creates a single point of failure to the whole OT environment and makes it more susceptible to an attack. In the Purdue model, this IoT gateway represents the level 3 as it works as an intermediary between IT and OT (Mission Secure, 2021). However, the Purdue model does not provide any more security with its layering because layer 3 could also be considered as a single point of failure. Especially, since in the Purdue model, the layers typically have static rules and boundaries.

The hierarchical architecture that the Purdue model proposes is no longer compatible with the increasing amount of incorporation of IT in OT. IoT requires a more streamlined architecture because they communicate directly with services that are hosted outside of company premises. The layering and hierarchy of Purdue model do not create additional security for physical devices that need to bypass several layers in order to reach their destination.

The Purdue model aims to provide security by categorizing different processes by their sensitivity. Bypassing those categorized layers creates insecurity. The more IT is incorporated into the OT, the more data is being hosted outside of the enterprise, and therefore a more streamlined architecture is needed (Mission Secure, 2021).

4.2 Internet-of-Things devices

As previously mentioned, the drive towards X-as-a-Service models has pushed for solutions where connections from OT environment to cloud and outside of enterprise premises are made. The IoT devices, or more specifically industrial IoT devices, are a great example of this. IoT devices used for industrial purposes are implemented as a part of these as-a-Service solutions because the vendor needs them to offer their services. Unfortunately, these IoT devices are not usually designed to be compatible with older hardware, or they do not meet the modern requirements in security standards. On top of that, IoT devices usually serve only a handful of purposes and therefore their processing capabilities are quite limited. In this chapter is listed the various security issues that are related to IoT devices.

IoT devices are often very constrained with their security capabilities. This is because they are usually small devices with very little storage, memory, and processing power. These types of devices are designed to do only a small or limited type of operations. However, when these

devices are connected to the Internet, they pose a severe security risk. Because of their low processing capabilities, they cannot implement features such as encryption and decryption, or at least not sufficiently enough, which could be used for secure communications. This raises the risk factors in the environment, and therefore, there needs to be other methods for ensuring the security of communications (Gerber & Kansal, 2017).

Access control is one of the crucial security measures for IoT devices. Unfortunately, when these devices are configured to the network, it is common to use default and weak passwords (Pedamkar, 2021). The more there are IoT devices in the environment, the more substantial the risk factors become because each configured device is connected to the network. If one of these devices is compromised, there is a significant risk that other devices in the same operation are also vulnerable. Especially because these devices often operate in the same network segment.

Having many IoT devices poses a challenge from the management perspective. If the environment consists of dissimilar devices and parts, there is a security risk regarding mismanagement. Since IoT devices are usually designed to monitor or perform actual changes in the physical processes, it is likely that there are many varying types of IoT devices involved. When managing these devices, such as updating their software or applying security updates, there might be a need to do it in a synchronized way. Therefore, to manage the environment, there needs to be proper measures to secure various networking protocols which the devices use and have a software version tracker so that possible obsolete devices can be recognized in a timely manner (Gerber & Kansal, 2017).

The amount of IoT devices and variety of them also poses the risk of being unable to prevent and detect vulnerabilities. A common sentiment in cybersecurity is that security incidents are inevitable and will happen. When there are many IoT devices in a single environment, it can be challenging to identify whether, and which, devices are affected by certain vulnerability. It is also challenging to evaluate the extent of the repercussions (Gerber & Kansal, 2017).

The challenge of identifying and detecting vulnerabilities also means that there are security risks related to predicting and pre-emptively protecting against security threats. This lack of proactive security measures encourages automating security so that the need for human intervention is as minimal as possible (Gerber & Kansal, 2017). The reason why pre-emptive security measures are needed is that, for example, IoT manufacturers might want to push their products to market without proper testing for security vulnerabilities (Pedamkar, 2021). Also,

to reiterate, security incidents are considered inevitable, so pre-emptive security measures can ensure security even in cases where new vulnerability is encountered.

Related to the amount of varying IoT devices, and their complexity in different environments, it is likely that these devices have many dependencies with various other systems. In terms of these dependencies, the IoT devices may use multiple technologies in cross-platform implementations where the systems cannot operate without each other. These interdependencies pose a security risk where a single vulnerability can expose the whole environment to a security threat (Pedamkar, 2021).

Besides securing IoT devices and their environment, there is also an aspect of ensuring the privacy and integrity of the data that is produced by IoT devices. Data privacy and integrity heavily correlate with cybersecurity, and therefore should be specifically mentioned. The data produced by IoT devices needs to be transmitted, processed, and stored appropriately to achieve complete security. IoT data can be sensitive and depending on the use-case, should be anonymized or pseudonymized. With the proper processing and secure transmission of the data, the integrity of the data can be ensured (Gerber & Kansal, 2017).

Somewhat related to data privacy and integrity is ensuring the high availability of IoT devices. High availability can be a significant security aspect. Depending on the purpose of the IoT device, there might be a need for constant availability. Especially in operational technology, it is very likely that these IoT devices are business critical and high availability is a mandatory requirement. Depending on the purpose of the IoT device, unavailability could have severe consequences (Gerber & Kansal, 2017). For example, in health care, the unavailability of an IoT device that monitors or controls some health-related operation could mean a loss of life. Another example would be in an energy sector, such as in a power plant, where an outage to IoT device could have severe environmental consequences. In general, outages to these types of IoT devices that require constant operationality could mean a significant loss of revenue.

The importance of high availability and risks associated to it are amplified when the IoT devices are accessed through various platforms, such as the Internet, mobile connections, cloud services, and others. This means that not only is it enough to guarantee redundancy of the IoT device, but also the accessibility methods as well. The more there are ways of accessing these devices, the more it is crucial that these devices do not have a single point of failure.

4.3 Cloud

As previously discussed, there are severe security threats related to IoT devices, and an increasing need to have them communicate with services hosted outside of enterprise premises. The cloud has become a major factor in modern technological solutions because of its ease of access and ability to scale. Cloud computing can lower operating costs, decrease complexity, increase data availability, and boost innovation (Eltaeib & Islam, 2021).

Compared with cloud computing, hosting a dedicated datacenter, and maintaining it can become easily very costly. Also, if a company is expanding rapidly, a datacenter may not keep up at the same pace. That is why the cloud is so popular. With the cloud, the is no worry whether there are enough resources and computing power to complete some operations. The management and provision of cloud services is the responsibility of the cloud vendor. The customer merely buys cloud services.

However, regardless of the numerous benefits that the cloud provides, it does not mean that it is completely safe. Cloud services are shared by many other participants. The cloud is also quite inconspicuous, so the customers cannot know which services are being shared. Therefore, the shared environment presents challenges such as data separation, theft, and integrity (Eltaeib & Islam, 2021). There are numerous security threats related to the cloud and in this chapter the major security risks related to the cloud are discussed.

Misconfiguration is one of the major aspects that can lead to security incidents. Even though the cloud is provided by a third party, depending on what has been purchased, the management of cloud settings might be the customer's own responsibility. On top of that, organizations might have multiple cloud environments, and this increases the chance of misconfiguration because different cloud solutions have varying setups.

Cloud services are known for using application programming interfaces (API) which serve different purposes. APIs are commonly used for computer-to-computer communications. If these APIs are not properly configured, there is a chance of accidentally creating vulnerabilities. This could lead to malicious entities being able to exploit that vulnerability to gain access to sensitive data (Check Point, 2020).

One of the goals of using cloud is to provide ease of access and usability. This means that data gets shared often and broadly. One typical cloud-based data sharing solution is the link-based sharing. For example, if there is a file share in a cloud and access to it for an external

party needs to be given, a link can be easily generated and shared to those that require it. However, this link-based sharing poses a security risk where it is challenging to manage and control who has access. Also, when links are shared, it cannot be ensured that it is only used by one party (Check Point, 2020).

The ease of access and usability of cloud is achieved by having resources accessible through the Internet. However, this also means that those resources are more accessible for malicious entities. This poses a challenge of ensuring that the data is only accessed by authorized individuals. Therefore, proper access control is required. However, with web-accessible resources, hackers can try to steal and hijack cloud accounts by guessing weak passwords and phish credentials from legitimate users (Makkaoui, Ezzati, Beni-Hssane & Motamed, 2016). The major risk with a breached user account is that the credentials give full control over the account and places where those credentials are used in.

The cloud infrastructures do not have the same security measures as on-premises solutions, which makes detecting credential misuse much more challenging. Even more so, if there is a malicious insider (Check Point, 2020). A malicious system administrator on the side of cloud service-provider can exploit their privileges to access and tamper with the organization's sensitive data.

The cloud infrastructure is hosted by the cloud service provider (CSP) and outside of the organization's premises. This makes it directly accessible from the Internet, and therefore more prone for cyberattacks. Especially with all the possible sensitive and confidential data, which is stored in the cloud, cloud services are an attractive target for hackers. Because cloud solutions expand the organization's operating environment, they are required to re-evaluate their security policies so that they will cover cloud solutions as well.

One of the most common types of cyberattacks that target Internet-accessible resources is a Denial-of-Service (DoS) attack. DoS attack can allow the attacker to breach the cloud infrastructure and steal sensitive data. Even if the attacker fails to gain access, there is still a matter of having the business function inoperable because the Internet traffic between on-premises and cloud services is not functioning which might lead to the loss of revenue (Check Point, 2020).

The cloud being in the public Internet and outside of organization's premises also means that the organizations do not have full visibility to the cloud infrastructure and its configuration.

Also, many of the traditional tools for monitoring and controlling such infrastructure that are used in the on-premises solutions may not be viable. If the organization’s cloud security is insufficient, it could lead to a breach of the company's cloud infrastructure. Often, the organization needs to rely on the CSP that there are sufficient security measures in place (Check Point, 2020).

Cryptography is a big part of ensuring that the security of the cloud can be guaranteed. Encryption is one of the key pillars of security because it can ensure data confidentiality and integrity through various phases of data life cycle. However, even with encryption, there might be configuration errors that can make decryption easier, and the data still traverses through the Internet. Even if the private key used to decrypt the data on cloud is only known to the cloud consumer, attackers can use various attack vectors to reveal and alter the data (Makkaoui, Ezzati, Beni-Hssane & Motamed, 2016).

4.4 Expanding Network Edge

In causation to the previously mentioned IoT and cloud as well as the drive towards as-a-Service type of solutions, the network perimeter is expanding. More and more of the organization’s resources are being hosted outside of their own premises. The increase in technologies such as cloud, software defined networking, and 5G, has also led to the number of physical and virtual devices to increase as well. The number of internet-connected devices and the need for various services to expand produces a significant amount of data that organizations are required to look for more feasible solutions to accommodate and process that data. The amount of data that is required to be processed has grown exponentially which has led to organizations deploying more and more resources to the network edge (Lakhani, 2019).

The network edge refers to the area where locally established and managed network interfaces with the Internet. Due to the rise of IoT and cloud services, organizations have faced more challenges defining their network’s edge. More and more services are pushed towards the internet, which has led to the network’s edge going even further away from on-premises solutions. Inherently, the lines between controlled and uncontrolled networks are getting blurrier the more these technologies are developed and implemented. Besides the network edge getting blurrier, there is also a challenge of managing devices on the edge. The closer the edge the devices are, the less control there typically is over them. This means that

organizations are more reliant on the service provider and the product itself in terms of security and reliability.

The digital transformation to utilize cloud, IoT and as-a-Service type of solutions has happened in multiple industries because of the benefits they provide for the business operations. However, with the increase in utilizing and deploying these technologies, the security aspects have been forgotten or undermined. Organizations aim to increase their profitability and if some technology significantly improves that, it is likely that those types of solutions will be implemented without making a thorough security assessment of their impact.

Due to this digital transformation, the resources on the network edge have increased and so have the attacks on them. According to Cyber Threat Alliance, there has been an increasing amount of sophisticated malicious activity on the edge devices in recent years as they have become a target for attackers (Jenkins, 2019). The lack of overall control and visibility to the network edge leads to organizations focusing more on securing their local resources, such as workstations, IoT devices, and other locally managed hosts (Lakhani, 2019).

Regarding the security aspects of the network edge, the hardware and software hosted there needs to be secured thoroughly because of their potential reachability from the Internet. These are ideal targets for attackers because they allow them to possibly steal and corrupt the data that is being transmitted. Because of the lack of control on the edge devices, it can be easier for attackers to inject malicious software into them (Daniel, 2020). By infecting a device on the network edge, the attackers can masquerade as the service provider without raising alarms. Also, if one device gets infected, it is likely that the attackers can move laterally in the network and infect multiple edge devices. At that point, it is called a supply chain attack since the service provider’s infrastructure is infected.

The more network edge expands, the more attack surface it creates. Even though the subject matter is not about edge computing, the network edge is, by its nature, the locating of computational resources closer to data sources and assets further away from local management to ensure availability. This means that attacks, such as tampering and Denial-of-Service attacks, on the network edge are more likely to happen. The attackers hijack the resources on the edge and use them to, for example, power botnets, mask their operations, or mine cryptocurrencies (Daniel, 2020).

Of course, there are many other purposes for attackers to infect and take control of the edge resources. If the attackers are more malicious in nature, they can perform reconnaissance to steal credentials, redirect traffic, and install malware onto various targets (Daniel, 2020). Because of the data processing moving closer to data sources, the attackers no longer need to use these edge devices as a gateway to the organization's internal resources. Instead, they can just monitor and intercept the data at the edge which makes it even more difficult to detect (Daniel, 2020).

4.5 Bring-your-own-device

Related to the expanding network edge, it is worth mentioning the bring-your-own-device (BYOD) model. BYOD is seen as a way for organizations to cut costs by allowing employees to work with their own more preferable equipment instead of purchasing dedicated work equipment. BYOD means that employees use their personal devices to do their work. These devices might range from laptops, phones, tablets, and so on.

BYOD brings many security challenges. First and foremost, there are the privacy issues. When the employees are using their own equipment to do their work, there is an issue of separating work-related things from personal things. After all, security usually comes with the cost of privacy. In order to ensure security, there needs to be measures in place that might be seen as an infringement of privacy. For example, for organizations to scan their network traffic from malicious activities, they need to decrypt the encrypted traffic. The encrypted traffic might contain sensitive or confidential personal information for the employee.

Employees using their own equipment for work means that the organizations lose some control over the data that is being processed and transmitted. It is also possible to happen vice versa where an employee loses control over that data. Depending on how strict the organization's security measures are for their BYOD users, there is a possibility that employee's personal data is not distinguished from malicious data, and it gets lost because it is removed based on false positivity (Hoelscher, 2021).

The lack of control and management is highlighted by the fact that there cannot be control over the employee's personal stuff. The employee might unwillingly visit malicious websites that they would not otherwise with separate work devices. There is also a possibility of employees sharing their personal devices with, for example, other family members, which increases the risk factors around lack of management and control (Ogden, 2017).

Another concern for organizations is the possibility of data leakage. A data leakage happens when non-disclosed company information is made public or publicly accessible. Data leakage is more susceptible to happening when employees use their personal devices for work. Of course, data leakage does not mean that employees are deliberately misplacing or leaking data. It is possible that malware in the employee's device is stealing data from the device.

5 Recommended solutions

In this chapter, potential solutions for previously highlighted challenges are considered. The research method is briefly described and then for each challenge a possible solution or solutions are described. The aim in considering various solutions is to discover solutions that solve different challenges, and these can then be reflected on for forming a definitive proposal which would achieve the goals of this thesis.

5.1 Research method

The research method used for finding possible solutions was done by performing a literacy review. The main source for literacy and research papers was IEEE. For each of the challenges, a search was made that included results from approximately the last ten years. This was to filter some older research papers and focus on more modern solutions. Those results were then narrowed down to focus on cyber and network security, and architecture. Previous knowledge about the industry was also utilized in filtering the results accordingly. Research papers were chosen by seeing what they were trying to solve and if they offer a viable solution for the purposes of this thesis.

5.2 Solutions for Purdue model

The Purdue model is, in a way, a very straightforward reference architecture since it is hierarchical, and it separates the architecture into different layers or perimeters where assets can be located to. This hierarchy makes it easy to picture the Purdue model in a logical architectural form for various systems and applications. When researching for an alternative architecture model that would be more up to date with modern day standards and requirements, there really did not seem to be a direct alternative model that would answer those needs, especially from a network point of view. However, one architecture model that was often mentioned was the zero-trust architecture.

5.2.1 Zero-trust architecture

Zero-trust is like a buzzword in modern cybersecurity topics. Zero-trust is often seen as the modern-day solution for cybersecurity risks. It aims to solve the issues brought up by evolving technologies, such as Internet of Things and edge computing, which challenge the perimeter-based approach in cybersecurity (Syed et al., 2022). However, zero-trust

architecture is not strictly speaking a logical architectural model, nor is there a single technological solution that will help achieve zero-trust (Syed et al., 2022).

Zero-trust architecture is more like a framework, or a concept. It is an approach to cybersecurity that aims to individually secure enterprise resources and ensure data security, instead of creating static network segments and security perimeters (Rose et al., 2020). The zero-trust architecture model aims to achieve security by providing various guiding principles (Syed et al., 2022).

The core of zero-trust is that there is no implicit trust. Accesses between assets and accounts are denied or non-existent by default, and therefore, zero-trust revolves heavily around authentication and authorization. In zero-trust architecture, every established session would require authentication and authorization, and ideally the access control would implement context- and risk-awareness, while also being continuous. Also, the access control should not just rely on authentication which happens only on entry points of the protected environment (Syed et al., 2022). This way the security risks are evaluated before granting the access, the access would be continuously evaluated, and there would not be a single point of failures in terms of controlling accesses.

As seen in the following Figure 2, Syed et al. (2022) composes zero trust as the combination of access management, segmentation, encryption, and security automation. In their survey, Syed et al. (2022) highlights that a lightweight authentication mechanism is required to be able to manage access for all the various clients which exist in the environment, and the authentication process would implement risk-awareness by utilizing information from different threat-intelligence sources (Syed et al., 2022). Threat-intelligence evaluates the trust within the environment and that should be used to create policies for security automation. For proper automation, the policies should be closer to resources, and for that micro-segmentation is required. Also, due to the high volume of data produced in the environment, Syed et al. (2022) recommends utilizing some type of machine learning algorithms for effective security monitoring, and that the data should be protected in every stage of its lifecycle. This means that modern encryption methods are required (Syed et al., 2022).

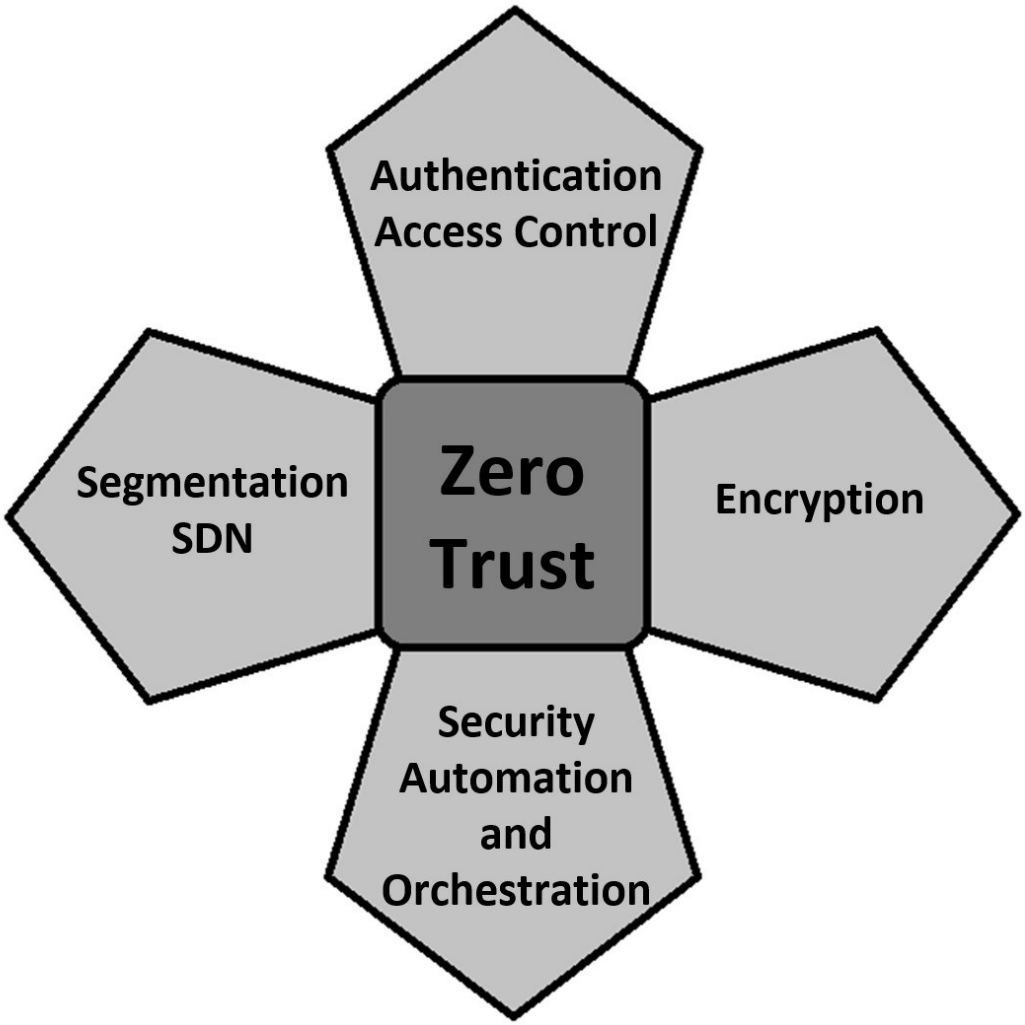

Figure 2 Fundamentals of zero trust (Syed et al., 2022)

Whereas Syed et al. (2022) composes zero-trust architecture at a more tangible level by giving concrete guiding principles, the NIST publication for zero-trust architecture divides the architecture into following logical components: a policy engine, a policy administrator, and a policy enforcement point (Rose et al., 2020). The policy engine works as a decision maker that applies policies to grant, deny, or revoke access from resources. The policy administrator, on the other hand, manages the communications between resources. The policy administrator is responsible for establishing or shutting down communication requests between the subject and the resource via policy enforcement points. This also means that the policy administrator communicates with policy enforcement points to establish proper communication paths. The policy enforcement points are the actual components that enable and terminate connections while also monitoring those connections (Rose et al., 2020).

Other core components Rose et al. (2020) list are a continuous diagnostics and mitigation system, industry compliance system, threat intelligence, network and system activity logs, data access policies, public key infrastructure, ID management system, and security information and event management system (SIEM) (Rose et al., 2020). Of course, these are only a few examples of components but there can be others as well. The purpose of these components is to support the policy engine by providing various information which can be used to create and develop policies to be more accurate and more secure. The following Figure 3 depicts the zero-trust architecture with its logical components as described by Rose et al. (2020).

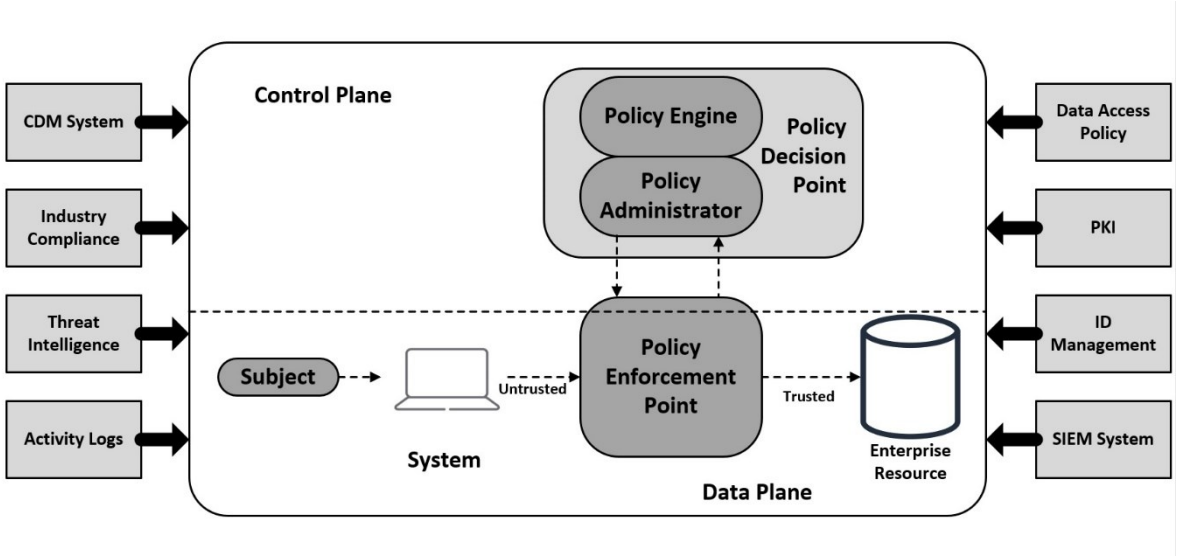

Figure 3 Core Zero Trust Logical Components (Rose et al., 2020)

In Figure 3, the policy decision-making happens in the control plane which is separated from the data plane where the actual communication happens. In this model, the communications and access requests are managed in a separate layer which mitigates the possibility of relying on static and local configurations. Instead, every request is handled in the control plane and subjects in the data plane only forward them.

Considering the previously highlighted issues with some of the modern technologies, such as IoT devices, their resource-constrained capabilities are a significant security risk. One of the major challenges with devices like IoT is that they are very heterogeneous and therefore have different requirements. By separating the control and data planes from these types of devices, their management comes much easier, and it would overall harmonize the environment.

The separation of control and data planes relates to one of the fundamentals of zero-trust architecture which is the aim to secure processes and functions individually. Instead of creating a hierarchical architecture where different assets and resources are categorized based on their sensitivity and criticality as in the Purdue model, the zero-trust architecture aims to increase security by properly isolating various processes and functions from each other. This means that those processes and functions operate in their own segments.

Organizations typically have multiple processes and functions for their business operations and that is why for zero-trust architecture micro-segmentation and software-defined perimeters are essential. Micro-segmentation is a concept that allows for a better separation of services from each other compared with the Purdue model. Instead of setting boundaries for a certain layer, the process can completely be isolated from others while ensuring that it can communicate with all the necessary resources. By separating the services and functions, the ability to enforce policies for protected resources and manage the network in smaller logical segments are increased (Syed et al., 2022).

5.2.2 Zero-trust in network architecture

From a network perspective, micro-segmentation is very relevant in achieving zero-trust architecture. Micro-segmentation could be accomplished with traditional methods such as subnetting, virtual LANs (VLAN), firewalls, and with physical network segmentation in general. However, these technologies and concepts are difficult to manage in a large-scale network with multiple operations happening simultaneously. Even though network equipment and devices use distributed control and transport protocols which are widely adopted, these devices are often manually configured using vendor specific commands (Kreutz et al., 2015). Therefore, using these traditional methods is very complex and not easily managed, and a need for a more autonomous and centralized configuration and management solution is required.

As mentioned by Syed et al. (2022), to achieve autonomous, and centralized management and control of networking equipment, the ideal implementation would utilize Network Function Virtualization (NFV) and Software Defined Networking (SDN). The purpose of NFV is to decouple software and hardware from each other. This means that network functions, such as routing and switching, are not dependent on specific hardware. The use of NFV allows for the increased scalability and rapid deployment of networks. On top of that, NFV can increase

fault tolerance because of the decoupling of hardware and software. This means that there is a decreased risk of faults occurring because of hardware failure (Lina & Dongzhao, 2020).

As depicted in Figure 3, SDN is a technology that separates control and data layers from the network equipment by having a centralized controller that controls the state of the data layer. In SDN, the network equipment becomes forwarding devices where the control logic is implemented in a logically centralized controller. This makes the network environment easier to evolve by having a simpler way of enforcing policies. The separation creates flexibility to the network while dividing it into more manageable sections (Kreutz et al., 2015).

Threat intelligence and machine learning were also mentioned as requirements for zero-trust architecture. These should be utilized for a proper implementation of SDN to achieve zero-trust. Threat intelligence can be used as a feedback mechanism, which in turn helps with the automation of security. The aim of threat intelligence is to provide information for the policy engine for creating and enforcing policies. For optimal results, the threat intelligence solution would need to be able to interpret data from various devices to recognize threats and risks.

Machine learning would also automate security. The purpose of machine learning algorithms is to remove human elements from the data-processing and interpretation. When working with heterogeneous systems, the chance for human errors is increased. Therefore, by using machine learning algorithms the evaluation of security in an environment would be more coherent and harmonic.

5.2.3 Policy-based security architecture for Software-Defined Networks

The management of devices in network environments that comprise of different devices which use different technologies can be challenging. Therefore, a centralized control solution that can manage various devices in the environment has great benefits. A centralized controller would manage the devices in the underlying network, and those devices would become simple forwarding devices that do not require specific and individual configurations.

SDN is a solution which helps to solve challenges with expanding networks and their complexity by separating control from the actual network devices. With a centralized controller, there is less likely chance for configuration errors to happen, reacting to security incidents and suspicious activities is enhanced, and implementing complex network functions becomes simpler (Varadharajan et al., 2019). Because SDN can apply changes to the

infrastructure much faster and more precisely compared with doing manual configurations, the network stays more stable and systematic.

In terms of achieving zero-trust with SDN, one such way is to use policy-based security architecture. A policy-based security architecture for SDN can specify and enforce access policies for various communications within the environment. The communications can be between users or devices that are trying to reach a service (Varadharajan et al., 2019). These communications could be managed with policies that use context or labels to classify the traffic. For dynamic and context-aware policies, the classifications could utilize, for example, location, routing information, or previously accessed services as parameters (Varadharajan et al., 2019).

By using classifications to manage network communications, it is possible to restrict the traffic to follow only certain paths. For example, traffic can be restricted to only travel through devices which have a certain security classification. This way, sensitive and confidential data stays isolated and is only transmitted via secure channels (Varadharajan et al., 2019).

The objective of this architecture is to enforce security policies which are specified for the SDN controller. Every connection from the endpoints is subjected to security policies specified in that domain's SDN controller. The aim of the policies is to keep communications authentic, secure, and integral, and ensure that each communication is referenced to applied policies (Varadharajan et al., 2019).

The capability of assigning dynamic policies in a policy-based security architecture achieves a couple of the elements of zero-trust architecture. An access control that can segment and isolate traffic, and security automation can be achieved with dynamic policies. For example, by having a proper integration with Security Operations Centre tools, policies can be applied whenever malicious activity or an attack is detected (Varadharajan et al., 2019).

The following Figure 4 shows how a policy-based security architecture in an SDN environment is structured. The architecture has three layers. From top to bottom, there are an application plane, a control plane, and a data plane. The control plane hosts the SDN controller. The controller, or multiple controllers, are managed via the application plane where the policy management happens, or the actual policy-based security architecture is located. The policy management can also be part of the control plane instead of running

separately in the application plane. Below the control and application plane is the data plane which hosts all the network equipment (Varadharajan et al., 2019).

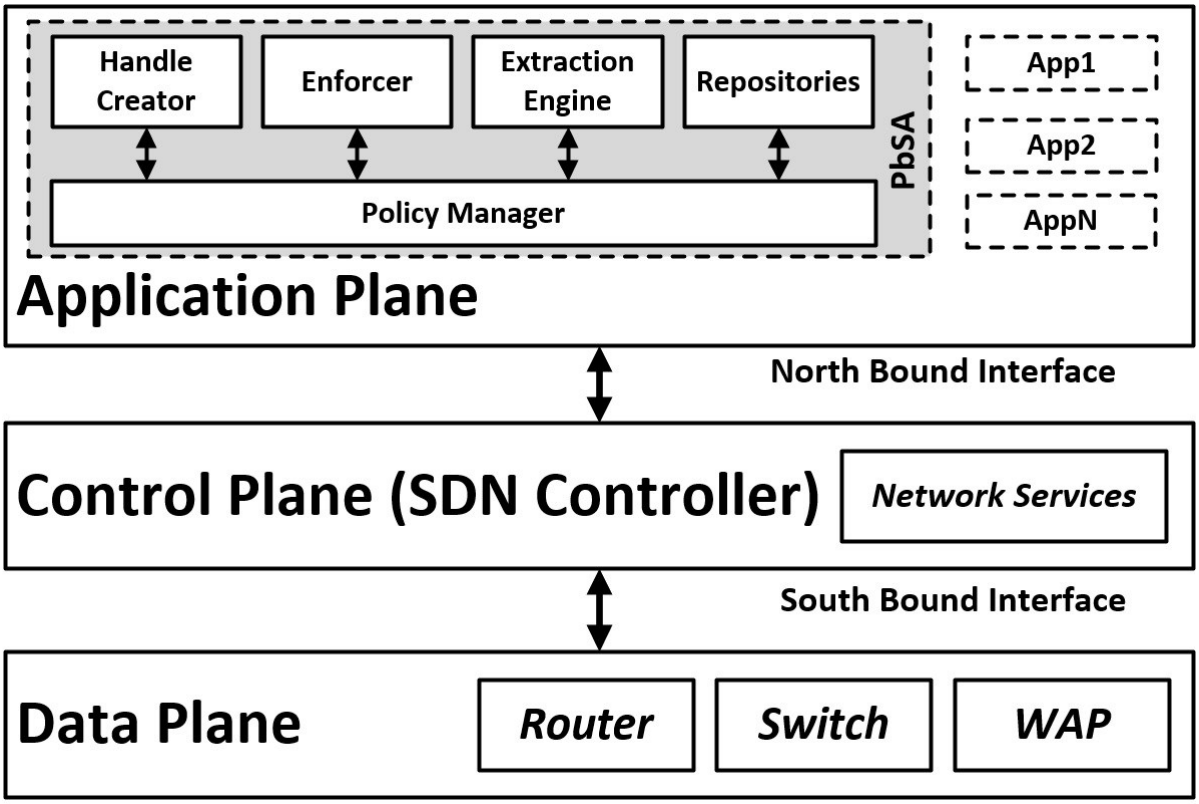

Figure 4 Policy based security architecture for SDN (Varadharajan et al., 2019)

In this architecture, the SDN controller has a policy server. Policy server refers to the policy-based security architecture which is in the application plane in Figure 4. The policy server is formed by the following five components:

- **Topology and policy repositories:** Up to date network topology, and definitions and specifications of the expressed policies.
- **Policy manager:** Management of the security system.
- **Policy evaluation:** Traffic analysis in reflection to applied policies.
- **Policy enforcement:** Enforcing the rules and traffic flow obtained from policy manager.
- **Handle creation:** Creates handles to check traffic authenticity and policy enforcement.

Whether there are multiple controllers or not, each of the controllers need to be up to date with the network topology and required policies (Varadharajan et al., 2019).

With this policy-based approach, it is possible to achieve the principles of zero-trust. For example, by implementing rules to deny communication by default, traffic from host to host can be blocked unless the communication is allowed by the policy (Varadharajan et al., 2019). When the policy repository is aware of the different servers and services running in the infrastructure, it is possible to identify authorized communications from malicious and unauthorized.

Also, with this architecture it is possible to block attacks to the infrastructure. If someone targets a device in the network, for example a denial-of-service type of attack, the traffic is blocked or dropped because of policy. The attackers cannot target a specific host or resource because they cannot specify the traffic route in a dynamically established environment. For the network packets to go via a certain path, the packets need to be specified for a such purpose, and they need to be allowed via policy (Varadharajan et al., 2019).

Of course, denial-of-service type of attacks do not usually originate from a single host. There are usually a great number of hosts generating traffic to overload the system. However, it is possible to implement flow-based thresholds. If some path exceeds that threshold, then another one can be dynamically established. If another route cannot be established or a host exceeds the flow threshold, then the architecture can dynamically implement a drop or deny rule (Varadharajan et al., 2019).

5.2.4 Integrated Security Architecture for Software-Defined Networks

Another solution to achieving zero-trust in an SDN environment is the Integrated Security Architecture (ISA). ISA utilizes the previously described policy-based security architecture and expands on it. The following Figure 5 shows how the integrated security architecture is structured:

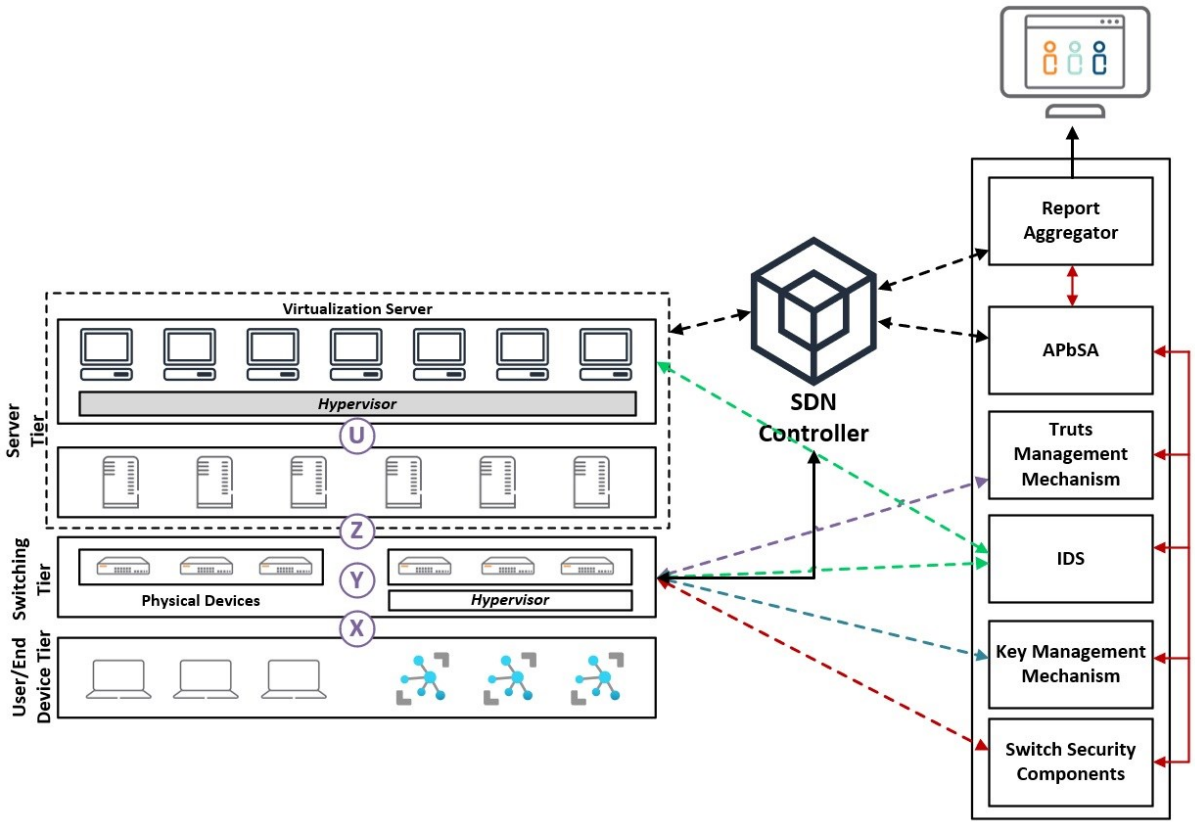

Figure 5 Integrated Security Architecture using SDN (Karmakar et al., 2020)

As it can be seen in Figure 5, the architecture is quite similar to the policy-based security architecture. ISA does not highlight the application, control, and data planes, but instead has the four following tiers:

- **User/End Device Tier -** End-user and IoT devices.
- **Switching Tier -** Switches, routers, firewalls etc.
- **Server Tier -** Various physical and virtual servers.
- **Security Mechanism Tier –** Security components, policy management, and architecture (Karmakar et al., 2020).

Even without the application, control, and data planes, those can still be pictured if the different components are considered. In Figure 5, server, switching, and end device tiers are the data plane where various clients and devices operate. The SDN controller, in the control plane, is separated from those tiers and manages the connections in the underlying environment. To manage the connections in the environment, the SDN controller receives policy rules from the security mechanism tier in the application plane.

This architecture utilizes Authorization Policy-based Security Architecture (APbSA) which derives from the previously described policy-based security architecture. It aims to distinguish different network flows to create path and flow-based policies. It utilizes security monitoring tools such as SIEM to detect malicious activities and report them. With proper integrations, APbSA could generate an appropriate path and flow-based policies to mitigate the threats (Karmakar et al., 2020).

5.3 Solutions for cloud security

The biggest concern regarding cloud security is the fact that cloud services are reachable through the Internet. This level of reachability makes it crucial to ensure that connections made are authenticated, authorized and accounted. This does not guarantee security, but it guarantees that cloud services are accessed in a managed way.

In research by Toth, they tried to identify the best security solutions that aimed to preserve data and maintain security. These solutions included access control, authentication, cryptography, intrusion detection, key management, network security, secure transmission, security of data, security policy, and software updates. It was discovered that cryptography is exceptionally relevant because it has connections to many aspects of security in cloud (Toth, 2021).

5.3.1 Cloud architecture

Cloud architecture typically consists of data, control, and application planes. Since cloud solutions usually include some sort of software-defined networking, the architecture is quite similar to the previously highlighted layering in SDN environments. This also means that each of these planes have different threats they are more susceptible than others.

One of the most important aspects of cloud security is to protect the data that it holds. Cloud solutions are typically used to increase the availability and scalability of resources, which means that the data it holds can be quite substantial. Therefore, it is crucial that the data, or more specifically, the data plane is secured accordingly.

The data plane consists of many different endpoint devices. These devices produce various types of data that is communicated to different destinations. To ensure the integrity of the data produced by these devices, some of the recommended solutions are access control,

encryption, decentralization, intrusion prevention and detection, policy-based approaches, data analysis, and having up to date firmware (Toth, 2021).

One example of endpoint devices in the data plane is IoT devices. IoT devices have become quite common, and it is possible that they connect to cloud services. For example, an organization might purchase a service from a vendor who implements IoT devices into the organization's environment. Depending on the type of service, to control and manage the IoT devices, those devices can communicate to cloud where the control or application is hosted.

Toth argues that edge computing will allow more resources for IoT systems and provide features such as end-to-end security (Toth, 2021). A way to increase the security of IoT systems is to locate services closer to the network edge. Edge computing would increase the capabilities of the IoT systems, and implementing security features could become easier.

Security in the cloud can also be increased by placing middleware between communication channels and using firewalls on the perimeters. Toth argues that the management of firewalls would be easier because there is only one central firewall. Also, because the management would be simpler, the IoT systems and their subsystems would more easily adapt to security changes. These same firewalls would then be used to monitor the environment and have intrusion detection and prevention features in place (Toth, 2021).

The information going from the data plane to the application plane needs to be properly secured. In the cloud, the control plane works as an intermediary between the endpoints in the data plane and applications running in the application plane. One way of securing this traffic is to place traffic flow analyzers in the control plane for monitoring the traffic that is being transmitted. These analyzers analyze the packets and their frequency to identify and prevent malicious traffic from being transmitted across the network. The traffic flows can then be classified to increase the security and efficiency of the network (Toth, 2021).

To ensure data security in every instance, it also needs to be secured in the application plane. Toth recommends that having flexible access control in place would increase security in the application plane. Even though the application plane does not necessarily host data, it is used to host services that utilize that data. To limit who and what has access to the application plane, the authentication should be continuous. Also, to reduce unnecessary accesses being left allowed, there should be clear policies about how, why, and when data should be accessible (Toth, 2021).

As previously indicated, data integrity is an important part of the application plane. To achieve data integrity in the application plane, Toth recommends implementing encryption and monitoring of data, as well as using data segregation where more sensitive data is separated from others. Also, the data in the application plane is often related to application programming interfaces (API), which means that there should be measures to prevent data loss or data getting tampered with. For this, Toth recommends automated backups and patching to increase security and availability (Toth, 2021).

5.3.2 Preventative vs detective approaches

When it comes to securing cloud, the security measures can be preventative or detective approaches. Both of them have their pros and cons. Preventative controls aim to mitigate and prevent unwanted actions and activities from taking place in the environment. Detective approaches, on the other hand, aim to identify actions and activities that are unwanted in nature. A benefit detective approaches have over preventative is that they are usually better at recording events which can be used for future developments (Ko, Kirchberg & Lee, 2011).

Cloud security solutions are more catered towards preventative approaches, such as access control, encryption, and intrusion prevention. However, even though these measures are utilized, data breaches still occur. Also, when these data breaches happen, the preventative solutions fail to provide transparency and accountability of the service. Therefore, Ko et al. (2011) argues in their research that detective solutions are needed more to achieve better security and trust (Ko, Kirchberg & Lee, 2011).

5.3.3 Data and system centric logging

Regarding cloud security, logging is one of the crucial ways of collecting event information. Logging can be data- and system-centric. Ko et al. (2011) argues that data-centric logging is especially needed with cloud solutions. Since virtualization is a big part of cloud and it can cause identification issues, the links, location, and how data is written between virtual and physical systems are not as transparent as they should (Ko, Kirchberg & Lee, 2011). This is because the identification happens on both the physical and virtual side. The virtualization also blurs the lines between other physical and virtual layers.

Relating to virtualization, another issue with data on cloud is that the operating systems running in cloud are not specifically designed for it. Therefore, traditional process or event-

based logging does not suffice. Since data is the major element of cloud, the logging processes should also focus on the data more than on the systems and hardware that are running in the cloud. After all, the aim of data-centric logging is to track and analyze the data from the very beginning until it is destroyed (Ko, Kirchberg & Lee, 2011).

Ko et al. (2011) recommends data-centric logging because it is not dependent on the environment where the data is. Its sole purpose is to focus on the data. This does not mean that system-centric logging should be forgotten. It is still useful for logging the events happening on the operating systems. However, with the cloud the emphasis is on the data and therefore data-centric logging should be prioritized (Ko, Kirchberg & Lee, 2011).

To achieve data-centric logging, there needs to be tracking in various instances. Cloud storage is very prominent nowadays because it guarantees that files are not lost when hardware fails. Beyond just cloud storage, various applications also store files for different purposes. Therefore, tracking files is one of the most important aspects of cloud security. It enables the monitoring of data lifecycle in the cloud. By monitoring different read and write events, changes in location within the cloud, and origin and destination, the data integrity is enhanced. Also, because of cloud's aim to provide high availability, this constant logging and monitoring achieves the possibility of restoring data in certain points of time (Ko, Kirchberg & Lee, 2011).

Tracking data history is essential because it validates the processes used in the creation and obtaining of data, and in the detection of malicious activities (Ko, Kirchberg & Lee, 2011). This is also called data provenance. In order to achieve data provenance, the data must be efficiently managed and consistently gathered while ensuring integrity, and all the confidential and sensitive data must be secured appropriately. Ko et al. (2011) envision that data-centric logging can, among other things, increase consistency, rollback, recovery, replay, backup, and restoration of data (Ko, Kirchberg & Lee, 2011).

Another aspect of data-centric logging is the value of the information it provides. This translates to tracking information flows and auditing the data on those flows. Accountability in the cloud is essential and to manage it, it is crucial to monitor and control the information flows, whether they are done by services or business functions (Ko, Kirchberg & Lee, 2011). By logging various data, it can be used to further develop future solutions.

5.3.4 Cloud security summary

Considering the issues and solutions highlighted regarding cloud, those are heavily related to how data is managed and accessed. From a network point of view, the clear objective is to ensure the security of data being transmitted and isolated from other processes, as well as ensuring the security of accessing these resources. This leads back to zero-trust principles.

By combining the objectives of cloud security and principles of zero-trust architecture, conclusions as to where changes are required and what can be done can be drawn. For example, the data on cloud needs to be properly secured and isolated. In terms of zero-trust architecture, this could mean the implementation of micro-segmentation, access control, and encryption.

5.4 Solutions for Internet-of-Things security

The main issue with IoT devices is the lack of management capabilities and control. Their unidirectional purposes do not leave much room for security implementations. The devices are designed to perform only certain tasks, and therefore are missing features such as access control, virus detection and encryption. Therefore, these security-constrained devices need multiple layers of security.

Since security features cannot be implemented directly on to the devices, they need to be applied separately. Network segmentation is one such solution. Because of the limited processing power of the IoT devices, there should be network segments that implement separate security functions to the traffic. Also, by separating different processes from each other, it is easier to ensure data integrity (Gerber & Kansal, 2017).

Another solution would be to adopt an IoT platform which works as middleware for connecting and managing IoT devices. By having a separate management platform for IoT devices, the device maintenance can be automated. The purpose of management platforms is to also keep a record of version numbers and backups so that availability can be ensured (Gerber & Kansal, 2017).

More importantly, by having an IoT platform, the policies can be applied to the IoT environment which would otherwise be very limited. IoT platforms remove the need for hardware segmentation by enabling the use of virtualization and software-defined methods

instead. Also, the IoT platform can operate as a monitoring tool for the IoT network and can therefore check and analyze traffic for anomalies (Gerber & Kansal, 2017).

5.4.1 Zero-trust

Zero-trust architecture is one way of securing IoT environment. Because zero-trust architecture focuses on securing the networks and the data, it can be seen as a modern solution for new technologies and trends, such as IoT. To secure IoT environments, Zeng et al. (2021) recommends building a zero-trust protection system (Zeng et al., 2021).

The suggested model by Zeng et al. (2021) follows the principles of zero-trust by featuring systems that use access control based on user identities instead of network perimeters. The model assumes that there are no trusted platforms, and aims to hide all business resources, such as application, servers, and data. For the continuous security measures, Zeng et al. (2021) implements a continuous trust evaluation into their model, which also achieves dynamic access control (Zeng et al., 2021).

Zeng et al. (2021) divides zero-trust architecture into three layers: a data platform, a control platform, and an identity authentication platform. The data platform includes various trust agents that are used for dynamic access control. These agents are used by the control platform which processes and verifies the requests via identity authentication (Zeng et al., 2021).

In the model suggested by Zeng et al. (2021), every request is authenticated and authorized. The authorization has four functions. Those functions are access gateway control, authority management control, identity and terminal management, and security detection and analysis (Zeng et al., 2021). With these functions, dynamic access control can be achieved.

The model uses the least privilege -principle and divides resources based on sensitivity. Access gateway control manages this resource division and who accesses them. Identity and terminal management are used for maintaining records of the identity information which in turn is used for authorization by authority management control. Lastly, the security detection and analysis monitor the access requests and analyzes the traffic for malicious activity and abnormalities (Zeng et al., 2021).

5.4.2 Software-Defined Networking and Network Function Virtualization

As Zeng et al. (2021) focuses more on having no implicit trust and securing networks, so does Farris et al. (2019) with their survey on SDN and NFV mechanisms in IoT environments. According to their survey, to achieve an SDN and NFV based IoT environment, there needs to be a good understanding of the conventional security measures that are being used. These include measures such as authentication and authorization, traffic filtering, encryption protocols, and detection systems (Farris et al., 2019).

According to the research by Farris et al. (2019), dedicated and intelligent access control solves many security and privacy issues. By having an authentication, authorization, and accounting (AAA) framework that uses credential-based authentication where tokens are used to map out authorized actions, the security of network services and interfaces is increased, and those same tokens can be used to enforce policies. The tokens can be either based on the user or the role (Farris et al., 2019).

The AAA framework suggested by Farris et al. (2019) can also be applied to network traffic control. When the tokens are used to map out authorized actions, it becomes possible to identify legitimate traffic flows more easily. However, with larger IoT environments, the traffic control might cause scalability issues because of the resource-constrained gateways that would be required for the whole implementation (Farris et al., 2019).

The constraint with IoT gateways is also highlighted by encryption methods. Encryption is a good way to ensure data integrity but the IoT devices themselves cannot achieve this due to their limited resources. According to Farris et al. (2019), a conventional way of achieving this would be to use a proxy. A proxy would handle the encryption by acting as an intermediary between the endpoints. Then a key manager, that works as a separate entity, would ensure that public encryption keys are forwarded to correct destinations for data decryption (Farris et al., 2019).

The last highlighted conventional security measure by Farris et al. (2019) is intrusion detection systems (IDS). These systems are usually divided into signature- and anomaly-based systems. Signature-based IDS is a more static solution with a library of attack signatures it uses to cross-reference transmitted traffic with. Anomaly-based IDS is more proactive because it is event-based. This means that it establishes a normal behavior to which every event in the network communication is cross-referenced to. However, the issue with

IDS systems in IoT environments is the heterogeneity of devices and possible interoperability issues (Farris et al., 2019).

Farris et al. (2019) argues that adopting an SDN solution for IoT systems would enhance the network programmability by moving the control of the network to a centralized SDN controller. It would reduce the complexity of the network and allow moving the processing away from endpoints. By separating the control and forwarding of the network devices, the complexity gets reduced without affecting the data flows (Farris et al., 2019).

For IoT environments, an SDN-based solution would increase the security of the devices by isolating the network traffic. This would be achieved by deploying various logical networks for client devices. To this end, a framework is required that creates separate paths for network traffic while enforcing policies (Farris et al., 2019).

With the proposed SDN solution, the security attacks would decrease because every connection from and to IoT environments would be verified through the SDN controller. The connections would be analyzed and referenced to the applied security policies. This way, legitimate connections would be allowed by providing forwarding rules for the SDN-enabled network devices and malicious connections would be blocked by applying access lists. This would also work in limited environments where the SDN controller does not manage the whole network infrastructure as well. For example, it is possible to specify policies for traffic flow coming from IoT gateways (Farris et al., 2019).

According to Farris et al. (2019), the added network monitoring in an SDN-based IoT environment would increase the security. Since the network devices, such as switches and routers, would become mere forwarding devices, the SDN controller could provide more information about the underlying network infrastructure to the applications running in the control plane (Farris et al., 2019). By having better visibility on the network infrastructure, there is more control and ability to develop security measures.

One of the key elements regarding security with an SDN-based solution is the dynamic capabilities that it provides. Forwarding rules can be applied to network devices as the connections are being requested. When an SDN-enabled network switch receives a packet from an IoT device, it does not have the necessary routing information to forward it to the correct destination. Instead, it sends a request to the SDN controller which processes the request and decides whether it complies with the policy. If allowed, the SDN controller sends

necessary routing information for the network switch, otherwise the packet gets dropped. By having this type of mechanism, it is possible to implement features such as dynamic access control (Farris et al., 2019).

Farris et al. (2019) argues that dynamic flow control provided by SDN solution will increase resiliency against security threats. This is because forwarding rules can be dynamically updated, and the responsiveness can be delegated to IDS. Moreover, when involved with sensitive data coming from IoT devices, the traffic flow can be dynamically adjusted to different routes if one is suspected to be malign. The traffic can also be duplicated and forwarded to different channels to negate packet loss and improve availability (Farris et al., 2019).

Another overarching solution to increasing security in IoT environments, that was suggested by the research of Farris et al. (2019), was to use Network Function Virtualization (NFV). According to Farris et al. (2019), the adoption of NFV would help solve the issues related to IoT systems by separating the software from hardware. This would reduce operating costs, increase the ability to manage and scale the network, and make the network more tolerant to faults (Farris et al., 2019).

By virtualizing the network functions, the need for specific hardware reduces. Instead, standard servers where the network functions will be hosted can be utilized. These servers can be designed based on the function they provide. For example, firewalls using deep packet inspection might require more processing power. The only requirement is that, for the successful implementation of NFV, the network devices need to have appropriate traffic forwarding rules in place for the servers running the actual network functions.

The NFV can also be used to relocate security functions. The issue with IoT devices is the lack of management capabilities and processing power. Since the devices are designed to perform only certain tasks, security features are often lacking. With NFV, those security functions can be offloaded to an external entity which can unify all the heterogeneous devices. (Farris et al., 2019).

The benefit of decoupling software from hardware is that there is no longer a need for new appliances whenever operations are scaling (Farris et al., 2019). It is much easier to duplicate a virtualized network function than install a new hardware appliance. Network functions can be established, or retired, based on the changes in the operating environment. Also, the fault

tolerance is increased by duplicating the network functions virtually instead of configuring two hardware appliances redundantly. The duplication of network functions also means that NFV can increase availability.

Lastly, Farris et al. (2019) highlight the challenge of providing security with all the possible mobile IoT devices. With NFV, however, there is more flexibility to support these types of devices because the packet processing can be brought closer to the IoT devices (Farris et al., 2019). This increased flexibility also allows for chaining security services. With virtualized network functions, the traffic can pass through multiple virtualized instances which provide different security services. This way the operational costs can be reduced because of the improved resource utilization (Farris et al., 2019).

5.4.3 Internet-of-Things security summary

Considering the challenges and possible solutions related to IoT platforms, those are heavily related to the limited processing power of the devices, and the operations they are designed to do. As with cloud security, from a network point of view, the clear objective in securing IoT platforms is to ensure that the transmitted data is kept secure and integral. Also, IoT platforms need to be properly secured from malicious accesses since those can be more vulnerable due to the limited processing power of the devices. This leads back to zero-trust principles again.

Zero-trust principles and elements can be utilized to secure IoT platforms. The limited processing power of the devices means that security functions need to be established separately. Therefore, elements such as segmentation, security automation, and encryption are relevant. Also, because these types of devices can be very business critical, managing the access is essentially important, which means that proper access control is required.

6 Suggested solution based on literature review and use cases

The ideal way forward would be to start modifying the existing architecture. Suggesting a whole new architecture is quite challenging for any enterprise because it is not very realistic or feasible to completely replace existing architecture. There are different applications and services that need to be considered before making changes to the operating environment. Moreover, some of these applications and services might be business critical where any disruption to their operations can cause significant operating loss. This issue is especially highlighted when there are legacy technologies in place. Therefore, a more granular approach would be required.

The suggested solution needs to address the challenges in the current model and implement modern security methods. It was previously concluded that the Purdue model is not suitable architecture for today's standards from a technical point of view. Also, when discussing different solutions for various issues, the zero-trust architecture was brought up many times. Therefore, the suggested solution should consider how to implement zero-trust principles in an architecture based on Purdue model. The objective is not necessarily to overhaul the architecture but implement zero-trust principles in various stages.

The Purdue model is still viable for categorizing resources and assets based on their sensitivity and criticality. It was only concluded that network and technical architecture should not follow Purdue model as it does not provide any added security with modern cyber threats nor comply with new technological standards and trends. Therefore, a solution which utilizes the conceptual categorization of Purdue model and implements the elements of zero-trust would be ideal. Categorizing resources and assets from an enterprise architecture point of view is still valid, and networks that implement zero-trust elements can respond to issues posed by modern technological advancements and threats.

From a network point of view, the hierarchical categorization of resources does not provide sufficient security with modern technological solutions. Therefore, the following concept was designed (Figure 6). In this design, the resources are still categorized by their sensitivity and criticality but instead of limiting connectivity to resources in other containers, the access is managed by a separate overlay. The access overlay works as a control plane for requests happening between resources that are conceptually categorized in labels. The labels in this

model depict the data plane in a zero-trust architecture. Within the data plane, there are policy enforcement points where the access overlay applies policies for every access request.

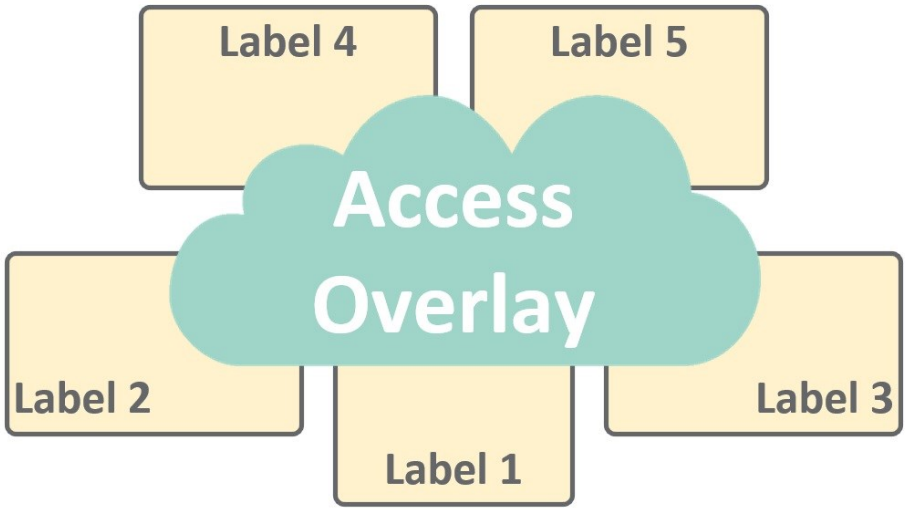

Figure 6 Access Overlay

The core elements of zero-trust architecture are formed by access control, micro-segmentation, encryption, and security automation and orchestration as depicted by Syed et al. (2022) In terms of achieving zero-trust, it is not very feasible to apply zero-trust principles to the network devices themselves. Enterprise networks consist of various network devices, such as routers, switches, firewalls, and access points, among other things. This means that environments are heterogeneous and often include devices from various vendors. These devices commonly use standardized network protocols which enable their interoperability but with vendor-specific commands and configurations, the complexity increases.

It is possible to achieve zero-trust with network devices to a certain extent, but it also has its challenges. Micro-segmentation could be achieved by using VLANs and subnetting to create subnetworks that include only certain types of devices and connections, access-lists could be created for access control, some encryption protocols are available, and security automation could be achieved with some type of system logging procedures. However, on an enterprise level scale the complexity would only increase and make the infrastructure more prone to errors.

To achieve zero-trust more efficiently, centralized control for network devices would be required. By having a centralized control over the network devices in the environment, the complexity is reduced, and manageability is increased. With centralized control, the chance for configuration errors to happen is lessened, and scalability is increased since the actual configurations are not performed individually. For example, micro-segmentation would be simpler since configurations for such requirements would happen centrally. Otherwise, it would require a lot more resources to configure each network device to limit or exclude certain connections to certain network paths.

The zero-trust architecture assumes that when accessing resources there is no implicit trust. Therefore, any device connecting to a network should not be trusted. This poses a challenge from the access control and encryption point of view. Some devices in the network might have better encryption capabilities than others. A workstation might have sufficient processing capabilities to utilize advanced encryption protocols, but an IoT device most likely does not. This means that the access control should not rely on the device, and encryption methods should be applied outside of connected devices.

Lastly, for any kind of security automation to work, there needs to be the ability to either apply security measures on to the client devices themselves or to the connections they make. Because enterprise networks are very heterogeneous, it is more feasible to apply those measures to the network instead of to the connected devices themselves. By applying security measures to the network, regardless of the device connected to the environment, the security measures get applied to the connections created by the device. If the security measures were to be applied to the devices themselves, it would mean that there is an implicit trust between the device and the environment it is connecting to.

Software defined networking is one solution for centralized network management. In SDN, the network components, such as switches and routers, are managed by a centralized controller. Instead of applying configurations on a device-basis, the configurations are applied by a controller. Since the configurations are no longer implemented into the devices individually, the only operation left for network equipment is traffic forwarding. The benefit of centralizing the controls allows for making changes to the network rapidly, avoiding configuration errors, and increasing scalability.

There are couple of downsides with an SDN implementation. One of them is that SDN requires some sort of decision-making process or an entity which gives the controller the

commands for desired configurations that need to be applied to the environment. Therefore, a separate tool or a process is required to achieve the security automation and orchestration. For example, a SIEM could be utilized in a way that the SDN controller can make dynamic changes to the environment based on the received information.

Another challenge is to ensure that the network devices support some centralized management protocol or a framework. SDN solutions require that the controller is able to read, write, and view the existing configurations in the network devices. It is possible that older network hardware does not support such functionality.

Zero-trust is not achieved by solely implementing an SDN solution. To achieve zero-trust with software-defined networking, a policy-based security architecture needs to be established. In this architecture, the environment is divided into application, control, and data planes. The data plane consists of SDN-enabled devices which are controlled by the SDN controller in the control plane. Depending on the implementation, the decision-making process can happen parallel to the SDN controller in the control plane, or separately in the application plane. To achieve the decision-making process in a policy-based security architecture, there needs to be a policy engine and a policy administrator. The policy engine will apply policies for accessing resources and the policy administrator then manages the communication requests between the subject and the resource via policy enforcement points.

The purpose of dividing the architecture into separate planes, or layers, is to simplify the architecture of the environment. By separating the control from the devices in the data plane, the overall manageability and scalability of the environment is increased. The control and management of devices in the data plane is no longer reliant on the actual devices. Instead, the management happens via centralized control plane which is supported by the application plane. While the control and data planes form the underlying infrastructure, the application plane supports both by, for example, gathering data which can be used to create policies.

As established previously, it is more beneficial to apply security measures to the network instead of to the devices connecting to it. Therefore, the network equipment in the environment should be the policy enforcement points. Some of the end devices might be limited with their processing capabilities, such as IoT devices, so it is much more feasible to make the network devices as the policy enforcement points because all the clients would communicate through them.

Considering the core zero-trust logical components figure (Figure 3) and a network architecture based on Purdue model, the security and policy components are not separately featured. The security and policy components refer to various systems and guidelines which support the creation and management of policies. In the Purdue model, the security policy is that only communications between adjacent layers are allowed, and resources are allocated to them based on their sensitivity. Whether an access request is allowed or not is based on the sensitivity of the resource, and from which layer the request comes from. This means that even if these security and policy components are utilized in the architecture, the interoperability with the control plane is not guaranteed. By separately highlighting the security and policy components, there is a better chance to also integrate them with other systems and processes.

For achieving a policy-based security architecture, the Integrated Security Architecture proposed by Karmakar et al. (2020), which creates a framework for SDN, should be referred to (Karmakar et al., 2020). This framework enables the interoperability between the control and data plane by setting up a policy-based security mechanism that integrates various security and policy components with the SDN controller. The SDN controller then uses the information received from those components to make appropriate configurations to the operating environment.

In the figure by Karmakar et al. (2020) (Figure 5), the Security Mechanism Tier is the policy decision-making point located in the control plane of the zero-trust architecture. The Security Mechanism Tier uses multiple data channels to create and adjust policies. The SDN controller takes those policies and translates them into configurations for policy enforcement points which are the SDN-enabled network devices.

One difference between a network built on Purdue model and a software-defined network is the use of firewalls. In the Purdue model, the security layers are separated with firewalls that have rules for allowed and blocked traffic. However, in the policy-based security architecture the SDN controller would manage access between subjects and resources. Therefore, the need for firewalls would decrease. The SDN controller would verify that the connection request abides policy and would act accordingly. There would not be a need for dedicated firewalls because there can be default deny-policies defined for the SDN controller.

Implementing a policy-based SDN solution to achieve zero-trust architecture does not mean that the existing Purdue model needs to be completely replaced. In a zero-trust architecture,

the enterprise resources might still have implicit trust. Especially depending on the industry and the type of assets the enterprise holds. These assets and resources usually contain valuable information or data for the enterprise and its business operations. In the Purdue model, different layers, and communications between them, are defined based on the risk acceptance level. For example, an access request from layer three to layer two has smaller risk when compared with access request coming from layer four. This means that there exists an implicit trust between some entities. This implicit trust could be utilized when implementing the new architecture, as in creating access policies based on existing risk acceptance factors.

6.1 Step one: Implementing software-defined networking

In the first phase, the aim is to lay a foundation for each communication and access request to pass through the SDN controller. There will not be drastic architectural changes to the environment, but the changes made will make the transition easier. The environment will still look quite the same, but it will slowly start to implement SDN features.

The first step of implementing an SDN solution would look something like pictured in the following Figure 7. The following Figure 7 still retains the hierarchy of Purdue model but implements an SDN controller which manages the underlying network. In this step, there is no need to start managing access requests between subjects. The purpose is to ensure that the environment is SDN-enabled, and the most important part is to make sure that the SDN controller can view and make configuration changes to the operating environment reliably. Once the environment is SDN-enabled, it becomes possible to start making further implementations to a policy-based security architecture.

The following Figure 7 also retains the conceptual categorization of Purdue model so that resources within a certain layer can communicate freely with each other. Depending on the capabilities of the network equipment, it is possible to start processing connections centrally via the SDN controller by converting them into forwarding devices. However, in a Purdue model access requests are not limited when subjects are in the same network layer, so that is still retained to ensure business continuity. Implementing SDN to fully manage access requests within a network layer requires a more granular process since there are no existing access rules which could be copied.

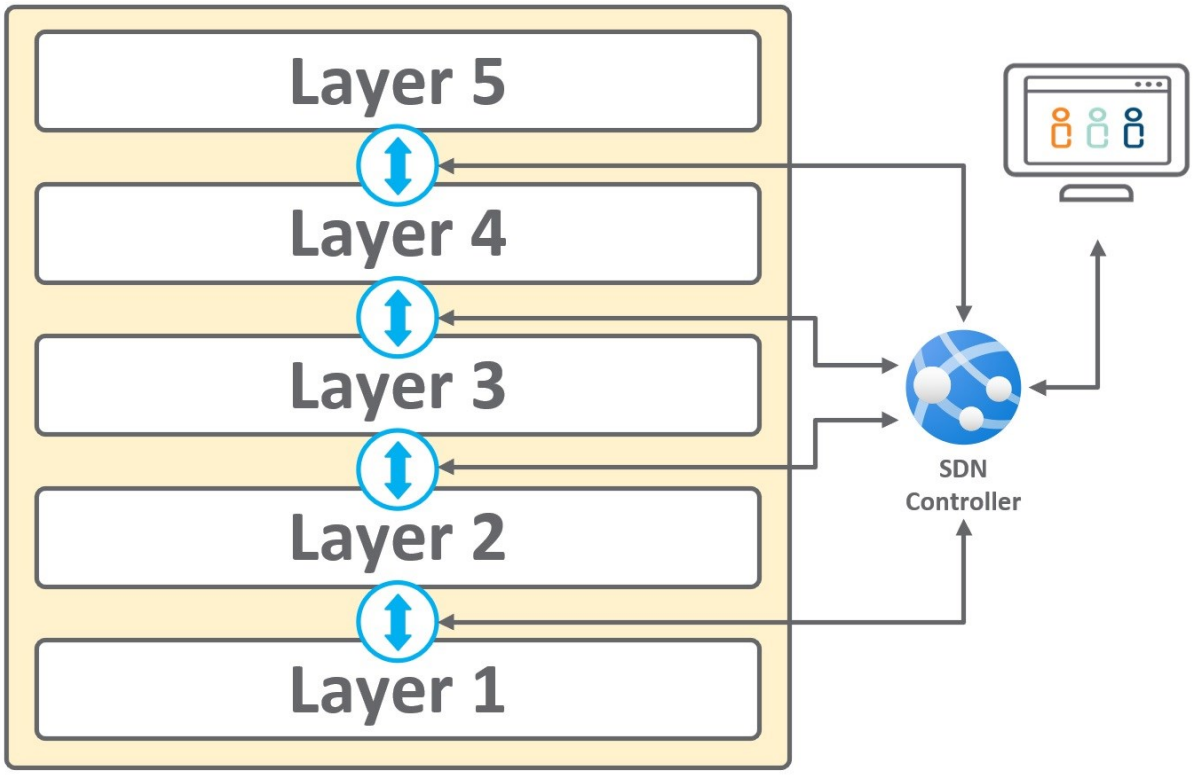

Figure 7 First phase of SDN implementation

6.2 Step two: Increasing utilization of software-defined networking

In the second phase, the aim is to ensure that the SND controller is capable of creating, managing, and configuring access rules. Those rules should be based on policies and other measures which are defined in the architecture, such as security events and activity logs. To achieve zero-trust and have a successful implementation of policy-based security architecture utilizing SDN, the SDN controller requires this various information from the underlying network environment.

From a security point of view, in order to achieve zero-trust, the network needs to be able to respond to security threats dynamically. This means that the SDN controller should be able to apply policies to prevent and isolate certain connections when a security incident is detected. Integration with the security information and event management (SIEM) would allow the SDN controller to react to anomalies within the network much quicker compared with more traditional ways of responding to network anomalies.

When the SDN controller is able to respond dynamically to security events, a certain level of security automation would be achieved. One of the key elements of zero-trust architecture is

the security automation. Security automation requires that there are dynamic elements in the environment that can be utilized in the management process. The ability to combine security events with the policy decision-making process, for example, means that the environment is capable of responding to security incidents without human intervention.

In this second phase, the transition towards using labels instead of layers, when categorizing assets and resources, would be started. The aim is to get rid of the hierarchical Purdue model and set the layers into the same level. This still allows for the conceptual categorization of Purdue model, but the access requests would not be determined by from which layer the requests are coming from.

The removal of hierarchy means that, instead of just managing connections between layers, the connections within the layers would also be managed. In the Purdue model, the access requests are determined by a hierarchical policy. Since using that is no longer viable, every access request needs to be managed, even if the access is requested to an asset or a resource within the same layer.

The second step would look like as the following Figure 8. The assets and resources are still categorized into layers to simplify the transition process. However, in the following step, and in the future, the architecture would use labels instead of layers.

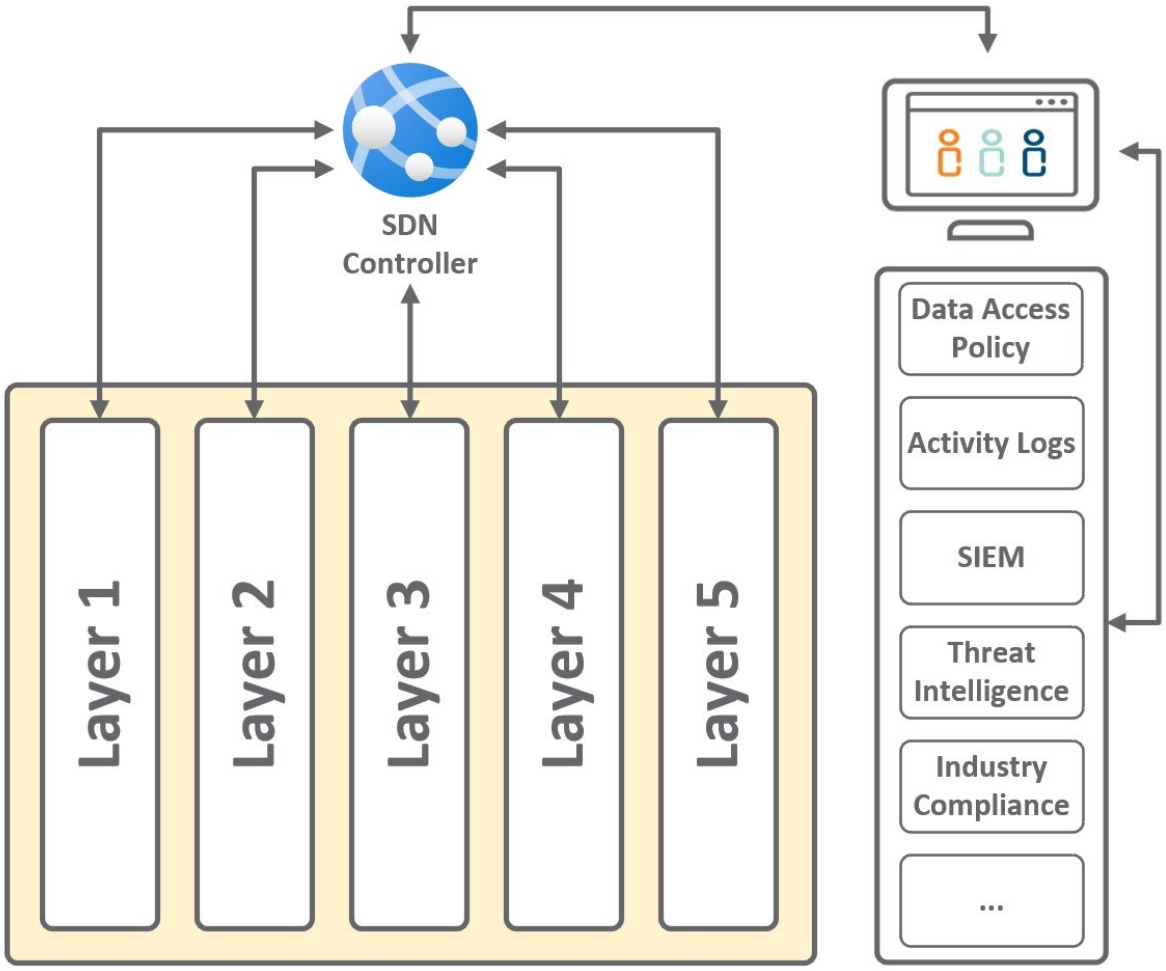

Figure 8 Second phase of SDN implementation

6.3 Final step: Complete utilization of software-defined networking

The next and final phase would look like as the following Figure 9. In this model, the resources are categorized into labels based on their criticality and sensitivity to business operations. There is no implicit trust between the resources, so they cannot communicate anywhere without having access granted via SDN controller. This also applies to resources within a certain label.

In this model, once a communication request is created, an SDN-enabled network device relays that request to the SDN controller. The SDN controller then references the access request to the applied policies. In an allowed instance, the SDN controller sends the necessary forwarding instructions to all the SDN-enabled network devices to route the traffic appropriately.

As previously established, the policies applied by the SDN controller are defined by various attributes, such as SIEM, access policy, et cetera. Some of these attributes monitor and surveil the infrastructure and that data can be utilized for creating dynamic access control.

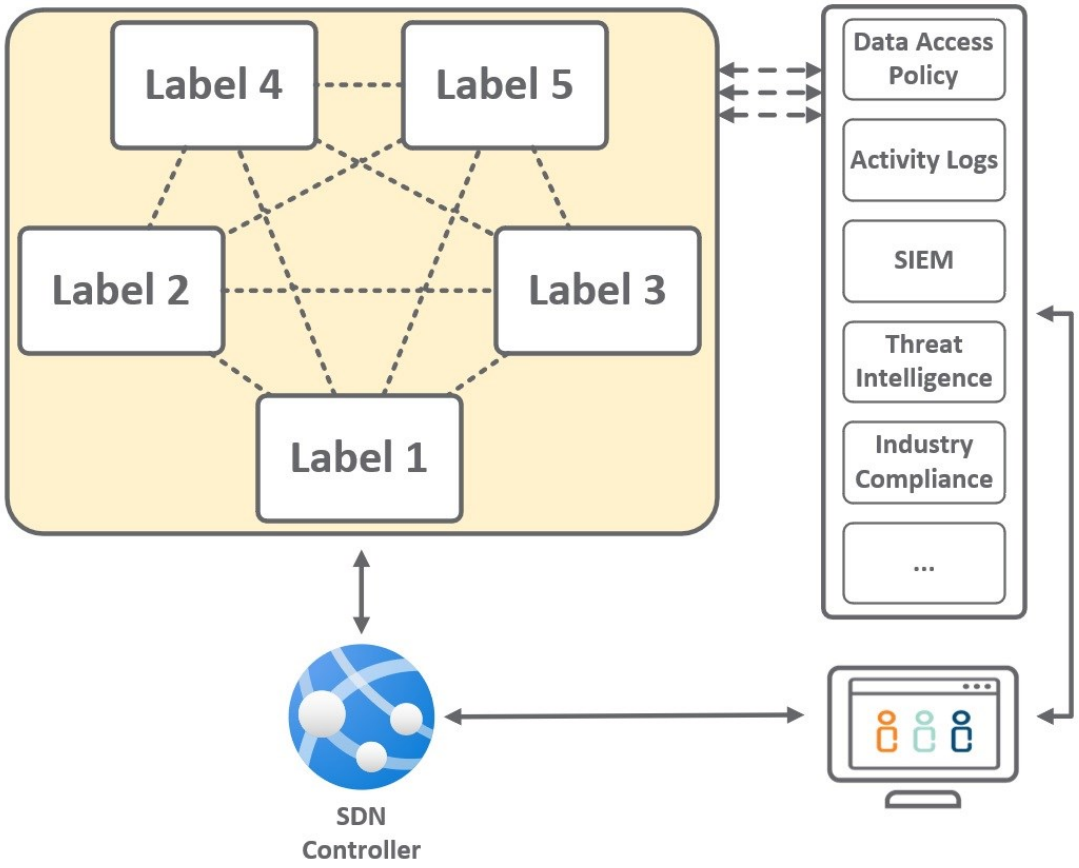

Figure 9 Final design of SDN solution

6.4 Alternative final solution

One consideration is to ensure the operationality of the OT environment. OT usually includes highly sensitive and business critical assets that need to operate continuously without error. Having dynamic elements in an environment that requires stability and continuous availability can be counterproductive. The OT environments typically rely on static configurations with redundant measures that ensure operational continuity even when issues in connections with counterparts are encountered.

Looking at the previous Figure 9 that suggests the final solution, one could make an argument that the SDN controller works as a single point of failure. Even if the SDN controller was implemented in a way that it would be redundant, it would still mean that the network devices in the OT environment are relying on the SDN controller for network traffic routing and

device configurations. Managing device configurations is not problematic because it does not affect the ongoing operations. However, the network traffic routing needs to be static. In case there occurs an issue with the SDN controller, it could have significant impact on the OT environment's operationality.

To solve this reliance issue with the OT environment, one possible prospect is to keep the OT environment logically separate from the IT environment. This means that the OT environment can maintain operationality without any dependencies. The communication between the IT and OT environments would still be available but the OT environment could operate totally independent of the IT environment. The following Figure 10 is the expanded concept of previously established solution with OT and IT environments separated.

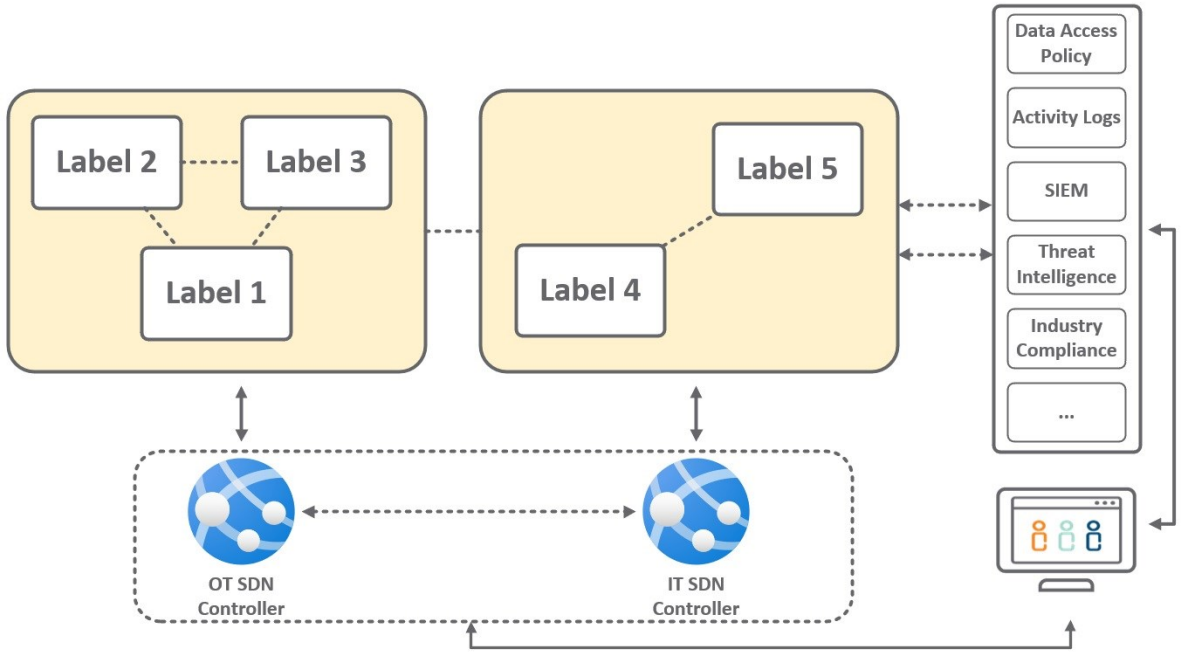

Figure 10 SDN implementation with split OT and IT environment

In this solution, there would be two SDN controllers. OT and IT environments would have their dedicated SDN controllers that ensure operationality. The suggested solution would mean that IT and OT have their individual domains and the communication between the two is handled by their respective SDN controllers. To ensure interoperability between the two environments, the SDN controllers would need to be configured in a way that they can communicate, manage, and apply appropriate policies.

Due to the legacy infrastructure and resource-constrained devices in the OT environment, it is likely that the SDN controller cannot be used to manage access requests in the OT

environment. However, it can still be used for managing infrastructure. In this instance, the SDN controller would be only used to manage network configurations in the OT environment, instead of applying policies for each separate access request. This also means that the policy engine would not create policies based on the information received from the OT environment. More specifically, the network configurations in the OT environment would follow existing policies, and the policy engine would not receive any information from the OT environment.

In case the OT SDN controller is used for only managing device configurations, then the two-domain solution needs to be tweaked. This is because there would no longer be two domains. Therefore, to ensure interoperability and maintain policy-based security architecture in the IT SDN environment, there would have to be some sort of gateway for the OT environment. This way, there are not two separate domains, and the IT SDN controller would apply policies to the network traffic coming from the OT gateway.

In this solution, where OT SDN is only used for configurations, zero-trust would not be achieved as it is intended. Static rules and configurations would mean that there is an increased risk potential because of having implicit trust between resources. However, the benefit of using an SDN solution to manage these configurations still increases the overall manageability and scalability. It also lays a foundation for developing the environment for more modern solutions since management is centralized.

7 Conclusion

The objectives of this thesis were to research and identify, in terms of security, whether a network architecture based on the Purdue model is still viable for modern day technologies, what would be the alternative that supports current trends, and present a logical network architecture with required components. Based on the research done for this research, it was concluded that the Purdue model is no longer a viable network architecture. Concepts such as zero-trust, SDN, and policy-based approaches were more prominent to increase the overall security and manageability of a network infrastructure which implements modern digital platforms, such as cloud and IoT.

The thesis began by getting familiar with cybersecurity in general, reviewing some of the current threats that affect digital platforms, and researching challenges with the Purdue model. Once a clear picture of the baseline was established, various solutions for each of the challenges were presented and discussed. Once that was done, a set of concepts and technologies were utilized to design a new logical network architecture.

The research approach was to perform a literacy review of relevant studies, surveys, and other researches. This was done to examine if there were commonalities between the established challenges and their solutions. Those commonalities were then referenced when researching possible solutions.

It was expected that the research would lead to zero-trust as a possible solution since it has been a buzzword in cybersecurity and IT for a few years now. Before this thesis, the concept of zero-trust was understood to a certain extent but applying it in practice was unknown. The research helped understand the key elements of zero-trust, and when researching potential network architectures, that understanding made it possible to make certain conceptual connections between subjects.

The research led to the suggested solution, which is as a logical reference architecture for networks. The issues highlighted in this thesis were strongly related to the Purdue model's inability to conform with modern digital requirements. The suggested solution takes into account the highlighted challenges and proposes an alternative architectural network model which can implement zero-trust elements. The suggested solution even incorporates the Purdue model's intended purpose of setting security perimeters based on the sensitivity of assets.

Unfortunately, the final suggested solution still left some research questions. As it can be seen, the final solution has an alternative approach due to possible limitation within the target environment. Applying zero-trust elements into an environment that requires static elements causes fundamental issues. Zero-trust means that there is no implicit trust and that can be difficult to implement in certain cases. More research is needed to design a solution that would entirely implement zero-trust elements in these types of environments.

References

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems* (2nd ed.) (pp. 58-59). Wiley Publishing Inc.

Check Point. (n.d.). *Live Cyber Threat Map: Check Point*. Retrieved December 13, 2022, from https://threatmap.checkpoint.com/

Check Point. (2020, August 28). *Top cloud security issues, threats and concerns*. Retrieved April 28, 2022, from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

Check Point. (2021, July 13). *Purdue model for ICS Security*. Retrieved April 11, 2022, from https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

Daniel, B. (2020, December 9). *Is edge computing secure? here are 4 security risks to be aware of.* Trusted Computing Innovator. Retrieved May 3, 2022, from https://www.trentonsystems.com/blog/is-edge-computing-secure

Farris, I., Taleb, T., Khettab, Y., and Song, J. (2019). A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. *IEEE Communications Surveys & Tutorials, vol. 21*(1), 812-83. https://doi.org/10.1109/COMST.2018.2862350

FireEye. (n.d.). *Cyber Threat Map*. Retrieved December 13, 2022, from https://www.fireeye.com/cyber-map/threat-map.html

Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components and examples*. CSO. Retrieved April 12, 2023, from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Fruhlinger, J. (2022, August 24). *WannaCry explained: A perfect ransomware storm.* CSO. Retrieved April 12, 2023, from https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html

Gerber, A., & Kansal, S. (2017, November 17). *Top 10 IoT security challenges - From device security, to network security, to application security, and more*. IBM developer. Retrieved April 26, 2022, from https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/

Hoelscher, P. (2021, July 23). *BYOD security: What are the risks and how can they be mitigated?* Comparitech. Retrieved May 2, 2022, from https://www.comparitech.com/blog/information-security/byod-security-risks/

International Society of Automation. (n.d.). *ISA99, Industrial Automation and Control Systems Security*. Retrieved April 11, 2022, from https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

Jenkins, N. (2019, April 30). *Living on the Edge*. Cyber Threat Alliance. Retrieved May 22, 2022, from https://cyberthreatalliance.org/living-on-the-edge/

Karmakar, K. K., Varadharajan, V., Tupakula, U., and Hitchens, M. (2020). Towards a Dynamic Policy Enhanced Integrated Security Architecture for SDN Infrastructure. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 1-9. https://doi.org/10.1109/NOMS47738.2020.9110405

Kaspersky. (n.d.). *Kaspersky cyberthreat real-time map*. Retrieved December 13, 2022, from https://cybermap.kaspersky.com/

Ko, R. K. L., Kirchberg, M., and Lee, B. S. (2011). From system-centric to data-centric logging - Accountability, trust & security in cloud computing. *2011 Defense Science Research Conference and Expo (DSR)*, 1-4. https://doi.org/10.1109/DSR.2011.6026885

Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE, vol. 103*(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

Lakhani, A. (2019, April 30). *Securing the Network Edge*. Fortinet Blog. Retrieved May 3, 2022, from https://www.fortinet.com/blog/threat-research/research-report-securing-the-network-edge

Lina, Z., and Dongzhao, Z. (2020). A New Network Security Architecture Based on SDN / NFV Technology. *2020 International Conference on Computer Engineering and Application (ICCEA)*, 669-675. https://doi.org/10.1109/ICCEA50009.2020.00146

Linthicum, S. (2020, December 2). *Understanding Network Data Delivery: Layers 2 and 3 of the OSI model*. CompTIA. Retrieved April 12, 2023, from https://www.comptia.org/blog/layers-2-and-3-osi-model

List of data breaches. (2023, March 6). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=List_of_data_breaches&oldid=1143273955

Makkaoui, K. El, Ezzati, A., Beni-Hssane, A., and Motamed, C. (2016). Cloud security and privacy model for providing secure cloud services. *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, 81-86. https://doi.org/10.1109/CloudTech.2016.7847682

Mission Secure. (2021, January 27). *ICS Purdue model in Industrial Internet of Things (IIOT) & cloud*. Retrieved April 11, 2022, from https://www.missionsecure.com/blog/purdue-model-relevance-in-industrial-internet-of-things-iiot-cloud

Mullins, T. (2021, September 27). *The OSI model: 7 layers of security*. Fortress Consulting Group. Retrieved April 12, 2023, from https://gofortress.com/osi-model-7-layers-of-security/

Ogden, J. von. (2017, February 16). *The 7 scariest byod security risks (and how to mitigate them!).* Cimcor. Retrieved May 2, 2022, from https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

OWASP Top 10 team. (2021). *What's changed in the Top 10 for 2021*. Retrieved April 15, 2023, from https://owasp.org/Top10/

Pedamkar, P. (2021, August 20). *IoT security challenges: Factors, Effect & security measures of IoT*. EDUCBA. Retrieved April 26, 2022, from https://www.educba.com/iot-security-challenges/

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero trust architecture. *National Institute of Standards and Technology Special Publication 800-207*, 59. https://doi.org/10.6028/NIST.SP.800-207

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2021). Developing cyber-resilient systems: A Systems Security Engineering Approach. *National Institute of Standards and Technology Special Publication 800-160, Vol. 2*(Rev. 1), 310. https://doi.org/10.6028/NIST.SP.800-160v2r1

S4 Events. (2019, August 16). *Is The Purdue Model Dead?* [Video]. YouTube. https://www.youtube.com/watch?v=KfxPF9xjFrE

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., and Hahn, A. (2015, June 3). Guide to industrial control systems (ICS) security. *National Institute of Standards and Technology Special Publication 800-82, Revision 2*, 247. Retrieved May 7, 2023, from https://doi.org/10.6028/NIST.SP.800-82r2

Strain, L. (2018, December 28). *2018: The year of the data breach tsunami*. Malwarebytes Labs. Retrieved April 9, 2023, from https://blog.malwarebytes.com/101/2018/12/2018-the-year-of-the-data-breach-tsunami/

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., and Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access, vol. 10*, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679

Toth, A. (2021). Cloud of Things Security Challenges and Solutions. *2021 Communication and Information Technologies (KIT)*, 1-6. https://doi.org/10.1109/KIT52904.2021.9583760

Varadharajan, V., Karmakar, K., Tupakula, U., and Hitchens, M. (2019). A Policy-Based Security Architecture for Software-Defined Networks. I*EEE Transactions on Information Forensics and Security, vol. 14*(4), 897-912. https://doi.org/10.1109/TIFS.2018.2868220

Zeng, R., Li, N., Zhou, X., and Ma, Y. (2021). Building A Zero-trust Security Protection System in The Environment of The Power Internet of Things. *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, 557-560. https://doi.org/10.1109/AINIT54228.2021.00114

Zscaler. (n.d.). *What is the Purdue Model for ICS Security?* Retrieved April 11, 2022, from https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security