Operational Technology Services to Support Business Activities

Master of Science in Technology
Thesis
University of Turku
Department of Computing
MDP in ICT, Cyber Security
May 2021
Daniele Del Sale

Supervisors:
Seppo Virtanen
Petri Sainio

UNIVERSITY OF TURKU
Department of Computing

Daniele Del Sale: Operational Technology Services to Support Business Activities

Master of Science in Technology Thesis, 58 p.
MDP in ICT, Cyber Security
May 2021

The operational technology (OT) environment is a vital part of several businesses around the world. While most of these businesses rely on the activities conducted there in order to generate revenue, it is not always correctly secured, and it is treated as a mere extension of the company's IT network.

In this thesis it is described how OT-specific services were designed to protect the company business while, at the same time, keeping into consideration the needs of the people operating in the environment. It is also described how the design was implemented in practice, describing the technology and the entities involved. Finally, the use case definition and the testing phase is described to report what kind of problem arose only later and how they were approached to be solved.

In short, this thesis follows the entire development of these services, starting from the very beginning until the present moment, meaning the successful conclusion of the testing phase and the start of the operational phase.

Keywords: OT, processes, cybersecurity, services, security, production

Contents

List of acronyms

AD Active Directory

ICS Industrial Control System

IT Information Technology

LAN Local Area Network

NOC Network Operation Center

OS Operating System

OT Operational Technology

PLC Programmable Logic Controller

SCADA Supervisory Control And Data Acquisition

SCCM System Center Configuration Manager

SOC Security Operation Center

UAT User Acceptance Testing

..

1 Introduction

In the last ten years, digitalization and innovation have profoundly changed the way industries operate and conduct their businesses [1]. Thanks to constantly improving information technology capability and the visible advantages, most companies have started to connect more and more of their devices to exchange information more quickly and optimize their processes [2].

A relatively new aspect that most companies now adopt is that IT does not only serve the purpose of storing and computing pure information but is also used for efficiently control and monitor various devices, including the ones that have a tangible impact on the physical world [3]. For example, a diesel engine in a power plant used to produce electricity cannot function autonomously without being connected to a computer that monitors its performance and lets technicians tune it and control various operational settings. In the past, that was not possible and not needed, but today the constantly increasing requirements in performance, united with the cost reduction for these systems, is making these examples more and more common.

The hardware and software that detects or causes a change in industrial equipment, assets, or processes is called **Operational Technology** (commonly abbreviated as **OT**) [4]. This definition is a guideline for defining what OT is. In practice,

OT networks also involve all the software and hardware that supports the activities above, even if it does not directly affect the industrial processes by itself [5].

The direct consequence of having industrial equipment connected and controlled by software is that this same equipment becomes then vulnerable to cyber threats that can violate the security of these devices and cause problems that can directly affect the industrial process by disrupting it. As these machines often operate in the same location as human personnel, the fact that a vulnerable device can directly control moving parts makes clear the most significant risk in the OT environment. An eventual security incident can cause people to get hurt or even lose their lives with a financial and reputational loss for the victim company [6].

While this is by far the main concern for security specialists operating in this domain, there is another huge aspect to consider. These are the potential costs that a production plant would face if an incident in the devices or in the network would cause the production activities to slow down or even stop altogether. Depending on the plant size, this would amount to millions of euros per day in certain companies [7].

As described above, the OT environment, even if at the general level, is composed of very similar devices foundable in the more common IT environment (e.g., computers, network switches, firewalls, servers), has different risks and thus security and operational requirements. Due to these fundamental differences, several OT/ICS (Industrial Control System) security standards have been written during the years. One of the most famous and widely adopted is **IEC 62443** [8]. This series of standards is composed of different sections and covers different aspects of OT security, starting with defining basic terminology, explaining security requirements for the environment, and providing a risk-based approach for different parties to recognize and mitigate the various risks that would arise.

Standards like IEC 62443 (or NIST 800-82 [9]) are vital to follow for companies to increase their security maturity and adapt to the constantly increasing security incidents amount and resulting cost. However, implementing successfully the changes required by best practices is easier said than done, and doing this usually requires heavy changes in the infrastructure and the processes inside a company. Ignoring this need would make the problem worse, and industries have started to address this, even if the amount of work required to adapt legacy systems to continually increasing security requirements demands many resources and time.

Another aspect that must be taken into account is that cybersecurity is never done for cybersecurity itself. Instead, it should assist the business in successfully conducting its operations without experiencing problems. The phrase above is a crucial point, and it is also true in the OT environment. All the cybersecurity processes that need to be implemented and maintained in this domain cannot ignore the various needs that the business itself may have. It is quite the opposite: cybersecurity must take the needs of the company representatives and implement measures to satisfy these requirements while increasing the overall security of the environment [10]. While it may seem an obvious point, it is a challenging topic because the best solution from the cybersecurity point of view does not satisfy the business needs and, vice versa, the most convenient option for a business would often not take into account cybersecurity risks.

Business requirements are various, but in general their final goal is to have a fully functional environment that has as little downtime as possible and can operate without requiring additional workload [11]. In addition to this, the business site prefers to be as much independent as possible in its decisions. This means that if a change in the configuration of a particular device is needed, the shortest and fastest way to perform it (so the one that involves fewer parties) is the one that it would

choose. Often this means cutting out vital steps for cybersecurity, primarily the risk analysis of the change in question, that would ensure that no security issue would arise from the activity.

Of course, the need for the business side of being independent is related to the fact that on the site level there are deadlines to honor, and these cannot always be met if some issues put the production on hold waiting for another office to fix the issue, instead of letting the local engineers solve it by themselves. For this, any cybersecurity process oriented towards this kind of environment must be flexible and optimized enough to ensure that cybersecurity practices would not slow things down in a way that makes them counterproductive.

This thesis analyzes and shows how these cybersecurity services for the OT environment were designed and developed in Wärtsilä. As these services are a new trend for most companies, both big and small, this thesis highlights how the entire development process took place, what were the findings and the changes that took place during the development of the project, and also what were the issues that arose during the testing phase, that forced the team to redesign certain aspects to make the solution viable. This thesis serves as a guide to other companies that want to bring or improve cybersecurity in their OT environment and provides insights and findings from *lessons learned* to make the process easier and effective.

The rest of the thesis is composed as follow:

2. **Background:** In this chapter, it is analyzed if already existing IT solutions are solving the needs of the OT environment properly. As the answer is 'not really', the problem is introduced. There is a need to develop dedicated OT solutions to address these requirements.

3. **Requirements:** This chapter describes in detail what are the requirements

that must be kept into consideration while designing an OT solution. The requirements address business needs by referencing the guidelines and best practices to use in the OT security frameworks (IEC 62433).

4. **Design:** Here it is described how the different streams of the development process took shape. OT NOC processes, OT SOC processes, OT Asset Management, OT PC management tools, OT remote connectivity, and supporting activities are different streams that are described.

5. **Implementation:** Here it is described how the implementation process progressed and how multiple streams were handled while having a lot of integrations and common dependencies between them. It is highlighted the complexity of handling such big changes altogether and how collaboration between different teams was vital for proceeding with the project.

6. **Use Cases:** After the implementation phase, before introducing the pilot testing, it is described what are the use cases that were defined for the OT services. It is introduced, for example, the role of SOC/NOC processes and how internals and externals operate in various services.

7. **Testing:** This chapter covers how the solution performed in the pilot testing in the company, how new problems arose, and how they were addressed. It also describes how the various OT services behaved during the testing, if and how they provided an added value in operational activities, and they are compared on how this would have been handled if the solution would not in place to highlight the real benefits that these bring.

8. **Conclusions:** This chapter wraps up what was observed during the entire development process and provides ideas for future works. It also addresses any non-solved problem, proposing at a high level how it might be addressed in the

future. It also talks about the future of OT security and marks the importance of developing new solutions for it, using the study above to illustrate how much cybersecurity in a business can improve if addressed correctly.

2 Background

In chapter 1 it is introduced the topic of Operational Technology environment, and it is explained how this is fundamentally different from a more natural IT environment such as an office. However, it is not yet clear if already existing IT cybersecurity services could provide a sufficient level of security maturity and at the same time integrate correctly with business requirements, thus not requiring specific development.

At the high level, it appears that the OT environment needs to be protected in a very similar way to an IT environment. This means providing services that ensure the security of the network and the security of the various devices connected to it. It can be theoretically possible then to provide the same services already provided to IT with slight adaptations. That would save time and resources, and if the result were acceptable for both cybersecurity and business needs, it would not make sense to invest in ad-hoc solutions.

Before analyzing what kind of solutions already exist, it is necessary to list the OT environment's needs. During the initial study, these requirements have been identified:

- Need to properly identify and block malicious activity on the network that could cause security incidents

- Need to ensure that the OT network operates continuously without disruptions or low performance (e.g., packet loss, slow connection)
- Need to keep an accurate inventory of all the active devices present in the environment to ensure that the various services keep the real environment into consideration(or in other words *"You cannot protect what you do not know"*).
- Need to secure the endpoints from cyber attacks, in particular computers, that are the most commonly attacked devices
- Need to provide a secure and reliable way for people and systems to connect remotely, without sacrificing network security

2.1 Analysis of needs

It is now analyzed each of these requirements, highlighting how a traditional IT approach would tackle the needs and its limits.

2.1.1 Need of proper identification and blockage of malicious activity on the network that could cause security incidents

Both in IT and OT, network attacks could cause different issues for the devices operating in it. For this, there is the necessity of a service that monitors the network 24/7 and that can intervene in case a malicious activity is detected. The incident response happens first by blocking the attacker from executing additional actions and then removing the root cause that caused the incident to occur to avoid that the attack is executed again.

Most companies address this demand by creating a Security Operation Center (often referred to as SOC) [12]. A SOC takes care of both of the monitoring activities as well as responding to incidents. The SOC operates 24/7 to ensure continuous protection.

While this service itself is perfect for the OT domain also, there is a substantial difference in how a network operates in an ICS environment versus how it operates in an office one. For example, monitoring solutions that are designed for operating in an IT environment are great in analyzing and detecting anomalies in a network where most of the traffic is exchanged between computers, internal servers, and cloud services (primarily). In an OT environment, vice versa, the devices that are talking on the network are way more various and use very different protocols than the ones most standard network monitoring solutions are supporting [13]. For example, PLCs (Programmable Logic Controller) and SCADAs (Supervisory Control And Data Acquisition) use protocols such as Profinet, Modbus, Profibus, and ControlNet. These protocols are used to get data from automation machinery and also to control them. It is then clear the importance of being able to detect if one packet that travels on the network is malicious and would cause, for example, a PLC to disable a safety device that needs to stay on. Another critical difference is how much more alarming is an anomalous connection from or to the internet. In an office network, most devices regularly exchange data with various resources around the internet (imagine how many different websites a person visits during a regular workday). On the other hand, in an OT environment, any connection between a local device and an external resource must be fully known and allowed. While this does not make sense in an office, on a factory floor, the simple detection of a never seen IP that exchanges data with a local machine should be enough to raise alarms and people to start investigating.

2.1.2 Need to ensure that the OT network operates continuously without disruptions or low performance

Having reliable network connectivity is vital for most systems, independently from their purpose and what is connected to them. What is usually different is the priority and the criticality for the network operativity itself.

Based on how fast the connectivity must be re-established in case of issues, there are different approaches that a company can take to ensure that the network stays operative even if some network devices fail. First of all, using a network topology composed of redundant devices to ensure that the failure of one of them would not cause the entire network to collapse. While this may be sufficient in most environments, it cannot be a solution in the OT environment. Because the activities in the factory are so heavily dependent on a fully functional network, there is a necessity to introduce a dedicated Network Operation Center [14] (also called NOC). A NOC can monitor the network 24/7 and intervene in case of issues, restoring as quickly as possible the connectivity by monitoring and controlling network devices such as switches, firewalls, or routers remotely.

This service has to be established with the right priorities kept in mind. As a network outage might cause production activities to stop, and as we saw in chapter 1 this is one of the highest risks for the OT environment, a service like NOC must be able to restore the connectivity very quickly at any time of the day or night. This is because production activity can happen even during the night or weekend, and even some minutes of network interruption could cause a severe problem in the factory. For this, response times must be as low as possible, on the average way faster than average IT network troubleshooting times.

2.1.3 Need to keep an accurate inventory of all the devices active on the environment

Keeping an accurate asset inventory for all IT assets of a company is a good security practice well-known in the industry [15]. There are hundreds of ways to implement this. However, the components that are most needed are a place to store all the asset information and one (or more) ways to automatically gather data from assets in the network to update the asset inventory automatically if some assets change their attributes such as, for example, firmware version, or IP address.

While also this solution is existing for years for handling various IT devices, depending on how each company has implemented it, it may be limited in its capabilities and not fully supporting the OT environment needs. One limitation, for example, can be how the data model for each asset has been designed. If it does not include essential attributes needed for cataloging OT assets (such as automation device type or manufacturer), it can be less effective in displaying information about various devices. Furthermore, the components that monitor the devices on the OT network to gather their information and update the asset database need to be tuned for the OT network. Similar to the situation of SOC (see section 2.1.1), the solution must be able to understand the various packets traveling on the network even if the protocols are not the most common ones. Also, most asset discovery solutions that operate with IT devices (e.g., PCs, Servers) operate in active polling mode, meaning that they contact device per device to ask them what their attributes are. That is not possible on the OT network because such high polling activity would impact negatively the performance of the network in a way that would be acceptable for an office, but when this network is used to exchange time-sensitive packets that control automation processes, this type of solution creates serious problems [16]. For this, a different kind of scanning is needed, meaning a passive scan that detects asset

information from what is gatherable by sniffing the regular network activity of the device itself.

2.1.4 Need to secure the endpoints from cyber attacks, in particular computers, that are the most commonly attacked devices

Even in the OT network, computers are still a common target for attackers [17]. It can be said that as being the same type of device used everywhere else in the company, it could be protected in the same way as all the other computers in the other environments. However, this is far from true. While still being technically identical, different computers may need different hardening policies based on how and where they are planned to be used. The most straightforward example that can be made is, again, the fact that office computers are expected to interact a lot with the internet and with various files. For this, they must be protected from remote attackers while still allowing certain freedom to its user. At the same time, it has to be avoided that the PC user could execute potentially dangerous actions by limiting his permissions (for example, by not conceding administrative rights).

On the other hand, OT computers, since they are designed to be installed and used in a segregated OT network where internet access is limited to specifically allowed resources, need to be hardened in a more robust way to restrict their usage as much as possible. Their infection by a hacker could potentially cause him to have direct access to the devices connected to that machine, such as PLCs that are controlling physical processes. At the same time, factory technicians need to be allowed to execute higher privilege actions on the devices when needed. While this in an office scenario would require the raise of a ticket to authorized personnel that

would execute the privileged action, for factory technicians, this step would cause additional hassle that would increase process times. For that, privileged accounts must be conceded to certain key people to conduct their business.

Finally, an OT-specific PC management service solves a big issue of many OT environments: unpatched and vulnerable computers used in factory floors [18]. Usually, office computers in big companies are leased for a specific amount of years, and they are changed frequently to keep them constantly updated to the latest system version. This is not always the case for factories, as most computers there cannot be substituted very often, which leads to a very heterogeneous amount of computers that are difficult to keep protected as years pass. With a dedicated service that addresses this issue by providing an OT-specific PC image and processes to support their maintenance and lifecycle, this issue can be significantly reduced.

2.1.5 Need to provide a secure and reliable way for people and systems to connect remotely, without sacrificing network security

Remote access is a very particular need that most companies are facing, especially since 2020 when the COVID-19 outbreak forced more and more people home and created a strong need for solutions that allowed users to safely and reliably connect to devices in the internal company networks without physically connecting to the LAN [19]. This is a very critical aspect for cybersecurity because a not well implemented remote connectivity solution would cause several potential incidents, from data being intercepted by remote attackers to the worst scenario of having an attacker bypass the authentication measures and connecting from the internet directly to a sensitive local resource [20].

Remote connectivity solutions are wildly adopted in IT environments, particularly screen sharing solutions that allow a user to see and control a computer of another user remotely. However, as they are implemented most of the time, they are not sufficient to cover all the OT environment's needs. This is because other remote connectivity needs are not addressed by this, notably having zero trust access. Zero trust approach means allowing external resources to access internal ones implementing a proper authentication process to allow the connection [21]. The most significant advantage is that, with this solution, almost every network integration is possible, allowing complex interactions between, for example, two OT sites in different parts of the world.

Also, zero-trust is not an OT-exclusive solution. Plenty of IT scenarios might see advantages in implementing zero-trust access. However, introducing, and especially managing, one in an OT network requires additional knowledge because of how the OT network is segregated behind several layers of firewalls. Thus it cannot be adequately done without the right expertise. The fact that OT networks must be as filtered and protected as much as possible from internet traffic creates a requirement for additional care to avoid exposing sensible assets to remote attackers.

2.2 Problem definition

As the analysis above shows, it is clear that IT services, while providing solutions somewhat similar to what OT environments require, do not fully answer the needs.

This is because it is not simply necessary to provide a service based on the type of devices that the service is intended to protect. It is also crucial to consider various factors such as overall goals, required expertise, and priorities. Talking about priorities, another important aspect for OT that is drastically different from IT, is

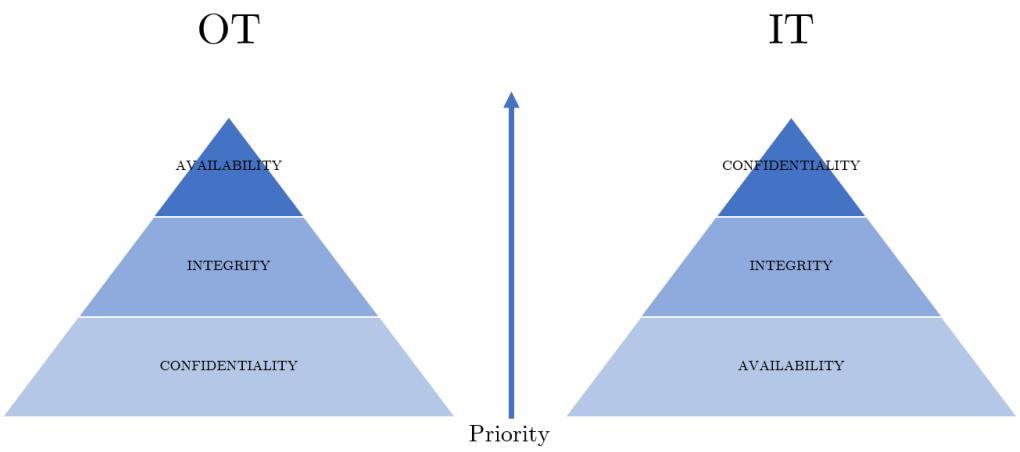

Figure 2.1: IT vs OT prioritization diagram

how cybersecurity prioritizes actions. A common concept in information security is the **CIA triad** [22]. CIA is the abbreviation of the three aspects of information that are important to protect: Confidentiality, Integrity, and Availability. While all these three aspects are essential to protect in IT security, priority is usually given to the confidentiality of the information. That is because particular attention is posed to keeping sensitive data secure from leaks and disclosures. In OT, however, the prioritization goes oppositely, meaning that confidentiality is somewhat less critical, while the highest effort made is to avoid availability issues because they could disrupt automation or, worse, create physical danger for people and things (see figure 2.1) [23].

With such profound differences between the two kinds of environments and how important it is to protect the OT environment, it is impossible to rely only on existing services. Instead, dedicated services and processes must be created to address OT needs, keeping the OT/ICS standards in cybersecurity in mind from the beginning of the design phase until the completion of the implementation and testing.

3 Requirements

This chapter lists the main requirements for the various OT services gathered before the design phase and explains the reasoning behind the definition of these requirements. The chapter is divided into sections, one for each development stream created for the various OT services.

3.1 OT SOC

3.1.1 Understanding of OT network activity

The first requirement is that the OT SOC service that will be created must have a profound understanding of OT network activity. As we saw in chapter 2, without proper knowledge of the environment, the service will not be able to operate correctly. For this, it is necessary to have trained personnel in the SOC service that has experience in OT to correctly monitor and operate on the network.

3.1.2 Close interaction between business sites and SOC

As Wärtsilä operates in multiple sites worldwide, it is impossible to implement a fully functional central service without considering the involvement of personnel

onsite. Their role in the environment consists of two primary responsibilities; they are necessary for assisting SOC in its proactive detection activities but also in acting directly in case any physical action is required onsite.

For monitoring activities, their value is very high. Even if the SOC detects some anomalous activity that potentially can be a security incident, only the local engineers can say if it is something unrecognized or part of legitimate activities made on the site. This communication is also valuable for helping SOC tuning their scanners to reduce the number of false positives in the long term. Finally, there are certain operations that, due to their nature, cannot be done remotely by SOC. For this, local engineers who operate in the OT environment must be ready to contacted by SOC to perform certain activities under SOC guidance and supervision.

3.1.3 Proactive monitoring of the network to identify potential threats

As somewhat introduced above, SOC needs to proactively monitor the network to intervene promptly if big "red flags" are raised. The damage of an incident can be significantly reduced or even completely avoided if proper actions are taken in time and, for this, being alerted before end-users start complaining about issues is of extreme importance. Furthermore, even false positives in the detection may highlight potential security gaps that malicious users may exploit.

3.1.4 Being able to provide support based on business time requirements

Different sites, and different zones in a site, may have different operational times. For example, some production activities may run 24/7 while others are active only during workdays. Regardless of the differences, SOC service should assist them whenever needed and plan its activities based on the operational requirements of the areas affected by them.

3.2 OT NOC

3.2.1 Operating as required by production times

Operating as required by production times is by far the most crucial requirement identified for NOC operation. While most of the time the NOC is simply monitoring the network, ensuring that everything is working correctly, sometimes issues in network connectivity or other aspects (such as network device updates pending) may require them to directly intervene on the network by remotely connecting to devices and rebooting them or edit their configuration. These actions may cause abnormal network connectivity, and they must be conducted prior accordance with local personnel. The approval of the local site, before any action is executed, is mandatory because while a network outage in an IT environment may cause certain services to become unavailable for some time, in an OT environment could cause physical damage to people present if, for example, they are connecting devices with safety systems. As was explained in section 2.2, availability is the most critical aspect in the OT environment, and a switch reboot at the wrong moment could cause what

all the service is designed to prevent.

3.2.2 Low response time

OT NOC should operate with very short response times, lower than the average response time given for IT infrastructure. This because even 10 minutes of downtime could cause important issues in the environment. In addition to this, being the NOC centralized and the sites scattered around the globe, the service must be developed to optimize the communication between the two entities to ensure that from the detection of the problem to its solution, the overhead time is as low as possible.

In addition to this, NOC monitoring needs to be immediate in providing notification to interested parties in case it detects network issues and not delay raising the alarm.

3.2.3 Being able to provide support based on business time requirements

As in section 3.1 for SOC, also NOC needs to operate in a way that ensures network availability to business based on their operational requirements.

3.3 OT Asset Management

3.3.1 Asset discovery solution needs to be designed for the OT network

Asset discovery is important because the large number of assets present in the OT network makes it difficult to manually insert and keep updated information in the asset database. For this, the discovery solution can be used, but it must be designed to operate in the OT network [24].

As it was already explained in section 2.1.3, the solution needs to be a passive scanner to avoid potential network congestion caused by the scanner pinging devices and these replying [25]. Also, the device should understand the different protocols that PLCs and other ICS systems use.

3.3.2 Integration of asset information with Incident management and change management processes

Having an asset management system is helpful if this information can then be used for something and not collected just for the sake of collecting them. For this, the final solution must be able to integrate seamlessly with incident and change management processes. These are processes that also involve SOC and NOC, as they are the entities that most often open incidents and act to solve them. Having the possibility of linking an incident to the affected asset increases the efficiency of these processes as the information would be easier to obtain.

In the same way, also change management processes see the benefit of this integration. If we take as an example a change request opened for substituting a switch,

the linkage of this request to the asset to be changed would first allow the people approving and executing the change to clearly understand what the device affected by the change is, but also it would allow an easier update of the asset database after the change, as the record to update is clearly stated.

3.3.3 Possibility of storing documentation related to specific assets

Even if asset attributes in most situations are sufficient to have a complete overview of the asset itself, in some cases, especially for more complex systems, it is better to have additional documentation in different forms to be attached to the asset itself.

For example, it is useful to see what the integrations involving one system or how to reach a specific device remotely. All these various information should be stored with the asset and need to be available only to specific people, following the least privilege principle [26].

3.3.4 Implementation of processes for ensuring proper update of asset information

As not all the information can be updated automatically by the asset discovery tool, there is also the need to implement processes that allow asset information to be updated in these other cases. For example, if an asset has its owner changed, there is no way to detect this by analyzing network activity. Processes must then be implemented to ensure this information is kept up-to-date. Business-related information is as essential as technical information. If there is an issue, it is vital that who is responsible for a device can be identified. Also, it is a must to understand

in what area it operates and what its function is.

Understanding and tracking asset owners is also more complex than in the IT environment because of the multiple parties involved in the ownership of the assets. Having an asset management database of IT PCs makes it easy to keep the information updated, as it is the IT office that assigns the devices to the end-users and takes care of changing them once their lifecycle requires. In OT environments, different parties are involved in buying new assets and handling them, making it difficult for a centralized solution to keep accurate information.

3.4 OT PC Management Tools

3.4.1 Development of OT PC image created for suiting OT PCs

As described in section 2.1.4, PCs used for different purposes need to be treated differently. Operating systems can be tailored to suit end-user needs by configuring them in different aspects. For example, their policy settings can be set as more or less restrictive based on what the end-user is allowed to do, but also their update schedules can be tuned to ensure that the updates are done regularly but not in a way that makes the device unusable when needed.

Also, the software available in the device can be fine-tuned to the environment the device is used in. In Microsoft Windows, for example, a common way this is done is by configuring the SCCM (System Center Configuration Manager) [27]. The SCCM allows a company to set up a software center where the end users can install company-licensed software without requiring administrative rights. The SCCM has

other functionalities, such as patch management and network protection, thus being a powerful tool for managing many Windows devices.

3.4.2 Flexible lifecycle of devices to adapt to business needs

Production sites are very different from offices also in how devices are kept. Usually, changing a device when it is used for general IT work is nothing complex. It requires a backup of the work documents and general user data to remote storage (inside company network or in the cloud), and the device can then be substituted with a new one, where then the user can log on using his company credentials to find everything he had ready to be downloaded. The software has to be reinstalled, but in general, it is a quick operation. This process makes it very convenient for companies to lease devices for their employees, meaning they are used for a predefined period, and at its end, the device is returned to the lender. Leasing ensures that employees always get modern machines to work with and, at the same time, protect the company from the need of paying for computer issues outside of warranty; if a computer gets malfunctioning because of hardware failure, the lender covers the expense by providing a new device.

In the OT environment, this can become a bit more complex. First, usually, cloud backups are not used due to security concerns. Of course, this can be addressed by creating dedicated network storage that resides inside the company LAN. But the biggest issue is the fact that the devices cannot always be substituted as easily because they are used in connection to specific hardware, meaning they have special drivers and software installed that allow peripherals to communicate with the computer. As these computers are then used for controlling these devices, often involved in the operational processes, it cannot be expected that they are treated as normal computers that can be easily swapped every 2 or 3 years when the lease contract

requires it. Another approach is then needed, allowing machines to be used for a predefined period, but with the possibility of extending their usage when required.

3.4.3 Centralized user directory with group admins to execute locally privileged actions

Most computers in the OT environment, differently than office ones, are shared by multiple technicians. Having multiple employees working on a machine simultaneously means that using personal accounts, which are the way people log in to their desktop in IT computers, is not always as convenient. If a user is logged on and running a task on an engine connected to the computer, and someone else needs to monitor the parameters, he will use the user account that is already logged on. This scenario usually leads to shared local accounts (so not company managed) being created on the machines and left unlocked to be easily accessible while working. This situation is less than ideal, and while revamping the way OT PCs are handled, it is also a requirement to solve this issue by finding a way to centrally manage the OT PCs accounts and not make their usage too cumbersome for OT engineers.

3.5 OT Remote Connectivity

3.5.1 Be able to solve screen sharing and zero trust access needs

As described in section 2.1.5, the need is to find one or multiple solutions to solve both screen sharing and zero trust access needs. Screen sharing can be used for multiple purposes, from letting a technician monitor a process simply connecting

to the computer that controls it to offering technical assistance remotely in case of issues. Zero trust access is way more versatile. It allows integration between systems treating internal and external traffic in the same way. It always requires authentication to allow a connection, no matter if the source is the internal LAN or the cloud. This solution allows great flexibility because it lets an internal device operate with a cloud one without requiring complex configuration to implement it securely; once the zero trust appliance is deployed in the network and configured, it will be easily adaptable to all required use cases.

3.5.2 Necessity to solve both internal and externals needs

The solutions that will be used need to solve all the needs related to remote connectivity, including managing both external and internal users. It can be expected that remote connectivity sessions would not only be used by Wärtsilä employees. Some sessions, especially screen sharing ones, would see the involvement of external users such as device manufacturers for technical assistance and Wärtsilä partners and suppliers. For this, the solutions identified need to allow easy user provisioning both for Wärtsilä employees and externals while also allowing great user rights management to avoid allowing external users to perform unwanted actions.

3.5.3 Complete logging of sessions

Logging users' and systems' actions is one of the most common best practices in cybersecurity [28]. Logging allows accountability for actions taken, but it also proves very useful in troubleshooting issues for identifying the root cause. Remote connectivity solutions, since it involves remote users executing actions on local machines, require verbose and complete logging of actions done during the remote session [29].

Screen sharing sessions should be able to log both screen recording and any action or command executed by the guest in the host computer.

3.5.4 Be convenient to implement correctly in a fully segregated network without requiring workarounds that may affect the security

Ideal solutions should be deployed in complex networks such as those in OT sites, meaning that then should work in a heavily segmented network. The solutions should not need complex network changes or, worse, workarounds that may affect the network's security. They should natively support implementation in all kinds of networks and, once deployed, function without excessively complex firewall configurations that make it more difficult to manage the security of the LAN.

4 Design

After defining the requirements, the first phase of the project began, meaning the design of the various solutions. The design of the solutions was made before their implementation. Because of that, it has not foreseen various problems that arose in the later phases that required the design to be adapted to solve them. In this chapter, it is not described the final solution, rather how the initial requirements shaped into the first idea of a solution that could start being implemented.

4.1 OT SOC

For starting designing the Wärtsilä OT SOC, the first step was understanding how things were handled in the general IT environment. Wärtsilä already has a SOC internally that is responsible for responding to security incidents. As Wärtsilä SOC was already in charge of security incidents management, it had great expertise in incident management inside Wärtsilä, as well as excellent knowledge of the company, something that no external service would be able to provide. However, it lacked OT-specific tools and would not efficiently monitor the OT network for anomalies without additional resources.

For this, it was planned to acquire an external supplier (from here on called

supplier A) that took care of network monitoring and collaborate with Wärtsilä SOC. This supplier already had other responsibilities in managing the Wärtsilä network and seemed a perfect candidate also for this new role, as they were able to provide also OT oriented resources to assist Wärtsilä during the deployment of the service as well as to conduct it during the operational mode. One of its responsibilities was to provide 24/7 monitoring of the OT network, they provided the monitoring solution to be installed in the various sites and took care of its management.

The monitoring solution it was agreed to use was great for Wärtsilä needs because of multiple factors:

- It is designed to monitor OT-specific network traffic, supporting a large number of OT related protocols
- It provides passive scanning of the network
- It offers asset discovery capabilities, proving useful also for being used as part of asset management solution

Supplier A not only forwards alerts coming from the monitoring solution to Wärtsilä SOC. It also has to process any alert directly, providing a parallel SOC service, also active 24/7 to respond to potential incidents. Depending on where the alert was coming from (monitoring or incident report), both Wärtsilä SOC or the supplier could open an incident ticket that is then processed by both parties in collaboration.

Incident analysis often requires information gathering from all informed parties. This often includes people working in OT sites, meaning OT engineers, that operate the devices in the network monitored. For this, it was planned that, during the

information gathering phase, Wärtsilä SOC gets in contact directly with OT engineers through the Wärtsilä ticketing system, allowing them to reply to SOC inquires to assist them in determining what false positives are and what incidents are to be further investigated.

This information can be used by supplier A to tune the monitoring solution to reduce the number of false positives in the future. The monitoring process, and all the incident management process is subject to a constant improvement based on the study on closed incidents.

4.2 OT NOC

Thanks to their experience with the OT network, it was planned to use supplier A also for ensuring that the network is kept operational through a NOC service.

Unlike for OT SOC, it was not planned to have an internal one as it was not deemed necessary and would only increase overhead times. As in SOC, monitoring is also a big part of the NOC service. NOC has direct access to the network device management to be able to check their status as well as intervening in case of issues.

In case an incident is detected, NOC has to notify Wärtsilä and act to re-establish connectivity. Incidents can also be opened by Wärtsilä by getting in contact with the NOC service directly. In any case, NOC takes the lead in acting to solve the issue at the agreed time. At the same time, it keeps in contact with Wärtsilä, addressing directly local OT engineers in case any information or physical action is required to solve the issue. The Internal OT security team may also be consulted in case an additional opinion is needed.

In case a permanent change in the network is required, Wärtsilä still has to

approve the change through an approval chain that involves in the first place the internal OT security team, but also other network teams inside Wärtsilä as the change could also affect devices outside the OT network. A change request in the OT network can be opened by NOC in case the change is needed to solve an incident but can also be requested by OT engineers in the site if they need any change in the OT network. No matter what is the source of the request, it still has to be approved by the OT security team if it involves changes in security configuration or any setting that can affect the overall security of the network. OT NOC would execute any change required after obtaining the required approval. Wärtsilä internals, primarily OT engineers, need then to check that the change is working as expected and not causing any issue in the environment. After the change has been concluded, the internal security team takes care of documenting it. This activity includes updating the asset management solution better described in section 4.3.

NOC, finally, also takes care of operational tasks related to network devices, such as ensuring their software is updated to the latest version. Any activity that affects network operativity (e.g., device upgrade) needs to be agreed upon by NOC and the OT site following the same communication channel used for incidents (see section 5.2 for details regarding the implementation). As explained in section 3.2, the agreement between NOC and local business is critical before any action on the network is executed to avoid that network downtime could cause production issues or, worse, physical incidents.

4.3 OT Asset Management

The asset management solution was designed keeping in mind that its primary purpose is to support various services in the OT environment and to help the various

teams involved in having a clear understanding of the environment.

For storing the information about the various assets, it was planned to use the same platform that was used for all incident management processes, which is *ServiceNow*. ServiceNow supports natively the creation of a CMDB (Configuration Management DataBase) [30], that proves perfect for this purpose. Note that a CMDB is not an asset management solution by itself, but it is a good starting point to create one for various reason:

- It allows the creation of a database of devices that can be accessed easily
- The data model is flexible, meaning it can be adapted to the needs of OT environment assets cataloging
- Every asset is linked to a CI (Configuration Item) that can then be used as a reference to the CI in any ticket (both incident ticket and change management ticket)
- ServiceNow is a well-recognized solution for managing company workflow in various areas, and using this solution will allow future integration between other systems still not in the scope
- ServiceNow also allows handling company knowledge base, making it easy to create additional documentation for a specific asset and then liking them together

The OT asset data model was designed to store all the information deemed necessary for having a good understanding of any OT asset, this includes:

- **Asset name**, or how is identified in the company

- **Device type**, such as PC, Switch, SCADA, PLC, sensor, etc.
- **Business information**, such as asset owner, location, and department
- **Software information**, such as firmware, operative system, CPE [31]
- **Hardware info**, such as device manufacturer and model
- **Criticality**, to highlight how important that specific asset is for site operations

Also, the CMDB was divided into three major categories: OT Servers, OT Network devices, and OT other devices to make the CMDB easier to browse.

A CMDB, however, is just a database used for storing information about assets, and alone it cannot be considered a valid solution because it lacks all the processes that are required for keeping it updated and accurate. The first way the CMDB is kept updated is through the asset discovery solution, also used by OT SOC. The solution needs to automatically send data to ServiceNow CMDB and update the asset information automatically without requiring user interaction. This is helpful also for filling up the CMDB the first time, as manually inserting thousands of devices into the database manually would have required too much effort. However, automatic updates should not happen in some instances, primarily when an update would edit an attribute that is not supposed to change autonomously. For example, a device is not expected to change its IP address automatically, and if that would happen the automatic update should not execute, and a notification is sent to the OT security team for manual check and eventual update.

Of course, there are plenty of cases where a manual update of the CMDB needs to be done instead, primarily when an asset gets retired or has some settings changed due to a change process. In the case of retirement, it is the asset owner itself that needs to report it to the correct office for them to update the CMDB, while in case

of change, it is defined in the change process itself who is responsible for updating the documentation (including CMDB). For example, in the case of network devices, the OT security team must document the change after NOC has executed it.

4.4 OT PC Management Tools

OT PC management tools stream applied various changes in how OT PCs were handled. Probably the biggest one of these was the creation of the OT PC image. This is a version of Microsoft Windows 10 that has different settings than the one that is normally installed in Wärtsilä company devices.

The first change is the more restrictive hardening settings that are applied compared to standard computers. For example, certain internet-related services are disabled on these machines to reduce the number of external connections of these devices. The policies are not only more restrictive but also more adapted to the specific device situation, as a general policy could not address all OT use cases due to how different the activities are from one area to the other. Another change is what software is installed natively on these devices. As these machines are not supposed to access the cloud, several internet applications such OneDrive or Office 365 are not available on these devices, being replaced by offline versions where required. Of course, some online connectivity is kept for authorized integration and for keeping the devices updated to the latest OS version.

Also, these devices need have a completely separate Active Directory domain, so the accounts and the policies are handled separately from the IT environment. OT computer accounts can then have, for example, different maximum password age or complexity requirements to better adapt to the security level that was planned to be achieved but at the same time not overcomplicating things for OT engineers.

Moreover, a new SCCM had to be developed to handle software installation and device patching, so company software needs to be approved for OT usage separately.

Furthermore, the OT computer lifecycle has been designed differently than regular PCs. OT computers will be purchased from the same supplier that leases our devices. This will allow the devices to be kept in operation as much as needed, even if it was designed for a nominal life of 5 years. In case it is needed, the lifecycle can be extended. For example, if a computer is connected to a system that is replaced in 2 years, the computer renewal can wait for that moment.

4.5 OT Remote Connectivity

It was planned to have two different sub-streams for OT remote connectivity. One stream researched for a solution regarding a valid screen sharing application, and another looked into finding one that solved the need for zero-trust access. As these solutions are relatively complex to be developed internally, it was opted to look in the market and find the most appropriate solutions that would have been suitable for our needs while having a pricing model that would be convenient for our use case.

While the two solutions are different, they still both require to be used in the OT environment and, for this, it was set as a vital requirement the possibility of integrating these with the OT Active Directory, so OT user accounts can be granted various rights related to remote access, without needing additional accounts. Also, the solution should support accounts coming from different organizations natively; in short, being able to implement federated access.

Both solutions need to have a very granular permission control. For example,

certain users may be allowed to connect only to some machines at certain hours remotely; and others may connect to other devices but only after approval by a responsible group. This is important as it would be risky to allow unauthorized users to connect to factory machines. Also, the actions that can be taken by a guest should be defined by the role of the user. For example, in a screen sharing session, certain users may not be allowed to transfer files from and to the host or may not be allowed to access peripherals or execute commands directly.

Finally, as defined better in the requirements solution will have strong logging capabilities to ensure that no action can be performed remotely without knowing. This has a double use: first, it makes people accountable for their actions, even when remotely controlling another user, but also this logging can be used as a "black box" to diagnose any issue that may arise after a remote session. The ideal solutions support different kinds of logging:

- Logging of sessions and connections
- Logging of failed authentication attempts
- Screen sharing session recording
- Remote commands logging
- Chat host-guest logging
- Logging of particular actions done by the guest (e.g., blocking host mouse/keyboard, send files from/to host machine, taking screenshots)

5 Implementation

This chapter will describe how the services were implemented, starting from the design drafted in chapter 4. It will be described more in detail how integrations between service components were handled. These streams were developed simultaneously except for OT remote connectivity where, due to various reasons, the development started some months later. However, since this stream is more independent from the others, timing has not caused issues. Differently, the other streams needed parallel development as they rely on each other. For example, SOC service would be less effective without proper integration with OT asset management.

5.1 OT SOC

The implementation of SOC service included two main parts. The installation of the OT network monitoring solution and the implementation of the processes in ServiceNow. Of course, also on the supplier side, some development was needed to put their SOC up and running. The development of this part was done outside Wärtsilä, and it is not part of the scope of this thesis.

5.1.1 Implementation of the monitoring solution

For the monitoring solution to work, it needed to have complete visibility of the network. As this solution cannot scan the network by itself being passive, the network needed to be adapted to route copies of the traffic to the solution for it to record and analyze it. This adaptation is easily doable by modern network devices thanks to traffic mirroring, allowing network packages to be duplicated and sent to multiple destinations, such as the intended receiver and the monitoring solution.

The monitoring system then sends the data directly to the Supplier SOC through the cloud so that they could access the data collected, and alerts can be raised to Wärtsilä in case issues are detected.

The most challenging part in this part of the implementation certainly is to configure the network in a way that all the traffic is received by the appliance, and, as a second challenge, to implement authentication correctly so that highly sensitive data such as that stored in the IDS are not accessible by unauthorized people.

5.1.2 Implementation of the SOC processes

This second part was certainly more complex to implement than the one above. Incident management handling of a completely new service in ServiceNow requires multiple actions to be done.

First, the integration between the supplier and Wärtsilä systems needed to be implemented to enable the supplier to start the incident management process without additional manual activities. This development was a relatively quick process as the integration between the supplier and ServiceNow was already existing because of other IT services they were already providing to us. Thus it only required

a reconfiguration to open the ticket with the correct categorization and for the ticket to be assigned to the right support group (Wärtsilä SOC). The integration is practically done through simple RESTful APIs. For this kind of application, they provide simple implementation while still achieving good security through proper authentication.

Once this part was done, it was a matter of involving the right people in the process and enabling them to process the incident through the platform. For this, support groups were created in ServiceNow. Support groups are simply groups of one or more people that can have some tickets assigned to them, and they are responsible for processing the ticket in question. As Wärtsilä SOC, because was already existing in solving IT incidents, did not need a group for them, the groups that had to be created were the ones of the internal OT team and the ones of local OT engineers working in the sites. The internal OT team comprises the people working in Wärtsilä as cybersecurity specialists for the OT infrastructure and was needed mainly when a particular incident would require their consultancy for addressing the issue. For the local OT engineers, instead, for each Wärtsilä site, a single group is created. When Wärtsilä SOC analyzes an incident and needs information from the site, it would not be manageable if that ticket goes one single group counting multiple sites. It would cause two main issues: first, the ticket would most probably be left unanswered as it would be problematic to understand for local OT engineers to understand if the ticket is related to their site; secondly, it would cause a severe confidentiality issue, as information of a specific site network activity cannot be shared with other sites.

Finally, how incident tickets were decided to be handled was this: for each incident detected or reported, an incident ticket is created. Every incident then has multiple sub-tickets, called incident tasks, that can be created and assigned to various support groups. This method allowed SOC to centralize incident management

but allowing the delegation of a specific task to some groups without losing ownership of the incident in question. This results in multiple tasks being opened and closed for each incident and allows better logging of the actions conducted to process each incident. Once all the tasks are closed, the SOC can close the main incident, officially marking it as solved (or, in some cases, unsolved).

5.2 OT NOC

OT NOC service is somewhat simpler than SOC in terms of incident handling as it does not involve such complex incidents, and the lead in processing incidents and solving them is done by the supplier.

Allowing supplier A to monitor our network devices was a matter of setting up a way to securely access Wärtsilä internal OT network, for example, with a VPN tunnel. The complexity in implementing the NOC processes, similarly to SOC, is to correctly enable various parties to process both incident and change management efficiently.

This service was developed by improving the implementation multiple times because, due to company needs, it was needed to start piloting the service even before the optimal implementation was achieved. The first way the process was implemented was to use direct email communication between the NOC and various Wärtsilä groups. Whenever an incident is detected, NOC contacts internal OT support and local OT engineers, thanks to a contact list shared with them. This list included the name of the contact, email, telephone number (for high priority incidents), and area of competence. These are enough details for NOC to address the right people in case information or actions are needed. This simple email communication is enough for handling simple incidents as tracking the ticket is done on

the supplier's internal system by using the email conversation as ticket notes. This has some limitations, however. First, it can become hard to keep track of the opened incidents through email conversations alone, and while the tickets are tracked and stored in the supplier platform, there is no long-term storage of tickets inside the company, and that may be needed for future analysis and general logging purposes.

While this first process went into testing during the piloting phase (see chapter 7), the development of the improved version immediately started. The new process utilizes ServiceNow to keep track of open tickets on the Wärtsilä side. If an internal employee notices a network issue in the OT environment, it has to contact the company service desk instead of contacting NOC directly. The service desk would then open a ticket in ServiceNow and send an email to NOC linking the entire email conversation to the ticket. In this way, all the exchange between NOC and Wärtsilä support groups happens through ServiceNow and will be automatically registered in the ticket. If it is NOC to detect an issue, they will contact the Wärtsilä service desk themselves, obtaining the same result. In this way, both Wärtsilä and NOC always have any incident ticket registered in their respective systems. The disadvantage of this methodology is that the standard process became a bit more complex, with NOC having to get in contact with local OT engineers through ServiceNow, but this can always be avoided in an emergency; in that case, NOC could get in contact directly through the phone and any action planned is be registered in the ticket thanks to the email integration afterward.

This new system is better for handling change management because, in this way, only tickets approved by the internal OT team are sent to NOC by ServiceNow for them to execute the change. With direct email exchange, it was possible for locals to ask for actions directly to the NOC and, if these were executed without internal OT team approval, there would a potential risk of security issues if no security specialist

would properly analyze and approve the change.

5.3 OT Asset Management

The OT Asset Management development was required mainly to prepare the ServiceNow CMDB for storing OT asset data, setting up the integration to get the data from the monitoring platform to the CMDB, and implementing the processes to have the manual updates regularly executed.

5.3.1 Implementation of the CMDB

Implementing the CMDB was not starting from scratch as ServiceNow natively supports CMDBs, and it mainly required configuring the CMDB instance to be compliant with the asset model created in the design phase.

However, the initial asset data model did not consider some attributes included during implementation time. For example, when OT PC management tools stream implementation and, in particular, the OT PC order process proceeded, it was understood that it was necessary to add some attributes to store OT PC-specific information such as device delivery date and warranty expiration. Thanks to the flexibility of the platform, these changes could be implemented in a very short time. It was implemented the possibility of assigning each asset to incidents and problems, as it was one of the requirements set in the beginning.

In general, the implementation of this was completed without significant issues. Some minor bugs were quickly fixed after an accurate User Acceptance Testing (UAT) phase, where all the essential features were tested to ensure nothing was

missing and assets could be created and processed correctly.

5.3.2 Implementation of the integration

However, integration between the monitoring solution and ServiceNow CMDB was trickier and required more time and effort to complete. The integration consisted of a ServiceNow application developed for Wärtsilä by the manufacturer of the security monitoring solution. The application works by using the monitoring solution APIs to authenticate and fetch a list of assets and their attributes from the solution and match these to the ServiceNow CMDB table. IP and MAC addresses are used as unique identifiers for the assets to match the data and update the correct fields in the CMDB. The solution is scheduled to run every 12 hours, deemed acceptable as the maximum delay time for updates.

The significant issues that were encountered in this phase were various. The first version of the application developed by the manufacturer could not update asset information but only able to create new assets. That was not ideal because it would have served well the purpose of populating the CMDB with all the OT equipment, but it would not be able to keep the database updated, which is one of the main requirements set at the beginning of the project. After clarifying the issue, it was possible to start developing this feature, but this raised another issue. ServiceNow applications require a lengthy verification process before being available to install on the platform, and this applies to updates too. This problem increased the development time by weeks and required to postpone the testing of the asset management solution. Luckily SOC and NOC processes and PC management tool stream were able to move into testing sooner, operating without the support of the assets data.

5.3.3 Implementation of the processes

Processes were reasonably easy to implement as manually updating device information was something most teams were already doing for the IT CMDB. Mainly the most important part was to define who was responsible for each asset group. For servers, it was decided that the same team handling IT servers was going to be the one responsible for managing also OT ones, meaning their responsibility was also to ensure that any change was correctly reported in the CMDB after the execution. For OT PCs, these changes are handled by the PC supplier's local support, while for network devices, it is NOC's responsibility. However, as NOC cannot access Wärtsilä CMDB, it is the responsibility of the OT team to update the CMDB record for the affected asset. Updates on the CMDB are planned to be executed after the closure of the change during the documentation update step.

5.4 OT PC management tools

OT PC management tools implementation required multiple activities. One was developing the OT PC order process, making OT PC available in the company tools catalog, and ensuring that when a user orders one, all the necessary information is being passed to the proper parties and recorded in the OT CMDB. Another critical step was to deploy the systems necessary to make OT PC images run (Active Directory and SCCM) and, finally, migrate the already existing OT PCs to the new environment.

5.4.1 OT PC order process implementation

To allow OT engineers to buy OT computers, it was needed to create a process that allows them to make a simple tool order, as for other IT devices, and handle all the phases of the order from the buy phase up to the moment the PC is ready for pickup at the location selected by the purchaser.

The first step was to create a product entry for the selected models in the company IT catalog. The order form was also modified to add a new checkbox where the user can specify that the computer would be used in the OT environment. When this option is selected, the computer is reported as OT in the order, and the supplier, knowing that, would not pre-install the 'standard' operative system, delivering directly to the factory specified by the person that made the order. When the order is confirmed, and when the device is shipped, the purchaser is notified through email and, during these steps, various information about the computer is gathered and used to create a record in the OT CMDB. Once the device has arrived in the factory, the local support of the supplier takes care of installing the OT PC image in the device. After the installation is performed by the local support, the purchaser is notified that the computer is available for pickup, and the OT engineer would have a machine ready for use.

Particular issues found during this implementation were how to get enough data to create the asset record during the order process. This because MAC address was a critical attribute necessary to get at order time; otherwise, the discovery solution would not be able to recognize the record created during the order and would create a duplicate entry when the device would appear on the network. To cope with this issue, it was agreed with the device distributor that the confirmation of dispatch of the device has to include also the MAC address of the machine. In this way, the

attribute is available to be used as a unique key to identify the PC asset record.

5.4.2 Preparation of the environment and migration of existing computers

Migration of the IT PCs present in the OT network to the new OT PC image was undoubtedly the most challenging part of the stream, requiring multiple changes in the approach before being conducted successfully.

Initially, the thought was to divide the existing computers into batches and upgrade them by reinstalling the new image. This soon was proven impossible for multiple reasons. First, there were not enough spare machines to allow this without disrupting operations in the factory. Most of these computers are needed every day, and even a stop of 2-3 days on multiple machines would affect site operations. As a second issue, reinstalling machines without testing that the business application would work with the new policies and hardening rules creates the risk that machines would stay unavailable for weeks before the issues are fixed.

For this, it was planned a more careful approach. Instead of requiring the machines to be formatted and reinstalled, the changes brought by the OT PC image were manually implemented, but in 3 phases instead of a single one, starting with only 2-3 machines for each area. The migration proceeded as follows. First, the pilot machines were identified, and Office 365 was substituted with Office 2019 to allow these to run without connection to Microsoft servers. The same was done for the antivirus, to connect it to the OT controller instead of the IT one. Then, the new hardening settings were applied, and the various business application could be tested with the new settings. As soon as all the applications were tested and working successfully, the rest of the computers could be divided into batches and hardened

safely. Only then were the PCs finally moved to the new OT Active Directory, and the new OT SCCM substituted the IT one.

5.5 OT remote connectivity

After testing multiple solutions, it was opted to go with one that was able to address both the screen sharing and the zero-trust access needs. The solution required one master node to be deployed and to be reachable by all the sites. For this, it was decided to opt for renting an IaaS (Infrastructure as a Service) machine on the cloud and installing the virtual appliance provided by the solution there. An alternative would have been to install a physical solution on our environment and configure the firewalls to allow other sites to be able to connect, but it was decided that having the central node in the cloud is more convenient to deploy and maintain without having additional risks as the traffic has to travel through the internet in any case.

All the remote connections are started by contacting this appliance, and this one, after checking that the connection is authorized, initiates a connection to the target host. In every site, a jump host is placed in the OT DMZ. This allows to create a single rule in the firewall, the one that allows the connection between the cloud appliance and the jump host, instead of allowing all the clients to be reachable remotely by the appliance. Then the jump host relays the connection to the client.

Authorization of connections is implemented by defining multiple user groups. To each group, plenty of privileges can be defined, from what type of connection they are allowed to open to precise settings such as what folders in each machine are allowed to access. Then groups of approvers are created. These users receive an email notification whenever someone is trying to open a connection, and they can allow or deny it. This is very useful, especially for externals such as vendors, to have

complete control over their connection to internal systems.

This system will be used whenever needed, also to allow connections between IT and OT devices. In this way, it is possible to have a single firewall rule instead of opening multiple paths that can be exploited by an attacker. With this approach, the IT network is treated in the same way as the cloud, requiring a strong authentication in any case (following the principles of zero trust).

It was decided to use LDAP as the protocol for handling user accounts as it was the most adapt to our use case, as all the users in the OT environment would have a personal account in the OT Active Directory. Externals have accounts in this AD too, of course, their privileges are limited based on their needs.

Finally, the solution fully supports all the kinds of logging expected to have, down to the forensic analysis of each connection, tracking every action done, and allowing for easy search. It is also possible from the log to go precisely to the point any action was done in the video recording. This functionality can be helpful to observe why, for example, a command was typed in the console.

5.5.1 Implementation of the processes

Parallel to the technical implementation of the solution, the implementation of the various processes for enrolling users and machines to the platform was defined.

In order to ensure that local users are easily able to be enrolled in the platform, it was agreed that the OT support team needs to authorize only privileged accounts and accounts that require abnormal permissions (for example, a user in Spain requiring unattended access to machinery in Finland). For standard requests, local supervisors can authorize the request to reduce processing time.

6 Use Cases

After the services were implemented, various use cases to perform testing without forgetting important aspects were defined. This step is essential as testing could not be adequately done without a clear understanding of the various ways the system was expected to be used.

6.1 OT SOC

For security incidents, every user needs to be able to report a security incident, and that needs to be received by SOC. At the same time also alerts from monitoring needs to be escalated to incidents whenever the supplier A SOC deems it necessary. The incident process needs to progress without problems, and, more importantly, SOC needs to be able to contact the other support teams (primarily OT local support), and the incident tasks need to be processed and closed correctly.

6.2 OT NOC

In the case of NOC, OT engineers have to be able to report network problems quickly, and NOC has to be able to start working for a solution quickly. At the same time,

NOC monitoring should prove capable of quickly detecting any disruption without relying on user reporting to start acting. Also, the process should proceed smoothly in this service, and communication between Wärtsilä and NOC should not be slowed by unnecessary delays.

Furthermore, OT engineers should also be able to request changes to be done on the network, such as assigning a switch port to a specific VLAN or allowing integration between two systems. However, the OT team needs to be always able to verify the change before the execution made by NOC.

6.3 OT Asset Management

The OT asset management system also has to be tested thoroughly. In particular, it must be tested that all kinds of OT assets can be correctly assigned to tickets by any party taking part in incident and change management processes. Then OT support team also needs to be able to edit manually any attribute in the assets, even the ones created automatically by the monitoring solution.

OT support, Wärtsilä SOC, and OT local support should be able to use the search functionality to quickly get information about assets from basic information such as IP address or device name. Moreover, any documentation related to the asset should be easily reachable. Incidents related to the asset should be available on the asset page. This also includes past incidents to monitor assets that have an anomalously high number of incidents. Finally, changes should always include asset database update as part of their process.

6.4 OT PC Management Tools

For OT PCs to successfully pass the testing phase, users should not report significant issues using their machines. The devices should be fully able to perform the activities they are appointed for, but at the same time, the hardening should block any potentially risky operation. The responsible of the various OT areas should be able to use privileged accounts to perform maintenance actions without additional assistance, but these actions must be logged appropriately.

Also, the PCs that have been migrated and are not newly ordered should operate in the same way as brand new OT machines, without exceptions.

6.5 OT Remote Connectivity

Defining a complete list of use cases for remote connectivity to test is problematic because, thanks to the nature of the solution implemented, the ways it can be operated are various.

For sure, one of the first needs is remote screen sharing, allowing users to remotely connect to their machines in the OT environment and enable them to operate from anywhere in the world. Also, for the cybersecurity team, logging these sessions should be easy to analyze to detect anomalous actions.

A complete list of different types of connections to be tested would not be possible to be done here, but the testing can be considered successful if all the possible kinds of remote connections can be set up securely. Primary examples are the connectivity to PLCs and other ICS equipment and integrations between multiple OT sites.

7 Testing

Testing of the solution was done starting from one single site to limit any issue that could arise to that site only. The plan was to pilot the changes in the first site and learn what can be improved so that the rollout in the other site would progressively be optimized. In this section, it is highlighted for each stream what were the major issues found in the testing and how it was planned to address them as well.

7.1 OT SOC

OT SOC service did not immediately proceed with full operational mode since the start. As the monitoring solution required some time to learn what regular network traffic is on the site. Initially, a high number of false positives was expected. It was opted not to report any incident and have a weekly meeting to analyze the main alerts coming from monitoring. In this meeting, supplier A's SOC shows the alerts raised, and the OT engineers in Trieste, based on the IPs and the date and time of the alarm, try to understand if that was an actual alert or a false alarm. As expected in the first weeks, several of them were normal and legitimate operations, and with this collaboration, the monitoring could be tuned for reducing these warnings. This phase of the testing went well as the people in the local site were aware of what was happening in the network, even recognizing devices just by knowing the IP or even

the Mac address. An asset management system provides a great help in this step as it can keep all this information, but it was not available since the beginning of the SOC stream.

When the monitoring solution was deemed sufficiently accurate, the normal SOC processes started as described in the previous chapters. As Wärtsilä SOC was already used to these processes, the most significant effort to be made was more on the local site engineers' side. They needed to be trained for the new way of handling security incidents. All OT engineers were entirely new to incident management processes, which was the biggest challenge to solve during the testing phase. However, the usage of a platform like ServiceNow simplified the workflow. It helped OT engineers to learn the process faster and, thanks to multiple training sessions, the engineers understood their duties in processing incident tasks, and the process started to work as expected, even with some minor delays due to the response time of the OT local support group. This delay has been deemed not a big issue as high priority incidents would be appropriately marked to achieve a faster response time.

7.2 OT NOC

As described in section 5.2, the testing of the NOC services started before the ServiceNow platform was ready to handle incidents. For this, the first incident was addressed using standard emails between NOC and Wärtsilä.

NOC monitoring proved to be very reactive in communicating network issues to the OT support team, and most of the incidents were easily solved in a short amount of time. Also, the requests from the local site were properly reaching NOC and were addressed as expected. One crucial issue emerged. When OT local site engineers were requesting NOC changes, they sometimes ignored involving the OT

support in evaluating and approving the change in question. This lack of OT support moderation was a problem not tolerable in operational mode, and for this specific reason, the involvement of ServiceNow change management has proven to be helpful.

After implementing a proper ticketing system, the tickets were easier to process, still maintaining the necessary speed thanks to the possibility of using telephone calls whenever an action was considered urgent. Collaboration between the local site and NOC met the expectations, and for this, the solution was accepted as valid.

7.3 OT Asset Management

As explained in section 5.3, asset management service faced issues during implementation, primarily integrating the asset discovery solution and the OT CMDB. For this, the piloting of the asset management started without any automatic feed from the monitoring solution but simply by manually adding the most important assets such as network switches and OT PCs to the CMDB. In this way, these assets could be tracked in other processes such as change requests in the network or security incidents.

Even with this limitation, the CMDB proved helpful in supporting the other services and tested successfully providing valuable insights during incident and change management processes.

When the implementation of integration was completed, the service became even more effective, storing even more devices that were not possible due to the large number to be manually added. This capability decreased the time and effort required for solving incidents as, for example, SOC could check information related to site assets without requiring local engineers' consultancy.

7.4 OT PC Management Tools

OT PC ordering process was tested successfully, and the devices were delivered as expected from the supplier. The OT PC image was proven capable of responding to the needs of the OT site.

Migration activities proceeded even with some issues. One issue faced in the migration was how to handle existing devices that were of the most various models and system versions. While the new models were limited to 4-5 different types, the old PCs to be migrated were various. Some of them were not even upgraded to Windows 10, and this caused issues with the Office 2019 installation as having the latest version of Windows was a minimum requirement for the installation. However, the migration proceeded with the rest of the devices, and the business applications were tested successfully by the OT local engineers.

The more complex machines needed manual hardening, and the oldest ones, which were too difficult to be migrated and kept supported, were substituted with new OT machines ordered using the new order process already successfully tested. This caused some additional costs for local sites as they had to substitute multiple devices, but they believed that keeping old devices in an active production environment would not be sustainable in the long term.

7.5 OT Remote Connectivity

OT Remote Connectivity solution testing was the latest to be started and, while still ongoing, it is showing very promising results. The testing was conducted in the same ways as for the other services: piloting sites were utilized to check how the solution worked and gather feedback. The users of the designated sites stopped

using the locally-managed remote connectivity solution and got enrolled in the new solution.

The practical use of screen sharing and remote access solutions was already known for local engineers so learning a new solution was not problematic. They, however, had to learn how to request adding new machines to remote access properly. As these requested must be approved by a supervisor, it was not possible anymore for local businesses to install a remote access client on the target machine as any unauthorized connection would be blocked by the firewall. Instead, they had to manually raise a change request for a machine to be added as a possible host device and, after the request was approved, the requested machine would be reachable remotely by that user. This ensured a better analysis of business reasons behind every request and easier traceability of every remote connection allowed in Wärtsilä.

8 Conclusions

While a first attempt in trying to resolve the problems caused by the particular needs of the OT environment, these services made a significant difference for both the overall security maturity of the sites and the people who worked in them.

Implementing services specifically targeted to the production environment and appointing dedicated people to run them ensured that the right priorities were always taken into account by all the parties involved. The close integration of local OT engineers in the various processes was one of the most positive changes relative to the past as they demonstrated to be an excellent source of information for understanding what is happening in each area of the site. It also let them express their needs without the need for intermediaries that would have increased the process complexity while losing contact with the real needs of the business.

Including local businesses in the centralized cybersecurity processes required a special effort to train them in executing these new roles they had to cover, but the positive note is that they recognized why they were needed and put high effort into making the project successful.

These services will need further improvement over time, but they are a good starting point, and they already showed promising results during the piloting phase. What is sure, however, is that OT security would become a more and more important

aspect for companies that have to rely on production sites to conduct their business. Addressing these sorts of needs now would put the companies that decide to do so in the lead in terms of security and would potentially save millions of euros in avoiding expensive security incidents.

It is possible that in the future new approaches for the OT environment will rise, and these services will not prove sufficient for all the needs that we have identified at the beginning of the project. We plan to have a continuous improvement approach where we are constantly considering what can be done to offer better security to production environments without disrupting business activities over-complicating their work.

8.1 Future work

The services that we have implemented are not considered completed as they are, and at the moment this thesis is written, there are already plans for improving the various services by optimizing and extending their functionalities.

For example, while at the moment, NOC service is only partially integrated with ServiceNow, the plan is to have a full API integration like it already happens OT SOC, and this will be one of the first improvements that will be put in place. This would allow for a better integration both in terms of efficiency and security.

Another improvement that we are planning to make is to optimize the asset management solution to expand the amount of data that can be gathered automatically by various systems, and this development is ongoing with the various vendors and suppliers currently part of the service itself.

Finally, regarding OT PCs, there are plans to ensure proper protection and

management also for PCs that are not bought from the company itself, like devices provided by machinery manufacturers together with the system they sell. These devices are more challenging to reconfigure as they often have constraints such as fixed IPs or policies to work with industrial machinery correctly. However, they should be addressed and protected as much as possible.

References

[1] World Economic Forum. (2016). "Digital transformation of industries", [Online]. Available: https://www.accenture.com/t00010101T000000Z__w__/ru-ru/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/ru-ru/PDF/Accenture-Digital-Transformation.pdf. (accessed: 20.04.2021).

[2] J. Zhou, "Digitalization and intelligentization of manufacturing industry", *Advances in Manufacturing*, vol. 1, no. 1, pp. 1–7, 2013.

[3] K. Sharma, *Overview of industrial process automation*. Joe Hayton, 2017, vol. 1, pp. 1–14.

[4] Gartner. (2020). "Definition of operational technology (ot) - gartner information technology glossary", [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot. (accessed: 02.03.2021).

[5] L. Horwitz. (2018). "Ot networks and it networks are closely intertwined", [Online]. Available: https://www.cisco.com/c/en/us/products/security/ot-networks.html. (accessed: 20.04.2021).

[6] A. Di Pinto, Y. Dragoni, and A. Carcano, "Triton: The first ics cyber attack on safety instrument systems", *Proc. Black Hat USA*, vol. 2018, pp. 1–26, 2018.

[7] Manufacturing.net. (2006). "The $22,000-per-minute manufacturing problem", [Online]. Available: https://manufacturing.net/home/article/13055083/the-22000perminute-manufacturing-problem. (accessed: 20.04.2021).

[8] International Society of Automation. (2018). "New isa/iec 62443 standard specifies security capabilities for control system components", [Online]. Available: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c. (accessed: 02.03.2021).

[9] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. (2015). "Guide to industrial control systems (ics) security", [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. (accessed: 02.03.2021).

[10] R. Phillips and B. Tanner, "Breaking down silos between business continuity and cyber security", *Journal of business continuity & emergency planning*, vol. 12, no. 3, pp. 224–232, 2019.

[11] S. Snitkin. (2021). "Business continuity strategies for securing industrial control systems", [Online]. Available: https://www.arcweb.com/industry-best-practices/business-continuity-strategies-securing-industrial-control-systems. (accessed: 20.04.2021).

[12] P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers", in *2013 Information Security for South Africa*, IEEE, Johannesburg, South Africa, 2013, pp. 1–7.

[13] C. E. Pereira and P. Neumann, "Industrial communication protocols", in *Springer Handbook of Automation*, S. Y. Nof, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 981–999.

[14] Splunk. (2021). "What is a network operations center (noc)?", [Online]. Available: https://www.splunk.com/en_us/data-insider/network-operations-center.html. (accessed: 20.04.2021).

[15] E. Gelle, T. Koch, and P. Sager, "It asset management of industrial automation systems", in *12th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'05)*, Greenbelt, MD, USA, 2005, pp. 123–128. DOI: 10.1109/ECBS.2005.49.

[16] J. Gonzalez and M. Papa, "Passive scanning in modbus networks", in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, Eds., Boston, MA: Springer US, 2008, pp. 175–187, ISBN: 978-0-387-75462-8.

[17] J. Cocker. (2021). "Rise in attacks on ics computers in second half of 2020", [Online]. Available: https://www.infosecurity-magazine.com/news/attacks-ics-computers-rise/. (accessed: 20.04.2021).

[18] R. Brash. (2020). "Is patch management relevant in ot/ics cyber security?", [Online]. Available: https://verveindustrial.com/resources/blog/is-patch-management-relevant-in-ot-ics-cyber-security/. (accessed: 20.04.2021).

[19] T. Ahmad, "Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity", *Available at SSRN 3568830*, 2020.

[20] F. Malecki, "Overcoming the security risks of remote working", *Computer Fraud Security*, vol. 2020, no. 7, pp. 10–12, 2020, ISSN: 1361-3723. DOI: 10.1016/S1361-3723(20)30074-9.

[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture", National Institute of Standards and Technology, Tech. Rep., 2020. DOI: 10.6028/NIST.SP.800-207.

[22] L. O. Nweke, "Using the cia and aaa models to explain cybersecurity activities", *PM World Journal*, vol. 6, XII 2017.

[23] W. A. Conklin, "It vs. ot security: A time to consider a change in cia to include resilienc", in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, 2016, pp. 2642–2647. DOI: 10.1109/HICSS.2016.331.

[24] A. Wedgbury and K. Jones, "Automated asset discovery in industrial control systems-exploring the problem", in *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3*, University of Applied Sciences Ingolstadt, Germany, 2015, pp. 73–83.

[25] C. Mavrakis, "Passive asset discovery and operating system fingerprinting in industrial control system networks", *Wayback archive: http://web. archive. org/web/20190307110951/https://pure. tue. nl/ws/files/46916656/840171-1. pdf*, pp. 840 171–1, 2015.

[26] M. Gegick and S. Barnum. (2005). "Least privilege", [Online]. Available: https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege. (accessed: 18.03.2021).

[27] ComputerHope. (2017). "Sccm", [Online]. Available: https://www.computerhope.com/jargon/s/sccm.htm. (accessed: 19.03.2021).

[28] M. Muggler, R. Eshwarappa, and E. C. Cankaya, "Cybersecurity management through logging analytics", in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed., Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA: Springer International Publishing, 2018, pp. 3–15, ISBN: 978-3-319-60585-2. DOI: 10.1007/978-3-319-60585-2_1.

[29] S. Heiney. (2019). "Best practices for security logging while using remote access", [Online]. Available: https://blog.netop.com/security-logging-best-practices/. (accessed: 20.04.2021).

[30] J. Montgomery and E. Mixon. (2020). "Cmdb (configuration management database)", [Online]. Available: https://searchdatacenter.techtarget.com/definition/configuration-management-database. (accessed: 23.03.2021).

[31] NIST. (2021). "Official common platform enumeration (cpe) dictionary", [Online]. Available: https://nvd.nist.gov/products/cpe. (accessed: 23.03.2021).