Report summary

Abstract

Industry 4.0 have led to changes in OT environments which require a rethinking of how OT is secured. Industrial networks are now reachable via the internet and with the addition of Covid-19, the use of remote desktop solutions have increased.

This has highlighted the requirement for secure solutions for remote access to devices within industrial zones. Cisco has launched Secure Equipment Access (SEA) in an attempt to meet the requirement.

Telenor has, based on their experiences with their customers, defined four use cases for us to evaluate how SEA covers their needs.

We will also briefly evaluate how SEA lives up to the IEC 62443 and NIST SP 800-82 standards.

Sammendrag

Industri 4.0 har ført til endringer i OT-miljøer som krever en revurdering av sikkerhetstiltak innen OT. Industrielle nettverk er nå tilgjengelig via internett som sammen med Covid-19 pandemien har ført til økt interesse for løsninger som tillater sikker fjerntilgang.

I samsvar med denne økte interessen for fjerntilgangsløsninger, har Cisco lansert 'Secure Equipment Access' (SEA) for kunder som trenger sikker fjerntilgang til industrielt utstyr.

Oppdragsgiveren vår, Telenor, har formulert fire brukerfortellinger, basert på erfaringer med deres kunder for å evaluere funksjonaliteten til SEA.

I tillegg til funksjonaliteten til SEA vil vi også gjennomføre en begrenset vurdering av sikkerhetsnivået til SEA basert på de anbefalte sikkerhetsstandardene IEC 62443 og NIST SP 800-82.

Preface

We would like to thank everyone that supported us throughout the project period both directly and indirectly. The NTNU university library, our friends and family, as well as NTNU, Telnor Norge and Cisco Norge.

NTNU

From NTNU we especially thank:

Our supervisor Erjon Zoto for his assistance and guidance, and

Eigil Obrestad for allowing us to utilise the networking lab for the project.

Telenor Norge

The project was performed in collaboration with security consultants from Telenor Norge.

From Telenor we would like to express our thanks to Tor Martin Slåen Skaar and Stian Borgvin-Dørre for their time, experience and guidance throughout the project.

We would also like to thank Øystein Berg who suggested the initial theme of the project and put us in contact with the other individuals we worked with from Telenor.

Cisco Norge

Frank Tuhus and others from Cisco Norge that helped with our questions and set aside time to give us an overview of the service and Cisco Norge.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Problem area

Throughout the history of humankind we have gone through multiple industrial revolutions. The first industrial revolution with water and steam powered mechanical production, the second industrial revolution with electrically powered mass production, the third industrial revolution with electronics and information technology (IT) for increased automation. Now however, we are in the fourth industrial industrial revolution, which is defined by cyber-physical systems and the Internet of Things (IoT).

The fourth industrial revolution, also referred to as Industry 4.0, have provided multiple opportunities for increased automation and optimisation while it also creates some new challenges. Industry 4.0 is a strategy developed in collaboration with universities, research institutes, industrial companies and governments (Rolstadås et al. 2017). Industry 4.0 is especially relevant for the Norwegian industry where labour is more expensive than the majority of other countries (SSB 2021), as it can allow fewer employees to maintain the same level of production due to highly developed automation systems.

However, when more of the industrial infrastructure is connected to the internet to simplify control and maintenance, it also creates a new risk for the organisation. That which previously was inaccessible from the internet is now within reach of new threats, and creates the need to secure the operational technology (OT) infrastructure differently. Previously when OT did not require an internet connection and a problem occurred the technician travelled to the factory. OT was then sufficiently protected by an airgap. Now, with Industry 4.0, OT is connected to the internet and problems can be solved remotely by the technician.

Telenor is in contact with multiple customers which is searching for solutions to securely access their services and systems remotely. When the Covid-19 pandemic caused large parts of the world to grind to a halt in 2020, it caused multiple organisations to accelerate the implementation of remote access to systems which previously was protected by strict firewalls and airgap (SSB 2019).

In July 2021 Cisco launched the service Secure Equipment Access (SEA) which is meant to facilitate remote access to OT and other IoT devices for both the owner of the systems as well as technicians from service providers (Cisco 2021b). Telenor has requested a service evaluation of Cisco SEA where the team will evaluate the functionality and security of the service.

1.2 Goal

The primary goal of the project is to evaluate to what degree Cisco SEA is ready for industrial use.

To simplify the evaluation of how we reached the primary goal and to outline our path we defined the following effect and result oriented goals.

1.2.1 Effect oriented goals

1. To produce a comprehensive simulation of Cisco SEA usage.
2. To evaluate the security of Cisco SEA according to specific industrial security standards.
3. To present alternative solutions for areas where the service is insufficient.

1.2.2 Result oriented goals

Based on the specific tasks from the client detailed in Appendix A, we defined the following result oriented goals.

1. Perform a brief evaluation of the service. Try to find previous relevant studies and whitepapers which provides insight to the service specifications and area of use.
2. Test and setup use cases based on the provided user stories.
3. Produce a template for each user story which describes prerequisite, recipe and security evaluation.

1.3 Target audience

The target audience for this report is someone with at least two years of experience with IT or cyber security, either in a professional or educational setting. This project is also intended towards organisations or individuals looking to implement or use SEA or similar systems. The report was created based on the task provided by the client, Telenor Norge, and is intended for their use.

1.4 Project boundaries

As parts of the project's task could be interpreted broadly, we set some boundaries to the subject in addition to the practical boundaries set by the university.

1.4.1 Subject

As the project's theme of Industry 4.0 and remote access could be vast, the project is limited to a few of the Cisco IoT Operation Dashboard functions (IoT OD). Namely Cisco Edge Device Manager (EDM) and Cisco SEA.

1.4.2 Practical

The projects designated duration is from 10th of January until the 7th of June 2022, and consists of three main phases.

- Pre-project planning
  January was used for pre-project planning and is where we created the project plan in Appendix D.
- Project report
  Once the project plan had been approved, we moved on to the main phase which was completing the project tasks and writing the project report. This was from February until the project report due date on the 20th of May 2022. Suggested report size is $40 + (teamsize \times 10)$ pages excluding preface and appendices, which in our case would be 70 pages. This does not mean the report has to exactly meet the suggested size, but that we had a guide for approximate report length.
- Project presentation
  The final phase of the project is the project presentation which was set for the 7th of June 2022. The presentation consists of 20-30 minutes for setup, presentation and questions from the audience, and the presentation itself should be no more than 15 minutes.

1.5 Team and background

The team consists of three students from NTNU in Gjøvik studying a bachelors degree in Digital Infrastructure and Cyber Security.

1.5.1 Background

As part of the bachelor's program we have learned a number of skills useful to the project, including:

- Intermediate network knowledge and Cisco IOS
  Multiple subjects regarding computer networking and Cisco IOS. Including themes like switching, routing, subnetting, and more.
- Decent programming and scripting skills
  Multiple subjects regarding programming using C, C++, PHP and Javascript as well as scripting using bash and powershell.
- General cyber security and risk management knowledge
  A majority of the subjects have had elements of cyber security and/or risk management.

1.5.2 New knowledge and skills

Throughout the project the team have had to learn a couple of new skills:

- Cisco IoT Operations Dashboard - GUI and API
  Our previous experience with networking was mostly limited to IOS, so both the IoT OD and the API were new to us. The GUI was fairly straightforward, but the API had not yet been documented. We were able to get an example of how to use the API which provided us with the pieces we needed to accomplish our goals.
- Cisco Plug and Play (PnP)
  We had a fair amount of complications with the PnP of the device, and therefore had to learn more than anticipated regarding PnP.
- Python for API calls to ciscoiot and for sending e-mails
  We had to learn how to use python to make API calls and then send the relevant response as an e-mail.

- ISA/IEC 62443
  While we have worked with other standards for cyber security like ISO/IEC 27001 and its differences to ISA/IEC 62443 regarding OT and ICS

- OT infrastructure and security
  There are some differences between IT and OT we have had to learn throughout the project. One notable element is the potential impact an attack on OT infrastructure can cause. An attack on IT infrastructure can cause chaos and financial loss, while an attack on OT infrastructure can directly cause fatalities.

1.6 Practical information

The task is provided by Telenor Norge AS which in the report is referred to as ‘client’.

Use cases in this document are referred to using the abbreviation UCX where X is the number of use case.

Referenced figures and tables will be above the text unless we clearly specify otherwise. Most common exception will be for references to appendices. If the report is read digitally, the ‘figure X’ text should be clickable and show the relevant figure.

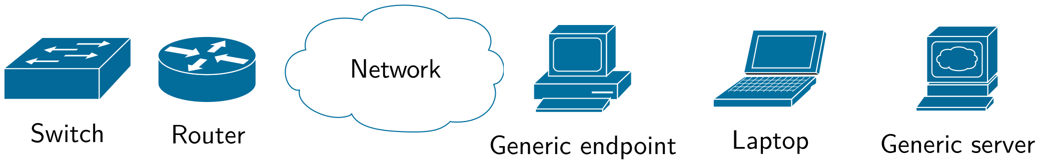


Figure 1: Explanation for symbols used in this document

The symbols used in document are described in Figure 1, the symbols were provided by Cisco n.d.(c).

For sources, citations and references, the year should lead to the relevant element in the reference list when read digitally.

2 Theory

In this chapter we will introduce the core background and theories that motivated the creation and our subsequent choosing of this project. The theories presented will provide crucial context to the necessity of our system under consideration (SuC). As mentioned earlier, this rapport is intended for an audience with basic IT and cyber security knowledge, therefore the explanations of background knowledge will be brief. We are going to reference in-depth articles for those interested in more details.

2.1 Subject theory

The following sections will briefly explain theory related to components required to meet our goals.

2.1.1 Cisco IoT Operations Dashboard

Cisco IoT OD is a web-based service that provides an industry leading end-to-end IoT management. The IoT OD features many different core functionalities such as the Edge Device Manager (EDM) that provides automated solutions to device management problems, asset owners and operators face on a day to day basis.

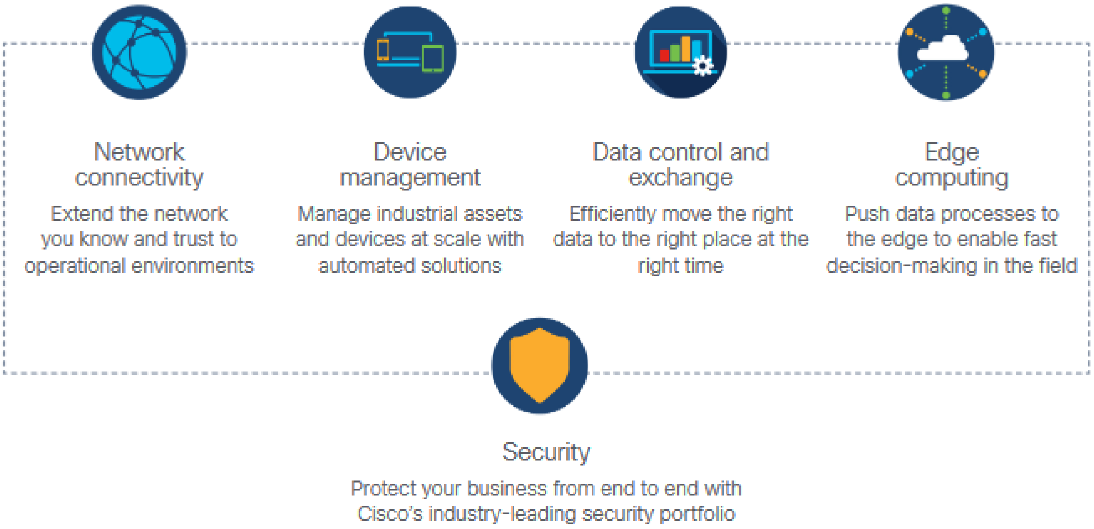

Network connectivity
Extend the network you know and trust to operational environments
Device management
Manage industrial assets and devices at scale with automated solutions
Data control and exchange
Efficiently move the right data to the right place at the right time
Edge computing
Push data processes to the edge to enable fast decision-making in the field
Security
Protect your business from end to end with Cisco's industry-leading security portfolio

Figure 2: Core goals of Cisco IoT OD, figure from Cisco n.d.(b).

Figure 2 provides a brief overview of the core goals of IoT OD. In addition to the core functionality mentioned above, other features such as Edge Intelligence (EI) and

Industrial Asset Vision (IAV) allows the user to extend the preexisting inter-connectivity of its network and easily add new operation zones, exchange data between interconnected devices and introduces the concept of ‘edge computing’. In other words, providing edge devices with appropriate configuration and instructions for fast problem solving in the field. In addition to the previously mention features, using Cisco devices and software ensures a long history of experience and guarantee of security to important assets and infrastructure (Cisco 2021c).

2.1.2 Edge Device Manager

Cisco EDM is a cloud based tool which provides scalability, management and monitoring of your supported IoT devices securely. This tool is included with a license of Cisco IoT operations Dashboard and acts as its core feature set. On-boarding of devices happens automatically after acquiring Internet access through, either cellular or ethernet. This is thanks to, a zero touch deployment (ZTD) system that uses Cisco PnP which is explained later. Using Cisco EDM allows for instant visibility and configuration of your remote devices through a web browser. The user can initiate software updates remotely, push new pre-established device configuration files to one or more on-boarded devices and receive device notification when some incidents happens (Cisco 2021c).

2.1.3 Secure Equipment Access

Cisco secure equipment access (SEA) is a remote access tool provided optionally with a license of Cisco IoT OD. This tool provides secure remote access of IoT equipment with a fair selection of audit and scalability features that are constantly being improved. In order to use this service, the Cisco platforms need to be on-boarded via the previously mentioned EDM service. Cisco SEA provides precise access control based on a user role hierarchy. Users and IoT devices are given groups to isolate important devices to admins with higher remote access privileges. In addition to precise access control, SEA also provide audit logs through GUI and API. (Cisco 2021c)

2.1.4 Plug and Play

Cisco Plug and Play (PnP) is a function provided on all enterprise Cisco platforms that allows seamless on-boarding of devices to the IoT operations dashboard the moment you plug in your device. Cisco PnP is a zero touch solution that allows enterprise devices to automatically find its controller eliminating the requirement for a technician on site for initial set up. This results in cost saving for pre-staging of devices and also eliminates manual configuration errors. The application infrastructure policy controller PnP uses is called APIC-EM (Shahrukh Raheem 2017).

2.2 IEC 62443

The International Electrotechnical Commission (IEC) 62443 is an international cyber security standard tied to defining processes, techniques and requirements when industrial automation control systems (IACS) are involved. These sets of standards are determined through the IEC standards creation process which includes the intervention of all national committees connected to IEC and therefore can be considered a 'horizontal standard', meaning this standard is required when evaluating operational technology (OT) systems. This requirement exists in order to prevent conflicting requirements when evaluating the cyber security of OT systems regardless of differing industry sectors.

IEC 62443 is divided into four main categories, these being general, policies and procedures, systems and lastly component, each with their own sub categories as shown in the figure below.

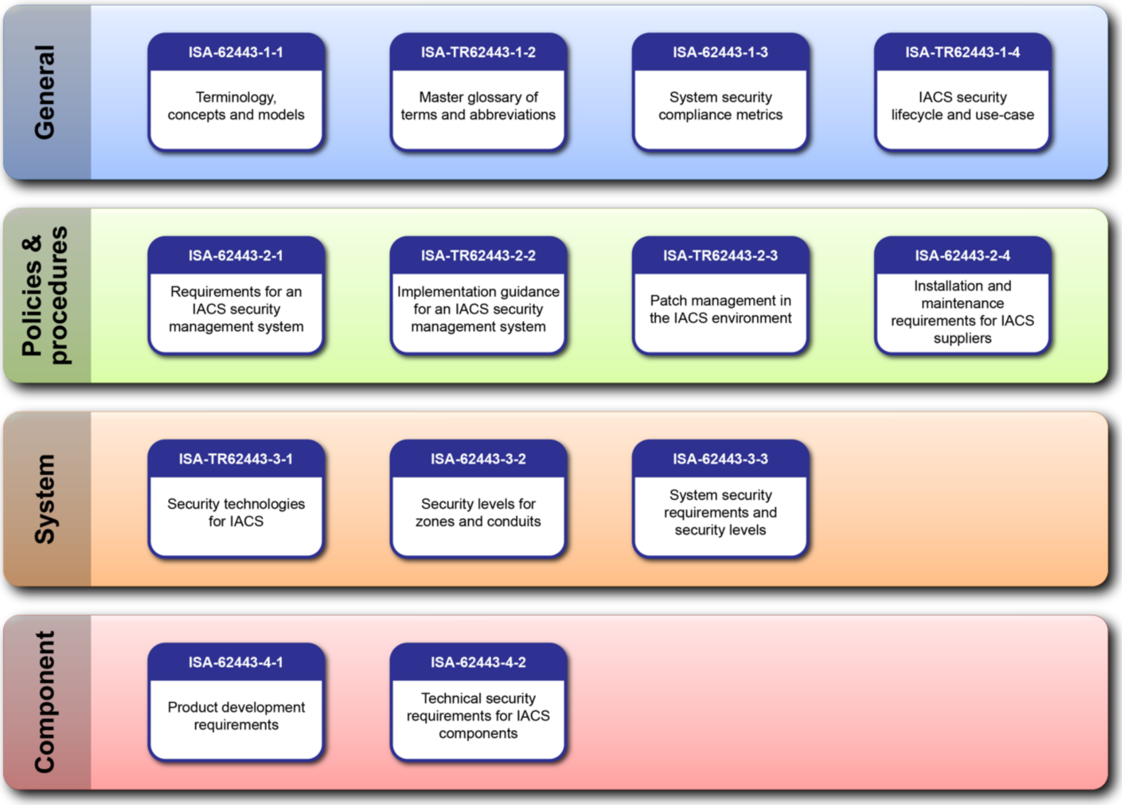

General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Installation and maintenance requirements for IACS suppliers
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components

Figure 3: A graphic showing the structure of IEC 62443 (International Electrotechnical Commission 2019)

The category that is most commonly referenced and applied is systems, more specifically IEC 62443-3-3 system security requirements and security levels (SL). In this sub category, the criteria for each SL is described as:

0. No identification or authentication of users to access control systems
1. Authentication and identification of users by procedures against casual and unintentional access to control systems
2. Authentication and identification of users by procedures with limited resources, low motivation and generic methods, attempting intentional access to control systems
3. Authentication and identification of users by procedures with moderate resources, moderate motivation and IACS specified methods, attempting intentional access to control systems
4. Authentication and identification of sophisticated users by procedures with extensive resources, high motivation and IACS specified methods, attempting intentional access to control systems

In IEC 62443-1-1 the foundational requirements (FR) of the standard is divided in to seven different zones and conduits. These FR's being:

- Identification and authentication control (IAC)
- Use control (UC)
- System integrity (SI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA)

Each of these FR's should be evaluated individually and given a SL score. IEC 62443-3-3 also defines the concept of target security level (SL-T) being the SL that is desired, achieved security level (SL-A) being the currently achieved SL of the SuC, and capability security level (SL-C) being the possible SL after configuration. SL-C is only required if SL-A is less than SL-T after comparing the two.

Lastly, in order for a company to be compliant with the IEC 62443-3-3 standard, it is also highly recommended that they have already achieved a high level of maturity in terms of security. Achieving a high maturity level means that there are procedures within the system under consideration (SuC) that are repeatable, practised and continually improving. The criteria for maturity levels is as follows.

- Initial - follows a reactive approach with little to no documentation
- Managed - the operator is managed and follows written rules and guidelines. The procedures to ensure this is repeatable.
- Practised - there are procedures in place that are followed and practised. Follows a proactive approach.
- Improving - procedures are constantly monitored and measured in order to gauge its effectiveness. There is constant improvement to said procedures.

We will look into how Cisco SEA fits in with this standard in Section 4.5.1. Evaluations of our SuC's security and maturity levels will be conducted in a later chapter (International Electrotechnical Commission 2019).

2.3 NIST SP 800-82

The US National Institute of Standards and Technology (NIST) have published a Cyber security Framework aimed at providing optional measures to mitigate cyber threats for critical infrastructure owners and operators. Adoption of these measures will help owners and operators of critical infrastructure better identify, evaluate and respond to cyber threats in a cost-effective and timely manner.

The NIST special publication 800-82 revision 2, is a set of guidelines aimed at asset owners and operators of industrial control systems (ICS). In this standard, there is details of typical ICS architectures and how they are commonly implemented. Along side that, you will also find the common vulnerabilities and risk factors. Therefore, it is paramount that organisations follows its guidelines and best practices to hopefully mitigate those risks.

The NIST SP 800-82 rev. 2, commonly refers and include recommendations from the aforementioned IEC 62443 industry standard. What NIST refers to as Industrial Control Systems (ICS) is essentially referencing to Industrial Automation and Control Systems (IACS).

NIST categorises ICS's into three specific categories, these being Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC).

- SCADA systems manage assets across different plants. They are responsible for monitoring, collect data and distribute instructions to automation systems. They may even manage, one or more DCS's
- DCS is used to control and monitor automated systems within the same plant in almost real-time. A single DCS may even be responsible for the entire plant's automation system. DCS is also what controls the PLC's in a plant
- PLC's are the controllers that receive instructions from DCS and tells the physical actuators how to operate. PLC's are essentially the bride between control system and the real world operators.

ICS systems are extremely common in almost every industry sector and critical infrastructure. The implementation and architectures of these systems are often very complicated, but highly inter-dependant, and the absence of any part of the hierarchy can lead to catastrophic failure and lost revenue.

Cyber security for ICS systems is a relatively new concept due to ICS's in the past being proprietary solutions without access to internet. Essentially, they were being protected by an air gap to the plethora of cyber security threats in the open web. With the coming of Industry 4.0, this has changed, and considering ICS's are devices that can interact with the real world, there is a greater need to safeguard them against potential threats.

ICS's are designed to interact with physical object in real-time, they also require a high degree of reliability and availability. Disruption to any of these qualities can lead to catastrophic consequences to operation, health, safety, monetary loss and even environmental damage. Therefore, cyber security needs to be implemented, without disrupting its reliability, performance and availability. NIST SP 800-82 rev. 2 lists the following to be the most common incidents among ICS systems:

- Critical data flow is disrupted leading to unsafe operation of the ICS devices.
- ICS devices could receive altered or unauthorised instructions leading to impairment or disruption of dangerous processes, leading to environmental damage and even loss of life.
- Asset owners and operators receiving incorrect alerts, leading to incorrect actions causing disruption to function and control.

- Infection of malware, causing unauthorised modification of software and instructions, in turn leads to negative outcomes.
- Loss of function/disruption to safeguards of dangerous and expensive equipment, leading to destruction of hard to replace equipment.
- disruption of safety systems, endangering the workplace.

The standard also lists the following goals for every implementation of ICS systems:

- Restrictions to logical access to network of ICS systems
- Restrictions to physical access to devices and network
- Protecting each individual component with tailored solutions
- Restrictions to modification of data flow, especially across networks
- Detection systems of security breaches and cyber incidents
- Capacity to maintain operation and functionality during difficult situations
- Procedures to restore system functionality and data after incidents

In order to address all the aforementioned risks, vulnerabilities and requirements, the NIST SP 800-82 rev.2 requires the cyber security team of the organisation to consist of at least IT-staff, control engineer, control system operator, network and system security expert, a member of management staff, and a member of physical security department. In addition, an in-dept defence strategy is to be created, in order to respond and mitigate the impact and possibility of failure in any of the aforementioned components of an ICS (Keith Stouffer (NIST) et al. 2015).

3 Method

We will in this section describe what we used for the project and how we used it in specific cases. This is to enable others to replicate our results.

3.1 Equipment

We used a selection of hardware and software to complete our tasks set for the project.

3.1.1 Hardware

To complete the tasks the following hardware, or equivalent, is required.

Cisco Catalyst IR1101
To utilise Cisco SEA we were provided and used an IR1101 router, specifically an IR1101-K9. This is one of the industrial routers which are supported by SEA (Cisco n.d.[d]).

Cisco Catalyst 3560-CG
We were provided a 3560-CG switch which we used to connect endpoints as well as power the Raspberry Pi with Power Over Ethernet (PoE).

Raspberry Pi 3 Model B Plus Rev 1.3
To complete UC2 we required a device to use as jump host and opted for a Raspberry Pi (RPi) with a PoE hat as this allowed us to keep the device connected without the need for an additional power supply cable. A RPi with a PoE hat is not strictly necessary for the tasks, however it was an uncomplicated option that provided what we required.

One desktop computer
Multiple use cases required an endpoint connected to one of the VLANs. The only requirements for this device is support for 64-bit Windows 10.

3.1.2 Software

We used the following Software for this project. Some software may or may not need to be the exact same to replicate our results and how we achieved them.

Cisco IOS XE Software, Version 17.07.01
The Cisco Catalyst IR1101 router we used ran this version of IOS XE. This is important because Cisco SEA can only be connected to an IR1101 running version 17.04 or newer

(Cisco n.d.[d]).

Cisco IOS, Version 15.0

The Cisco Catalyst 3560-CG switch we used, ran this version of IOS.

Cisco Secure Equipment Access, Version 0.31

This is the version of SEA we had installed on our router. SEA runs in a docker container on the device and communicates with the service in Cisco IoT OD.

Raspbian GNU/Linux 11 (bullseye)

This was the operating system used by the Raspberry Pi jumphost. It was chosen since we were familiar with it and it came with or it was simple to set up the essential tools needed.

Windows 10 Education

This was the OS installed on the desktop we utilised. It was already installed and we did not require anything else.

Tight VNC 2.8.63

Tight VNC is a light weight VNC server. It was chosen because it ran on windows and was straight forward to set up.

RealVNC

Tight VNC is a light weight VNC server. It was already installed on the Raspberry Pi and we did not require anything else.

RDP Wrapper Library

We were unable to set up a native RDP server due to the fact that the Windows version installed on the desktop was neither Pro nor Enterprise. We choose RDP Wrapper Library by Stas'M on github (https://github.com/stascorp/rdpwrap) as our utility.

OpenSSH client and server

On the RPi and the Windows desktop, we utilised OpenSSH to connect to other devices and to allow other devices to connect to it.

Firefox Web browser

Firefox was utilised to access the Cisco IoT dashboard. The only reason we chose Firefox over other browsers was because it was already installed on our own laptops.

Postman 9.15.0

Postman is a tool for testing and developing web based APIs. We utilised it during the development of program contacting the REST API in UC4.

3.2 Approach

3.2.1 Study of the System under Consideration

Finding information about SEA on Cisco's own platforms, such as Cisco DevNet, was quite the task.

Searching for 'Secure Equipment Access' on Cisco DevNet, produced 800 results for sources containing the words anywhere in the text. Since the search terms were very general, the majority of the returned results were irrelevant. Instead of reading through all of them to find one that might be pertinent, we decided to use Google and restrict our search to Cisco DevNet. Using this search term ' secure equipment access site:"developer.cisco.com"', we could search for sites on developer.cisco.com containing this specific string. This search returned 119 results, and going through them all, they all pointed to the same resource, mainly the documentation for how to use the Cisco IOT Dashboard (Cisco n.d.[b]) , which is where SEA is located.

Using google search and google scholar we were able to find a few results about Secure Equipment Access. These where the resources we found.

- On blogs.cisco.com, we found one article tagged with 'Secure Equipment Access'. This article (Lobo 2021) was referencing a report by The Forrester Wave in which different management solutions for remote access of industrial control systems were compared (Kime et al. 2021).
- On dcloud-cms.cisco.com, we found one newsletter (Cisco 2021a) for November 2021 titled 'Cisco Edge Device Manager & Secure Equipment Access – IoT Operations Dashboard Instant Demo v2'.
- On cisco.com, we found one whitepaper (Cisco 2021d) about how to securely manage IOT devices used to make roads safer. It was not specifically about SEA but did mention it as part of a solution.

These findings are further discussed in in the Section 4.2.

3.2.2 Infrastructure

The first step of the project work was to set up the necessary equipment and infrastructure.

Description	VLAN ID	IPv4	Netmask	Default gateway
Industrial DMZ	110	192.168.110.0	255.255.255.0	192.168.110.1
Industrial zone	120	192.168.120.0	255.255.255.0	192.168.120.1
Enterprise zone	130	192.168.130.0	255.255.255.0	192.168.130.1

Table 1: VLAN definition

The client provided us with the required network equipment, which we were given permission to install at the NTNU Cisco lab. We installed it as illustrated in Figure 4, with TL-SG1024 being the top-of-rack (TOR) switch. We defined the VLANs as detailed in Table 1 based on the infrastructure illustration provided by the client in the task description, which is available in Appendix A.

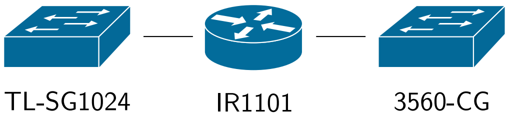


Figure 4: Basic infrastructure connection

We had some issues configuring trunking for router-on-a-stick with IR1101 and opted for traditional inter-VLAN routing instead, as trunking was not required for the tasks. The VLANs 110, 120 and 130 were assigned to the routers interface FastEthernet 0/0/1, 0/0/2 and 0/0/3 respectively, which were configured to switchport mode for the relevant VLAN. Static routes to the VLANs were added to facilitate inter-VLAN routing.

The full network details is described in Table 2 and illustrated in Figure 5

Device	Interface	IPv4	MAC	Destination	VLAN
IR1101	Gi 0/0/0	10.10.0.9	7cad.4f08.8980	TL-SG1024	N/A
	Fa 0/0/1	192.168.110.1	7cad.4f08.8981	Catalyst 3560-CG	110
	Fa 0/0/2	192.168.120.1	7cad.4f08.8982	Catalyst 3560-CG	120
	Fa 0/0/3	192.168.130.1	7cad.4f08.8983	Catalyst 3560-CG	130
	Fa 0/0/4	Down	7cad.4f08.8984	N/A	1
3560-CG	Gi 0/1	192.168.110.5	c414.3c81.5081	IR1101	110
	Gi 0/2	192.168.120.5	c414.3c81.5082	IR1101	120
	Gi 0/3	192.168.130.5	c414.3c81.5083	IR1101	130
	Gi 0/4	Down	c414.3c81.5084	N/A	N/A
	Gi 0/5	N/A	c414.3c81.5085	Raspberry Pi	110
	Gi 0/6	N/A	c414.3c81.5086	Laptop 1	110
	Gi 0/7	N/A	c414.3c81.5087	Laptop 2	120
	Gi 0/8	N/A	c414.3c81.5088	Laptop 3	130
	Gi 0/9	N/A	c414.3c81.5089	Desktop 1	120
	Gi 0/10	N/A	c414.3c81.508a	Desktop 2	130
Rasp. Pi	eth0	192.168.110.6	b827.eb0d.f5cc	3560-CG	110
Desktop 1		DHCP		3560-CG	120
Desktop 2		DHCP		3560-CG	130

Table 2: Infrastructure overview table.

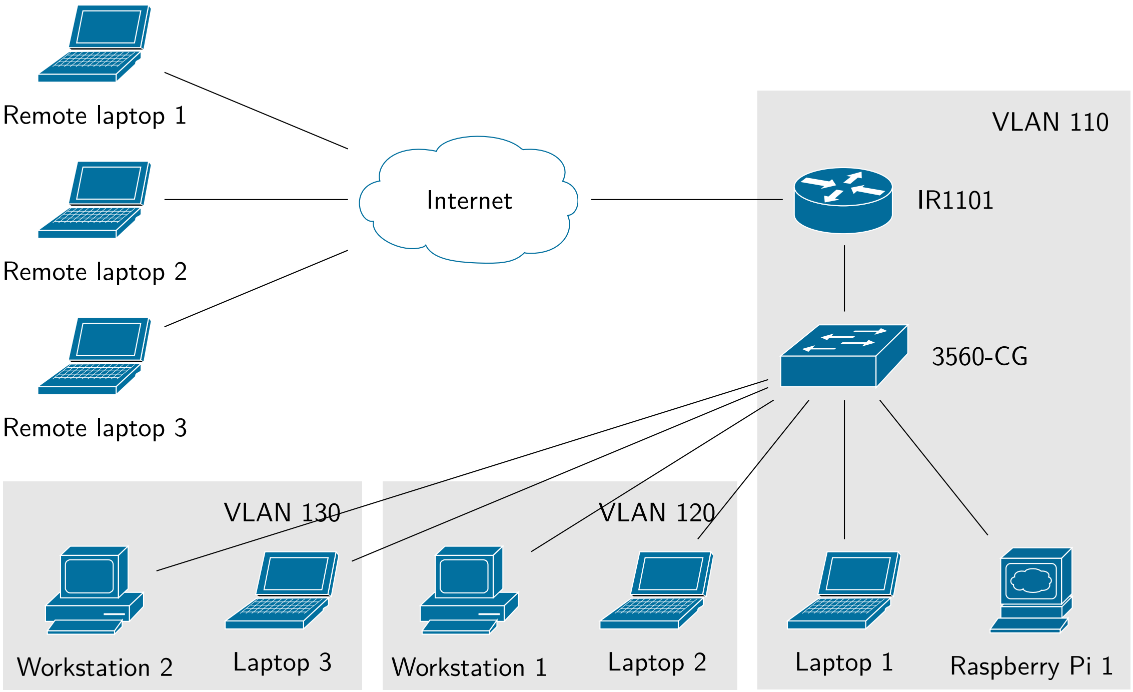


Figure 5: Overview of devices we control and how they are connected to the internet. Internet in the figure includes NTNU LAN.

3.2.3 Proof of Concept

The 'Proof of Concept' in this context is documenting to which degree Cisco SEA is able to provide the services intended.

To test how Cisco SEA provides the services, we did the initial setup of the infrastructure as described in Section 3.2.2 as well as the UC-prep steps detailed in Section 3.2.4.

We then connected some endpoints with the services Cisco SEA is meant to support and added these to SEA on IoT OD. Those services being SSH, RDP, VNC and Web application.

For Web application we used the IR1101 routers web interface. SSH to IR1101, 3560-CG and Raspberry Pi, VNC to the Raspberry Pi and Desktop 1. RDP to Desktop 1.

The final step is accessing the endpoints via IoT OD on a web browser. The further analysis of our results from the PoC can be found in Section 4.3.

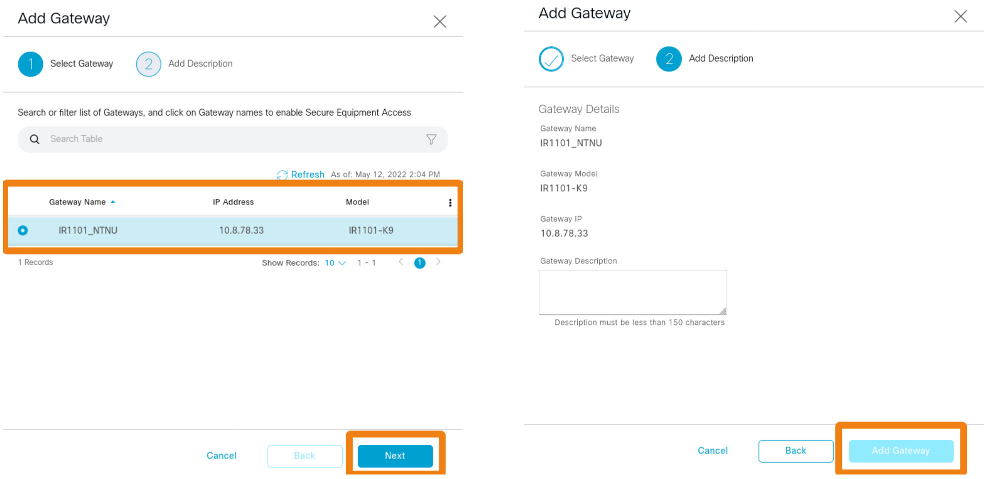
3.2.4 Use cases

As part of our task, we were provided with four use cases to examine by the client which are detailed in Appendix A.

For all the following use cases, the following steps are required to have been completed.

UC-prep

1. Add the router to EDM.
2. Add the router as an IoT gateway for SEA as illustrated in Figure 6.



Search or filter list of Gateways, and click on Gateway names to enable Secure Equipment Access

As of: May 12, 2022 2:04 PM

	Gateway Name	IP Address	Model
●	IR1101_NTNU	10.8.78.33	IR1101-K9

1 Records Show Records: 10 1 - 1

Gateway Details

Gateway Name
IR1101_NTNU

Gateway Model
IR1101-K9

Gateway IP
10.8.78.33

Gateway Description

Description must be less than 150 characters

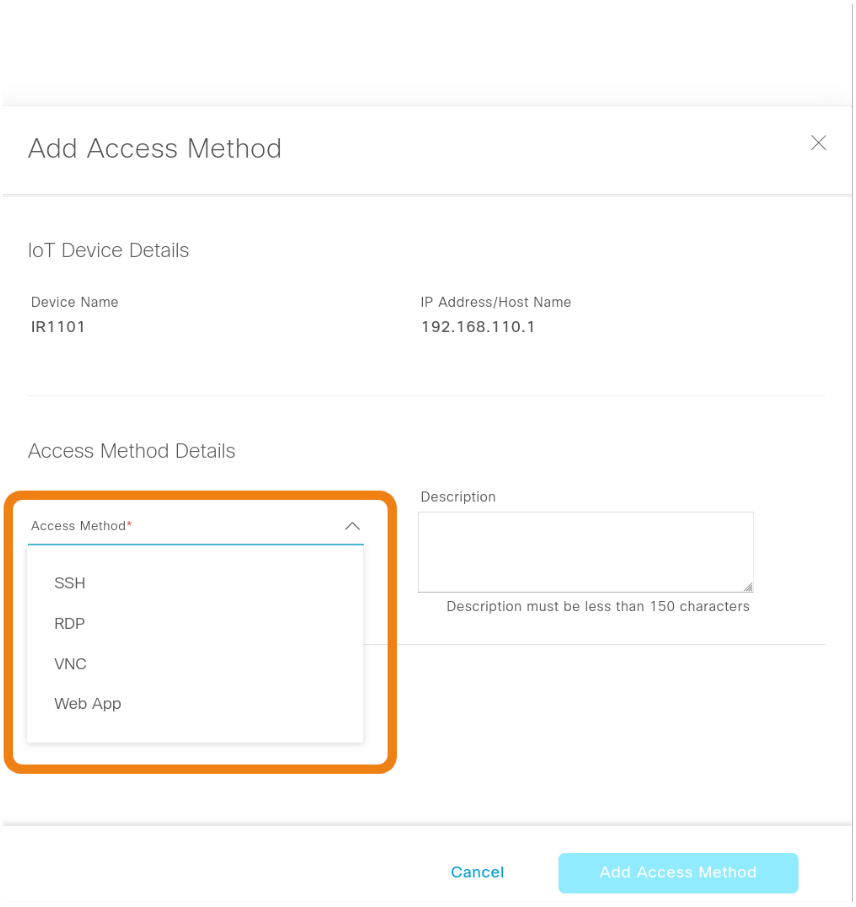
(a) Select the gateway to the network that was added to EDM.

(b) Enter the necessary details for the gateway.

Figure 6: Screenshots showing the steps for adding a gateway from EDM to SEA.

UC1

The first use case was regarding IP connectivity from a program on a technicians device to a target device through SEA. While the documentation from Cisco claims this is a functionality that is directly provided by SEA (Cisco 2021c), we were not able to accomplish this and did not find any guide or documentation that explained how it is possible.



Add Access Method

IoT Device Details

Device Name
IR1101

IP Address/Host Name
192.168.110.1

Access Method Details

Access Method*

Description

Description must be less than 150 characters

Figure 7: Screenshot of available access methods on IoT OD for SEA.

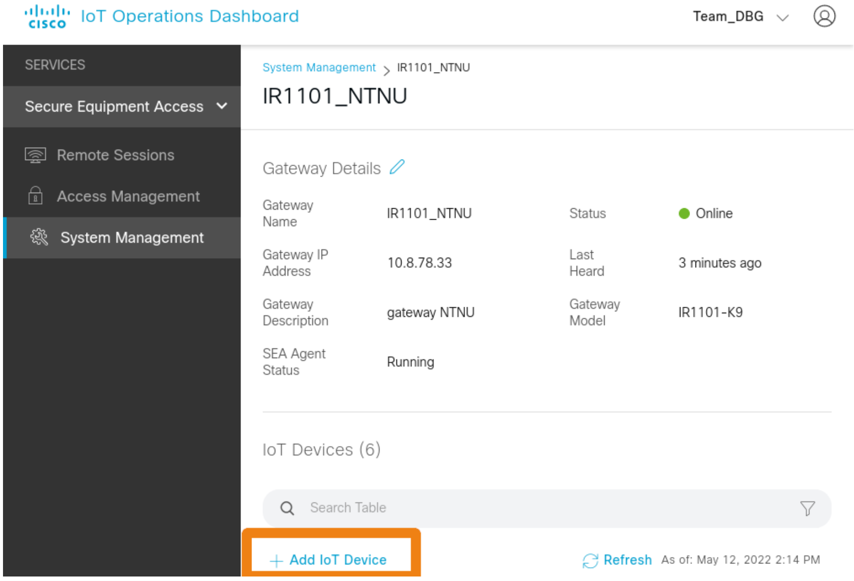
Based on the available access methods for devices connected to SEA, see Figure 7, we determined that it is not possible through SEA, or that it is not sufficiently documented how to configure it.

UC2

In the second use case, an external technician needs remote desktop access to a jumphost within the IDMZ.

The group opted to interpret and complete the task in two distinct ways. The first was that the external technician actually required a remote desktop with a graphical user interface to the jumphost. The alternative interpretation, was that an SSH connection to the jumphost would suffice. Both of these functions are core functionality provided by SEA and is fairly straightforward to configure and use. We started from the point of having the gateway for the router added in SEA as described in the preparation steps, Section 3.2.4.

1. The first interpretation of the task was solved by installing RealVNC as a VNC server, and the second one by utilising the existing OpenSSH server already installed.



IR1101_NTNU

Gateway Details

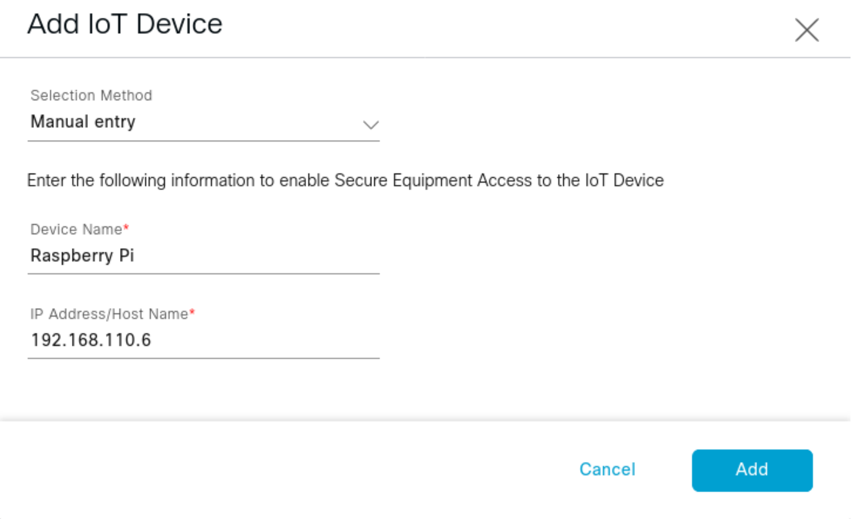
Gateway Name: IR1101_NTNU
Status: ● Online
Gateway IP Address: 10.8.78.33
Last Heard: 3 minutes ago
Gateway Description: gateway NTNU
Gateway Model: IR1101-K9
SEA Agent Status: Running

IoT Devices (6)

As of: May 12, 2022 2:14 PM

Figure 8: Select the gateway that the target device is connected to and add IoT Device.

2. We then added the jumphost as an IoT device to the gateway. This was done by selecting the gateway in ‘System Management’ menu and clicking ‘Add IOT device’ as shown in Figure 8.


Add IoT Device

Selection Method: Manual entry

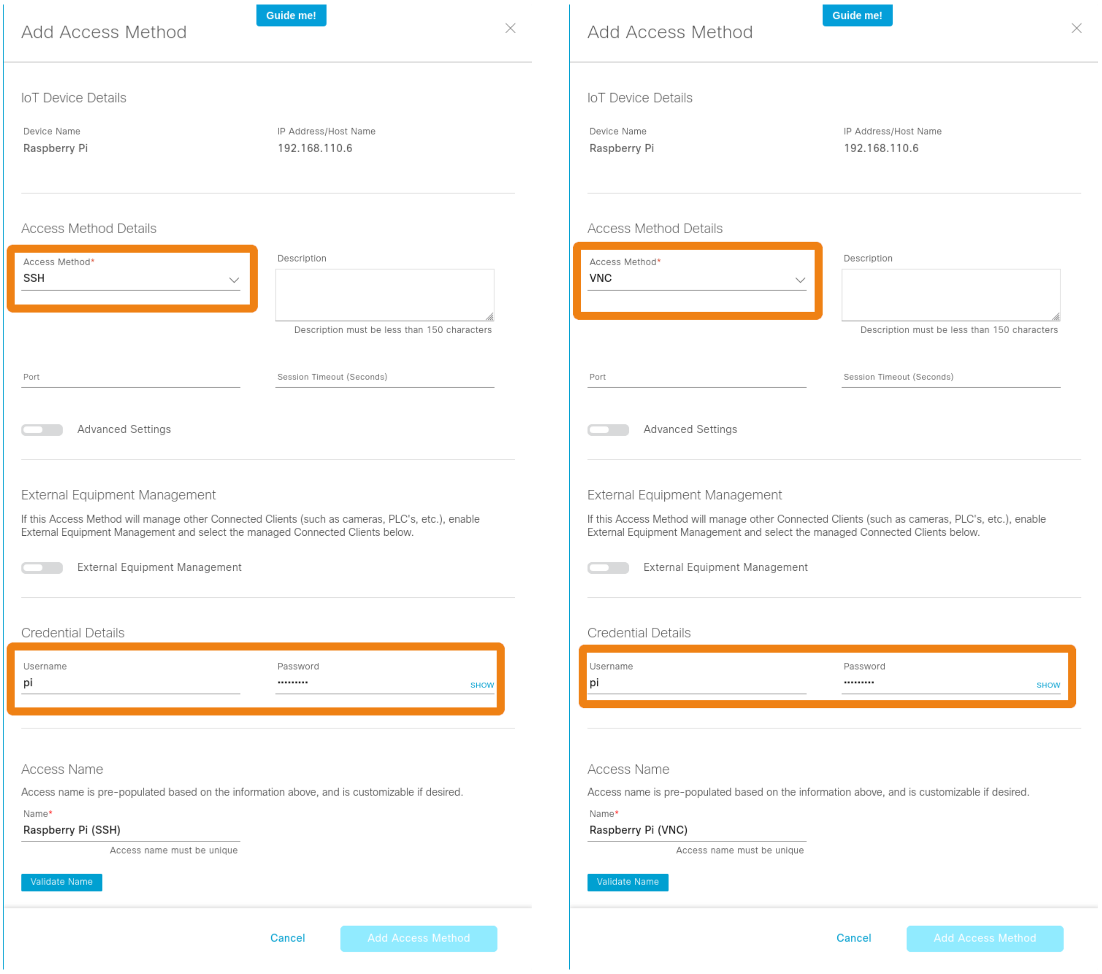
Enter the following information to enable Secure Equipment Access to the IoT Device

Device Name*: Raspberry Pi

IP Address/Host Name*: 192.168.110.6

Figure 9: Adding general information about IoT device

3. Then we use manual entry, as shown in Figure 9 to add the device details for the jumphost. We used static IPs in the project, but management could be made simpler by utilising local hostnames instead.



Add Access Method

IoT Device Details

Device Name: Raspberry Pi

IP Address/Host Name: 192.168.110.6

Access Method Details

Access Method*: SSH

Description

Description must be less than 150 characters

Port

Session Timeout (Seconds)

Advanced Settings

External Equipment Management

If this Access Method will manage other Connected Clients (such as cameras, PLC's, etc.), enable External Equipment Management and select the managed Connected Clients below.

External Equipment Management

Credential Details

Username: pi

Password: ·········

Access Name

Access name is pre-populated based on the information above, and is customizable if desired.

Name*: Raspberry Pi (SSH)

Access name must be unique

(a) SSH

Add Access Method

IoT Device Details

Device Name: Raspberry Pi

IP Address/Host Name: 192.168.110.6

Access Method Details

Access Method*: VNC

Description

Description must be less than 150 characters

Port

Session Timeout (Seconds)

Advanced Settings

External Equipment Management

If this Access Method will manage other Connected Clients (such as cameras, PLC's, etc.), enable External Equipment Management and select the managed Connected Clients below.

External Equipment Management

Credential Details

Username: pi

Password: ·········

Access Name

Access name is pre-populated based on the information above, and is customizable if desired.

Name*: Raspberry Pi (VNC)

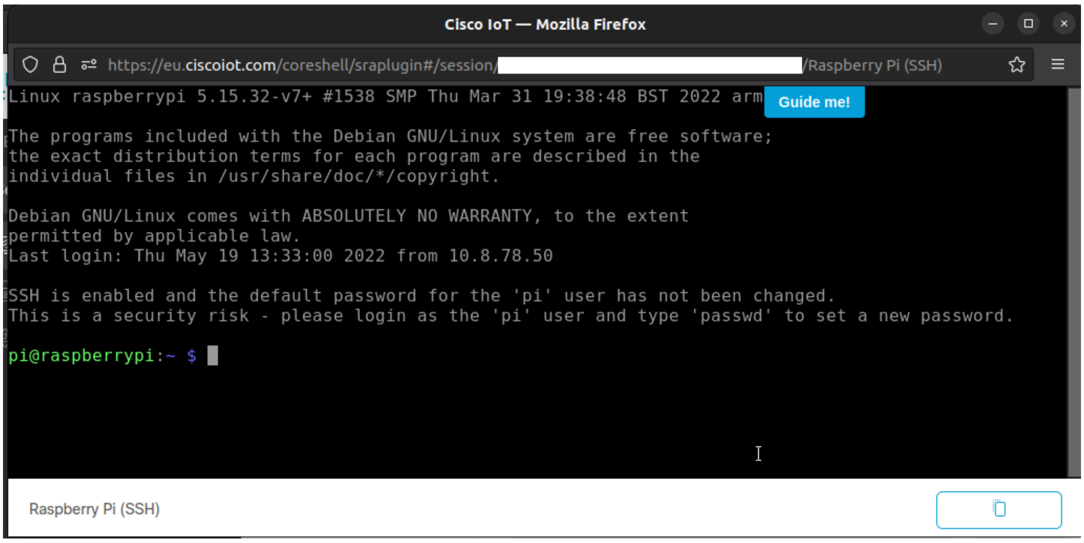
Access name must be unique

(b) VNC

Figure 10: Screenshots of how VNC and SSH access methods are added.

4. We then configured the access methods for both VNC and SSH as illustrated in Figure 10.

5. After this was configured, we could then use the device and the access method in the Remote sessions menu.


Cisco IoT — Mozilla Firefox
https://eu.ciscoiot.com/coreshell/sraplugin#/session/[redacted]/Raspberry Pi (SSH)
Guide me!
Raspberry Pi (SSH)

```
Linux raspberrypi 5.15.32-v7+ #1538 SMP Thu Mar 31 19:38:48 BST 2022 arm

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 19 13:33:00 2022 from 10.8.78.50

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $ 
```

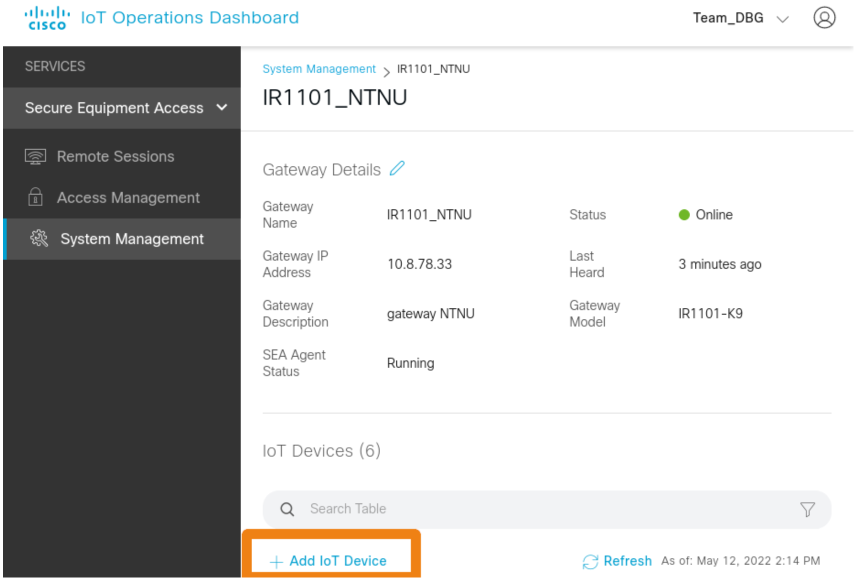
Figure 11: SSH session

Figure 11 is what it looks like when connecting to the jumphost over ssh.

UC3

An internal administrator needs remote desktop access to servers within the industrial environment. This is some of the main functionality provided by SEA and is fairly straightforward to configure and use. As the starting point for this use case, the IR1101 is already added to EDM and configured accordingly.

1. Set up RDP or VNC on the target device.
2. Ensure the required preparation steps, Section 3.2.4, are completed.
3. Once the gateway is added, we then add target device to the gateway from the page in Figure 12. Then use manual entry, Figure 13, to add the gateway details. We used static IPs for the project, but it could make management simpler with local hostnames.



IoT Operations Dashboard

Team_DBG

SERVICES

Secure Equipment Access

Remote Sessions

Access Management

System Management

System Management > IR1101_NTNU

IR1101_NTNU

Gateway Details

Gateway Name	IR1101_NTNU	Status	● Online
Gateway IP Address	10.8.78.33	Last Heard	3 minutes ago
Gateway Description	gateway NTNU	Gateway Model	IR1101-K9
SEA Agent Status	Running		

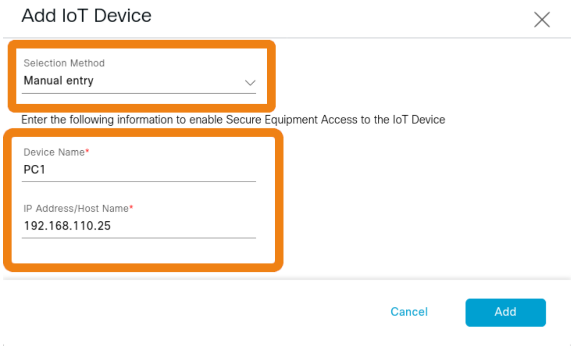
IoT Devices (6)

Search Table

+ Add IoT Device

Refresh As of: May 12, 2022 2:14 PM

Figure 12: Select the gateway that the target device is connected to and add IoT Device.



Add IoT Device

Selection Method: Manual entry

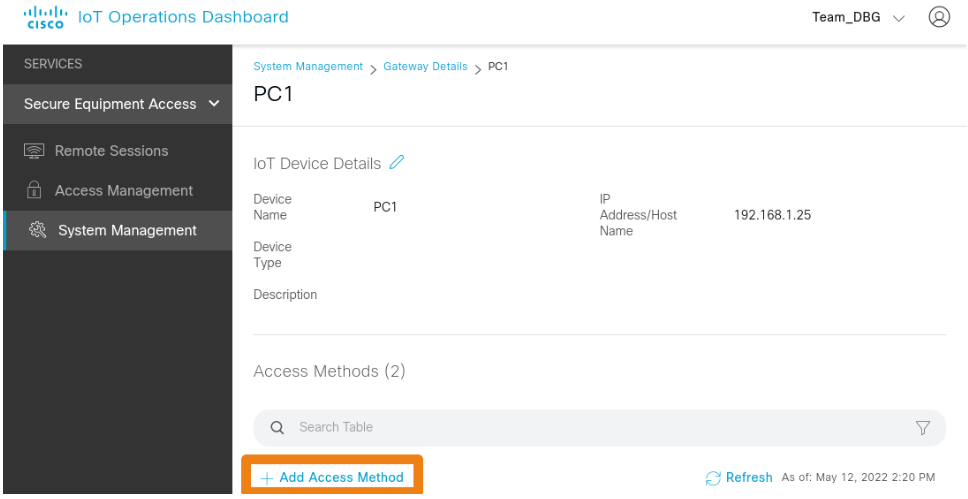
Enter the following information to enable Secure Equipment Access to the IoT Device

Device Name*: PC1

IP Address/Host Name*: 192.168.110.25

Figure 13: Use manual entry to add the device.

4. We are then able to add the access method for the device in SEA. As illustrated in Figure 14 and Figure 15.



PC1

IoT Device Details

Device Name PC1

IP Address/Host Name 192.168.1.25

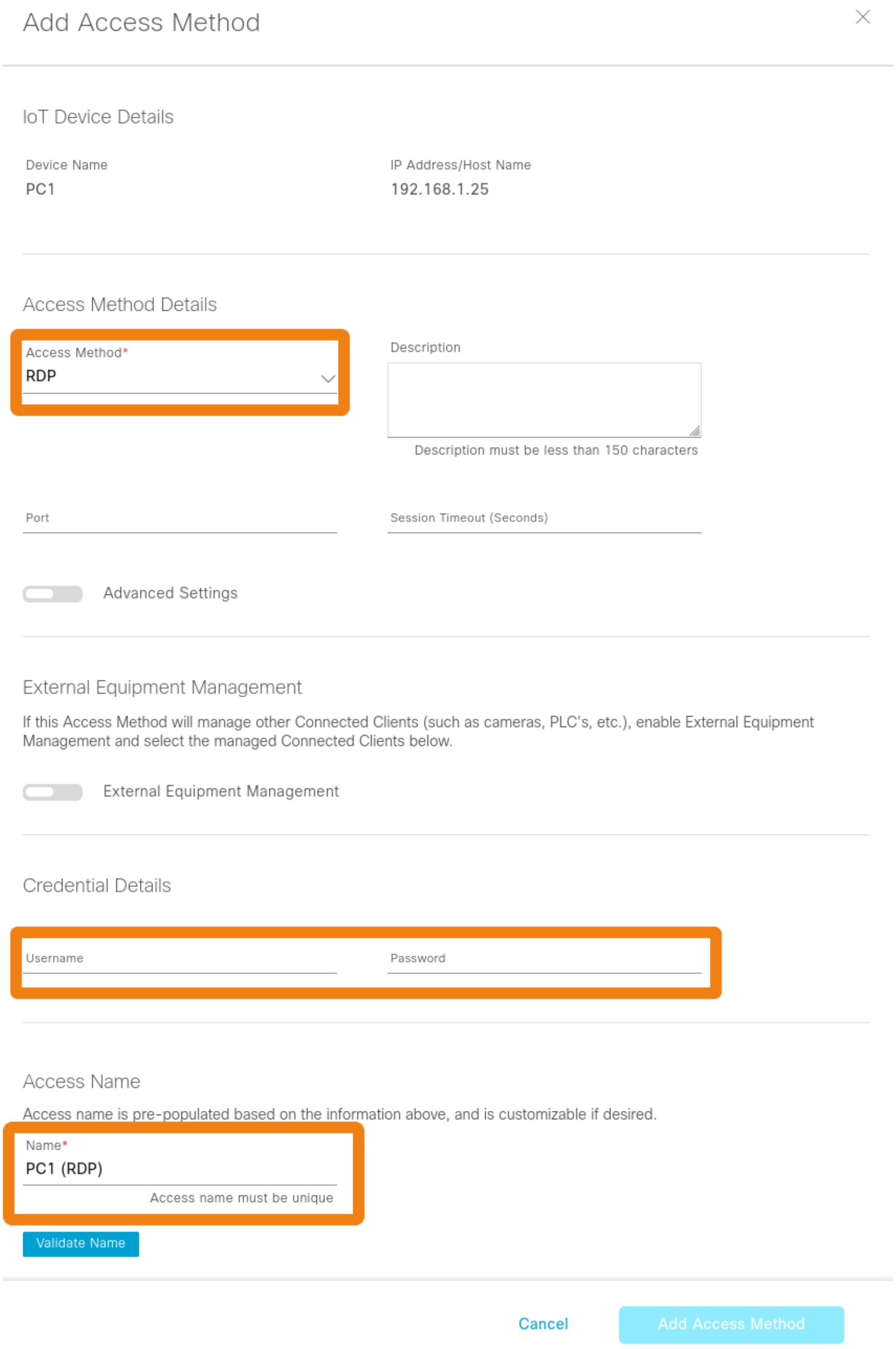
Device Type

Description

Access Methods (2)

As of: May 12, 2022 2:20 PM

Figure 14: On the system management for the device, select Add Access Method.



Add Access Method

IoT Device Details

Device Name
PC1

IP Address/Host Name
192.168.1.25

Access Method Details

Access Method*
RDP

Description

Description must be less than 150 characters

Port

Session Timeout (Seconds)

Advanced Settings

External Equipment Management

If this Access Method will manage other Connected Clients (such as cameras, PLC's, etc.), enable External Equipment Management and select the managed Connected Clients below.

External Equipment Management

Credential Details

Username

Password

Access Name

Access name is pre-populated based on the information above, and is customizable if desired.

Name*
PC1 (RDP)

Access name must be unique

Figure 15: Once the protocol is chosen from the dropdown, fill in the credentials and connection details.

5. Click the desired access method to the device in the remote sessions menu as shown in Figure 16. We chose VNC here, and the configuration from the earlier steps would be similar.

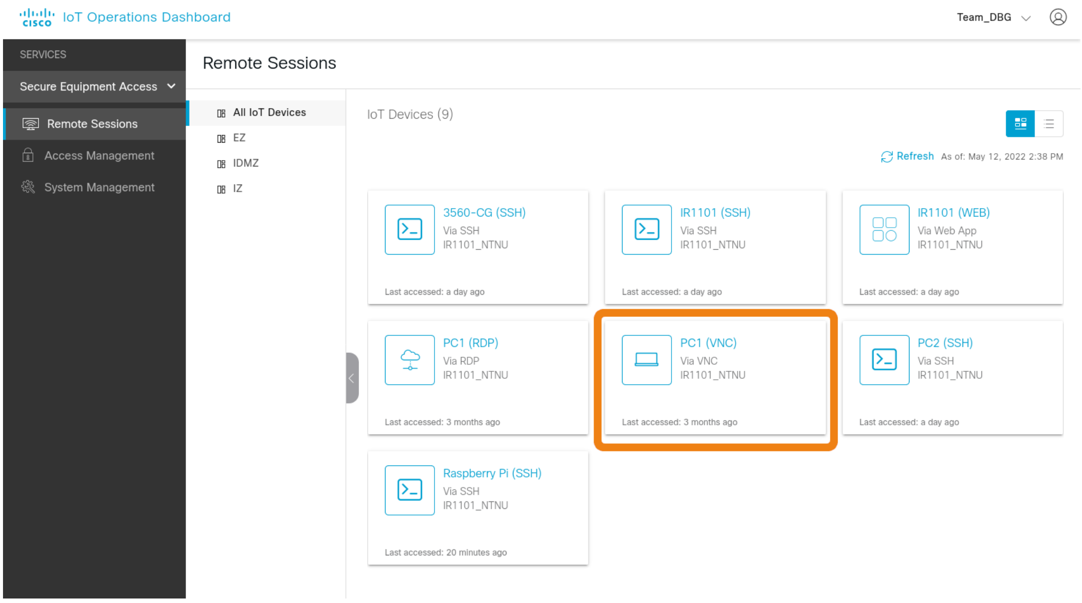
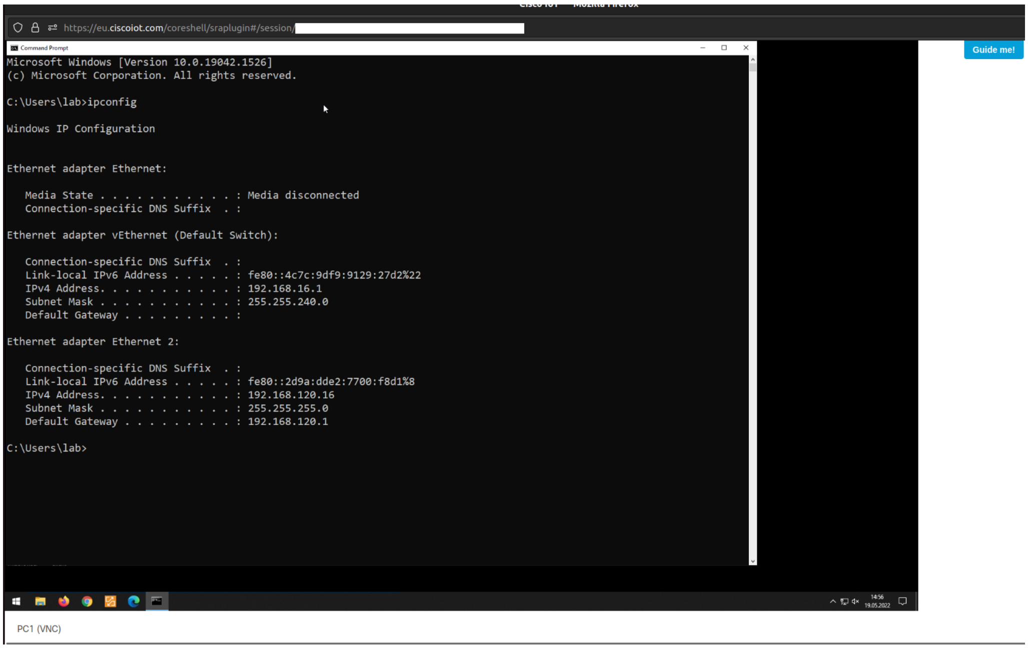


Figure 16: From the remote sessions menu, select the desired access method to the device.


https://eu.ciscoiot.com/coreshell/sraplugin#/session/[redacted]
Command Prompt
Guide me!
PC1 (VNC)

```
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lab>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4c7c:9df9:9129:27d2%22
   IPv4 Address. . . . . . . . . . . : 192.168.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2d9a:dde2:7700:f8d1%8
   IPv4 Address. . . . . . . . . . . : 192.168.120.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.120.1

C:\Users\lab>
```

Figure 17: Connected to PC1 with VNC via SEA.

When all the above steps are completed, you have a remote desktop access to a target device as shown in Figure 17 without the user needing to know the credentials for the specific target device. The figure is using VNC rather than RDP as it was easier to test, it also uses a different IP due to DHCP and because we did not spend time on managing IP addresses or hostnames.

UC4

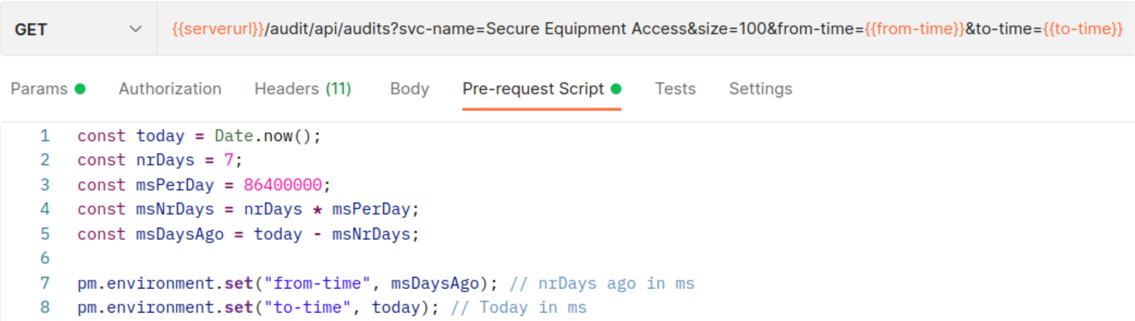
The final use case was to send an audit log of remote accesses from the past week to an e-mail address.

As this is not a function in SEA, we solved this using the IoT OD API, Postman and a python script. The following section has parts of the code we used to complete the use case, the full uninterrupted code can be found in Appendix C.

```javascript
const APIkey = pm.environment.get("API-key");
const keyname = pm.environment.get("keyname");
const xtenid = pm.environment.get("x-tenant-id");
const orgname = pm.environment.get("org-name");
const serverurl = pm.environment.get("serverurl");
const tokenpath = pm.environment.get("tokenpath");
const fullpath = serverurl + tokenpath;

// Content of request based on: https://github.com/etychon/rainier-api
const tokenReq = {
    url: fullpath,
    method: 'POST',
    header: {
        'Content-Type': 'application/json'
    },
    body: {
        mode: 'raw',
        raw: JSON.stringify({
            'grant_type': 'client_credentials',
            'client_id': orgname.toLowerCase() + "->" + keyname.toLowerCase(),
            'client_secret': APIkey
        })
    }
}

pm.sendRequest(tokenReq, function (error, response) {
    if (error) {
        console.error(error);
    } else if (response) { // If we recieved a body
        // Get the token from the response
        let token = response.json();

        // Log the body as debug information
        console.debug("Logging the body\n");
        console.debug(token);

        // Set the environment variable of the token type to be the access token
        pm.environment.set(token.token_type, token.access_token);
    } else { // Otherwise log the response itself
        console.debug("Logging the response\n");
        console.debug(response);
    }
});
```

Figure 18: Javacsript to get access token with an API-key using Postman.

To assess if it was possible to retrieve the desired data using the IoT OD API we first used Postman authorising with bearer token using the script shown in Figure 18.



```
{{serverurl}}/audit/api/audits?svc-name=Secure Equipment Access&size=100&from-time={{from-time}}&to-time={{to-time}}
```

```
const today = Date.now();
const nrDays = 7;
const msPerDay = 86400000;
const msNrDays = nrDays * msPerDay;
const msDaysAgo = today - msNrDays;

pm.environment.set("from-time", msDaysAgo); // nrDays ago in ms
pm.environment.set("to-time", today); // Today in ms
```

Figure 19: Screenshot of GET request for audit log in Postman.

Once we had recieved an access token we could send the GET request for the audit log, as shown in Figure 19.

After we confirmed the data was accessible from the API using an API key, we created a python script based on the script by Emmanuel Tychon, which fetched the relevant data from the API, created an e-mail and sent it.

```
def getAccessToken():

    headers = {'Content-Type': 'application/json'}
    task = {
        'grant_type':'client_credentials',
        'client_id': "%s->%s" % (constants.ORG_NAME.lower(),
                                 constants.API_KEY_NAME.lower()),
        'client_secret': constants.API_KEY_SECRET
    }

    res = requests.post(
        constants.SERVER_URL + constants.AUTH_PATH,
        json=task,
        headers=headers)

    if res.status_code == 200:
        if debugmode:
            print('Authenticated with API key   ',
                  res.status_code, ' ', res.reason)

        res_json = res.json()
        access_token = res_json['access_token']
    else:
        print('ERROR    ', res.status_code, ' ', res.reason)
        exit(1)

    try:
        access_token
    except NameError:
        print('No access token, aborting script.')
        exit(2);

    return access_token
```

Figure 20: Python code to get access token for UC4.

To make requests from the API, we first need to authenticate and receive an access token. The code in Figure 20 is how we requested the access token using an API key.

```
def getAuditLog():
    size = 100
    audits = []
    access_token = getAccessToken()
    nrDays = 7
    now = int(round(time.time() * 1000))
    headers = {
        'Content-Type': 'application/json',
        'Authorization': 'Bearer ' + access_token,
        'X-Access-Token': access_token,
        'x-tenant-id': constants.TENANT_ID
    }
    params = {
        'svc-name': 'Secure Equipment Access',
        'size': size,
        'page': 1,
        'from-time': now-(86400*1000*nrDays),
        'to-time': now,
        'sort': '-time'
    }

    while params['size'] > 0:
        # Intialize amount recieved to 0
        received = 0
        res = requests.get(
            constants.SERVER_URL + constants.AUDIT_PATH + paramToString(params),
            headers=headers
        )
        # Was the request successful
        if res.status_code == 200:
            res_json = res.json()

            # Ensure the values are comparable
            for key in res_json:
                if res_json[key] == None:
                    res_json[key] = 0
            if debugmode:
                print(res_json)
            if res_json['count'] > 0:
                received = len(res_json['audits'])

                # Only append if the audit is regarding remote access
                for val in res_json['audits']:
                    if val['status'] == 'SUCCESS: OPEN_REMOTE_SESSION':
                        audits.append(val)

            # Check if last page
            if received < params['size']:
                # End the loop
                params['size'] = params['size'] - params['size']
            else: # If not last page, get next page
                params['page'] = params['page'] + 1
        else:
            print('Error ', res.status_code, ' ', res.reason)
            exit(3);
    return audits
```

Figure 21: Python code to request audit log for UC4.

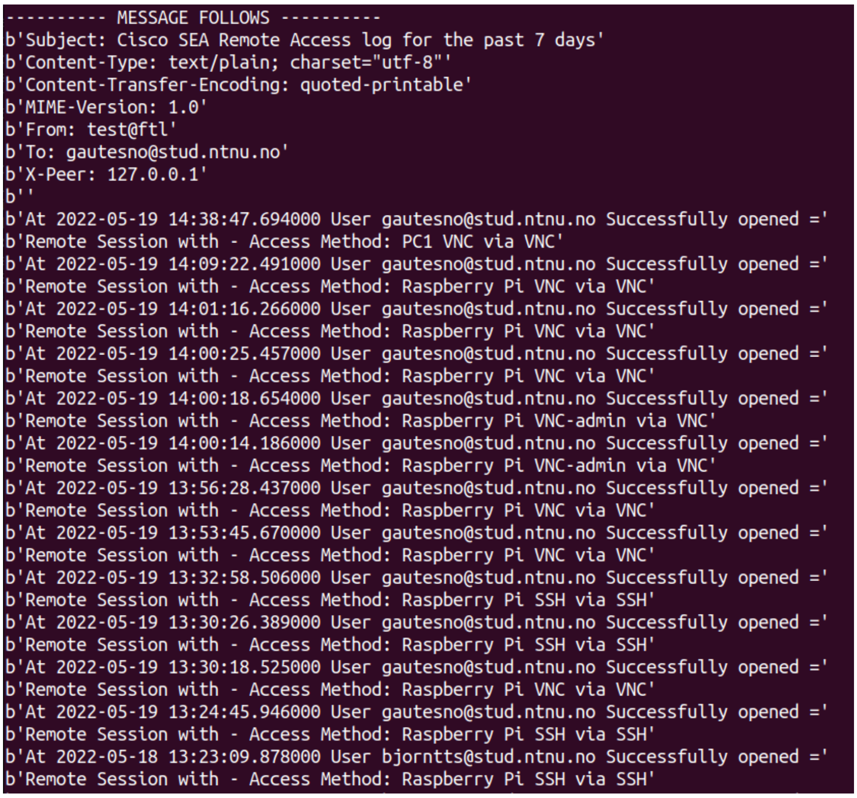
With the access token, we could then request the audit log from the relevant time frame with the code in Figure 21. It may be possible to filter the request further, but due to the lack of documentation we chose to filter the received data using python instead.

The final part of the use case is to e-mail the log of remote access sessions to a specified e-mail. Using `smtplib` and `email` libraries from the python standard library we are able to send an e-mail using the python script.

```python
# Define the EmailMessage() details with 'content'
def createEmail(content):
    msg = EmailMessage()

    msg['Subject'] = 'Cisco SEA Remote Access log for the past 7 days'
    msg.set_content(content)
    msg['From'] = constants.EMAIL_FROM    # From constants.py
    msg['To'] = constants.EMAIL_TO        # From constants.py

    return msg

# Send an EmailMessage()
def sendEmail(msg):
    s = smtplib.SMTP('localhost')
    s.send_message(msg)
    s.quit
```

Figure 22: The python code we use to create and send e-mail for UC4.

It is possible to send an e-mail without the `email` library, but it is recommended to use it to first create the message, which is what we chose to do. The functions we created to create and send the e-mail is shown in Figure 22.



```
---------- MESSAGE FOLLOWS ----------
b'Subject: Cisco SEA Remote Access log for the past 7 days'
b'Content-Type: text/plain; charset="utf-8"'
b'Content-Transfer-Encoding: quoted-printable'
b'MIME-Version: 1.0'
b'From: test@ftl'
b'To: gautesno@stud.ntnu.no'
b'X-Peer: 127.0.0.1'
b''
b'At 2022-05-19 14:38:47.694000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: PC1 VNC via VNC'
b'At 2022-05-19 14:09:22.491000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 14:01:16.266000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 14:00:25.457000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 14:00:18.654000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC-admin via VNC'
b'At 2022-05-19 14:00:14.186000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC-admin via VNC'
b'At 2022-05-19 13:56:28.437000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 13:53:45.670000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 13:32:58.506000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi SSH via SSH'
b'At 2022-05-19 13:30:26.389000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi SSH via SSH'
b'At 2022-05-19 13:30:18.525000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi VNC via VNC'
b'At 2022-05-19 13:24:45.946000 User gautesno@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi SSH via SSH'
b'At 2022-05-18 13:23:09.878000 User bjorntts@stud.ntnu.no Successfully opened ='
b'Remote Session with - Access Method: Raspberry Pi SSH via SSH'
```

Figure 23: The resulting e-mail generated from the script for UC4.

To test the script we utilised a python SMTP development server. This development server is started using the command:
`sudo python3 -m smtpd -c DebuggingServer -n localhost:25`
This prints the resulting e-mail in the terminal rather than sending it, as shown in Figure 23.

The audit data sent from the IoT OD API contains a lot of information regarding each event, and our script filtered out most of the data. This can be adapted to suit the clients requirements should they want more or less data per event.

4 Analysis

4.1 Asset owner requirements

The asset owner in the task (see Appendix A) has a set of requirements we used as basis for our analysis.

1. The asset owner needs a secure solution that enables their in-house technicians to work on industrial assets located within their industrial infrastructure from both internal networks as well as networks outside the company's enterprise infrastructure.
2. The asset owner needs a secure solution that enables their vendors and service/maintenance partners (located outside the asset owner's enterprise network) to work on industrial assets located and secured within their industrial infrastructure.
3. The asset owner needs a solution that enables them to control access sessions (from both local and remote) to their industrial infrastructure.
4. In-house technicians need to access control system applications or hosts running said applications through a variety of communication protocols. Protocols that must be supported are RDP, VNC, Telnet and SSH.
5. The customer needs a solution/service that enables in-house technicians as well as external vendors and service partners to transfer files to and from industrial components

4.2 Short study of the System under Consideration

As Cisco SEA is a new service, and that is shown by the fact that there is a lack of other documents and reports to consult. It was very hard to find any studies describing the capabilities and intended use of the system. The Forrester Wave report (Kime et al. 2021) does mention SEA in comparison to other industry alternatives, however it never goes into depth regarding the product's architecture and simply compares its features. The documentation provided on Cisco DevNet (Cisco 2021c) is a great recourse for setting up the system and using it, although some of the information is not up to date and the example provided were just wrong (see Section 4.4). The newsletter on dcloud-cms.cisco.com (Cisco 2021a), provides no information at all other than the fact that the service is available. The one whitepaper we did find by Cisco (Cisco 2021d), is about how to securely manage IOT devices used to make roads safer. It was not specifically about SEA but did mention it as part of a solution.

In general, there is a great deal of documentation on how to setup and use the system, but not any studies on system itself.

4.3 Proof of Concept

By using the basic setup described in Section 3.2.2 in addition to some basic endpoints. The setup will look like Figure 24.

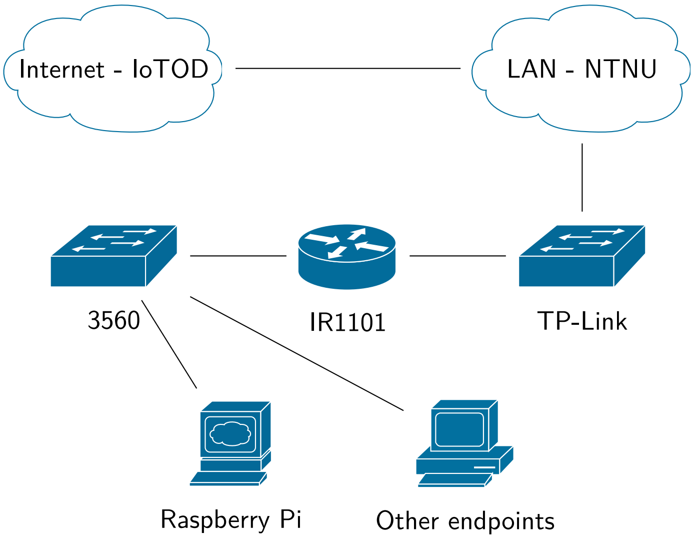


Figure 24: General overview of the setup

The proof of concept is essentially a practical pilot of the service we are attempting to evaluate. In Section 3.2.4 we provide templates and detailed instructions on how we configured and on-boarded enterprise devices to the IoT OD. In the same section mentioned previously, you will also find templates on how to perform the use cases outlined to us by our client. This also serves as an assessment of the platform

4.4 Use cases

Use case 1

Use case 1 requires that the system is able to provide direct IP access to equipment located within the industrial network so that an external maintenance technician can use proprietary software remotely from their workstation. According to the SEA

documentation on DevNet (Cisco 2021c), this should be part of the functionality of SEA. The documentation mentions as an example that 'An elevator technician can use SEA to establish IP connectivity between his PC and an elevator in another city. He can then use a diagnostics application on his PC to troubleshoot an issue, determine a solution, and dispatch a repair technician with the right parts for that issue'.
This does not work. Therefore we are unable to discern whether this use case fulfils the asset owner requirements. If it is possible, it is not obvious how and there is no documentation describing how to configure it.

Use case 2

An external maintenance technician needs remote desktop access to a jump-host located within the asset owner's industrial demilitarised zone.

This use case is easily solved by installing any computer, in our case, a raspberry pi within the industrial demilitarised zone to act as a jump-host. Cisco IoT dashboard allows access privileges to external technicians, all we have to do is create a user group with sufficient access control and add it to the target endpoint or access method.

- Is there any concern regarding security when critical infrastructure is accessible via enterprise and external networks?

Cisco SEA minimises this risk by installing an Agent on the IoT operation dashboard managed gateway which acts as a middleman when creating remote sessions between the remote user and the industrial equipment. There are no port forwarding needed because the device call home to the cloud and the cloud does not seek out the device. This way, we ensure that remote sessions are passed through an industrial demilitarised zone (IDMZ) before being routed to vulnerable infrastructure.

Use case 3

An internal administrator needs remote desktop access to servers within the industrial environment to maintain the operating system for servers which they are assigned to.

- Does the solutions for use case 2 and 3 fulfil asset owner requirements described in the project description?

The SuC fulfils most of the asset owner requirements, with the exception of the required support for the telnet protocol for remote access of terminal devices. In addition to that, the SuC also does not allow verification of access method ssh using a local RSA-key. Accounts accessing the IoT OD is also not protected by modern technologies such as two-factor authentication or smart card. All the previously mention reasons are discrepancies SEA has in functionality and security, in relation with the asset owner requirements.

Use case 4

The plant director needs access to reports showing all remote access sessions to industrial equipment within the asset owner's industrial infrastructure. This report shall be delivered to the plant director's email once a week.

Cisco IoT OD has a page providing audit logs of every remote access session. Through those logs, we can investigate suspicion activity in our SuC. The IoT OD also has API's that can be accessed directly in order to automate the process to deliver weekly audit logs to the plant director. However, we were not able to find instructions on how to utilise these API's and had to contact our client, and which conveyed this message to their Cisco representative. After receiving a code example from the Cisco representative, regarding a similar API, we manged to accomplish this use case. We also figured out through testing with postman, that the API provided much more extensive audit data, compared to the GUI version.

This use case is by far the most compliant with the asset owner requirements among the four. There were detailed and easy to access audit information about each remote access session in the GUI of IoT OD. Not only that, but by utilising Cisco's API's you can create scripts for fetching even more extensive and less recent audit data. However, the documentation for use of these API's are quire scarce at the moment, and unless you have contact with a Cisco representative, you would hardly find any relevant instructions to use them.

4.5 Risk

Cisco IoT Operations Dashboard lacks the option for MFA. Should be prioritised. Adding MFA would significantly lower the risk of using the platform.

4.5.1 Standards

This section will include the evaluation of the SuC, based on the relevant and recommended standards provided by our client.

ISA/IEC 62443

Evaluation of maturity level 1-4: The subject of our evaluation is the cloud based service Cisco SEA. Cisco is a seasoned veteran organisation in terms of providing secure network devices, and their software also follow the same standard of quality checks. Cisco SEA is a service that is constantly improving with regards to its functionality features and security measures. In conjunction with the remote access a infrastructure provided by our client, we believe our SuC to belong in maturity level 4, improving.

Evaluation of Security level 0-4: As Security service providers, we are supposed to strive for the highest degree of cyber security implementations, with a continual improvement approach. However, considering that Cisco SEA have been released for less than a year, and the fact that this project is the first time we are evaluating a service based on IEC 62443, we should temper our expectation somewhat. Therefore, we will be setting a target security level of 3 to each FR. SL-T{3,3,3,3,3,3,3}

Evaluation and justification of SL-A: IEC 62443-3-3 defines many requirements concerning the security of identification and authentication control. These requirements addresses identification and authentication of:

- Human users
- Software process and devices
- Account management
- Identifier management
- Authenticator management
- Wireless access management access
- Strength of password-based authentication
- Public key infrastructure (PKI) certificates
- Strength of public key
- Authenticator feedback
- Unsuccessful login attempts
- System use notification
- access via untrusted networks

The first requirement encapsulates identification and authentication of human users. The requirement are:

- Unique identification and authentication of user
- Multifactor authentication for untrusted networks
- Multifactor authentication of all networks

As of today there are no options to set up multifactor authentication for our accounts. Therefore, it only achieves maximum SL-A (IAC) 2, despite scoring higher on different requirements such as control groups, account management password strength, etc. Some requirements might be score lower, but this is already below our target security level and should be address in capability security level.

Security level of use control (UC) encapsulates requirements for:

- Authorisation enforcement
- Wireless use
- Use via portable and mobile devices
- Mobile code
- Session lock
- Remote session termination
- Concurrent session control
- Audtitable events
- Audit storage capacity
- Response to audit processing failure
- Timestamps
- Non-repudiation

Apart from wireless use and mobile code, which is not applicable to our IACS, most of the requirements regarding user control (UC) achieves security level 3 or above. The only uncertainties are authorisation enforcement, where Cisco SEA does not explicitly supports supervisor override of configurable time or event sequences, but this is achievable in different places of the ICS, in this instance utilising Linux Plugin Authentication Method (PAM). Another point of contention is with audit storage capacity alerts. All audit data is stored within Cisco's cloud, and we do not have access, nor did we find any documentation indicating that this requirement is fulfilled. Other than those two points, we believe this area of our ICS to be at SL-A (UC) 3, and does not need to be addressed at SL-C.

The security level of system integrity encapsulates the following requirements:

- Communication integrity
- Malicious code protection
- Security functionality verification
- Software and information integrity
- Input validation
- Deterministic output
- Error handling
- Session integrity
- Protection of audit information

Cisco SEA provides many safeguards naively, in order to ensure system integrity. These being, firewalls, dedicated IDMZ, enterprise network routing, API access to extensive auditing information, system alerts in the web interface and email, to name a few. In order to ensure the protection of auditing information when we are conducting the required weekly rapport, we include options to ensure that the data is only viewable and sent to authorised emails. With this in mind, this FR receives a SL-A (SI) of three and does not to be considered in SL-C.

Security level of data confidentiality encapsulates the following requirements:

- Information confidentiality
- Information persistence
- Use of cryptography

On a preliminary review of the requirements contained in this FR, it would seem like our SuC is mostly compliant. The only contentious part is the capability to purge shared memory resources. This can be implemented in the control system using a simple terminal command, however, Cisco SEA supports different users accessing the same instance simultaneously. This is an unfortunate consequence of the system design, and therefore i do not think the FR should be considered in SL-C. Therefore achieves a SL-A (DC) score of 3, until further notice.

SL of RDF encapsulates the following requirements:

- Network segmentation
- Zone boundary protection
- General purpose person-to-person communication restrictions
- Application partitioning

The current system have multiple different layers in terms of network segmentation and zone boundary protection. However, by the design of a remote access solution, the current system is unable to restrict or deny all access from outside sources or between boundary zones, which is indicated in the requirements of RDF. Therefore, this FR should be given a SL-A (RDF) of 2.

SL of TRE encapsulates the following requirements:

- Audit log accessibility
- Continuous monitoring

The Cisco IoT dashboard provides sufficient continuous monitoring of security measures and performance in order to detect, characterise and report security breaches. Our SuC also allows programmatic access to extensive audit logs, both of which is listed as requirements within the sixth FR TRE. Therefore, this FR achieves a SL-A (TRE) above 3 and does not need to be addressed in SL-C.

SL of RA encapsulates the following requirements:

- Denial of service protection
- Resource management
- Control system backup

- Control system recovery and reconstitution
- Emergency power
- Network and security configuration settings
- Least functionality
- Control system component inventory

Many of the requirements listed in this FR revolves around the configuration and implementation of the control system. This is outside of scope considering we are only evaluating the remote access mechanism of the SuC. Cisco SEA provides sufficient alerts and notifications and also configuration control for protection against DDOS attack by limiting packages from unverified sources and limiting data rate. Therefore this FR recieves the preliminary SL-A (RA) of 3. The final achieved security level is SL-A{2, 3, 3, 3, 2, 3, 3}.

There are several issues that needs to be resolved in order for the SuC to rise to an acceptable SL. After a preliminary review of the different requirements applicable to Cisco SEA, we have concluded that there are discrepancies in the FR's IAC, SI and RDF.

As previously mentioned, SEA users needs the option to active multi factor authentication, especially when because the system i access able through untrusted networks. In addition to this, the system currently does not provide hardware mechanisms for software processes that need additional identity credentials. Adding these features would lift the Cisco SEA to the recommended SL-C (IAC) of 3.

A requirement detailed in the RDF section of FR SL, describes a concept called zone boundary protection. There are three enhancements mentioned in this requirement, in order to achieve an SL score of 3 or above the system needs to satisfy all three of these enhancements. The first enhancement explains the need to be able to configure the system so that all network traffic are denied by default and allowed by exception. This enhancement is easily achievable by configuring ACL's on the router. The second and third enhancement is called island mode and fail close. Island mode means that the system needs to provide the capability to cut all communication throughout the control system boundary, essentially operating without outside influence. This enhancement is considerably harder, especially considering the nature of Cisco SEA being a remote access service that is connected to the IR1101 router through Cisco's cloud. The fail close enhancement is referring to the ability to close off any communication through the control system boundary when there is a hardware of power failure, causing boundary protection devices to malfunction or operate in a degraded mode. This feature must also be implemented in a way so that it does not interfere with other safety related function. This feature is configurable, but not the responsibility of a remote access part of the system such as Cisco SEA, and therefore out of scope. In order to raise the overall SL-C (RDF) the system needs to be able to operate properly without dependence to the Cisco cloud, however, operating in such a state would remove important auditing and monitoring features, making it harder to troubleshoot any potential issues. SL-C{3, 3, 3, 3, 2*, 3, 3}

The specific details of IACS security requirements can be find in the IEC 62443-3-3 standard, along with the different scoring methods and more details about SL's and FR's (International Electrotechnical Commission 2019).

NIST

As previously mentioned, the most effective way to mitigate security risks in an ICS is to gather a group of individuals from different departments, with a wide spectrum of responsibilities regarding the ICS in question. This group then needs to gather and implement best practices acknowledged as industry standards, collaborate on solutions to secure each facet of the ICS and continually improve upon their solution.

The standard also mentions a concept called defence-in-depth strategy to ensure all earlier mentioned security risks and goals are met. Cisco SEA is a newly launched service, and therefore lacks the appropriate training and educational documentation about the ICS in order to properly fulfil the requirements of the defence-in-depth strategy. In addition, the current system does not provide support for modern technology such as smart cards or two factor authentication for Personal Identity Verification (PIV), which is listed as a point in the defence-in-depth strategy.

Lastly, in order to be compliant to the NIST SP 800-82 rev. 2, the security team and service developers need to continually improve on the following aspects of the ICS. Deploying extensively verified security patches to the ICS, continually implement secure and reliable network protocols and services whenever possible, apply encryption and cryptographic hashes to ICS data that is deemed valuable and lastly, implement software that checks for file integrity, and detects intruders and viruses.

Finally, it is important to emphasise the fact that cyber security can not be solved by a fixed product, but rather a continuous process. As Malicious software and hackers become more sophisticated, so must procedures and individuals in the cyber security team improve and adapt in a race against any potential threat. Only after a collaborative effort, consisting of individuals from management, control engineers, operators, IT specialists and automation advisers, do organisations stand a chance against the plethora of cyber criminals that currently exist.

5 Discussion

5.1 Results

Most of the functional requirements provided to us by our client were met. However, none of the use cases were able to fully be compliant with the asset owner requirements also provided by the client.

The first use case was the only one who lacked the functional requirements demanded by the user story description. We were subsequently unable to even begin analysing whether it would be compliant with the asset owner requirements.

The second and third Use case was mostly compliant with the functional requirements, with the exception of support for all the listed remote accessing protocols. The same holds true in regards to asset owner requirements, where the SuC was compliant with most asset owner requirements, but lacked a few key security safeguards to be considered completely compliant.

Differing from the rest, the fourth use case was able to achieve all functional requirements described by our client. This use case would have been compliant with all the asset owner requirements as well, if the use of Cisco API's were fully documented in their DevNet. Researching methods to utilise the website's API's was a major inconvenience and would not have been possible without help from internal Cisco technicians.

5.2 Alternatives

After we received the detailed task description, there were little room for variation and alteration of the task. Our client did include us in the development phase of the task, before the details were decided. We could essentially formulate any task, as long as it was linked to Industry 4.0. We also decided to forego the national security standard 'Kraftberedskapsforskriften', considering it is a strictly national cyber security standard that specifically targets power providing control systems.

We were also instructed by out client to explore different solution to solve use cases, where the SuC were unable to perform the required task. This proved more difficult than expected, as finding an accessible service that provided IP connectivity to a remote device would yield disappointing results.

5.3 Issues

Initial connection to Cisco IoT OD did not work as expected. The IR1101 router is supposed to automatically on-board to the IoT OD after being connected to either Ethernet or celluar internet. This is supposed to be a zero-touch deployment (ZTD) using the earlier mention Cisco PnP service, that connects the router to a PnP server and fetches instructions in order to connect to the IoT OD. At first, we tried to erase the start configuration of the router, which is documented as a common problem for PnP nor working. This however, did not work, so we tried to on-board the device according to the Cisco DevNet (Cisco n.d.[a]). Again, this did not work, despite verifying that the router is able to contact the IoT OD using the following command line `telnet eu.ciscoiot.com 443`. Cisco DevNet instructed us to use the telnet protocol, because the website does not allow pings to communicate with the network. This issue was finally resolved by connecting the router to one of our phones to share its celluar data, after erasing the device's configuration. We later found out through the PnP summary logs that the router was routed to a local PnP server located in our universities computer lab, and therefore unable to fetch the proper instructions from the designated IoT OD PnP server.

After running perfectly fine for a few weeks, the IoT OD suddenly alerted us that our IR1101 router was down, meaning offline from the EDM. This prevented us from receiving diagnostic data and functionality of both EDM and SEA. We were also unable to gather necessary screenshots and verification of functionality for our rapport. However, after further inspection, we found out that despite the router showing up as down on EDM, it was still online on SEA. This should not be possible, according to the documentation, the router needs to be on-boarded to EDM in order to gain access to the SEA service. Our current system is only able to perform features tied to SEA, being remote access to the connected devices. The features tied to EDM, such as device monitoring, auditing logs, error alerts and pushing of device configuration is not available at the moment. We were unable to successfully troubleshoot this issue.

When adding an IoT device access with the SSH method, we noticed that the IoT OD does not require or allow adding a private key for added security. This means that the access method solely relies on the security provided by the specific user credentials. A core feature set of SSH is the ability to authenticate using a private key. The absence of this option is not a proper implementation of this protocol, in our opinion.

Establishing IP connectivity between a local computer and a remote device is something that is listed as a possible use case for Cisco SEA in their DevNet page. This is also a use case we have been tasked to test by our client. As of today, we are unable to accomplish this, Cisco SEA in its current form is only able to establish remote connection to devices connected to an IoT OD supported router using either SSH, RDP, VNC or Web. Neither of these remote connections allows us to establish direct IP connectivity with an IoT device such as an elevator, which is used as an example in Cisco DevNet. In order to run diagnostic software on a remote IoT device, we need the software to be installed in a computer located on the remote location rather than on our local computer.

The telnet protocol, is a standard protocol for remote access to terminal devices, similar to SSH, although lacking in security features in comparison. This protocol was included in the list of protocols where support were required from various clients. The Norwegian Cisco representative we met during our tour of the Cisco office, promised support for this protocol on an upcoming patch, but it has yet to arrive as of this date.

While browsing the documentation in Cisco DevNet, we noticed that neither release dates, nor change logs were showing or provided via an external link. This again, is a fairly minor issue, but would be useful considering the documentation for Cisco SEA is frequently updated with crucial information about added features and internal architecture.

5.4 Criticism

There was a lack of officially published documentation about Cisco SEA, which was a requirement we received from our client, to read white papers about the SuC and do a study of its capabilities and uses. This meant that, most of the time were spent either solving the use cases and reviewing the recommended security standards (IEC 62443, NIST SP 800-82), instead of researching about Cisco SEA.

5.5 Evaluation of the teams work

We did not spend as much time on the project as we should have. As is reflected in our work log, and possibly by the report.

5.5.1 Organisation

Throughout the project, we held weekly meetings with both our client and our supervising professor on Mondays and Tuesdays respectively. However, meetings with the client ceased right before easter, after we finished the use cases and there were no technical or functional issues we needed resolution from, regarding the SuC. We initially met up physically to the computer lab to work on the project, but after successfully on-boarding the IR1101 router, we switched to mostly work remotely from home. We also neglected the use of project management tools such as trello boards and time table.

5.5.2 Distribution of workload

Distribution of workload was essentially nonexistent, or only done at the very end of the work process. We mostly collaborated on testing the SuC for the specified tasks and for the rapport, we just assumed tasks based on what was missing. Distribution of tasks only happened after we had very few tasks left, and had to make sure we were not overlapping with another team member.

5.5.3 Project as a working method

As working methods go, project is a very good and realistic method to prepare the students for employment. The task that was given is relevant to the market, in other words, many organisations are looking for solutions to the problems we are tasked to solve. This makes transition from this school project to work life more manageable. We also learned a lot during the project. We utilised many skills and knowledge we learned throughout our degree, but there were also many now tools and concepts that we had to familiarise ourselves with, in order to complete the tasks we were given. Large projects, such as this thesis, teaches us how to quickly learn new methods and apply difficult concepts to real world issues.

6 Conclusion

Poor documentation inhibits the usability of the service. There is also a lack of API documentation and incorrect statements in the current documentation. We can clearly tell that the Cisco DevNet about SEA is a work in progress and based on intended functionality from future patches, rather than a reflection of its current capabilities.

The core functionality of the Cisco SEA and EDM is very userfriendly and well implemented. There are strong security measures built in to the solution, which mitigates common attack vectors by limiting attack surface by reducing open ports, and requiring tunnelling through Cisco cloud, with an SEA agent preinstalled on the gateway. Elaborate permission hierarchy and multiple layers of remote access protocols also reduce the risk of the system. However, the burden is placed on authentication of admin and tenant admin user accounts to IoT OD, which we could not find modern authentication tools for, such as two-factor authentication and smart cards. The absence of telnet support and access to direct IP connectivity to remote device also hurts the functionality prospects of the SuC, in the OT field. Therefore, we are hesitant to recommend Cisco SEA for general adoption.

6.1 Further tasks

Both the IEC 64423 and NIST SP 800-82 are such expansive and all encompassing standards, that a proper evaluation of the SuC, featuring only one of them warrants a full thesis to accomplish. In this bachelor thesis, we are more focused on extracting specific parts of the standard that fit out SuC. In addition, we only dive deeper into specific requirements within the standards that we believe is not met by our SuC after a preliminary evaluation.

We would also like to explore whether Cisco SEA can be expanded to support more commercial types of routers and switch to a commercial use case rather than specifically for OT operation. Access to remote devices is a feature that is highly sought after, not only in OT, but for commercial users as well. Cisco IoT OD, in conjunction with zero-touch deployment devices are extremely user friendly and highly GUI control-able. A commercial user would not have a problem utilising its features and setting up their devices.

References

Cisco (Nov. 2021a). *Cisco Edge Device Manager & Secure Equipment Access – IoT Operations Dashboard Instant Demo v2 | News | Cisco dCloud*. URL: https://dcloud-cms.cisco.com/demo_news/cisco-edge-device-manager-secure-equipment-access-iot-operations-dashboard-instant-demo-v2.

— (2021b). *Release notes - Cisco IoT Operations Dashboard*. URL: https://developer.cisco.com/docs/iotod/#!secure-equipment-access-overview-release-notes/july-13-2021.

— (2021c). *Secure Equipment Access overview*. URL: https://developer.cisco.com/docs/iotod/#!secure-equipment-access-overview-secure-equipment-access-overview/introduction.

— (Nov. 2021d). *Solutions - Six Ways to Secure Connectivity for Intelligent Roadways White Paper - Cisco*. URL: https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/six-secure-conn-intel-roadway-wp.html.

— (n.d.[a]). *Before you begin - Cisco IoT Operations Dashboard*. URL: https://developer.cisco.com/docs/iotod/#!before-you-begin/before-you-begin.

— (n.d.[b]). *Introduction to Cisco IoT OD*. URL: https://developer.cisco.com/docs/iotod/.

— (n.d.[c]). *Network Topology Icons - Cisco*. URL: https://www.cisco.com/c/en/us/about/brand-center/network-topology-icons.html.

— (n.d.[d]). *Supported network devices and firmware*. URL: https://developer.cisco.com/docs/iotod/#!supported-devices-and-firmware.

International Electrotechnical Commission (2019). *Industrial communication networks Network and system security Part 3-3: System security requirements and security levels*. URL: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1033411.

Keith Stouffer (NIST) et al. (May 2015). *SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security | CSRC*. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

Kime, Brian et al. (Nov. 2021). *The Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4 2021*. URL: https://reprints2.forrester.com/#/assets/2/154/RES176441/report.

Lobo, Ruben (Nov. 2021). *Cisco named a leader in The Forrester Wave™: ICS Security - Cisco Blogs*. URL: https://blogs.cisco.com/security/cisco-named-a-leader-in-the-forrester-wave-ics-security.

NIST (Dec. 2018). 'Risk management framework for information systems and organizations:' in: DOI: 10.6028/NIST.SP.800-37R2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

Rolstadås, Asbjørn, Arne Krokan and Lars Thomas Dyrhaug (2017). *TEKNOLOGIEN ENDRER SAMFUNNET*. Bergen: Fagbokforlaget. ISBN: 978-82-450-2297-1.

Shahrukh Raheem (2017). *Introducing PnP Connect - Cisco Blogs*. URL: https://blogs.cisco.com/networking/introducing-pnp-connect.

SSB (2019). *13305: Konsekvensar av koronapandemien. Fjerntilgang og nettsal, etter sysselsetting og næring (SN2007) (prosent) 2020. Statistikkbanken*. URL: https://www.ssb.no/statbank/table/13305.

— (Feb. 2021). *Lønn*. URL: https://www.ssb.no/arbeid-og-lonn/lonn-og-arbeidskraftkostnader/statistikk/lonn.

Tychon, Emmanuel (Mar. 2022). *rainier-api*. URL: https://github.com/etychon/rainier-api.

Appendices

A Task description

Cisco Secure Equipment Access service evaluation

Bacheloroppgave for Cyber Security studenter ved NTNU Gjøvik på vegne av Telenor Norge

The assignment

The assignment, as presented in this document, shall be solved using Cisco Secure Equipment Access (SEA). All hardware, software and licenses regarding Cisco SEA shall be provided by Telenor in conjunction with Cisco.

Items that will be made available to the group are:

- One IR 1101 industrial router or similar which is supported by Cisco SEA
- Software for the industrial router
- License for the router and access to the SEA deployment service (web-based)
- Cisco's Secure Equipment Access web portal
- One Cisco Catalyst switch

All equipment provided by Telenor must be returned once the assignment has been completed.

What needs to be sourced by the group are:

- One workstation to act as in-house clients and external (vendor) technician clients
- One or more workstation(s) which shall act as target systems (simulate engineering workstations, operator workstations, Human machine interface (HMI), ..., etc.)
- Internet access for the IR 1101 router

Assignment background

This assignment is based on real-world challenges and demands Telenor sees from its customers.

This assignment involves three fictional companies, one *asset owner* (the customer), one *industrial service provider (Servicio)* and one *security service provider (Securit)*. The customer is the owner of an industrial plant and the surrounding infrastructure and is referred to as the Asset Owner. The asset owner has hired an industrial service provider which is responsible for maintaining the plants industrial equipment. In addition to scheduled maintenance tasks, the industrial service provider can be called in if there are problems with the industrial equipment that cannot be handled by the asset owner's operators.

Formerly, the industrial service provider has been able to travel to the customer to fulfill their service agreement, but recent complications surrounding travel restrictions has hindered the industrial service providers physical access the plant. The industrial service provider must now get access to the industrial equipment located at the customers infrastructure using other methods.

You work at the *security service provider* and have been tasked to pilot and assess a remote access solution which has been suggested by the customer.

The asset owner is in this assignment a fictional company. It does, however, represent a number of customers known to Telenor and the challenge in this assignment is based on a generalization of these companies.

Assignment tasks

As you work for the security service provider and have been tasked to assess the remote access solution for your customer, you will need to be aware of the customers' requirements and the user stories for which the solution will be used. This document states some requirements from the customer as well as a few user stories for both the customers internal technicians and the industrial service providers technicians.

Tasks

1. Do a short study of the SuC (System Under Consideration). Try to find previously published studies as well as whitepapers describing the SuC, its capabilities and intended use.
2. Do a pilot/PoC (proof of concept) of Cisco's Secure Equipment Access and assess the functionality of the platform
3. Test the user-stories as they are presented by the customer and describe how the platform solves the difference use-cases
4. Do some research and try to describe the risk involved when industrial asset owners open remote access to remote service partners.
    a. What should be the requirements for the asset owners' internal LAN infrastructure to safely open access to external vendors. The network infrastructure inside OT/ICS environments are often non-hierarchical, lacks security features, are poorly documented and lacks a comprehensive and complete asset inventory.
    b. Will the solution provide the necessary security that is recommended by different well known international industrial security frameworks (IEC62443, NIST 800-82, …, etc.)? If possible, do consider national regulatory requirements like the Norwegian "Kraftberedskapsforskriften" for the power and utility sector.
    c. Will the solution provide the necessary traceability and audit capabilities in situations where an investigation of previously accessed systems are of interest?

Asset owner requirements

1. The asset owner needs a secure solution that enables their in-house technicians to work on industrial assets located within their industrial infrastructure from both internal networks as well as networks outside the company's enterprise infrastructure.
2. The asset owner needs a secure solution that enables their vendors and service/maintenance partners (located outside the asset owner's enterprise network) to work on industrial assets located and secured within their industrial infrastructure.
3. The asset owner needs a solution that enables them to control access sessions (from both local and remote) to their industrial infrastructure.
4. In-house technicians need to access control system applications or hosts running said applications through a variety of communication protocols. Protocols that must be supported are RDP, VNC, Telnet and SSH.
5. The customer needs a solution/service that enables in-house technicians as well as external vendors and service partners to transfer files to and from industrial components

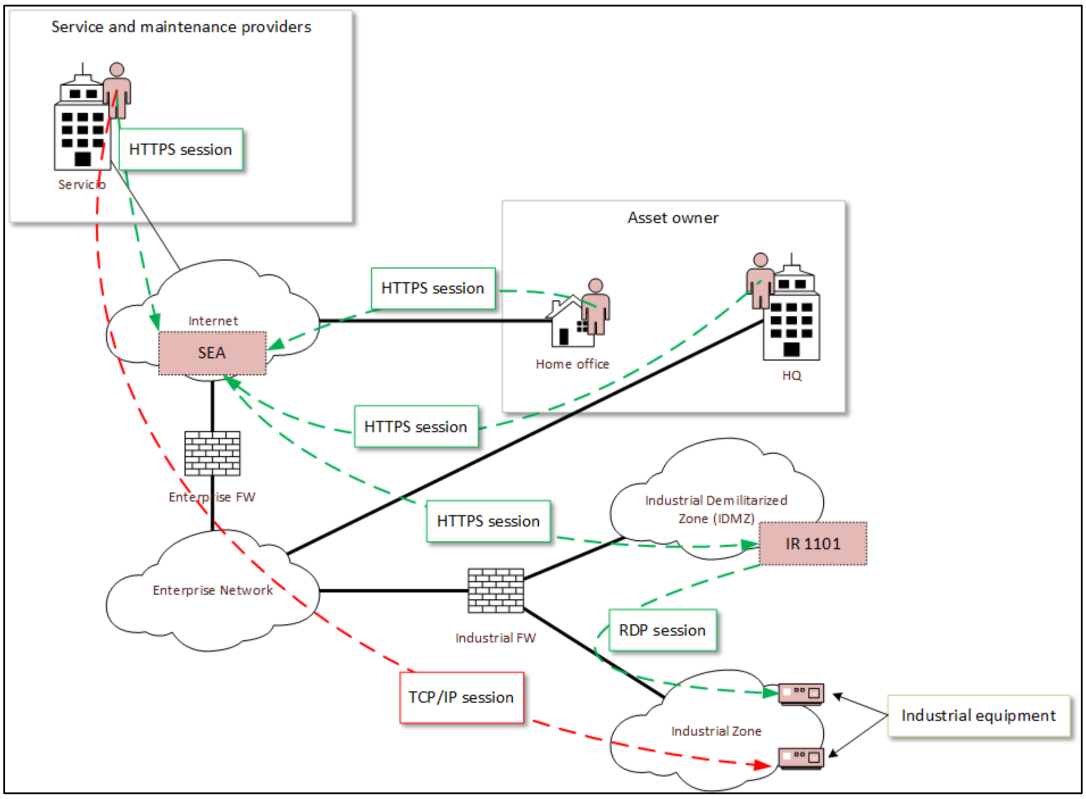
User stories

1. An external maintenance technician needs connectivity to industrial equipment (installed and maintained by his company) located within the asset owner's industrial infrastructure. The technician runs specialized software on his workstation that needs IP-connectivity from his workstation to the target system.
2. An external maintenance technician needs remote desktop access to a jump-host located within the asset owner's industrial demilitarized zone.

Sensitivity: Internal

3. An internal administrator needs remote desktop access to servers within the industrial environment to maintain the operating system for servers which he is assigned to
4. The plant director needs access to reports showing all remote access sessions to industrial equipment within the asset owner's industrial infrastructure. This report shall be delivered to the plant director's email once a week.

Infrastructure drawing



Sensitivity: Internal

B Glossary

Airgap - A security measure where a system or network that needs to be kept secure is physically isolated from the rest of the network or the wider internet.

Cisco Devnet - 'Cisco Devnet' is a learning and digital resource platform for Cisco products. The platform contains documentation, guides, and blog posts about Cisco products. The platform is made by Cisco and is meant to be the go-to for information for developers and system administrators using Cisco products.

Cisco IOS - 'Cisco Internetwork operating system' Is an operating system used on Cisco Routers and Switches.

Cisco SEA - Short for Cisco Secure Equipment Access

EDM - Edge Device Manager

Gantt chart - A type of planning chart that shows both an estimate of time to spend on a task and when that task is planned to be worked on.

HMI - 'Human Machine Interface' The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

Cyber-physical systems - Physical systems with logic, sensors and a Internet connection (Rolstadås et al. 2017).

ICS - 'Industrial Control System' General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) (Keith Stouffer (NIST) et al. 2015).

IOS - See 'Cisco IOS'

IoT - 'Internet of Things'

ISP - 'Internet Service Provider'

Jumphost - Connecting device used specifically for the purpose of connecting to something else within a network.

OT - ‘Operational Technology’ Is defined as programmable systems or devices that interact with something physical or that controls something that interacts with something physical. (NIST 2018) Often used in reference to it-systems that controls something in an industrial environment.

PoC - ‘Proof of Concept’

PoE - ‘Power over Ethernet’, electricity through ethernet cables eliminating the need for separate power supply for the endpoint.

SuC - ‘System under Consideration’

Whitepaper - A report containing information and suggestions for a topic/problem, often published by the state, institution or another authority.

C Full script for use case 4

```python
#!/usr/bin/env python3.10

import requests
import smtplib
import sys
import time
from datetime import datetime
from email.message import EmailMessage
from getopt import GetoptError, getopt
from os.path import exists
#from requests.packages.urllib3.exceptions import InsecureRequestWarning

if exists('constants.py'):
    import constants
else:
    print("Rename 'constants.py.template' to 'constants.py' and fill in the",
          "required constants before executing the script")
    exit(4)

HELPSTRING = 'uc4.py [-d]'

# Default debugging mode to false
debugmode = False

#requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

# Main program
def main(argv):
    # Enable setting the global variable
    global debugmode

    # Get CLI options
    try:
        opts, args = getopt(argv,'hd',['help','debug'])
    except GetoptError:
        print(HELPSTRING)
        exit(5)

    for opt, arg in opts:
        print('Checking: ', opt)
        match opt:
            case '-h' | '--help':
                print(HELPSTRING)
            case '-d' | '--debug':
                print('Enabling debugging')
                debugmode = True

    audit = getAuditLog()
    formattedAudit = formatData(audit)
    msg = createEmail(formattedAudit)

    sendEmail(msg)

# Convert dictionary to GET-request parameter string
def paramToString(p):
    paramString = "?"

    for key, val in p.copy().items():
        if len(paramString) > 1:
            paramString = paramString + '&'

        paramString = paramString + str(key) + '=' + str(val)

    return paramString


# Authentication - getting access token
def getAccessToken():

    headers = {'Content-Type': 'application/json'}
    task = {
        'grant_type':'client_credentials',
        'client_id': "%s->%s" % (constants.ORG_NAME.lower(),
                                 constants.API_KEY_NAME.lower()),
        'client_secret': constants.API_KEY_SECRET
    }

    res = requests.post(
        constants.SERVER_URL + constants.AUTH_PATH,
        json=task,
        headers=headers)

    if res.status_code == 200:
        if debugmode:
            print('Authenticated with API key   ',
                  res.status_code, ' ', res.reason)

        res_json = res.json()
        access_token = res_json['access_token']
    else:
        print('ERROR    ', res.status_code, ' ', res.reason)
        exit(1)

    try:
        access_token
    except NameError:
        print('No access token, aborting script.')
        exit(2);

    return access_token

# Fetching audit log
def getAuditLog():
    size = 100
    audits = []
    access_token = getAccessToken()
    nrDays = 7
    now = int(round(time.time() * 1000))
    headers = {
        'Content-Type': 'application/json',
        'Authorization': 'Bearer ' + access_token,
        'X-Access-Token': access_token,
        'x-tenant-id': constants.TENANT_ID
    }
    params = {
        'svc-name': 'Secure Equipment Access',
        'size': size,
        'page': 1,
        'from-time': now-(86400*1000*nrDays),
        'to-time': now,
        'sort': '-time'
    }

    while params['size'] > 0:
        # Intialize amount recieved to 0
        received = 0
        res = requests.get(
            constants.SERVER_URL + constants.AUDIT_PATH + paramToString(params),
            headers=headers
        )
        # Was the request successful
        if res.status_code == 200:
            res_json = res.json()

            # Ensure the values are comparable
            for key in res_json:
                if res_json[key] == None:
                    res_json[key] = 0
            if debugmode:
                print(res_json)
            if res_json['count'] > 0:
                received = len(res_json['audits'])

                # Only append if the audit is regarding remote access
                for val in res_json['audits']:
                    if val['status'] == 'SUCCESS: OPEN_REMOTE_SESSION':
                        audits.append(val)

            # Check if last page
            if received < params['size']:
                # End the loop
                params['size'] = params['size'] - params['size']
            else: # If not last page, get next page
                params['page'] = params['page'] + 1
        else:
            print('Error ', res.status_code, ' ', res.reason)
            exit(3);
    return audits

# Format the list to be more human-readable
def formatData(data):
    # Formatted data
    formatted = ""

    if len(data) > 0:

        for val in data:
            time = val['time']
            timeString = str(datetime.fromtimestamp(time/1000.0))
            user = val['user-id']
            desc = val['op-desc']

            temp = 'At ' + timeString + ' User ' +  user + ' ' + desc

            formatted = formatted + temp + '\n'
    else:
        formatted = 'No remote accesses in the time period.'

    return formatted

# Define the EmailMessage() details with 'content'
def createEmail(content):
    msg = EmailMessage()

    msg['Subject'] = 'Cisco SEA Remote Access log for the past 7 days'
    msg.set_content(content)
    msg['From'] = constants.EMAIL_FROM    # From constants.py
    msg['To'] = constants.EMAIL_TO        # From constants.py

    return msg

# Send an EmailMessage()
def sendEmail(msg):
    s = smtplib.SMTP('localhost')
    s.send_message(msg)
    s.quit


# Execute program
if __name__ == "__main__":
    main(sys.argv[1:])
```

D Pre-project plan

NTNU
Kunnskap for en bedre verden

Institutt for Informasjonssikkerhet og Kommunikasjonsteknologi

DCSG2900 - Bacheloroppgave i Digital Infrastruktur og Cybersikkerhet

Prosjektplan - Cisco Secure Equipment Access tjenesteevaluering

Skrevet av:
Chi Hou Fung, Gaute Saastad Nogva og Bjørn-Tore Semb

Veileder:
Erjon Zoto

2. februar 2022

1 Prosjektplan

1.1 Mål og rammer

1.1.1 Bakgrunn

Gjennom menneskehetens historie har vi gjennomgått flere industrielle revolusjoner. Den første industrielle revolusjon med vann- og damp-drevet mekanisk produksjon, den andre industrielle revolusjon med elektrisk masseproduksjon, den tredje industrielle revolusjon med elektronikk og informasjonsteknologi (IT) for økt automatisering. Men vi er nå i den fjerde industrielle revolusjon, som er definert med kybernetiske systemer og «Internet of Things» (IoT) (Holtskog 2018).

Den fjerde industrielle revolusjon, også kjent som Industri 4.0, har gitt oss mange muligheter for økt automatisering og optimalisering samtidig som det også skaper utfordringer. Industri 4.0 er en strategi utviklet i Tyskland i samarbeid mellom universiteter, forskingsinstitutter, industribedrifter og myndigheter (Rolstadås mfl. 2017). Industri 4.0 er særlig relevant for norsk industri hvor arbeidskraft er dyrere (SSB 2021) enn i en del andre land siden det kan føre til at man trenger færre personer for produksjon som følge av automatisering.

Men når mer av infrastrukturen kobles til internett for å forenkle styring og vedlikehold, så lager man også en ny risiko for organisasjonen. Det som tidligere var helt utilgjengelig via internett er nå innen rekkevidde for en rekke trusler og man er nå nødt til å sikre operasjonsteknologi-infrastrukturen (OT-infrastrukturen) på ny måte. Før trengte ikke OT å være koblet til internett og hvis det var et problem så kom teknikeren til fabrikken. OT var da tilstrekkelig beskyttet ved hjelp av airgap, altså at det ikke var koblet til internett. Nå, i industri 4.0, blir OT koblet til internett og ved problemer blir det vanligere at teknikeren kobler seg til over internett.

Telenor er i kontakt med flere kunder som er på utkikk etter løsninger for sikker tilgang til egne tjenester og systemer. Da COVID-19 pandemien førte til at store deler av verden stengte i 2020, akselererte mange bedrifter implementeringen for fjerntilgang på systemer som tidligere ble sikret av diverse brannmurer og airgap (SSB 2019).

Cisco lanserte i juli 2021 Cisco Secure Equipment Access (Cisco SEA) som skal tilrettelegge sikker fjerntilgang til OT og andre IoT-enheter for både bedriften som eier systemene og teknikere fra leverandører (Cisco 2021a). Telenor ønsker en tjenestevurdering av Cisco SEA hvor vi evaluerer funksjonaliteten og sikkerheten til tjenesten.

1.1.2 Prosjektmål

Hovedmålet med prosjektet er å vurdere i hvilken grad Cisco SEA er klart for industrielt bruk.

For å enklere kunne vurdere i hvilken grad prosjektet har oppnådd prosjektmålet og hvordan vi kan jobbe mot det har vi definert følgende effektmål og resultatmål.

1.1.2.1 Effektmål

Ønsket effekt av denne oppgaven er:

1. Å framstille en omfattende simulering til bruken av Cisco SEA
2. Vurdere sikkerheten til Cisco SEA tjenesten mot konkrete industrielle sikkerhetsstandarder.
3. Presentere løsninger ved utilstrekkelighet eller mangler av systemet.

1.1.2.2 Resultatmål

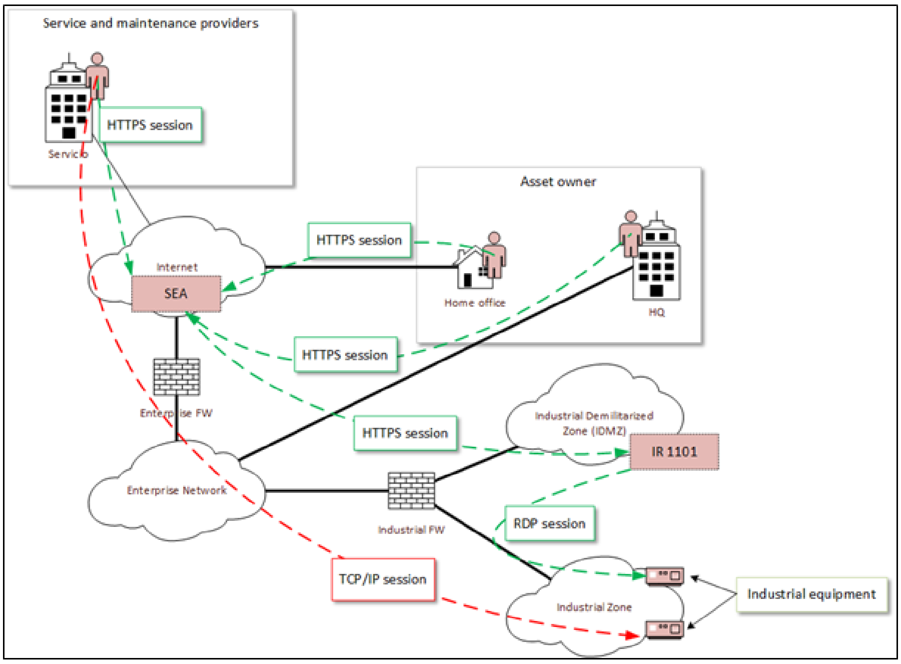
Her har vi satt opp konkrete resultatmål:

1. Gjennomføre en kort undersøkelse av systemet. Prøv å finne relevante tidligere studie og «whitepapers» av systemet som gir innsikt til systemets bruksområde og spesifikasjoner.
2. Test oppsett for «User stories»
   (a) Ekstern vedlikeholdstekniker skal ha IP-tilkobling fra deres maskin til et målsystem.
   (b) En ekstern vedlikeholdstekniker skal ha fjernstyring til den industrielle demilitariserte sonen.
   (c) Intern administrator skal ha fjerntilgang til skrivebord på servere innenfor det industrielle miljøet for å vedlikeholde operativsystemet på serverene.
   (d) Anleggsdirektøren trenger tilgang til rapporter som viser alle fjern-styringssesjoner til det industrielle utstyret innen kundens industrielle infrastruktur. Denne rapporten skal sendes via mail hver uke.
3. Produsere mal for hver «user story» som beskriver forutsetning, oppskrift og sikkerhetsvurdering.

1.1.3 Rammer

Oppgaven har definert tre fiktive selskaper, en kunde, en tjenesteleverandør og oss som representerer leverandør av sikkerhetstjenester. Oppgaven tilsier at vi vurderer sikkerheten og funksojnaliteten av Cisco SEA, som er en skytjeneste knyttet til «standard IoT Operations Dashboard» abonnement lisens.

Prosjektet er hovedsaklig basert på skytjenesten Cisco SEA. Dersom tjenesten ikke klarer å oppfylle brukerfortellingene beskrevet i oppgaven så er vi fri til å undersøke alternative løsninger. Dette gjelder også dersom systemet ikke er i henhold til de industrielle sikkerhetsstandardene nevnt i oppgaven.



Figur 1: Illustrasjon av nettverket til oppgaven.

Oppgaven sier at vi skal følge en slik nettverksinfrastruktur som er sterkt inspirert av purdue sikkerhetsmodellen. Modellen legger mye vekt på en «industrial demilitarized zone(IDMZ)» slik at industrisonen er aldri i direkte kontakt med det offentlige internett (Mazur mfl. 2016). Det er også viktig i følge modellen at det blir brukt forskjellig tilkoblingsprotokeller fra bedriftens nettverk til IDMZ og fra IDMZ til industrisonen.

1.2 Omfang

1.2.1 Problemområde

Fjerntilgang er en svært etterspurt funksjon spesielt som følge av COVID-19 (Adelmann og Gaidosch 2020), men også som et resultat av industri 4.0 og generelt digitalisering av operasjonsteknologi (OT). Ofte er det ikke hensiktsmessig for teknikere å reise til industrisonen hvor nettverksutstyret beligger seg. Med sikker og robust fjerntilgang til industrielt utstyr, kan teknikere både overvåke, vedlikeholde og feilsøke systemet uten fysisk tilgang. Implementeres fjerntilgangen på en dårlig måte vil det føre til flere potensielle sikkerhetshull.

1.2.2 Problemavgrensing

På grunn av eksisterende kompetanse hos teamet og behovene til oppdragsgiver har vi valgt å begrense oppgaven til utstyr fra Cisco. I tillegg har vi valgt å fokusere på en spesifikk tjeneste som ønsker å løse flere av utfordringene ved fjerntilgang.

Vi har sammen med oppdragsgiver og instituttet besluttet å fokusere på tjenesten Cisco Secure Equipment Access (Cisco SEA). Tjenesten er relativt ny og ble lansert av Cisco 13. juli 2021 (Cisco 2021a). Formålet med tjenesten er å gi sikker fjerntilgang til både nettverksenheter og tilkoblede enheter for å kunne direkte feilsøke eller overvåke IoT-enheter (Cisco 2021b).

1.2.3 Problemstilling

Gitt vårt problemområde og avgrensing har vi kommet frem til følgende problemstilling:

> Hvilke begrensinger og utfordringer har Cisco SEA i industrielle OT-miljø?

Med begrensning mener vi om Cisco SEA løser oppgavene tilfredstillende og med utfordringer mener vi om det er egenskaper som gjør tjenesten mindre anvendelig.

1.3 Prosjektorganisering

1.3.1 Teamet

Teamet består av tre personer som har jobbet mye sammen i løpet av studiene i digital infrastruktur og cybersikkerhet ved NTNU i Gjøvik.

Bjørn-Tore Semb

E-post	bjorntts@stud.ntnu.no
Valgfag	Datamodellering og databasesystemer, Algoritmiske metoder, Statistikk, Etisk Hacking, Introduksjon til hendelseshåndtering.

Chi Hou Fung

E-post	chihf@stud.ntnu.no
Valgfag	Datamodellering og databasesystemer, Algoritmiske metoder, Statistikk, Brukerkurs i matematikk A, Introduksjon til Brukerdesign.

Gaute Saastad Nogva

E-post	gautesno@stud.ntnu.no
Valgfag	Datamodellering og databasesystemer, Algoritmiske metoder, Statistikk, Software Security, Introduksjon til hendelseshåndtering.

1.3.2 Veileder

Fra NTNU er vi tildelt en veileder. Veilederens oppgave er å bistå teamet gjennom arbeidet med bacheloroppgaven.

Erjon Zoto, Universitetslektor - NTNU.
E-post: erjon.zoto@ntnu.no

1.3.3 Oppdragsgiver

Prosjektets oppdragsgiver er Telenor Norge AS og oppgaven ble utviklet i samarbeid mellom dem, NTNU og oss studentene.

Tor Martin Slåen Skaar, Security Architect - Telenor.
E-post: tor.skaar@telenor.no

Stian Borgvin Dørre, Senior Consultant - Telenor.
E-post: stian-borgvin.dorre@telenor.no

Øystein Berg, Chief Security Architect - Telenor.
E-post: oystein.berg@telenor.no

1.3.4 Ansvarsforhold og roller

Teamleder - Gaute Saastad Nogva
Denne rollen innebærer å være kontaktperson til oppdragsgiver og instituttet og å håndtere uenigheter eller konflikter om det skulle være nødvendig.

Referent - Chi Hou Fung
For at innholdet i møtene skal være dokumentert har vi valgt en person til å føre referat.

Andre roller
Teamet er forberedt på at det kan oppstå behov for ytterlige roller enn de som er definert her og at dette ikke er en uttømmende liste.

1.3.5 Rutiner og teamregler

1.3.5.1 Teamregler

1. Det forventes at alle gjør sitt ytterste for å møte på alle møter. Kan man ikke møte skal det gis beskjed på forhånd.
2. Det forventes at teammedlemmer er tilgjengelig mellom 09-16 i ukedager da dette er vanlige arbeidstid.
3. Frister satt av teamet, oppdragsgiver eller veileder forventes å holdes. Prosjektet er stort og det er mye som skal gjøres.

Brudd på teamregler vil avhengig av alvorlighetsgrad og antallet brudd, vil få konsekvenser. Disse kan bestå av muntlige advarsler, til i verstefall kontakt med veileder/studieansvarlig. Hvilke konsekvenser som tilfaller avgjøres av øvrige gruppemedlemmer.

1.3.5.2 Rutiner

- Ukentlige statusmøter
  - Med oppdragsgiver mandager klokken 14:00
  - Med veileder tirsdager klokken 14:00
- Agenda
  - Agenda sendes til oppdragsgiver hver fredag før klokken 12.
  - Agenda sendes til veileder hver mandag før klokken 12.
- Forberedelsesmøter
  - Teamet holder ukentlige forberedelsesmøter før statusmøtene med veileder og oppdragsgiver.

1.4 Planlegging, oppfølging og rapportering

1.4.1 Hovedinndeling av prosjektet

Vi har delt opp prosjektet i fem hoveddeler som hver har flere underaktiviteter vi kommer tilbake til i del 1.6.1 av prosjektplanen.

1. Prosjektforberedelse
2. Kartlegge Cisco SEA
3. Teste Cisco SEA
4. Skrive rapport
5. Prosjektpresentasjon

1.4.2 Plan for statusmøter og beslutningspunkter i perioden

1.4.2.1 Statusmøter

På statusmøtene vil teamet presentere hva som er gjort og stille spørsmål som har dukket opp siden forrige møte. Vi vil her få innspill til forbedringer, endringer eller prioriteringer til neste møte.

For å ha godt samarbeid med vår oppdragsgiver har vi avtalt å ha ett møte i uken og vi har avtalt en fast tid for møter gjennom hele prosjektperioden. Grunnen til å avtale møter til hele prosjektet tidlig er at det er mye enklere å avlyse et møte dersom noe skulle dukke opp eller man ikke har behov for det enn det er å avtale et viktig møte på kort varsel. Møter med oppdragsgiver er satt til hver mandag klokken 14:00. Siden oppdragsgiveren ikke er på Gjøvik så holdes møtene på Microsoft Teams.

Vi følger samme filosofi for statusmøter med veileder og avtalte å ha møte hver tirsdag klokken 14:00. Møter med veileder vil holdes på Microsoft Teams inntil koronapandemien tillater at vi møtes på Campus Kallerud og gitt at vi avtaler å holde møter fysisk.

1.4.2.2 Beslutningspunkter

I tillegg til de formelle fristene til prosjektet har vi definert et par egne punkter for når vi bør være ferdig med noen viktige aktiviteter.

2022-02-01 Levert ferdig prosjektplan. Formell frist.

2022-02-07 Satt opp nødvendig utstyr.

2022-04-08 Levert utkast av prosjektrapporten til veileder. Anbefalt frist.

2022-05-01 Hovedinnholdet i prosjektrapporten er ferdig og klart til finpussing.

2022-05-20 Innlevering av ferdig prosjektrapport. Formell frist.

2022-06-01 Presentasjon av prosjektet er klar.

1.5 Organisering og kvalitetssikring

1.5.1 Verktøy, Lagringsplattform, standarder, programvare og utstyr

1.5.1.1 Verktøy

Siden NTNU er koblet tett til Office365 valgte vi å benytte Microsoft Teams for møter og kommunikasjon innad i teamet, samt med veileder og oppdragsgiver.

For organisering av oppgaver og samarbeid i prosjektet har vi valgt å benytte Trello. Trello er et samarbeidsverktøy hvor man organiserer et prosjekt i tavler med oppgaver. Der får vi oversikt over planlagte oppgaver, hva som jobbes med, hvem som jobber med hva og når fristen til oppgaven er.

Vi får dokumentasjon fra Cisco angående enhetene og tjenestene vi skal bruke.

1.5.1.2 Lagringsplattform

Vi har erfart i løpet av studiet at LaTeX egner seg bra til store prosjekt og valgte derfor å benytte Overleaf for oppgaven og vedlegg. Overleaf er en web-basert LaTeX editor som NTNU har avtale med og det har god funksjonalitet for samarbeid.

Ettersom vi i løpet av prosjektet skal teste ulike egenskaper ved Cisco SEA planlegger vi å lagre ulike konfigurasjonsfiler og potensielle skript i et Git repository som vi lagde på GitLab.

Alle andre filer som arkiv av møtereferat og agenda, mindre dokumenter og filer som skal deles med veileder og oppdragsgiver lastes opp på Sharepoint via Microsoft Teams.

1.5.1.3 Standarder

Det er en rekke standarder som er relevante for prosjektet som vi har valgt å følge eller bruke som veileder.

ISO 8601
ISO 8601 er den internasjonale standarden for utveksling av dato og tidsrelatert data og vi har valgt å benytte denne for alle datoer.

ISO/IEC 27005
Internasjonal standard publisert av «International organization for standardization(ISO)» og «interantional electrotechnical commission(IEC)» som definerer beste praksis til risikostyring rettet imot informasjonssikkerhet.

IEC 62443
IEC 62443 er en internasjonal serie standarder som omhandler cybersikkerhet innen operativ teknologi til automasjon og kontrollsystemer.

NIST 800-82
NIST 800-82 er en veileder for hvordan man kan sikre industrielle kontrollsystem.

IMRoD
For strukturen til prosjektrapporten har vi valgt å benytte en IMRoD variant.

1.5.1.4 Programvare og lisens

Cisco IOS
operativsystemet til nettverksutstyret til Cisco.

Cisco IoT Dashboard
Cisco SEA er en tilleggsfunksjon til Cisco IoT Dashboard.

Cisco Edge Device Manager
Cisco Edge Device Manager er en funksjon hos Cisco IoT Dashboard som er nødvendig til «onboarding» av gateway før man kan benytte Cisco SEA.

Cisco Secure Equipment Access lisens
Siden Cisco SEA er i en prøveperiode frem til 2022-12-31, så er lisenset gratis gitt at man har standardlisens til IoT Operations Dashboard.

Windows 10
Arbeidsstasjonene vi benytter på Ciscolabben hos NTNU kjører Windows 10 10 Education 20H2.

Ubuntu 20.04 LTS
Flesteparten av våre personlige PCer kjører Ubuntu 20 LTS.

Ubuntu 21.10
En av våre personlige PCer kjører Ubuntu 21 på grunn av at det er behov for en mer oppdatert kjerne enn det som tilbys fra Ubuntu 20 LTS.

Screen
For å konfigurere nettverksutstyret benytter vi Screen for kommunikasjon via USB.

SSH
Det kan bli aktuelt å benytte SSH for å konfigurere nettverksutstyret.

Firefox
Cisco SEA er web-basert og krever at vi benytter en nettleser, en av nettleserene vi kommer til å bruke er Firefox.

Google Chrome
Det kan også bli aktuelt å benytte nettleseren Google Chrome for samme formål som over.

1.5.1.5 Utstyr

For å gjennomføre prosjektet har vi benyttet disse enhetene

Ruter
Potensielt en Cisco ruter for å simulere ISP.

Industriell ruter
Cisco Catalyst IR1101 Rugged Series Router utlånt fra Telenor Norge AS. IR1101 er en industriell ruter laget av Cisco. Den er kompakt og tilbyr høy modularitet. Den tåler store temperatursvingninger, samling av støv, fuktighet og statisk elektrisitet. Alt dette gjør den egnet for utplassering i industriområder. Ruteren er ofte brukt i vann og høyspentlinje industrien, gass og olje industrien og av og til motorveitransport bransjen.

Svitsj
Cisco 3560-CG Series PoE utlånt fra Telenor Norge AS.

En PC
For å simulere interne klienter eller eksterne teknikere. Vi benytter en Dell Precision T1700 arbeidsstasjon som står på Ciscolabben på NTNU.

En PC
For å simulere målsystemet (ingeniørarbeidsstasjon, operatørarbeidsstasjon, HMI, og lignende). Vi benytter en Dell Precision T1700 arbeidsstasjon som står på Ciscolabben på NTNU.

Personlige PCer
Ved behov har vi benyttet våre personlige bærbare PCer for diverse oppgaver.
Lenovo ThinkPad L15 Gen 2 - Ubuntu 21.10
Lenovo Yoga slim 7 - Ubuntu 20 LTS
Lenovo ThinkPad E590 - Ubuntu 20.04 LTS

1.5.2 Plan for inspeksjoner og testing

Vi har ingen planlagte tester utenom at vi manuelt skal teste «User stores».

1.5.3 Risikoanalyse på prosjektnivå

Identifisere og beskrive mulige risikoer til prosjektnivået, med tanke på teknologisk, forretningsmessig og prosjektgruppemessige utfordringer vi kan møte på før prosjektstart. Dette er en uformell risikoanalyse og vi vil derfor ikke regne ut risikoscore basert på CIA og sannsynlighet. En formell risikoanalyse vil bli utført i hovedrapporten.

ID	Risiko	Beskrivelse	Alvorlighet
1	Sykdommer	Dersom en eller flere gruppemedlemmer blir syk og ikke kan delta i fysiske møter, eller lab økter for å teste utstyret. Sansynlighet for denne risikoen har økt drastisk med tanke på koronautbruddet.	Høy
2	Skytjenester er utilgjengelig	Ettersom prosjektet er avhengig av mye samarbeid i teamet har vi valgt å benytte flere skytjenester i prosjektet. Om disse skulle ha problemer over lengre tid så kan det begrense muligheten til å fortsette arbeidet.	Høy
3	Tilgang på utstyr	Dersom oppdragsgiver ikke klarer å sende oss nettverksutstyret i tide og vi er nødt til å oppsøke en erstatning fra instituttet.	Middels
4	Oppdragsgiver blir for opptatt	Dersom oppdragsgivern vår blir plutselig for opptatt for å møte opp i statusmøter eller bidra i prosjektet. For eksempel hvis Telenor møter på et cyberangrep/utsatt for hacking eller løsepengevirus.	Lav
5	Campus stenger ned	Dersom koronasituasjonen går ut av kontroll og universitetet bestemmer seg for å stenge campus, så har vi ikke tilgang til nettverksutstyret til å fullføre prosjektet.	Lav
6	Vi mangler ferdigheter	Dersom vi mangler de nødvendige ferdighetene eller ikke klarer å lære de i tide, til å konfigurere og teste utstyret og scenariet, og til slutt ikke klarer å levere et utfyllende oppgave.	Lav

Tabell 1: Risiko for prosjektet

Tiltak og oppfølging av tidligere definerte risikoer. Her definerer vi anbefalte handlinger før prosjektstart for å redusere teamets risiko.

ID	Tiltak	Beskrivelse	Effekt
1	Erstatningsutstyr	Det kan være lurt å etterspørre en erstatningsruter hos instituttet dersom det oppstår problemer fra oppdragsgiver sin side.	Lav
2	Smittevern	Nasjonale smittevernsregler som en-meters regelen, maskebruk og desinfisering av overflater og hender er viktig å følge både før og under prosjektarbeid.	Middles
3	«Due diligence»	Det er viktig å undersøke relevante sikkerhetstandarder og programvare slik at vi har god kontroll over scenariet og kan komme med fornuftige forventninger.	God
4	Lokal backup	For å mitigere konsekvensene til utilgjengelige skytjenester kan vi ha kopier av kritiske filer lokalt på våre maskiner slik at vi ikke er avhengige av tjenester vi ikke har kontroll over for å forstette arbeidet med prosjektet.	God

Tabell 2: Tiltak for å redusere prosjektrisiko

1.6 Plan for gjennomføring

Vi har delt opp prosjektet i flere aktiviteter for å ha en idé over hvordan fremgangen vil være. Aktivitetene blir så visualisert ved hjelp av et gantt-skjema.

1.6.1 Aktiviteter

Prosjektets aktiviteter er delt opp i fem faser; Prosjektforberedelse, Kartlegge funksjonalitet, Utprøving, Skrive rapport og prosjektpresentasjon.

Hver av fasene har en eller flere aktiviteter. Innholdet til fasene og aktivitetene er beskrevet mer detaljert i tabell 3.

ID	Aktivitet	Start	Slutt	Beskrivelse
1	Prosjektforberedelse	2022-01-10	2022-02-28	Denne fasen inneholder aktiviteter som må fullføres før vi kan begynne på selve prosjektet.
1.1	Prosjektplanlegging	2022-01-10	2022-01-31	Lag en prosjektplan og dokumentér hvordan prosjektet skal gjennomføres.
1.2	Undersøke fagfelt	2022-01-20	2022-02-28	Gå dypere inn i OT og finn hovedutfordringene knyttet til vår problemstilling. Finn whitepapers og dokumentasjon som beskriver vårt System under Consideration (SuC).
1.3	Sette opp utstyr	2022-02-01	2022-02-07	Sett opp all nødvendig hardware og software vi trenger for å gjennomføre prosjektet.
1.4	Bli kjent med utstyret	2022-01-24	2022-02-14	Gjennomføre grunnleggende oppgaver med utstyret for å lære bruken.
2	Kartlegge funksjonalitet	2022-02-07	2022-02-28	Denne fasen går ut på å kartlegge funksjonaliteten til tjenesten.
2.1	Eksisterende og planlagt	2022-02-07	2022-02-21	Lag en oversikt over både eksisterende funksjonalitet og det som er planlagt i fremtiden.
2.2	Ønsket og optimal	2022-02-07	2022-02-28	Lag en oversikt over hva tjenesten burde gjøre. Både det som er kritisk for at tjenesten skal være brukbar og det som kan være fint å ha.
3	Utprøving	2022-02-14	2022-04-29	I denne fasen skal vi se i hvilken grad tjenesten løser «User stories» fra oppdragsbeskrivelsen.
3.1	Teste utstyr	2022-02-14	2022-03-25	Gjennomføre «User stories» fra oppdragsbeskrivelsen.
3.2	Vurdere resultater	2022-02-28	2022-04-29	Dokumentere og hente ut informasjon fra resultatet av testene.
4	Skrive rapport	2022-02-15	2022-05-20	Denne fasen omfatter skriving av rapporten.

Tabellen fortsetter på neste side.

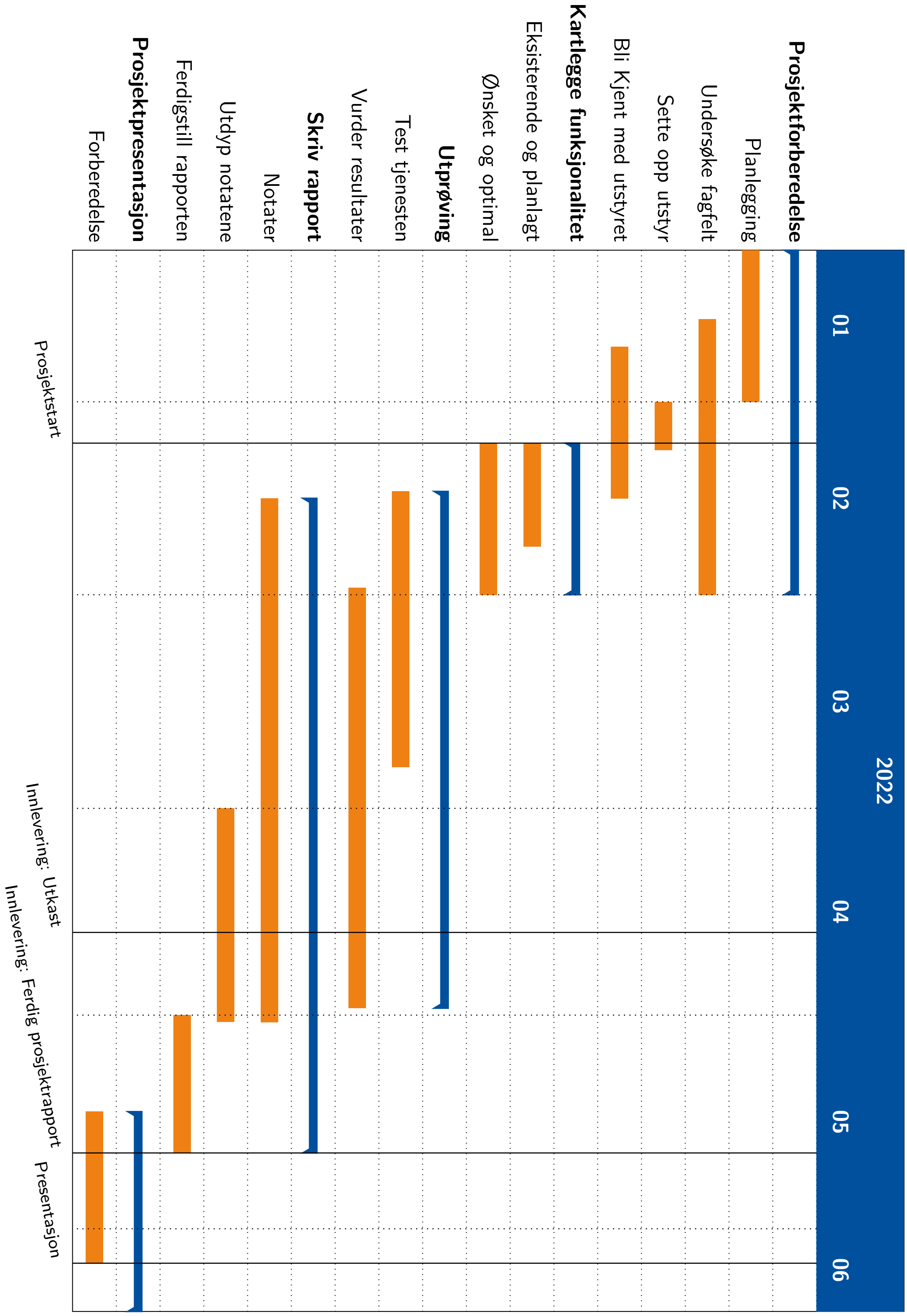
Fortsettelse av tabellen fra forrige side

ID	Aktivitet	Start	Slutt	Beskrivelse
4.1	Skrive notater	2022-02-15	2022-05-01	Legge inn stikkord og korte setninger gjennom prosjektperioden.
4.2	Utdype rapporten	2022-04-01	2022-05-01	Utdype stikkordene og de korte setningene som vi skrev i løpet av prosjektet.
4.3	Ferdigstille rapport	2022-05-01	2022-05-20	Finpusse og avrunde rapporten så den er klar for innlevering 20. mai.
5	Prosjektpresentasjon	2022-05-15	2022-06-12	Siste fase i prosjektet går ut på å lage og holde en presentasjon av rapporten.
5.1	Forberedelse	2022-05-15	2022-06-05	Forberedelse til en 15 minutters presentasjon av rapporten etterfulgt av 10 minutter spørsmål.

Tabell 3: Oversikt over planlagte aktiviteter og tidsplan.

1.6.2 Gantt-skjema

Aktivitetene beskrevet i tabell 3 er visualisert med et gantt-skjema for å gi bedre oversikt over prosjektets planlagte fremgang. Gantt-skjemaet er også nyttig for å se hvilke aktiviteter som overlapper og kan utføres samtidig.



Figur 2: Gantt-skjema for visualisering av prosjektets planlagte fremgang og tidsplan.

Referanser

Adelmann, Frank og Tamas Gaidosch (mai 2020). *Cybersecurity of Remote Work During Pandemic*. URL: https://www.imf.org/-/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx.

Cisco (2021a). *Release notes - Cisco IoT Operations Dashboard - Document - Cisco DevNet*. URL: https://developer.cisco.com/docs/iotod/#!secure-equipment-access-overview-release-notes/july-13-2021.

— (2021b). *Secure Equipment Access overview*. URL: https://developer.cisco.com/docs/iotod/#!secure-equipment-access-overview-secure-equipment-access-overview/introduction.

Holtskog, Halvor (2018). *Overgang til Industri 4.0*.

Mazur, David C. mfl. (mai 2016). «Industrial demilitarized zone». I: *IEEE Transactions on Industry Applications* 52.3, s. 2731–2736. ISSN: 00939994. DOI: 10.1109/TIA.2016.2530045. URL: https://ieeexplore.ieee.org/abstract/document/7406704.

Rolstadås, Asbjørn, Arne Krokan og Lars Thomas Dyrhaug (2017). *TEKNOLOGIEN ENDRER SAMFUNNET*. Bergen: Fagbokforlaget. ISBN: 978-82-450-2297-1.

SSB (2019). *13305: Konsekvensar av koronapandemien. Fjerntilgang og nettsal, etter sysselsetting og næring (SN2007) (prosent) 2020. Statistikkbanken*. URL: https://www.ssb.no/statbank/table/13305.

— (feb. 2021). *Lønn*. URL: https://www.ssb.no/arbeid-og-lonn/lonn-og-arbeidskraftkostnader/statistikk/lonn.

E Work log

1 Bjørn-Tore Semb

Timer	Start	Slutt	Dato	Aktivitet
01:30	14:30	16:00	2022-01-10	Møter & team og Telenor
02:00	10:00	12:00	2022-01-11	Lynkurs
00:30	13:30	14:00	2022-01-11	Spørrerunde
00:15	11:00	11:15	2022-01-13	lagde timeplan
00:58	12:35	13:33	2022-01-13	jobba med prosjektplan
02:07	11:26	13:33	2022-01-14	prosjektplan++
00:45	13:15	14:00	2022-01-17	Teammøte
00:46	14:00	14:46	2022-01-17	Møte med Telenor
00:20	14:00	14:20	2022-01-18	Statusmøte med Erjon
00:37	13:43	14:20	2022-01-19	prosjektplan++
03:10	12:30	15:40	2022-01-20	Oppfrisking av nettverk
01:04	11:20	12:24	2022-01-24	prosjektplan++
00:40	13:15	13:55	2022-01-24	Forberedelse til møte
00:30	14:00	14:30	2022-01-24	Statusmøte med Telenor
00:16	14:30	14:46	2022-01-26	prosjektplan
04:00	13:25	17:25	2022-01-28	prosjektplan
02:00	12:00	14:00	2022-01-31	Cisco SEA presentasjon
00:25	14:00	14:25	2022-01-31	Statusmøte med Telenor
00:40	16:05	16:45	2022-02-01	prosjektplan
02:00	08:00	10:00	2022-02-02	Prosjektplan

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

05:00	10:00	15:00	2022-02-02	Sette opp nettverksutstyr
03:15	09:15	12:30	2022-02-03	jobba med nettverk stuff
02:00	13:00	15:00	2022-02-03	jobba med nettverk stuff
01:30	15:30	17:00	2022-02-03	leste på standardene
01:00	09:30	10:30	2022-02-04	Sette opp nettverksutstyr
02:00	11:00	13:00	2022-02-04	Sette opp nettverksutstyr
00:40	13:15	13:55	2022-02-07	Forberedelse til møte
00:30	14:00	14:30	2022-02-07	Statusmøte med Telenor
02:25	10:00	12:25	2022-02-08	
03:00	10:30	13:30	2022-02-09	troubleshoot PnP
16:50	02:10	19:00	2022-02-09	troubleshoot PnP
03:30	09:30	13:00	2022-02-10	satt opp Edge device manager
01:30	13:30	15:00	2022-02-10	satt opp SEA tilgang
02:30	11:00	13:30	2022-02-11	config av svitj
02:00	14:00	16:00	2022-02-11	RDP
01:00	14:00	15:00	2022-02-14	møte med oppdragsgiver
00:30	14:00	14:30	2022-02-15	møte med Erjon
02:00	12:00	14:00	2022-02-18	leting i dokumentasjon
00:30	14:00	14:30	2022-02-21	møte med oppdragsgiver
01:00	12:00	13:00	2022-02-22	leiting i dokumentasjon
01:00	10:30	11:30	2022-02-23	møte med veileder
03:00	12:00	15:00	2022-02-23	leste dokumentasjon
04:00	11:00	15:00	2022-02-26	på labben

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

00:30	11:00	11:30	2022-02-27	checklist arbeid
00:30	13:15	13:45	2022-02-28	Forberedelse til møte
00:30	14:00	14:30	2022-02-28	Statusmøte med Telenor
00:10	14:30	14:40	2022-03-01	Statusmøte med Erjon
00:30	13:15	13:45	2022-03-07	Forberedelse til møte
00:25	14:00	14:25	2022-03-07	Statusmøte med Telenor
00:15	13:15	13:30	2022-03-14	Forberedelse til møte
00:30	14:00	14:30	2022-03-14	Statusmøte med Telenor
02:00	12:00	14:00	2022-03-15	planlegging
04:25	11:00	15:25	2022-03-15	litt av hvert
05:00	11:00	16:00	2022-03-15	artikler/rapporter
00:30	13:30	14:00	2022-03-21	Forberedelse til møte
04:00	12:00	16:00:00	2022-03-24	leita og leste
00:34	10:26	11:00	2022-03-28	innledning
02:00	14:00	16:00	2022-04-18	rapport
04:00	11:00	15:00	2022-04-19	rapport
04:00	11:00	15:00	2022-04-20	rapport
08:00	07:00	15:00	2022-05-09	rapport
05:00	11:00	16:00	2022-05-10	rapport
00:20	13:50	14:10	2022-05-10	Statusmøte med Erjon
14:00	10:00	1630	2022-05-11	metode
06:00	10:00	16:00	2022-05-11	rapport
05:00	11:00	16:00	2022-05-12	rapport

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.				
03:00	11:00	14:00	2022-05-13	rapport
04:00	12:00	16:00	2022-05-15	rapport
08:00	10:00	18:00	2022-05-18	rapport
15:40	07:00	22:40	2022-05-19	rapport
02:00	09:00	11:00	2022-05-20	Finpussing
00:30	11:00	11:30	2022-05-20	Innlevering

Table 3: Work log for BT

2 Chi Hou Fung

Timer	Start	Slutt	Dato	Aktivitet
01:30	14:30	16:00	2022-01-10	"Møter & team og Telenor"
02:00	10:00	12:00	2022-01-11	Lynkurs
00:30	13:30	14:00	2022-01-11	Spørrerunde
01:00	12:00	13:00	2022-01-13	prosjektplan
01:00	12:00	13:00	2022-01-14	prosjektplan
00:45	13:15	14:00	2022-01-17	teammøte
00:45	14:00	14:45	2022-01-17	møte med oppdragsgiver
01:15	14:45	16:00	2022-01-17	møtereferat
00:20	14:00	14:20	2022-01-18	møte med Erjon
00:40	14:20	15:00	2022-01-18	møtereferat
01:00	12:00	13:00	2022-01-19	prosjektplan
02:00	12:00	14:00	2022-01-20	risikoanalyse
00:40	13:15	13:55	2022-01-24	Forberedelse til møte
00:30	14:00	14:30	2022-01-24	Statusmøte med Telenor
00:20	14:00	14:20	2022-01-25	statusmøte med veileder
00:30	14:20	14:50	2022-01-25	møtereferat
01:00	15:00	16:00	2022-01-25	prosjektplan
02:00	02:00	04:00	2022-01-27	prosjektplan
01:00	15:00	16:00	2022-01-27	prosjektplan
02:00	12:00	14:00	2022-01-28	prosjektplan
01:30	14:30	16:00	2022-01-28	research
02:00	12:00	14:00	2022-01-31	Cisco SEA presentasjon

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

00:25	14:00	14:25	2022-01-31	Statusmøte med Telenor
00:20	14:25	14:45	2022-01-31	referat
01:45	14:45	16:30	2022-01-31	prosjektplan
00:35	14:00	14:35	2022-02-01	statusmøte med veileder
01:25	14:35	16:00	2022-02-01	prosjektplan
00:45	07:00	07:45	2022-02-02	møtereferat
00:45	08:15	09:00	2022-02-02	prosjektplan
06:00	09:00	15:00	2022-02-22	nettverkutstyr
03:15	09:15	12:30	2022-02-03	jobba med nettverk stuff
02:30	13:00	15:30	2022-02-03	jobba med nettverk stuff
01:00	09:30	10:30	2022-02-04	jobba med nettverk stuff
01:15	11:00	12:15	2022-02-04	jobba med nettverk stuff
00:40	13:15	13:55	2022-02-07	Forberedelse til møte
00:30	14:00	14:30	2022-02-07	Statusmøte med Telenor
00:15	14:30	14:45	2022-02-07	referat fra møtet
04:00	09:30	13:30	2022-02-09	troubleshoot PnP
16:50	02:10	19:00	2022-02-09	troubleshoot PnP
03:30	09:30	13:00	2022-02-10	"oppsett av IoT dashboard & møte med veileder"
01:30	13:30	15:00	2022-02-10	satt opp SEA tilgang
03:15	10:15	13:30	2022-02-11	configurasjon av switch
02:00	14:00	16:00	2022-02-11	sikkerhetstandard(lesing)/RDP
01:00	14:00	15:00	2022-02-14	møte med oppdragsgiver
00:30	14:00	14:30	2022-02-15	møte med Erjon

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

02:00	12:00	14:00	2022-02-18	checklist for use case 1
00:30	14:00	14:30	2022-02-21	møte med oppdragsgiver
01:00	12:00	13:00	2022-02-22	oppsett av use case 1 scenario
01:00	10:30	11:30	2022-02-23	møte med veileder
01:00	12:00	13:00	2022-02-23	use case 1
02:00	15:00	17:00	2022-03-21	problem area
00:30	14:00	14:30	2022-03-22	møte med veileder
00:30	14:00	14:30	2022-03-28	møte med oppdragsgiver
03:00	09:00	12:00	2022-04-01	besøkte Cisco Norge
02:00	12:00	14:00	2022-04-01	besøkte Telenor kontoret
02:00	09:00	11:00	2022-04-04	undersøkte IEC standard
03:00	12:00	15:00	2022-04-05	undersøkte IEC standard
03:00	12:00	15:00	2022-04-06	rapportskriving
04:00	12:00	16:00	2022-04-08	rapportskriving
02:00	12:00	14:00	2022-04-16	undersøkte NIST standard
02:00	11:00	13:00	2022-04-17	undersøkte NIST standard
03:00	13:00	16:00	2022-04-18	rapportskriving
00:15	14:00	14:15	2022-04-19	møte med veileder
04:00	21:00	01:00	2022-04-20	rapportskriving
04:00	23:00	03:00	2022-04-30	rapportskriving
04:00	23:00	27:00:00	2022-05-02	rapportskriving
03:00	12:00	15:00	2022-05-09	rapportskriving
04:00	10:00	14:00	2022-05-10	rapportskriving

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.				
01:00	14:00	15:00	2022-05-10	møte med veileder
06:30	09:00	15:30	2022-05-11	rapportskriving
06:30	09:00	15:30	2022-05-12	rapportskriving
06:30	09:00	15:30	2022-05-13	rapportskriving
06:00	10:00	16:00	2022-05-15	rapportskriving
05:00	09:00	14:00	2022-05-18	rapportskriving
00:40	14:00	14:40	2022-05-18	møte med veileder
07:00	13:00	20:00	2022-05-19	rapportskriving
03:00	09:00	12:00	2022-05-20	finpussing

Table 4: Work log for Chi

3 Gaute Saastad Nogva

Timer	Start	Slutt	Dato	Aktivitet
01:30	14:30	16:00	2022-01-10	Møter, team og Telenor
02:00	10:00	12:00	2022-01-11	Lynkurs
00:30	13:30	14:00	2022-01-11	Spørrerunde
00:30	10:00	10:30	2022-01-13	E-poster
02:40	10:30	13:10	2022-01-13	Prosjektplan
01:20	13:30	14:50	2022-01-13	Prosjektplan
04:00	11:00	15:00	2022-01-14	Prosjektplan
00:15	10:30	10:45	2022-01-17	E-poster
01:15	10:45	12:00	2022-01-17	Prosjektplan
00:45	13:15	14:00	2022-01-17	Teammøte
00:45	14:00	14:45	2022-01-17	Statusmøte med Telenor
01:45	14:45	16:30	2022-01-17	Prosjektplan
00:20	14:00	14:20	2022-01-18	Statusmøte med Erjon
00:35	14:20	14:55	2022-01-18	Planlegging
00:40	09:30	10:10	2022-01-19	Planlegging
00:20	10:10	10:30	2022-01-19	E-poster
02:40	10:30	13:10	2022-01-19	Prosjektplan
02:10	13:30	15:40	2022-01-19	Prosjektplan
00:40	09:50	10:30	2022-01-20	planlegging
04:10	11:30	15:40	2022-01-20	Oppfrisking av nettverk
00:40	11:00	11:40	2022-01-21	Prosjektplan
01:20	12:00	13:20	2022-01-21	Oppfrisking av nettverk
Tabellen fortsetter på neste side.				

Fortsettelse fra forrige side.

00:20	13:20	13:40	2022-01-21	Planlegging
02:40	13:40	16:20	2022-01-21	Prosjektplan
01:15	12:00	13:15	2022-01-24	Planlegging
00:40	13:15	13:55	2022-01-24	Forberedelse til møte
00:30	14:00	14:30	2022-01-24	Statusmøte med Telenor
00:25	13:35	14:00	2022-01-25	Forberedelse til møte
00:30	14:00	14:30	2022-01-25	Statusmøte med Erjon
01:00	14:30	15:30	2022-01-25	Planlegging
02:45	10:30	13:15	2022-01-26	Prosjektplan
01:30	13:30	15:00	2022-01-26	Prosjektplan
02:05	11:15	13:20	2022-01-27	Prosjektplan
02:30	09:00	11:30	2022-01-28	Prosjektplan
03:35	11:45	15:20	2022-01-28	prosjektplan
00:30	11:30	12:00	2022-01-31	Forberedelse til møte
01:40	12:00	13:40	2022-01-31	Cisco SEA presentasjon
00:20	13:40	14:00	2022-01-31	Planlegging
00:25	14:00	14:25	2022-01-31	Statusmøte med Telenor
02:20	14:25	16:45	2022-01-31	Teammøte
01:00	18:00	19:00	2022-01-31	Teammøte
00:10	19:00	19:10	2022-01-31	E-poster
00:30	09:20	09:50	2022-02-01	Hentet pakke
01:10	09:50	11:00	2022-02-01	Planlegging
00:35	14:00	14:35	2022-02-01	Statusmøte med Erjon

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

01:26	14:34	16:00	2022-02-01	Prosjektplan
02:00	08:00	10:00	2022-02-02	Prosjektplan
05:00	10:00	15:00	2022-02-02	Sette opp nettverksutstyr
03:15	09:15	12:30	2022-02-03	Sette opp nettverksutstyr
05:00	13:00	18:00	2022-02-03	Sette opp nettverksutstyr
01:00	09:30	10:30	2022-02-04	Sette opp nettverksutstyr
02:00	11:00	13:00	2022-02-04	Sette opp nettverksutstyr
01:10	09:50	11:00	2022-02-07	Planlegging
01:15	11:00	12:15	2022-02-07	Sette opp nettverksutstyr
00:40	13:15	13:55	2022-02-07	Forberedelse til møte
00:30	14:00	14:30	2022-02-07	Statusmøte med Telenor
01:00	11:00	12:00	2022-02-08	Planlegging
01:30	09:30	11:00	2022-02-09	Feilsøking
02:00	11:30	13:30	2022-02-09	Feilsøking
01:30	14:00	15:30	2022-02-09	Feilsøking
03:30	16:00	19:30	2022-02-09	Feilsøking
00:30	10:30	11:00	2022-02-10	Planlegging
00:20	11:00	11:20	2022-02-10	Statusmøte med Erjon
01:10	11:20	12:30	2022-02-10	Feilsøking
01:00	13:00	14:00	2022-02-11	Lesing: Industri 4.0
01:00	15:00	16:00	2022-02-11	Lesing: IR1101
00:30	15:45	16:15	2022-02-12	E-poster
02:00	10:00	12:00	2022-02-21	Svitsjkonfigurasjon

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

01:00	13:00	14:00	2022-02-21	Forberedelse til møte
00:25	14:00	14:25	2022-02-21	Statusmøte med Telenor
00:50	10:40	11:30	2022-02-22	Infrastrukturdiagram
00:35	10:30	11:05	2022-02-23	Statusmøte med Erjon
02:45	11:15	14:00	2022-02-23	VLAN konfigurasjon
03:30	12:00	15:30	2022-02-26	VLAN konfigurasjon
00:30	13:15	13:45	2022-02-28	Forberedelse til møte
00:30	14:00	14:30	2022-02-28	Statusmøte med Telenor
00:10	14:30	14:40	2022-03-01	Statusmøte med Erjon
01:30	12:30	14:00	2022-03-02	VLAN konfigurasjon
00:30	15:30	16:00	2022-03-02	PAT-konfigurasjon
01:00	16:00	17:00	2022-03-02	VLAN konfigurasjon
00:30	18:30	19:00	2022-03-02	Rapportskriving
00:30	13:00	13:30	2022-03-04	Kabelmerking
01:00	13:30	14:30	2022-03-04	Rapportskriving
01:00	14:00	15:00	2022-03-05	Feilsøking
02:00	16:30	18:30	2022-03-06	Raspberry Pi konfigurasjon
01:30	11:00	12:30	2022-03-07	Rapportskriving
00:30	13:15	13:45	2022-03-07	Forberedelse til møte
00:25	14:00	14:25	2022-03-07	Statusmøte med Telenor
02:25	14:30	16:55	2022-03-13	API
01:00	12:00	13:00	2022-03-14	API
00:15	13:15	13:30	2022-03-14	Forberedelse til møte

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

00:30	14:00	14:30	2022-03-14	Statusmøte med Telenor
01:00	09:00	10:00	2022-03-15	API
02:00	12:00	14:00	2022-03-15	Rapportskriving
01:15	12:00	13:15	2022-03-16	API
04:15	12:00	16:15	2022-03-17	API-skript
00:40	11:00	11:40	2022-03-18	API-skript
00:30	13:30	14:00	2022-03-21	Forberedelse til møte
00:10	14:00	14:10	2022-03-21	Statusmøte med Telenor
00:30	14:00	14:30	2022-03-22	Statusmøte med Erjon
00:30	13:30	14:00	2022-03-28	Forberedelse til møte
00:25	14:00	14:25	2022-03-28	Statusmøte med Telenor
03:00	09:00	12:00	2022-04-01	Besøk hos Cisco Norge
02:00	12:00	14:00	2022-04-01	Besøk på Telenor Arena
06:00	14:00	20:00	2022-04-01	Opplegg med Telenor
02:00	12:00	14:00	2022-04-04	Rapportskriving
03:45	11:15	15:00	2022-04-05	Rapportskriving
05:30	10:30	16:00	2022-04-06	Rapportskriving
01:30	11:00	12:30	2022-04-07	Rapportskriving
03:30	10:00	13:30	2022-04-12	Rapportskriving
07:00	09:00	16:00	2022-04-13	Rapportskriving
03:00	12:00	15:00	2022-04-14	Feilsøking
01:45	12:00	13:45	2022-04-15	Rapportskriving
03:45	14:00	17:45	2022-04-17	Rapportskriving

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.

04:00	13:00	17:00	2022-04-18	Rapportskriving
00:30	11:00	11:30	2022-04-19	Feilsøking
00:30	11:45	12:15	2022-04-19	Rapportskriving
00:20	13:30	13:50	2022-04-19	Forberedelse til møte
00:10	14:00	14:10	2022-04-19	Statusmøte med Erjon
05:00	09:00	14:00	2022-04-20	Rapportskriving
05:45	09:15	15:00	2022-04-21	Rapportskriving
03:30	10:30	14:00	2022-04-22	Rapportskriving
02:45	09:45	12:30	2022-04-25	Rapportskriving
03:30	11:15	14:45	2022-04-26	Rapportskriving
06:00	09:00	15:00	2022-04-27	Rapportskriving
02:30	09:00	11:30	2022-04-28	Feilsøking
02:30	10:30	13:00	2022-04-30	Rapportskriving
01:45	17:15	19:00	2022-05-01	Rapportskriving
01:15	19:45	21:00	2022-05-01	Rapportskriving
02:30	14:00	16:30	2022-05-09	Rapportskriving
1:05	13:10	14:15	2022-05-10	Statusmøte med Erjon
06:00	09:15	15:15	2022-05-11	Rapportskriving
02:45	12:45	15:30	2022-05-12	Rapportskriving
05:10	10:20	15:30	2022-05-13	Rapportskriving
01:30	10:30	12:00	2022-05-15	Rapportskriving
03:00	13:00	16:00	2022-05-15	Rapportskriving
01:30	21:00	22:30	2022-05-15	Rapportskriving

Tabellen fortsetter på neste side.

Fortsettelse fra forrige side.				
02:45	11:00	13:45	2022-05-16	Rapportskriving
05:00	10:00	15:00	2022-05-18	Rapportskriving
08:45	13:00	21:45	2022-05-19	Rapportskriving
02:00	09:00	11:00	2022-05-20	Finpussing
00:30	11:00	11:30	2022-05-20	Innlevering

Table 5: Work log for Gaute.

F Meetings - agenda and minutes

1 2022-01-17 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-01-17 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Tor Martin Slåen Skaar, Stian Borgvin Dørre.
2	Språk for rapporten	Oppdragsgiver stilte ingen krav for hverken norsk eller engelsk, derfor ble det bestemt at rapporten skrives på norsk
3	HTTPS	Bekreftet med oppdragsgiver at TLS 1.2 var akseptabel for oppgaven framover.
4	Konfidensialavtale	Med tanke på at vi kommer til å jobbe med sikkerhetsansvarlige hos Telenor har vi i samtykke med oppdragsgiver bestemt oss for å signere konfidensialavtale. Kontrakten vil bli signert og klar til å videresendes til oppdragsgiver neste møte mandag 24.01.2022. Det samme vil bli gjort for arbeidskontrakt med arbeidsplan, rutiner og regler, en senere dato.
5	Utstyr	Kontaktinformasjon og adresse til mottakerperson fra fakultetet vil være klar til neste møte mandag 24.01.2022.
6	Vurderingspunkter	Vurderingspunkter er løst definert i den detaljerte oppgaven i form av ≪tasks≫ eller oppgaver og ≪user cases≫. Dette kan bli videre diskutert og er åpen for ønsker fra både oppdragsgiver og fakultet med tanke på vektlegging og direksjon av oppgaven.
7	Tips nr. 1	Lurt å se etter løsninger som tillater at software bli kjørt fra en ≪remote≫ maskin for å konfigurere industrisonens utstyr.
8	Tips nr. 2	Finne løsninger/om det er mulig slik at ≪service≫ klienter kan koble seg til ≪industrial demilitarized zone(IDMZ)≫ uten å traversere gjennom internett.
9	Tips nr. 3	Studere internasjonale og lokale sikkerhetsstandarder for industri IEC62443, NIST 800-82, og ≪Kraftberedskapsforskriften≫.
10	Tips nr. 4	Lage templates for hver ≪User story≫ som er definert i oppgaven. Spesifiser dersom det er mulig, hvorfor/hvorfor ikke, eventuelt forslag til å forbedre systemet slik at slike problemer ikke oppstår.
11	Firewall	Firewall er nevnt i oppgaven, men er ikke et krav for at vi skal konfigurere dette i oppgaven, siden vi ikke er velkjent med standarder som ≪Firepower≫ og dette kommer til å ta betraktelig med tid for å undersøke.
12	Tips nr.5	Viktig stikkord/rettninger for researchfasen: Defendable architecture", horisontal spredning og logging, vurdere arkitekturen for mulighet for å åpne opp og inkludere flere end pointstil remote access".

2 2022-01-18 - Statusmøte med veileder

Referat

Referat for Møte med rådgiver 2022-01-18 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Spørsmål om utsyr	Erjon ba oss om å henvenne oss til Erik(instututtansvarlig) om adresse/kontaktperson for å motta utstyret. En epost vil bli sendt angående dette fortløpende.
3	Oppdatert oppgave	Erjon fikk muligheten til å raskt gjennomgå den oppdaterte oppgaven fra Telenor og deretter var beskymret over arbeidsmengden. Erjon ønsker også at vi kan definere mål og problemstilling med hensyn til den oppdaterte oppgaven. Vi bør også si fra når vi laster opp dokumenter så Erjon vet det.
4	Teamroller	Erjon mente det ikke var nødvendig å definere roller for alle medlemmer i gruppa. Derfor fortsetter vi med bare ≪teamleder≫ og referent framover.
5	Status	Vi oppdaterte Erjon over progresjonen vår, med tanke på prosjektplan, arbeidsavtale og konfidensavtale.
6	Neste møte	Vi har etablert faste møter med Veileder Erjon hver Tirsdag kl 14:00 til 14:30. Til neste møte ønsker Erjon at vi fyller ut problemstilling og målsettings delen av prosjektplan og oppdaterer han på møteinnholdet fra møtet med oppdragsgiver samme uken.
7	Godkjenne referat	Godkjent av: Bjørn-Tore, Gaute
8	Møtet hevet	Møte hevet klokken: 14:18 av Gaute Saastad Nogva.

Møteleder: Gaute Saastad Nogva

Referent: Chi Hou Fung

3 2022-01-24 - Statusmøte med oppdragsgiver

NTNU

Agenda

Statusmøte med oppdragsgiver 2022-01-24 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Arbeidsplan	Presentasjon og diskusjon rundt foreløpig arbeidsplan.
3	Problemstilling	Bestemme prioritert liste av problemstillingsforslagene til teamet.
4	Prosjektmål	Har oppdragsgiver noen ønsker om resultatmål i tillegg til om Cisco SEA kan løse ≪User story≫ 1-4.
5	Avtaler	Status til samarbeidsavtalen og konfidensialitetsavtalen.
6	Nettverksutstyr	Oppdatering angående nettverksutstyret NTNU kunne låne til prosjektet. F.eks. om adresse og kontaktinformasjon til mottager av pakken er godkjent.
7	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
8	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

Referat

Referat for Møte med oppdragsgiver 2022-01-24 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Tor Martin Slåen Skaar, Stian Borgvin Dørre.
2	Arbeidsplan	Presentasjon av aktivitetsliste med beskrivelse og tidslinje av planlagte aktiviteter, sammen med gantt skjema for grafisk representasjon.
3	Problemstilling	Etterspurte innsikt til å formulere generell problemstilling. Foreslo ≪Hvilke begrensinger og utfordringer har Cisco SEA i industrielle OT-miljø?≫. Oppdragsgiver viste beskymring over mangel på kontekst eller relasjoner til oppgaven. Påpekte at det var usikkert om problemstillingen hadde noe å gjøre med sikkerhet. Oppdragsgiver foreslo å begresne problemstilling til hvilke industri Cisco SEA tilegner seg til og å nevne sikkerhetsstandardene som IEC62443 eller NIST 800-82 i problemstillingen.
4	Prosjektmål	Etterspurte innsikt til prosjektmål vi burde være ute etter, utenom de som er formulert i brukerscenarioet i oppgaven. Oppdragsgiver foreslo metoder for å løse ≪user cases≫ utenom Cisco SEA som alternative resultatmål.
5	Avtaler	Begge avtaler er underskrevet og unnagjort.
6	Nettverkutstyr	Oppdragsgiver må teste utstyret om de er klare til bruk og deretter er de klare til å sende utstyret.
7	Intro om Cisco SEA	Introduksjonsforelesing av Cisco SEA neste uke. Vi må sørge for at de har e-postadressene våre slik at vi får tilgang til nødvendige Cisco tjenester.
8	Til neste møte	Husk å sende møteagenda til møte i god tid slik at oppdragsgivere kan tenke/formulere svar.
9	Møtet hevet	Møte hevet klokken: 14:20 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

4 2022-01-25 - Statusmøte med veileder

Referat

Referat for Møte med rådgiver 2022-01-25 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Plan og gantt skjema	presenterte gantt skjema og prosjektplan.
3	Problemstilling	Formulere om problemstilling til forskningspørsmål, det vil si å formulere spørsmålet med et forord, for eksempel at ≪vi tenker å svaret på spørsmålet vi stiller≫.
4	Mål	Rådgiver foreslo at vi definerte klare hovedmål som er kjernen av oppgaven og mindre resultatmål som alternativer. Hen sa også at vi kunne se på effektmål i tillegg til resultatmål for prosjektplanen.
5	Innleveringer	For å lever prosjektavtale på blackboard må vi henvende oss til institutansvarlig for å gi oss tilgang. I tillegg avtalte vi å sende inn første skisse av prosjektplanen til Erjon for kvalitetsikring.
6	Utstyret	Rådgiver foreslo at vi skrev en introduksjon til den industrielle ruteren vi kommer til å bruke i løpet av prosjektet i prosjektplanen.
7	Møtet hevet	Møte hevet klokken: 14:27 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

5 2022-01-31 - Statusmøte med oppdragsgiver

NTNU

Agenda

Statusmøte med oppdragsgiver 2022-01-31 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Prosjektplan	Kort gjennomgang av prosjektplanen vi har levert til veileder.
3	Arbeidslogg	Kort om hva vi har arbeidet med siden forrige møte.
4	Ukentlig plan	Planlagt arbeid for den neste uken.
5	Fremtidige agendaer	Bestemme frist for når agendaer skal sendes ut.
6	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
7	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

Referat

Referat for Møte med oppdragsgiver 2022-01-31 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Tor Martin Slåen Skaar.
2	Gjennomgang av prosjektplan	Prosjektleder gikk gjennom prosjektplanen med oppdragsgiver. Forklarte tankeganger og avklarte spørsmål som dukket opp, forklarte hva vi mente med tjenestetest,
3	Cisco SEA mangler	Cisco SEA er et relativt nytt tjeneste og flere nyttige funksjoner er enda i utviklingsfasen. Oppdragsgiver anbefalte oss å se på PAM (privileged access management) løsninger, CyberArk og Thycotic som referanser til funksjoner som mangler i Cisco SEA.
4	Tips til oppsett av Ruter	Remote session til svitsj, to aksessporter til IoT dashboard, vlan 1 til internett, benytt første ethernet port.
5	Til neste møtet	Sette opp utstyret, konfigurere IR1101 ruteren i Cisco labben og forsøke å simulere «dummy systemet». Agenda skal sendes til oppdragsgiver senest fredag før lunsjtid. Uformell plan for omvisning hos Cisco/Telenor i Oslo rundt overgangen fra mars til april.
6	Møtet hevet	Møtet hevet klokken: 14:25 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

6 2022-02-01 - Statusmøte med veileder

Agenda

Statusmøte med veileder 2022-02-01 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Arbeidslogg	Kort om hva vi har arbeidet med siden forrige møte.
3	Ukentlig plan	Planlagt arbeid for den neste uken.
4	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
5	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

Referat

Referat for Møte med rådgiver 2022-02-01 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Presentasjon av prosjektplan	Teamleder presenterte prosjektplan til veileder.
3	Feedback fra veileder	Veileder kommenterte positivt om detaljert bakgrunn av prosjektmål og bruk av kilder. Han mente det var god inndeling av effektmål og resultatmål, men manglet beskrivelse av hvordan vi har tenkt å oppnå de målene vi har satt. Han viste også beskymring over at rammene for prosjektet var mangelfull. Videre hadde han likt om vi inkluderte detaljene fra oppgaveteksten angående de fiktive selskapene og spesifikke formål med oppgaven. Til slutt kommenterte han at dersom vi inkluderer tabeller er vi nødt til å beskrive de i et kort avsnitt.
4	Plan for uken	Veilder ville vite hva vi hadde planlagt å gjøre for resten av uken. Vi svarte med at vi har nettopp mottatt utstyret knyttet til prosjektet og vi hadde tenkt å dedikere resten av uken til å bli kjent med utstyret og validere at de funker som de skall på cisco-labben.
5	Til neste møtet	Til neste møtet så skal veileder lese grundig gjennom prosjektplanen og gi oss endelig svar om den er godkjent eller ikke. Etter innledende lesning så såg det akseptabel ut, og han mente det var greit for oss å starte med prosjektarbeidet.
6	Møtet hevet	Møtet hevet klokken: 14:35 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

7 2022-02-07 - Statusmøte med oppdragsgiver

Agenda

Statusmøte med oppdragsgiver 2022-02-07 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Arbeidslogg	Kort om hva vi har arbeidet med siden forrige møte.
3	Ukentlig plan	Planlagt arbeid for den neste uken.
4	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
5	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

Referat

Referat for Møte med oppdragsgiver 2022-02-07 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Stian-Borgvin Dorre.
2	Gjennomgang av det vi har gjort	Prosjektleder hadde en liten gjennomgang av det vi hadde gjort. Han gikk gjennom status for oppsett av utstyret med tanke på, plassering, internett tilgang, merkelapper med kontaktinfo/tilhørelse, grunnleggende konfigurasjon og varsel til labbansvarlig. I tilegg har vi oppdatert firmware til IR1101 ruteren, slik at den er støttet av ≪Cisco IoT dashboard≫ og dens medfølgende tjenester. Verken prosjektplan eller kontrakt er formelt godkjent, men veileder har raskt gjennomgått deler av prosjektplanen og gitt oss tommel opp til å fortsette med oppgaven. Kontrakten mangler fortsatt signatur fra oppdragsgiver og veileder.
3	Ubesvarte spørsmål	Tilgang til ≪Cisco Community guides≫ er noe vi trenger til å feilsøke configurasjon av IR1101 ruteren og ≪Cisco IoT Dashboard≫. I tillegg mangler vi nødvendig dokumentasjon til API bruk av ≪Cisco IoT Dashboard≫ og ≪Plug and play(PnP)/Smart-call home≫ funksjonalitet til ruteren.
4	Oppdragsgiver erfaringer	Oppdragsgiver delte noen innsiktsfulle erfaringer med bruk av den industrielle svitsjen IE4000. Han hadde brukt denne svitjen til oppsett av DNA senter, segmentering og Cybervision overvåkning av OT utstyr i anlegg, ubemannet drift av bensinstasjoner og overvåkning av kjøring og vifte i tunell. I eksemplet med tunnellen påpekte han at det måtte til 500 IR4000 svitsjer for å tilfredstille driften.
5	Møtet hevet	Møtet hevet klokken: 14:20 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

8 2022-02-08 - Statusmøte med veileder

NTNU

Agenda

Statusmøte med veileder 2022-02-08 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Arbeidslogg	Kort om hva vi har arbeidet med siden forrige møte.
3	Prosjektplan	Status til godkjenning av prosjektplanen og eventuelle mangler.
4	Ukentlig plan	Planlagt arbeid for den neste uken.
5	Fremtidig møteplattform	Bestemme om vi hovedsaklig skal møtes fysisk fremover.
6	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
7	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder: Gaute Saastad Nogva

Referent: Chi Hou Fung

Referat

Referat for Møte med veileder 2022-02-010 Kl: 11:00

Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Arbeidslogg	Teamleder presenterte hva vi hadde gjort så langt. Blant annet, å sette opp IR1101 ruteren i Ciscolabben, feilsøke tilkoblingsproblemer og sertifikater som ikke samsvarer med utstyr og tjeneste.
3	Prosjektplanstatus	Teamleder etterspurte formell status av prosjektplanen og veileder ga oss en formell muntlig godkjenning.
4	Fremtidige møter	Teamleder foreslo at vi holder fremtidige statusmøter fysisk, med tanke på at smittevern som meterregelen er løftet og at vi alle er tilstede i Gjøvik campus. Det vil også være større mulighet for bruk at grupperom i det nye bygget.
5	Forsover seg	Et av medlemmene i teamet har forsovet seg de to siste møtene og vi har i plenum snakket om dette og etter sitt beste innsats, sørger han for at det ikke skjer igjen. I tillegg er det bare disse to møtene hvor han har forsovet seg og han har vist god innsats både i arbeidsprosessen og engasjement.
6	Annet	Veileder henvendte oss om vi var i stand til å følge den planlagte timeplanen vi hadde satt opp. Feilsøking av tilkobling til skytjenesten har tatt lengre tid enn forventet, men vi burde klare å nå fristene vi har satt. I tillegg ville veileder at vi diskuterer målene og forventingene vi har skrevet om i prosjektplanen med oppdragsgiver.
7	Møtet hevet	Møtet hevet klokken: 11:20 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

9 2022-02-14 - Statusmøte med oppdragsgiver

NTNU

Agenda

Statusmøte med oppdragsgiver 2022-02-14 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beskrivelse
1	Start møtet	Velkommen, deltagere noteres.
2	Prosjektplan	Status og informasjon om prosjektplanen.
3	Arbeidslogg	Kort om hva vi har arbeidet med siden forrige møte.
4	Ukentlig plan	Planlagt arbeid for den neste uken.
5	Andre saker	Her er det åpent for å komme med saker som ikke var på agendaen.
6	Møtet hevet	Klokkeslett noteres i referatet.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

Referat

Referat for Møte med oppdragsgiver 2022-02-14 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Tor-Martin Slåen Skaar, Stian-Borgvin Dorre.
2	Det vi har gjort	Oppsett av IR1101 i Cisco datalabben på campus. Dette tok lengere tid enn forventet på grunn av en lokal PnP server som er satt opp i datalabben som blir prioritert når ruteren først starter og forsøker å få kontakt med skytjenesten. Dette ble løst av å koble ruteren til privat mobildata ved første oppstart og oppsett. I tillegg skjedde det en uoverstemmelse av CA sertifikat hos PnP kontrollerprofilen som stoppet oss fra å etablere kontakt med skytjenesten. Etter vellykket oppsett av ruteren, så testet vi funksjonaliteten til Cisco SEA løsningen, blant annet, protokoller for RDP, SSH, VNC, http og diverse GUI løsninger for adgangskontroll av flere bruker/grupper.
3	Plan til neste uke	Planen til neste uke er å teste brukerfortellingene eller scenariet fra oppgavebeskrivelsen. Oppdragsgiver påpekte noen punkter vi måtte ta hensyn til når vi starter utprøvingen: 1. Ta utgangspunkt i stordriftsmiljø, snakk om en administrator som må gi tilgang til opptil 1000 brukere, som kommer og går. 2. Identity and Access Management (IAM) platform som kan overordnet pushe brukerrettigheter til SEA/IoT Dashboard. (hiarki: IAM - Active Directory(AD)/eller lignende mappeløsning - IoT Dashboard) 3. Mangler når det gjelder design, brukervennlighet og skalarbarhet til store driftsmiljø. 4. Les nøye på kundekravene som er skrevet i oppgavebeskrivelsen. 5. At vi forbereder evalueringsskjema før vi starter med utprøving av brukerfortellingene.
4	Erfaringer fra oppdragsgiver	Oppdragsgiver delte noen erfaringer angående sikkerheten til dhcp og ipv6. Ipv6 i starten av sin livstid var det mange tilfeller hvor «hackere» brukte datamaskiner eller svitsjer til å annonsere seg som en ruter med hjelp av ipv6 prioriteringen over ipv4. Dette førte til at svitsjen tar over rollen som «default gateway» og all trafikk rutes til den. En lignende smutthull finnes på DHCP siden maskinen som svarer DHCP serveren blir automatisk «mester» av nettverket. Oppdragsgiver delte også erfaringen deres med å jobbe med kinesiske nettverksutstyr-leverandører som ZTE og Huawei. Hvor det fantes lite eller ingen relevant dokumentasjon av utstyret på nett, noe som vi gradvis opplever med Cisco SEA tjenesten.
5	Møtet hevet	Møtet hevet klokken: 14:28 av Tor Martin Slåen Skaar.

10 2022-02-21 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-02-21 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn Tore Semb, Chi Hou Fung, Tor-Martin Slåen Skaar, Stian-Borgvin Dorre.
2	Vlan	Teamleder snakket litt om planer om vlan oppdeling for å simulere ≪User cases≫ som er beskrevet i oppgaven.
3	Lite produktiv forrige uke	Forrige uke var det første oppstart av faget ≪IØ2000 - Hvordan bli en endringsagent? Innovasjon og entreprenørskap i praksis≫ som tok betraktelig med tid av arbeidsuka. I tillegg var teamlederen vår i ferd med å komme seg etter en forkjølelse. Han ble heldigvis testet negativ for covid-19.
4	Hva vi skal gjøre denne uken	I denne uken skal vi starte med ≪User case 1≫ som er å teste om en vedlikeholdstekniker klarer å få IP-tilgang til industrielle utstyret og kjøre programvare fra sin lokale maskin til målsystemet. Under testingen skal vi notere hvert steg i prosessen og komme med løsninger dersom det ikke er mulig eller ikke oppfyller brukerkravene beskrevet i oppgaven.
5	Møtet hevet	Møtet hevet klokken: 14:23 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

11 2022-02-22 - Statusmøte med veileder

Referat

Referat for Møte med rådgiver 2022-02-23 Kl: 10:30
Sted: rom A132, A-bygget.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Status på progresjon	Progresjon var tregt forrige uke på grunn av første oppstart av faget ≪IØ2000 - hvordan bli endringsagent?≫. Vi har så vidt begynt på å dokumentere detaljene til første ≪User case≫ som handler om at en ekstern eller intern teknikker vil kjøre spesialisert programvare fra sin maskin til fjernstyrt utstyr i industrisonen.
3	Diskusjon om hovedrapporten	Veileder anbefalte å inkludere så mye detaljer som mulig i hovedrapporten. Med tanke på hvordan feilsøkingen gikk da vi skulle sette opp utstyrsmiljøet/simulering av oppgaveteksten. I tillegg påpekte han at det er viktig å inkludere omfattende bakgrunn og detaljer om bruker av systemet, platform som han/hun bruker, versjonkontroll av programvare og operativsystem som blir brukt og et overordnet scenario av ≪user case≫.
4	Plan for språkbruk til hovedrapport	Sammen med veileder har vi bestemt oss for å endre språket av hovedrapport fra norsk til engelsk. Dette er på grunn av at de fleste relevante dokumentasjon/≪whitepaper≫ av tema vi skriver om er på engelsk og det er problematisk å oversette noen tekniske begrep over til norsk. I tilleg er norsk ikke morsmålet til veilederen vår, og det er mer komfortabelt for han å vurdere rapporten på engelsk i forhold til norsk.
5	Plan for neste uke	Plan for neste uke er å fullføre relevant testing av første ≪use case≫ og være godt i gang med dokumentasjon av scenario, notasjon under prøvetiden og eventuelt forslag til forbedring/andre muligheter dersom ≪user case≫ ikke er aktuelt.
6	Møtet hevet	Møte hevet klokken: 11:02 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

12 2022-02-28 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-02-28 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn Tore semb, Chi Hou Fung, Gaute Saastad Nogva, Tor-Martin Slåen Skaar, Stian-Borgvin Dorre.
2	User case 1	Fra forrige arbeidsuke så har vi konkludert at ≪user case 1≫ ikke er verken plausibel eller aktuell på Cisco SEA per dags dato. Vi har tenkt å komme tilbake til alternative løsninger for dette problemet når vi har gått gjennom alle user casene.
3	Router on a stick	Vi klarte ikke å dele opp gigabitethernet porten i subnet for å configurere router on a stick. Oppdragsgiver foreslo å først sjekke om det mangler lisenser som aktivererer funksjonaliteten, siden slike hendelser kan skje uten feilmelding.
4	Omvisningstur	Omvsining av Cisco Norge kontoret og potensielt Microsoft Norge kontoret er planlagt 1. april.
5	Møtet hevet	Møtet hevet klokken: 14:20 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

13 2022-03-07 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-03-7 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn Tore semb, Chi Hou Fung, Gaute Saastad Nogva, Tor-Martin Slåen Skaar.
2	User case 2	User case 2 er blitt ferditestet med hjelp av en ≪Raspberry pi≫ som fyller rollen som en ≪jump host≫ i IDMZ, som går videre til den industrielle sonen.
3	Plan til neste uke	User case 3 er alerede blitt testet fra da vi satte opp Cisco SEA og mangler bare noe dokumentasjon. Derfor starter vi med testing/utforskning av løsningene knyttet til user case 4 denne uken.
4	Oppgavepresentasjon	Vi har fått vite av institusjonen at oppgavepresentasjon vil foregå fysisk mellom 7-9 juni. Dette ble informert til oppdragsgiver dersom de var interessert i å delta.
5	Møtet hevet	Møtet hevet klokken: 14:16 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

14 2022-03-14 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-03-14 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn Tore semb, Chi Hou Fung, Gaute Saastad Nogva, Stian Borgvin Dørre
2	User case 4	User case 4 handler om å generere en ukentlig rapport via epost til soneansvarlig. Innholdet til denne rapporten finnes allerede i Cisco IoT dashboard under «audit» i profilmenyen, men vi har ikke funnet dokumentasjon som beskriver api som henter denne informasjonen. Tilgang til den nevnte api er svært hensiktsmessig for å automatisere en prosess som sender en epost til soneansvarlig om SEA bruk hver uke.
3	Mulige ting vi har utelatt	Fra developer.cisco.com har vi funnet noe api dokumentasjon fra industrial asset vision funksjonen, men det har vi ikke tilgang til og kan være urelevant for vår use case. I tillegg kan det hende at api tilgang krever lisenser vi ikke har tilgang til.
4	annet	Oppdragsgiver svarte på spørsmål angående DNA senter og trender med tanke på GUI bruk over «command line interface (CLI)». Vi ble også introdusert til Cisco Meraki som er et GUI alternativ med «easy to use» alternativer til CLI commando.
5	Møtet hevet	Møtet hevet klokken: 14:28 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

15 2022-03-22 - Statusmøte med veileder

Referat

Referat for Møte med veilder 2022-03-22 Kl: 14:00
Sted: rom T540, Topas.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	User case 4	Teamleader showed the gist of how we solved user case 4 using an API call example provided by the representative from Cisco Norway. We also explained the functions and set up of our system under consideration(SUC).
3	API security	Supervisor showed concern regarding the availability and usage of system API in our solution. He also provided improvements to our system for instance the ability to choose from a list of vetted email addresses in the script, instead of just any email.
4	Final rapport draft	Supervisor reviewed our current rapport structure and pointed out these considerations/improvment for when we start writing: • where should tables be, in appendix or under relevant chapters • pointed out a few missing or redundant sub-chapters • include describing paragraphs at the beginning of each chapter • agreed that abbreviations should be included at the beginning of the rapport instead of in appendix
5	Frequency of weekly meetings	Because we are going from testing phase to rapport writing, we agreed to reduce the frequency of meetings.
6	Final presentation	Supervisor was not certain that the final presentations would we live streamed, but was pretty confidant it would.
7	Møtet hevet	Møte hevet klokken: 14:40 av Gaute Saastad Nogva.

Møteleder: Gaute Saastad Nogva

Referent: Chi Hou Fung

16 2022-03-28 - Statusmøte med oppdragsgiver

Referat

Referat for Møte med oppdragsgiver 2022-03-28 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Stian Borgvin Dørre, Tor Martin Slåen Skaar
2	Behov for ukentlig møter	Gruppa har gått videre fra testing til rapportskriving og oppdragsgiver har meget trange timerplaner. Derfor har vi bestemt oss for å redusere mengden med statusmøter videre.
3	Usercase 4	Diskuterte detaljene angående user case 4 og scriptespråk generelt.
4	Tog bilett	Avklarte nøyaktig tidspunkt for tog biletter og oppdragsgiver bestilte de under møtet. I tillegg avklarte oppdragsgiver foreløpig plan for omvisningsdagen
5	Presentasjonsdag	Vi har enda ikke nøyaktig dato for presentasjonsdagen, men veilederen vår har var ganske sikker på at det kommer til å bli direkte sending av presentasjonen.
6	Møtet hevet	Møtet hevet klokken: 14:22 av Tor Martin Slåen Skaar.

Møteleder:	Tor Martin Slåen Skaar
Referent:	Chi Hou Fung

17 2022-04-19 - Statusmøte med veileder

Referat

Referat for Møte med veilder 2022-04-19 Kl: 14:00
Sted: Microsoft Teams.

Sak	Tittel	Beslutning
1	Start møtet	Tilstede: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Presentation date	The specific date is currently not decided, we will be contacting the professer responsible for our course to figure out the presentation order. We will also be asking about the specifics with streaming the presentation because some of our associates working in Cisco and Telenor were interested in watching.
3	Rough draft	The rough draft will be sent to our supervisor early tommorrow morning and we will be expecting feedback on that by the end of the month.
4	Confidentiality	We have signed a confidentiality contract, but so far, there are no sensitive information included in our rapport.'
5	Møtet hevet	Møte hevet klokken: 14:10 av Gaute Saastad Nogva.

Møteleder:	Gaute Saastad Nogva
Referent:	Chi Hou Fung

18 2022-05-10 - Statusmøte med veileder

Minutes of meeting

Minutes for Meeting with supervisor 2022-05-10 Kl: 13:10
Place: Topas T541.

Case	Title	Notes
1	Meeting start	Present: Bjørn-Tore Semb, Chi Hou Fung, Gaute Saastad Nogva, Erjon Zoto.
2	Splitting tasks	Erjon suggested that we split tasks so that we can write more efficiently considering there is not much time left and still a considerable amount of work left.
3	Sources	Considerable amount of sources missing in the project. Particularly of purdue model and IEC standard.
4	Paragraphs	There are a lot of short paragraphs that need elaboration and in-depth explanations.
5	Target group	Be specific with what the target group is, there is mentioning of telenor, owners and operators of OT and also any person working with IT. Supervisor also wanted us to preferably expand our target group to include as many people as possible.
6	Different paths	Supervisor suggested that we either elaborate in conclusion or add a discussion section talking about differnt ways to solve use cases, or about things we tried but ultimately abandoned during the testing period.
7	Delimitation	Elaborate or merge delimination with project boundary.
8	Shuffle items in the project	Description of tools and software used should be moved to method or a new section all together. Parts of use cases belong in appendix. Some points from analysis should be moved to discussion.
9	Images and steps	We should include more images that describes steps to performing certain tasks. We are supposed to make templates for completing each use case.
10	Final draft	Final draft to supervisor will be handed inn on monday morning next week sixteenth of may.
11	Feedback from client	Supervisor asked about feedback from client. We only showed them solutions of use cases and they have not yet read our rapport draft.
12	Meeting end	Meeting ended: 14:15 av Gaute Saastad Nogva.

Leader:	Gaute Saastad Nogva
Note taker:	Chi Hou Fung