Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Peder Grundvold
Jon Breivik Smebye

Remote Access Security Recommendations for Norwegian Petroleum Companies

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lars Bodsberg & Roy Thomas Selbæk Myhre
June 2021

NTNU
Kunnskap for en bedre verden

Peder Grundvold
Jon Breivik Smebye

Remote Access Security Recommendations for Norwegian Petroleum Companies

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lars Bodsberg & Roy Thomas Selbæk Myhre
June 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Title:	Remote Access Security Recommendations for Norwegian Petroleum Companies
Students:	Peder Grundvold Jon Breivik Smebye

Problem description:

The use of remote access (RA) solutions in industrial systems is becoming increasingly common. With the current COVID-19 pandemic, this trend has become even more apparent. While there are numerous benefits with the increased use of RA, it is also exposing industrial operational technology (OT) systems to a wide array of new cyber threats, as demonstrated by several recent attacks.

This trend is apparent in the Norwegian petroleum industry, particularly on offshore installations. By using RA, OT engineers are no longer required to be physically present on a platform to operate industrial processes. However, many companies experience difficulties in securely protecting and managing these RA solutions. Furthermore, existing frameworks are often hard to implement in practice, and are becoming outdated due to the rapid pace of technological advancements in today's changing cyber landscape.

This thesis will investigate current and emerging RA technologies in both the petroleum industry and other sectors and from that suggest improvements to current systems. The project's overall goal is to help the petroleum industry to securing its future RA solutions.

Date approved:	Feb 11, 2021
Responsible professor:	Maria Bartnes, IIK and SINTEF
Supervisors:	Lars Bodsberg, SINTEF Roy Thomas Selbæk Myhre, Sopra Steria

Abstract

Industrial Control Systems (ICS) that manage offshore petroleum installations have undergone a major shift and now increasingly depend on remote access solutions (RAS). Although such solutions have many advantages, the increased connectivity also exposes critical ICS to a new type of threat, i.e., cyberattacks. While many reports and standards outline security best practices for the industry, they tend to be either old or too vague in their actual recommendations. Furthermore, as these are *current* best practices, they only recommend proven solutions without considering recent research and the latest advances in the field. Thus, this thesis will explore how innovative solutions and emerging technologies can be used to develop new remote access security recommendations for Norwegian petroleum companies.

A literature review was conducted to identify present and emerging remote access solutions and technology. Based on workshops with two Norwegian petroleum companies, their current RAS were analyzed to determine their functional requirements, as well as potential threats to the systems. The workshops provided insights into two main focus areas regarding existing solutions, i.e. file transfer and general access management. Finally, a SWOT analysis was performed to evaluate potential new solutions in light of the three selected criteria: security, user-friendliness, and cost-effectiveness. The list of analyzed technologies included the following: VPN, Zero Trust, Next-Generation Firewall, OT-specific Firewall, Dedicated Desktop, Sheep Dipping, Sandboxing, and Unidirectional Gateway.

This analysis suggested several improvements that could be made to the current RAS used by Norwegian petroleum companies. The results offered five recommendations, ranging from small and basic changes to complex architectural transformations. In brief, it is recommended that Norwegian petroleum companies take steps towards implementing a Zero Trust architectural security model and utilize both Next-Generation and OT-specific firewalls. They should also implement a sandboxing solution in order to better secure file transfers to critical systems and utilize Unidirectional Gateways for all read-only access requirements. An analysis of these recommendations demonstrates largely positive effects when evaluated with regards to security, user-friendliness, and cost-effectiveness.

Sammendrag

De industrielle kontrollsystemene som opererer offshore petroleumsinstallasjoner har gjennomgått et stort skifte og er nå i økende grad styrt av fjerntilgangsløsninger. Dette gir åpenbart mange fordeler, men økt integrering gjør samtidig kritiske kontrollsystemer, som tidligere var beskyttet av deres naturlige isolasjon, svært sårbare for cyberangrep. Flere rapporter og standarder beskriver sikkerhetspraksis for industrielle systemer. Disse har imidlertid en tendens til å være enten utdaterte eller for vage i sine faktiske anbefalinger. I tillegg, ettersom dette er dagens beste praksis, anbefaler de også bare velprøvde løsninger uten å ta i betraktning nyere forskning eller de siste fremskrittene i feltet. Denne oppgaven vil derfor undersøke hvordan innovative løsninger og ny teknologi kan brukes til å utvikle et sett med nye sikkerhetsanbefalinger for fjerntilgangsløsninger til norske petroleumsselskaper.

Først ble en litteraturstudie gjennomført for å identifisere nåværende og ny teknologi brukt i fjerntilgangsløsninger. Ved hjelp av workshops med to relevante norske petroleumsselskaper analyserte vi deres nåværende fjerntilgangsløsninger for å bestemme funksjonelle krav samt for å finne mulige trusler mot systemene. Dette ga også innsikt for å definere to fokusområder i den eksisterende løsningen, nemlig filoverføring og generell tilgangshåndtering. Til slutt utførte vi en SWOT-analyse for å evaluere forskjellige løsninger med bakgrunn i de valgte kriteriene; sikkerhet, brukervennlighet og kostnadseffektivitet. Den samlede listen over analyserte teknologier er: VPN, Zero Trust, Next-generation brannmur, OT-spesifikk brannmur, dedikert datamaskin, Sheep Dipping, Sandboxing, og Unidirectional Gateway.

Analysen identifiserte flere aspekter som kan forbedre fjerntilgangsløsningene norske petroleumsselskaper bruker i dag. Dette resulterte i fem anbefalinger; fra små og enkle endringer til komplekse arkitekturelle transformasjoner. Kort oppsummert anbefales norske petroleumsselskaper å bevege seg mot en Zero Trust arkitektur, samt bruke både Next generation- og OT-spesifikke brannmurer. De bør også implementere Sandboxing for å bedre sikre filoverføringer til kritiske systemer og bruke Unidirectional Gateways for å overholde alle read-only tilgangskrav. Analysen viser at disse anbefalingene gir tydelige positive effekter når de vurderes mot kriteriene sikkerhet, brukervennlighet og kostnadseffektivitet.

Preface

This thesis is the final delivery of a Master of Science in Communication Technology and Digital Security at the Norwegian University of Science and Technology (NTNU). The research was mainly conducted between January and June 2021 and built upon a pre-project held the previous autumn.

Firstly, a big thanks must be given to our responsible professor Maria Bartnes and our supervisors Lars Bodsberg and Roy Thomas Selbæk Myhre, for their guidance that has been vital for the outcome of this research. Further, we would sincerely like to thank company Alpha and Beta for their participation and time spent giving us insight and helpful feedback throughout this thesis. Finally, we would like to thank everyone who gave advice on the *SANS ICS forum*.

Peder Grundvold
Jon Breivik Smebye
Trondheim, June 2021

Contents

List of Figures

List of Tables

List of Acronyms

ABAC Attribute-Based Access Control.

AC Access control.

ACSM Access Control Security Manager.

AD Anomaly-based Detection.

AM Access management.

AO Asset Owners.

APT Advanced Persistent Threats.

BYOD Bring Your Own Device.

CC command-and-control.

COTS Commercial off-the-shelf.

CPI Comprehensive Packet Inspection.

CPNI Centre for the Protection Of National Infrastructure.

CRS Cyber Requirements Specification.

CrySyS Lab Laboratory of Cryptography and System Security.

CSA Cloud Security Alliance.

DCS Distributed Control Systems.

DMZ Demilitarized Zone.

DPI Deep Packet Inspectio.

E-ISAC Electricity Information Sharing and Analysis Center.

FEED Front-End Engineering Design.

FTP File Transfer Protocols.

GRE Generic Routing Encapsulation.

HAZOP Hazard and Operability Analysis.

HMI Human Machine Interfaces.

HTTP Hypertext Transfer Protocol.

IACS Industrial Automation and Control Systems.

IADS Intrusion and Anomaly Detection System.

IAM Identity and Access Management.

IAT Inter-Arrival-Time.

ICMP Internet Control Message Protocol.

ICS Industrial Control Systems.

IDMZ Industrial demilitarized zone.

IDS intrusion detection systems.

IEC International Electrotechnical Commission.

IFT Intelligent Filtering Technique.

IIoT Industrial Internet of Things.

IKEv2 Internet Key Exchange version 2.

IPS intrusion prevention systems.

IPsec Internet Protocol Security.

ISBR Information Security Baseline Requirements.

ISE Identity Services Engine.

IT Information Technology.

L2TP Layer 2 Tunneling Protocol.

LAN Local Area Network.

MAC media access control.

MS Maintenance Service Provider.

NAC Network Access Control.

NAP Network Access Protection.

NGFW Next-generation firewalls.

NIST National Institute of Standards and Technology.

NOG Norwegian Oil and Gas Association.

OrBAC Organizational-Based Access Control.

OSDA Out-of-Sequence Detection Algorithm.

OSI Open Systems Interconnection.

OT Operational Technology.

OTP one-time passwords.

PAACS Privileged Account Access Control System.

PCSS Process Control, Safety, and Support.

PERA Purdue Enterprise Reference Architecture.

PIPEA Proprietary IndustrialExtension Algorithm.

PLC Programmable Logic Controllers.

PPTP Point-to-Point Tunneling Protocol.

PS Product Supplier.

QoS Quality of service.

RA Remote Access.

RAdAC risk adaptive access control.

RAS Remote Access Solutions.

RAT Remote Access Trojan.

RBAC Role-Based Access Control.

RDP Remote Desktop Protocol.

RiskBAC Risk-Based Access Control.

RTU Remote Terminal Unit.

SCADA Supervisory Control and Data Acquisition.

SCP Secure Copy.

SD Signature-based Detection.

SDP Software-Defined Perimeter.

SFTP Secure File Transfer Protocols.

SIL Safety Integrity Level.

SIS Safety Instrumented Systems.

SL-T Security Level Target.

SMTP Simple Mail Transfer Protocol.

SP Special Publication.

SRAM Secure Remote Access Method.

SSTP Secure Socket Tunneling Protocol.

SuC System under Consideration.

TCP Transmission Control Protocol.

TFTP Trivial File Transfer Protocol.

TNC Trusted Network Connect.

UDP User Datagram Protoco.

UM User Management.

VPN virtual private network.

WAN Wide Area Network.

WP Work Permits.

ZTA Zero Trust Architecture.

ZTN Zero Trust Network.

ZTNA Zero Trust Network Access.

Chapter 1
Introduction

1.1 Motivation

The use of remote access solutions for industrial systems is becoming increasingly common. This development is part of a broader trend known as the *Fourth Industrial Revolution*, or Industry 4.0, which describes the ongoing automation of traditional industries, including the introduction of the Industrial Internet of Things (IIoT). Furthermore, amid the current COVID-19 pandemic, the need for RAS has become even more apparent. However, while the increased use of remote access (RA) in ICS has many benefits, it also renders these systems more susceptible to cyberattacks, as demonstrated by several recent attacks [SFSC19, HEF]. The severity of this development was highlighted in 2020 when US-CERT published the following alert [AA20]:

> *"NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems"*

The alert points to the use of legacy operational technology (OT) assets. Unfortunately, these are not designed to defend against malicious cyber activities and new technologies, such as Shodan [Sho], which quickly identify OT assets connected via the Internet. Combine this with the extensive lists of ICS-related exploits available in online databases and we get what US-CERT calls a *"perfect storm"*.

As the number of cyberattacks on OT systems is steadily increasing, the urgent need for companies to implement improved security practices is apparent. Also, several incidents point to yet another trend: ransomware attacks that were previously limited to Information Technology (IT) systems are now being customized to target ICS and other OT networks [FWD19]. One such example is a ransomware designed for Windows industrial environments, named Ekans, that emerged in December 2019/citeEkans2020. Furthermore, as this thesis is being written, there was yet

another ransomware attack on an industrial facility. The American company Colonial Pipeline, responsible for supplying around 45% of the East Coast's fuel, had to temporarily halt its operations and ended up paying the attackers a ransom of several million dollars [Osb21]. This shows that also ICS now are targeted by cybercriminals and other malicious actors seeking financial gain. However, more dangerous actors have also been known to target ICS. These systems often manage critical infrastructure, and nation-states are believed to be responsible for several cyberattacks on high-value industrial targets. These are usually carried out without any repercussions due to anonymity and plausible deniability in the cyber domain. Examples of such attacks are the Stuxnet attack on Iranian nuclear facilities and the Ukrainian power grid attack of 2015.

In Norway, petroleum production is among the most dominant industries. The sector is vital to the Norwegian economy as it generates a steady stream of jobs and revenue. As discussed previously, this makes the petroleum industry a high-value target for potential attackers. Since offshore installations are physically isolated in the middle of open seas, accidents can be severe. For example, in 1980, 123 people perished in the infamous Alexander Kielland accident [**?**]. Another example, although outside Norwegian territory, is the Deepwater Horizon accident of 2010, which led to extreme environmental and economic damage [DAKH13]. Furthermore, as a key player in offshore technology, Norwegian industrial secrets could be valuable for criminals or other nation states. With access to large amounts of capital and systems with little acceptance for loss in availability, the industry is also the perfect target for ransomware attacks.

Traditionally, systems that control industrial processes have been completely separate from the outside world. This meant that systems such as ICS on Norwegian offshore installations were protected from cyberattacks (except those involving physical access) merely because of their isolation. To make any changes, an engineer would have to be physically present on the platform. However, the way of managing such systems is now changing. With Industry 4.0 and the transition towards increased connectivity in society at large, OT environments are becoming accessible via remote access solutions. This has several benefits: employees can work more efficiently since there is no commuting time between locations. Additionally, fewer workers need to be stationed on the actual offshore platforms, reducing operational costs and risk for human life and health.

Remote access in itself is not a new concept. The difference is that OT systems designed without security in mind due to their former isolation are now becoming accessible from remote locations. For instance, virtual private network (VPN) technology has been around since the 1990s, with protocols such as SSL and IPSec [HPV+99]. Yet, VPN has been mainly used between IT networks. Now, RA is

entering the OT world, and ICS are being connected to traditional IT systems. However, there are significant differences between the two systems: while IT has a long tradition of protecting equipment from malicious cyber actors, this is not the case for OT [FWD19]. Additionally, there are some fundamental differences between the priorities of the two systems, as highlighted in Figure 1.1. For example, in traditional IT, system confidentiality is the main priority, while in OT, control is the main priority, followed by availability [JWK21]

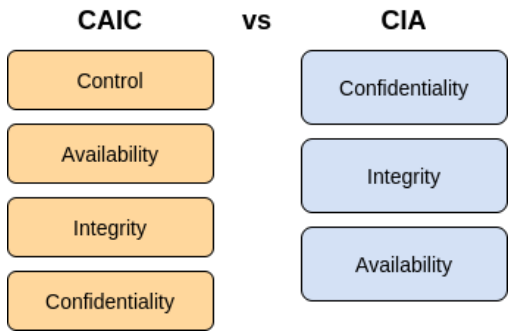


Figure 1.1: CAIC in OT compared to CIA in IT

Furthermore, as opposed to most IT devices, OT features a variety of components that can cause physical changes to its environment. In the worst case scenario, a maliciously modified device could shut down the power supply to an entire city or start a fire on an offshore platform. Thus, the danger of compromised security in such systems is obvious.

This potential risk of malicious actors accessing ICS in offshore installations means that RAS used for this purpose must be of the highest quality. However, the implementation of security measures can be a very complicated process due to the complex nature of the involved systems. Offshore platforms have a large variety of components from several different suppliers and vendors. They often use proprietary and equipment-specific protocols, and the various devices are typically not managed by the same personnel. For example, some employees only need specific measurement data from a Supervisory Control And Data Acquisition (SCADA) system. Other engineers working on platform operations may require data from the entire platform, as well as the option to change ICS configurations. In addition, several components are maintained by third-party vendors. This means that engineers from outside the operating company also need access to specific systems in order to perform software updates and other management activities. This all adds to the complexity of access control and user management for such systems.

It is important to note that the implementation of such a RAS is not a purely

technical issue. Technology is just one aspect of the widely used security risk categorization: *people, process, and technology*. Therefore, in order to identify a holistic solution, several factors must be considered. For instance, identity and access management (IAM) is an essential aspect of any RAS. It is important to have a clear understanding of who needs access and what level of access they should be granted; this requires clear classifications of different permission levels. A security rule of thumb is never to give more permissions than are necessary for someone to perform their work. However, this cannot always be easily defined and an employee who lacks the required permission can cause frustration and delays. This trade-off between usability and security is a typical issue in the design process and cannot be solved with a technical solution alone.

Compared to IT, securing interconnected OT systems is a relatively new field. However, it is also a field that is in a rapid state of development. Workshops with companies in the Norwegian petroleum industry together with their internal documentation indicate that the RAS currently used could benefit from additional improvements to reflect the newest academic and industrial advancements in the field. Current solutions work but are often based on standards and frameworks dating many years back. Furthermore, when components and functionality are added, this is often done on an ad hoc basis with no overall design goal extended to the functional level. This also appears to be the case for the many new security barriers that have been added. Even if the solution still complies with security requirements, this can cause unnecessary complexity that affects user-friendliness and cost efficiency. Guidelines such as IEC62443 and DNVGL-RP-G108 are helpful but the company workshops indicate that they lack sufficient details to be easily implemented. Furthermore, as these standards are for the *best current practice*, they do not include innovations and disruptive technologies that could offer better solutions.

Thus, the question is: are there better and more innovative ways of making a remote access solution for Norwegian offshore platforms? Would it be possible to combine the insights of petroleum companies with state-of-the-art research to create useful recommendations for their RAS? This is the goal of this thesis.

1.2 Objective

The overall objective of this thesis is to propose improvements to existing remote access solutions on the Norwegian Continental Shelf (NCS), in the form of a set of recommendations. Our hypothesis is that there is new RA technology and innovative solutions that are yet to be implemented by the companies operating on the NCS. With the goal of improving the RAS used by these companies, we have arrived at the following research question meant to facilitate reaching this goal.

RQ: *How can new ideas and emerging technologies in remote access be applied in the development of improved remote access security recommendations for Norwegian petroleum companies?*

In this thesis, new papers and emerging technologies in the field of remote access and ICS will be studied. The goal of *improved* regarding an RAS can be addressed in many ways. For instance, part of the existing RAS may already be sufficiently secure although there could be issues regarding user-friendliness or operating costs. Thus, an improved solution to this specific issue would be an easier and more cost-effective way of solving the same requirement. A solution can be improved in many different ways, be it security, usability, efficiency, reliability or economy.

To further help define our problem statement we have outlined three sub-research questions. These all build towards the goal of our overall objective, and also help to highlight how we would need to conduct our research.

Sub RQ A: *What are the functional requirements and threats related to a state-of-the-art remote access solution for Norwegian petroleum companies?*

Sub RQ B: *What are the key focus areas with the remote access solutions used by Norwegian petroleum companies today?*

Sub RQ C: *How can specific technologies improve existing remote access solutions with regards to the identified focus areas?*

1.3 Scope

This thesis revolves around RA to ICS and other OT networks. These systems are used in a variety of organizations and industries. In order to achieve more in-depth research, the scope of this study has been restricted to ICS in the petroleum industry. Further specified, this thesis studies RAS to ICS on petroleum installations on the NCS. The workshops in this study were conducted with two petroleum companies operating in this area (referred to as Alpha and Beta in this thesis). However, the results of this thesis could also be of use to companies operating in other geographical regions, as well as other sectors using ICS.

Remote access to ICS on Norwegian offshore installations is a broad field, involving multiple networks, locations and personnel. It would not be possible to explore all of these cases due to the time constraints of this thesis. We have therefore restricted

the scope of the thesis to the following two scenarios: connections from within the corporate network of the respective operating company and connections from the network of third-party suppliers. Excluded from this thesis, but also relevant to future studies are connections from onshore control rooms and RA connections from within the offshore platforms themselves.

1.4 Outline

Chapter 1 Introduction
Presents the motivation behind the thesis together with its objective and the research question it is based on. The scope of the thesis is also defined.

Chapter 2 Background and Related Work
Defines important terms used in the thesis. It also introduces relevant standards and guidelines, emerging RA technologies, and three selected cyberattacks from the past.

Chapter 3 Methodology
Describes the chosen research methods. It also reflects on the challenges and limitations of this research, as well as the ethical considerations that had to be taken into account.

Chapter 4 Results and Discussion
Presents findings from the literature review, workshops, and final evaluation. These are discussed in relation to the research questions, and finally, the developed recommendations are presented.

Chapter 5 Conclusion and Future Work
Presents the conclusion to the thesis and a brief reflection on future research on remote access to ICS, specifically on the NCS.

Chapter 2
Background

This chapter presents background information that has been deemed relevant for answering the research question. Most of this is the result of our initial literature review. Section 2.1 and 2.2 defines terms that will be important for this thesis. Next, in section 2.3, an overview of relevant standards and guidelines are presented, and in section 2.4 different emerging technologies and research suitable for remote access solutions are presented. Finally, section 2.5 features a discussion about various cyberattacks against ICS systems, and section 2.6 a summary of the literature review.

2.1 Operational Technology and Industrial Control Systems

This thesis explores secure remote access to the Operational Technology (OT) networks of Norwegian offshore installations. OT is the industrial equivalent of IT and refers to systems used to manage the operations of industrial processes. The main focus will be on Industrial Control Systems (ICS), a significant segment within OT, as shown in Figure 2.1. The National Institute of Standards and Technology (NIST) defines ICS as a general term encompassing several types of systems used to monitor and control industrial processes. Such systems can be supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), or distributed control systems (DCS). An ICS can be a combination of control components that work together to achieve an industrial objective, such as transportation of energy or matter.

2.2 Purdue Enterprise Reference Architecture

The Purdue Enterprise Reference Architecture (PERA) model, often referred to as The Purdue Model, is an enterprise reference architecture first outlined in the early 1990s. The model gives general architectural principles for the design of an OT environment and describes how organizations can logically segment their network into different layers. Today, the model is widely adopted for industrial networks

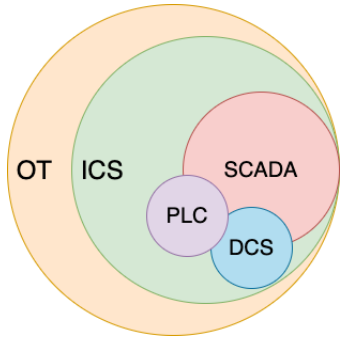


Figure 2.1: Overview of different terms connected to OT

and is used as a baseline for many standards and guidelines, for instance, the IEC 62443 series and NIST SP 800-82. Although the PERA model originally described how a network could be divided into five layers, a more novel approach is the enhanced PERA model. This model contains up to four additional layers, such as *external internet* and *demilitarized zones (DMZs)*. Figure 2.2 illustrates a hierarchical separation of an ICS network. Here level 1.5 is a logical level that we have added to separate level 2 *Area and supervisory control* from level 1, *Basic control domain*. The firewall between these domains governs OT-specific protocol messages that pass between the levels.

2.3 Standards and Guidelines

This section presents the standards and guidelines that are deemed most relevant for this thesis. In brief, the documents presented can be divided into three groups. All the groups elaborate on security recommendations; however, the targeted sectors differ. They either target ICS in general, ICS on the NCS, or RA for IT. The first category contains guideline NIST SP 800-82 and the IEC 62443 series of standards which is presented first [SPL+15]. Following this part are guidelines tailored for ICS cybersecurity on the NCS. This includes the NOG guidelines, DNVGL-GP-G108 and SINTEF A1626 [AS17] [GJ07]. Finally, RA for IT is presented, this includes the guideline NIST SP 800-46 [SS16].

2.3.1 IEC 62443

The IEC 62443 series is an international standard developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC). It is a multi-industry series aimed at giving cybersecurity procedures for securing ICS. The series contains standards and technical reports divided into the four areas; *general, policies*

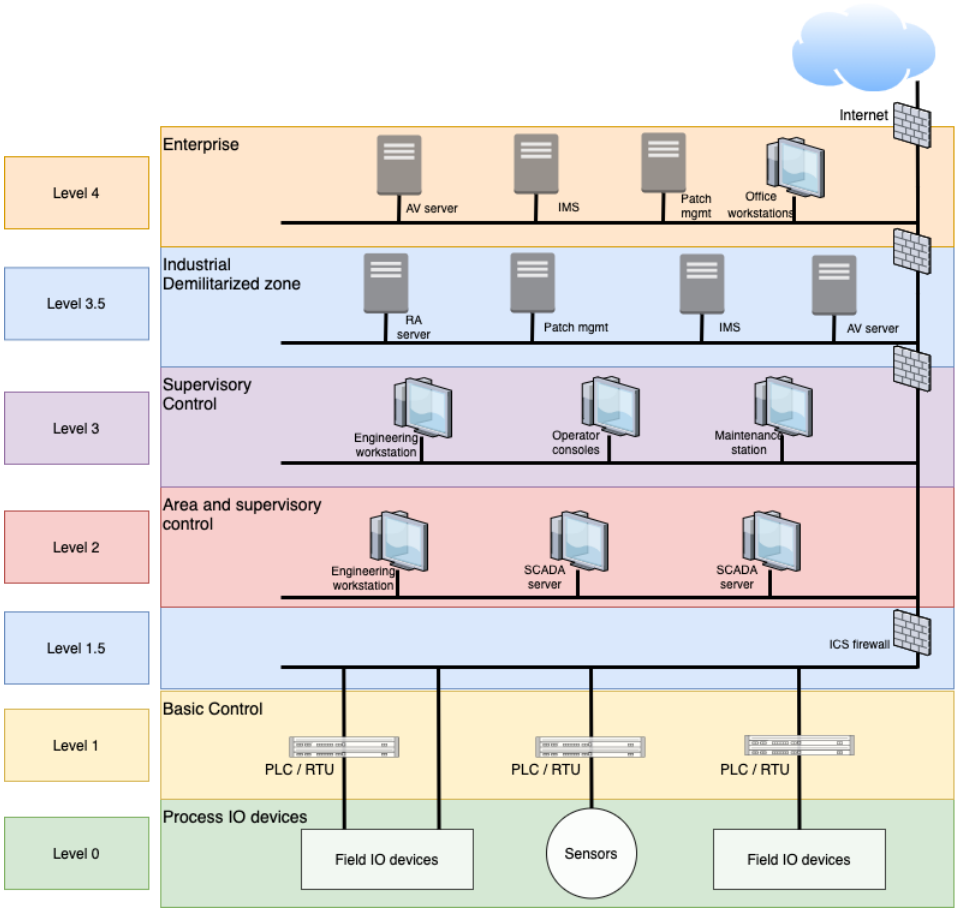


Figure 2.2: PERA's hierarchical seperation of ICS, with level 1.5 and level 3.5

& procedures, system, and *component*. All of these, with underlying standards, are shown in Figure 2.3.

IEC 62443 3-2

Security risk assessment and system design is a guideline contained in the IEC 62443 series. Its key concept is the application of ICS security zones and conduits [IEC18]. The standard describes how to reduce the risk of an ICS to a tolerable level by assessing and managing the potential vulnerabilities tied to it. This is achieved by a process split into three steps. Firstly, the System under Consideration (SuC) should be divided into zones and conduits. The the standard then describes how to assess the risk for each zone and conduit and establish Security Level Target (SL-T) for

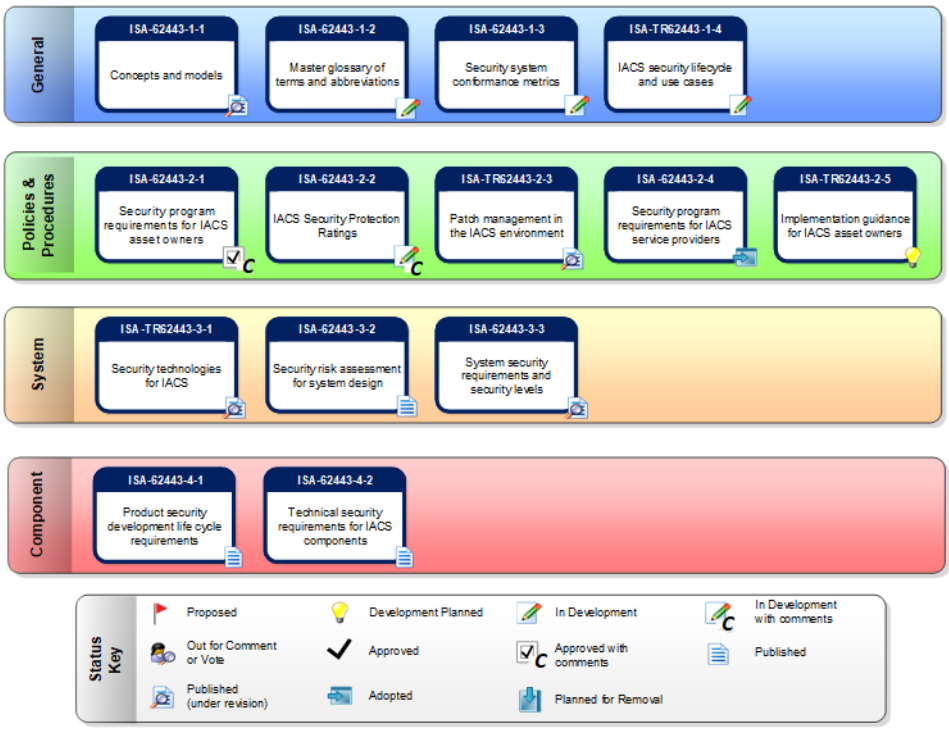


Figure 2.3: Overview of the standards and guidelines contained in the IEC 62443 series [IS16].

each of these partitions. Lastly, the Cybersecurity Requirements Specification (CRS) should document the security requirements derived in the previous step.

In its entirety, the process described is an iterative risk reduction technique. In the first step, the SL-T is defined, and after this security requirements for the evaluated threats are derived. A high-level cybersecurity risk assessment is then conducted. When posed risk does not exceed tolerable risk, a detailed cybersecurity risk assessment is completed. Finally, from this assessment, the CRS document should be produced. For further work and to assist the petroleum industry, it would be helpful to build upon the process presented in the document with a specialization towards RA for this sector.

IEC 62443 2-2

The standard named *IACS security program ratings* is part of the policies & procedures category of the IEC 62443 series. The document gives a methodology for

addressing the protection level provided by a holistic protection scheme of an ICS in operation. This is performed using security program ratings that are a combination of organizational and technical measures.

The standard defines the roles and responsibilities of asset owners (AO), the maintenance service provider (MS), the integration service provider (SI), and the product supplier (PS) during an Industrial Automation and Control System's (IACS) life cycle. A holistic protection scheme includes a combination of the area's technology, processes, and people. They are heavily connected to the operation phase, where the organization is in charge. Security program ratings are a numeric value that combines the organization's security- and technical measures. During the operation phase, the maturity level of the organization is essential. The organization's maturity level is measured in how skilled personnel follow documented security policies and procedures over time. Furthermore, the Maturity model [IEC20] divides the maturity into four different levels, from initial to optimizing. The technology part consists of cybersecurity- and physical security measures, which together make the technical measures applied to the automation solution. The SPR values are obtained from rating both the security levels provided by the organization's maturity level operating the IACS and the capabilities of the technical security measures. The standard proposes a framework for how values for SPR can be derived from qualitative analysis performed by experts. Although RA is not mentioned in the standard, we regard it as essential to consider the requirements for operating an IACS security management system when designing a RA solution for similar systems.

IEC 62443 2-4

Security program requirements for IACS service providers list a set of security requirements for RAS [IEC15]. Each of the requirements is tied to one of the two topics; *Security tools and software* or *Data protection*. Although the requirements give a useful sketch of prerequisites for the RAS, they could have given more technical details. However, the requirements presented in the document will be a good starting point for deriving security recommendations for the design of RAS for Norwegian petroleum companies.

2.3.2 DNVGL-RP-G108 - Cybersecurity in the oil and gas industry based on IEC 62443

DNVGL-RP-G108 is a guideline containing recommended cybersecurity practices for the oil and gas industry [AS17] and identifies how this sector should implement the IEC 62443 series. This report was made because of challenges experienced with the IEC 62443 series [AS17] and the need for a more specific recommended practice tailored for the petroleum industry. DNVGL-RP-G108 is the product of a joint effort

from several companies, aiming at defining a common way for securing ICS in the oil and gas industry using a practical approach. The report's target audience is everyone that in one way or another is involved with cybersecurity in ICS.

The guideline focuses on the standards 2-1, 2-4, 3-2, and 3-3 in the IEC 62443 series, an overview over how the IEC standards are used is shown in Figure 2.4. DNVGL-RP-G108 divides their recommended practice into four phases; concept, FEED, project, and operation. The *concept* phase defines roles and responsibilities. Next comes the *front-end engineering design* (FEED) phase, based on IEC 62443-3-2 /3/. This phase is separated into five different steps; identification of SuC, high-level risk assessment, partitioning into zones and conducts, detailed risk assessment, and documentation of CRS. The process is very similar to the IEC standard but DNVGL-RP-G108 also elaborates with practical information specifically aimed at securing industrial oil and gas operations. After this is the *project* phase, where systems are built and tested, and where the CRS previously defined, is implemented. Finally, the last phase is called the *operation* phase and gives principles for maintaining an implemented system, responding to incidents, and performing recovery if needed. The project- and operation phases are based upon IEC 62443-(2-4 & 3-3).

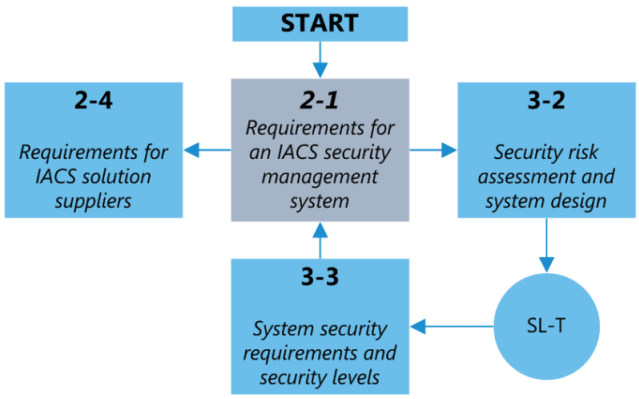


Figure 2.4: Overview over how the IEC standards are used in DNVGL-RP-G108 [AS17]

Cybersecurity regarding remote control of autonomous systems is discussed under the FEED and project part, and best practices for building such RAS are given in section 5.2.6 of the guideline. This section features seven security barriers for ensuring a secure RAS. Each barrier has several requirements as well as recommendations for best implementation. However, many of these are not actually listed and instead the guideline refers to sections in other standards such as IEC 62443. Despite this, compared to IEC 62443-3-2 /3/, the DNVGL-RP-G108 has more thorough

explanations for how the implementation of secure remote access could be done.

Regarding file transfers the guideline states that when the file originates from outside the process control domain this should only be allowed through the RAS server (also named jump server). The RAS server is an intermediate server that spans two distinct security zones and provides access between them. A file transfer solution should also implement two file storages. Firstly, there should be temporary storage where uploaded files are checked using malware scanning. If the files pass this first step, they should be sent to a second storage where they can be accessed from the internal network. The guideline also states that a remote file transfer solution is preferred over portable mediums when transferring files [AS17].

2.3.3 NOG Guidelines

The Norwegian Oil and Gas Association (NOG) is a professional body- and employer's association for oil and supplier companies in Norway. They have published several reports to support the industry, ranging from financial to geophysical guidelines. We have identified three of these to be related to our topic area. The first is *104 – Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems* [OA16], and features guidance on how to implement information security baseline requirements (ISBRs) in process control, safety, and support (PCSS) ICT systems. What is especially interesting here is ISBR-18, which details how to implement secure remote access in the systems mentioned above. It states the importance of establishing documented work processes for remote access and a policy for acceptable use of that access. More specific recommendations are also made, for instance, the use of time-limited work permits and dedicated secure terminal servers. It also suggests transferring data to the office, so users can access it there instead of giving remote access to the ICS.

The guideline briefly mentions file transfer over RAS. It states that a RAS should support a secure file transfer and that this solution is to be preferred over using a physical storage medium such as USB when transferring files into an ICS system. In addition, a file transfer solution should also perform scans for known and unknown malware. However, the guideline remains relatively vague on this topic, and more precise recommendations for how a file transfer solution should be designed could prove helpful for the industry [OA16].

123 - Classification of Process Control, Safety and Support ICT Systems Based on Criticality is another report by NOG, with its latest revision from 2009. It was meant to supplement the above-mentioned NOG report 104 and details how to classify PCSS ICT systems based on criticality. In this classification, regarding remote access, the report states that the required or acceptable access method should be documented for each system. This can be virtual private network (VPN) or remote login via

terminal server, but could also be limited to physical access, i.e., that remote access is prohibited for a given system.

NOG has also published a report describing the process of work permits for offshore installations on the NCS, named *088 - Recommended Guidelines for a Common Model for Work Permits (WP)* [OA15]. This model is not aimed explicitly at cyber, and therefore primarily focuses on physical security. However, which we will discuss in further detail later, this model is used as the baseline for the work permit system used by the companies Alpha and Beta.

2.3.4 Configuring and Managing Remote Access for Industrial Control Systems

In November 2010, Homeland Security and Centre for the Protection Of National Infrastructure (CPNI) published the report *Configuring and Managing Remote Access for Industrial Control Systems* [SC]. It describes best practices for secure remote access in ICS. The first part of the report covers control system architectures and the different roles connected to such systems. Among these roles are system operators, vendors, field technicians, customers, and business partners. The report then discusses remote access in traditional IT architectures, with different types of solutions and technologies, as well as several security considerations. It goes on to present remote access in control system architectures. It details security considerations unique to such systems and how to apply different security practices like full tunnels, DMZs, authorization levels, and password policy. Finally, the report wraps it all up with a case study where the techniques and best practices are applied to secure a fictional town named Marstad.

2.3.5 SINTEF A1626

The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems is a report created by Sintef for addressing security and safety for Safety Instrumented Systems (SIS). It investigates how a RAS into a SIS may represent a threat and could jeopardize its Safety Integrity Level (SIL). The report introduces the SeSa method, a method used to address to what degree remote access to an SIS impacts its integrity. Suppose the impact on the SIL is too significant. In that case, the SeSa method is used iteratively with a Hazard and Operability Analysis (HAZOP) to reduce the SIL impact to an acceptable level. The report lays out a thorough summary of threats that the system exposes itself to by having a RAS. This list of threats will be a good starting point when making a list of threats and attack stories.

2.3.6 NIST Guidelines - Special Publication 800 series

The National Institute of Standards and Technology is an association responsible for developing standards and guidelines in information security. The Special Publication (SP) 800-series consists of standards, guidelines, recommendations, and technical reports tied to NIST's cybersecurity activities. Under the 800-series are the guidelines 800-46 and 800-82 which give recommendations on how to secure RAS in IT and ICS.

NIST SP 800-46 Revision 2

NIST has published the guideline *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [SS16], giving recommendations on how to secure teleworks, remote access solutions (RAS), and BYOD technologies. Having a RAS and allowing BYOD technologies increases the attack surface of an organization. It would be safer to only access company resources from inside the organization's network and not allow the use of client devices. However, this is generally not a viable option. The NIST SP 800-46 standard emphasizes how to secure these types of solutions and devices. The recommendations given in this standard are meant for IT networks and not intended for any specific industry. Looking into how they can be transferred to ICS on the NCS may prove helpful.

NIST SP 800-82 Revision 2

The guideline *Guide to Industrial Control Systems (ICS) Security* provides recommendations for mitigating the risk associated with common threats to ICS systems, including SCADA, DCS, and PLC [SPL+15]. In the context of RAS, the guideline provides security recommendations and describes what considerations should be taken when connecting an ICS to an IT network.

The guide mentions that the file transfer protocols (FTP) and Trivial File Transfer Protocol (TFTP) are widely implemented in SCADA systems, DCS, PLCs, and Remote Terminal Unit's (RTU)s. However, neither of these protocols are secure and should therefore not be used. Instead, protocols such as Secure FTP (SFTP) or Secure Copy (SCP) are preferred. The standard provides recommendations for which protocols to use for file transfer between devices, but it does not specify how remote file transfer should be conducted.

The guideline also mentioned unidirectional gateways. These devices can only carry data in one direction, making them unable to send information back into the source network. The paper states that these are increasingly getting deployed and are usually deployed at the boundary between ICS and IT networks or between SIS and control networks. Unidirectional gateways will be further introduced in section 2.4.

Regarding firewalls, the guideline describes three different types: Packet Filtering, Status Inspection, and Application-Proxy Gateway. It states that the Application-Proxy Gateway can introduce a delay on the network performance that can be unacceptable to ICS environments. The guideline describes how firewalls implemented in an ICS environment can greatly restrict undesired access and thereby improve security. This topic will be elaborated further upon in section 2.4.

2.4 Emerging Remote Access Technologies

This section gives an overview of emerging technologies and new research related to remote access (RA). In this thesis, RA will be used as an umbrella term for several sub-technologies that together form a RAS. The technologies or solutions presented are VPN, Zero Trust, DMZ, firewalls, access management, network access control, sheep dipping, sandboxing, intrusion and anomaly detection systems, and unidirectional security gateways. Each concept is described with a general definition, followed by a discussion of the newest research. The aspects of the technologies discussed are not strictly tied to ICS or ICS on the NCS, but rather network security as a whole.

2.4.1 VPN

Virtual Private Networks (VPN) are among the most prevalent when it comes to remote access technologies. The basis of VPN is simple; it enables users to extend a private network over an insecure, public transportation medium as if their devices were located within the same physical network. During the 1990s, much effort went into developing this technology. The work on Internet Protocol Security (IPsec) started in 1992, and the Point-to-Point Tunneling Protocol (PPTP) was published in 1999 [HPV+99]. Some major VPN protocols today are Layer 2 Tunneling Protocol (L2TP)/IPSec, PPTP, Internet Key Exchange version 2 (IKEv2), and Secure Socket Tunneling Protocol (SSTP) [BRAA12]

In a paper by Nyakomitta et al., published in December 2020, four state-of-the-art RA VPN methods are presented. They are tunneling, portal applications, desktop application access, and direct application access[NA]. Tunneling involves establishing a communication channel between the endpoints, using cryptography to protect confidentiality and integrity. A vital aspect pointed out here is that this method enables the VPN gateway to control the amount of access the client gets after authentication. For example, it can restrict users to a specific subnet.

With *portal applications*, the client connects with a VPN tunnel to a portal server. This server has access to the internal network resources, and will decide what operations the client is allowed to do. This is similar to *desktop application access*,

but using this method, the client connects to an actual workstation inside the internal network. The proprietary protocol Remote Desktop Protocol (RDP) is typically used for this purpose. Nevertheless, Nyakomitta et al. also point out a critical issue with all these access methods; because of end-to-end encryption, other security controls such as firewalls and intrusion detection systems (IDS) cannot properly check the data coming into the network. The last method described by Nyakomitta et al. is *direct application access*. They point out that this method is only suitable for internal servers already facing the public internet. Since this is generally not the case for OT networks, we will not describe this method in greater detail.

Nyakomitta et al. also propose a new VPN solution, named Secure Remote Access Method (SRAM). It features prevention mechanisms to six named security threats, as shown in Figure 2.5. For instance, IP scanning will protect against source routing attacks where incoming packets have spoofed IP addresses to they look like internal addresses and trick firewall inspections. SRAM also use both media access control (MAC)- and IP addresses to identify clients and one-time passwords (OTP) to prevent privilege escalation. Thus, even if a malicious user gets access to one resource, another round of authentication would be needed to access anything else. This is similar to the principles of Zero Trust, which will be discussed later.

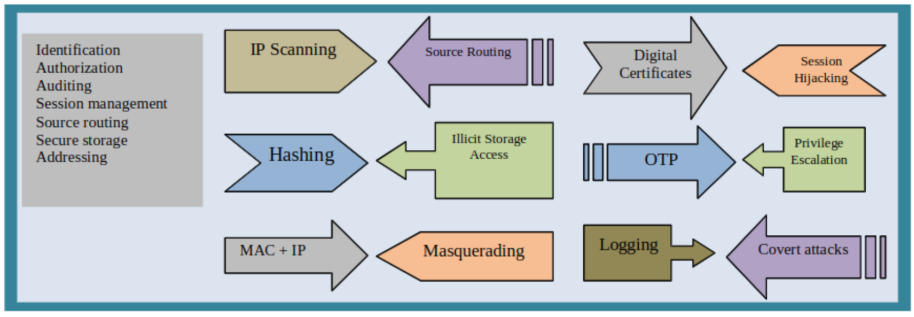


Figure 2.5: Prevention mechanisms in the VPN solution named SRAM

A paper by Jahan et al. from 2017 argues that different VPN solutions are not sufficiently classified based on organizations' application requirements [JRS17]. The paper features a comparison of the different VPN tunneling protocols Generic Routing Encapsulation (GRE), IPSec, PPTP, and L2TP. The evaluation shows that the optimal choice for remote access VPN services is to use L2TP in combination with IPSec. The rationale behind this solution is described as follows:

> *"The IPSec tunneling individually cannot create tunnel for layer 2 packets. Considering this situation, the L2TP and IPSec protocols are combined for ensuring security per-packet"* [JRS17].

Jahen et al. concluded that L2TP with IPSec is preferred with regards to security, as well as being fast enough for bandwidth- and time-sensitive applications.

Another paper, "Future After OpenVPN and IPSec" by Korhonen [Kor19], states that IPSec and SSL/TLS-based protocols, such as those mentioned previously, have superseded all older VPN technologies. However, the paper also points to a new open-source VPN application called WireGuard. This emerging technology aims to be faster, simpler, and more practical than older IPSec-based solutions. Korhonen also argues that another emerging technology, called Software-Defined Perimeter (SDP), could be significant in new remote access solutions. SDP is already featured in several commercial solutions, like Cloudflare, Pulse Secure, and Perimiter81 [Clo] [Sec] [per].

2.4.2 Zero Trust Security

Zero Trust is not a specific technology but rather a methodology that incorporates several security practices and techniques. As described by Rose et al. in NIST Special Publication 800-207:

> *"the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources"* [RBMC20].

It is location-agnostic, based on the notion that a company's internal network is never completely secure. With this idea as the basis for a network's security design, the Zero Trust model works just as the name suggests; never trust, always verify. In perimeter-based security, a user is authenticated before being admitted into a network. However, after this one authentication, the user can freely move around and access multiple resources within the network. This is not the case in a Zero Trust Architecture (ZTA). Here no implicit trust is granted based solely on a user's physical or network location. Both subject and device will have to be authenticated and authorized before a session to any company resource can be initiated. This is also the case for two resources communicating within the internal network, and both parties will therefore demand a mutual authentication. Rose et al. describe ZTA with the following seven tenets:

1. Every device in the network, both data sources, and services are considered resources.
2. All communication is secured regardless of its location.
3. Access to individual network resources is only granted on a per-session basis.

4. Access control with a dynamic policy that evaluates the identity and state of the client, application/service, and the requested asset. It may also include other behavioral and environmental attributes.

5. Continuous monitoring and measurement of the integrity and security posture of all owned and associated resources.

6. Dynamic and strictly enforced resource authentication and authorization before any access is allowed.

7. The solution collects as much information as possible from the current state of the system and uses this to improve its security posture. This data can, for instance, serve as input to an anomaly detection mechanism.

The above description is not directly aimed at enterprises with industrial networks. However, a yet unpublished paper by Boumhaout et al. proposes, according to themself, the first publicly available implementation of a ZTA for ICS [BD20]. The data flow of their solution is shown in Figure 2.6, but it should be noted that this figure is a modified model of Google's BeyondCorp architecture [SOMB16].

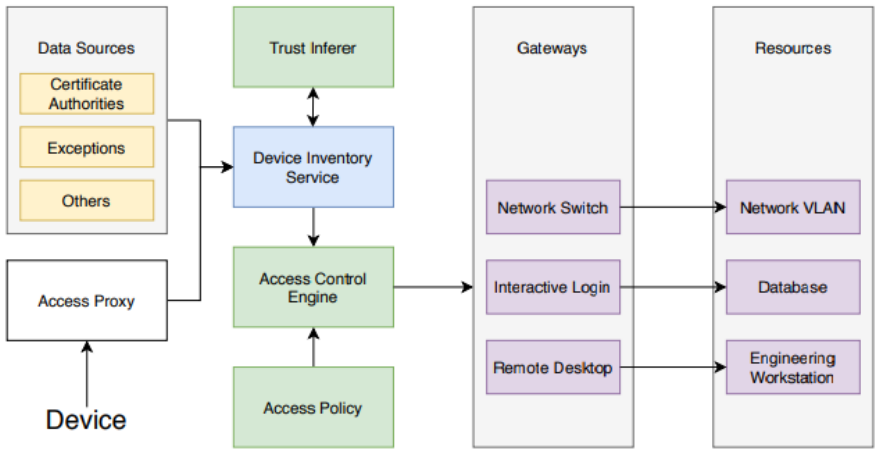


Figure 2.6: High-level Zero Trust architecture data-flow for ICS

2.4.3 Zero Trust Network Access / Software Defined Network

A subset of ZTA is Zero Trust Network Access (ZTNA), a term coined by Gartner in 2019 [Cam20]. Another term often used is Software Defined Perimeter (SDP), and this essentially refers to the same thing. It describes technology that creates a boundary, based on identity and context, around network applications and resources. In ZTNA, applications are hidden, and access is restricted using a trust broker to a set of named entities. Before allowing access, the broker verifies the specified users' identity, context, and policy adherence. Gartner has identified two different approaches that vendors have adopted for this solution; Client-Initiated ZTNA (following the Cloud Security Alliance (CSA) SDP specification) and Service-Initiated ZTNA (following the Google BeyondCorp vision). Figure 2.7 shows a conceptual model of the former [Gro19].

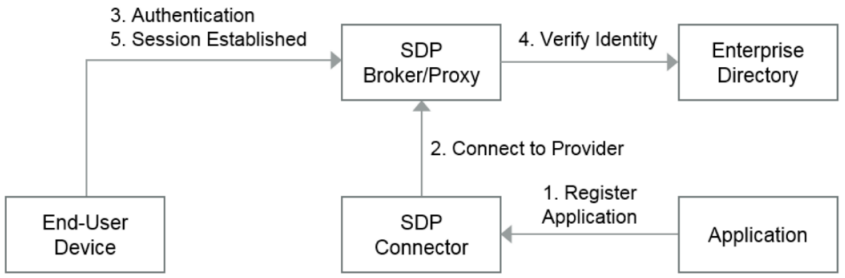


Figure 2.7: Client-Initiated ZTNA

Gartner estimates that 60% of enterprises will phase out VPN solutions in favor of ZTNA by 2023. This shift may take longer for industrial enterprises, however, it is likely that these will follow as well. Gartner also compiles a list with representative vendors providing ZTNA solutions, including well-known names such as Cisco, Cloudflare, Microsoft, and Google Cloud Platform. In addition, an open-source alternative, called OpenSDP, has been developed by Waverley Labs [Koi].

2.4.4 Demilitarized Zone

External facing services are generally exposed to a larger surface of threats than internal services. A Demilitarized Zone (DMZ) is a separate subnet of an organization's Local Area Network (LAN) that contains these external-facing services. The DMZ adds an additional layer of security by only exposing a selected few services while the rest of the network remains hidden behind a firewall. This protects the internal network if the DMZ gets compromised and adheres to the defense-in-depth strategy. Furthermore, traffic from either side of the DMZ is terminated here, meaning network traffic does not directly traverse this zone [DCB18].

Regarding the design of a DMZ design, the most basic approach is to create a zone using just one firewall. However, the single firewall is still programmatically configured to act as two virtual firewalls. With two firewalls (dual-firewalls), one is used at the internal border and one on the external. The external firewall hinders arbitrary packets from entering the DMZ while separating it from the public internet. On the other side, the internal firewall stops unwanted traffic that is already inside the DMZ from reaching the internal network [Aga04].

Industrial DMZ (IDMZ) is a subcategory where the DMZ is located between two subnets, both located within the organization's internal network. This means that the external firewall is not a frontier to the public internet but rather to the enterprise network, and the internal firewall separates the IDMZ from the OT environment. A paper by Ning et al. discusses the advantages of dual-firewalls in IDMZ compared to single firewalls [JLYZ18]. It states that the dual-firewall can provide stringent security and gives the benefits of clear management separation along with simplified firewall rules. The separation also makes it less likely that a compromised computer in the DMZ will allow for further penetration into the network [Aga04]. On the other hand, a single firewall is less costly, but it is a potential bottleneck for the network since it handles both external-to-DMZ and DMZ-to-internal requests on the same hardware.

2.4.5 Firewalls

A firewall is hardware or software that limits network access based on predetermined security rules. Firewalls can be network-based or host-based [MSR20]. Network-based firewalls are placed anywhere within a Local Area Network (LAN) or Wide Area Network (WAN). However, they are usually set at a domain boundary to control all outgoing and incoming traffic to a network. Here it often acts as a barrier between a trusted network and a less trusted one, as described in the previous section. Host-based firewalls run on individual devices and protect that specific device from viruses and malware. For this thesis, however, network-based firewalls are the most relevant.

The capabilities of firewalls have gradually improved since the concept was introduced in the 1980s. Since then, there has been a first, second, and now a third generation of firewalls. This last generation is also referred to as Next-generation firewalls (NGFW) [Che03]. The first generation firewall only had the capability to do packet filtering. This means that the firewall uses an access control list to filter packets based on their port numbers or source- and destination addresses [Che03]. Then, the second generation introduced stateful firewalls capable of keeping track of a conversation between two devices.

Finally, today's NGFWs is the state-of-the-art approach for separating and securing networks. As defined by Gartner:

> *"Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall"* [Gar17].

This type of firewall combines the functionality of several network security solutions into a single device. The third generation of firewalls has added the possibility to inspection packets at the application layer, instead of only on lower levels (3 and 4 of the Open Systems Interconnection (OSI) model) [NHC18]. In addition, NGFW can implement security policies for all the layers up to layer 7 of the mentioned OSI model. This means that the firewall can perform deep- and sometimes encrypted packet inspection. It can also perform antivirus scanning and use intrusion prevention systems (IPS) [NHC18]. These capabilities were introduced to combat the increased amount of advanced attacks that previous generations of firewalls were not able to defend against appropriately [NHC18].

Firewalls can be divided up into industrial/OT and enterprise/IT firewalls. An enterprise firewall is used in an organizational environment, while industrial firewalls are used in ICS, and other OT environments [MSR20]. Industrial firewalls have previously been somewhat behind regarding technological advantages; however, multiple companies are now claiming to have firewalls with NGFW capabilities for OT environments. These industrial firewalls, contrary to traditional IT firewalls, accept OT protocols and can implement filtering on OT-specific protocol messages [MSR20].

The paper *On the use of open-source firewalls in ICS/SCADA systems* investigates how open-source firewalls for IT networks can be used in SCADA networks [Niv16]. Nivethan et al. state that iptables (a tool used for managing IP packet filtering rules in the Linux kernel [Ipt]) can be used as an effective firewall for SCADA systems. By using advanced iptables features, the firewall can perform a dynamic inspection of packet data. The firewall must be able to define rules on Modbus Transmission Control Protocol (TCP) packets. By doing so, the authors created a firewall that defends against various attacks on SCADA protocols.

A paper by Li et al. from 2018 named *SCADAWall: A CPI-enabled firewall model for SCADA security* presents an OT-specific firewall called SCADAWall [LGZ+19]. It was created due to problems discovered with firewalls in SCADA systems and the fact that there are a limited number of open-source industrial firewalls. The paper

states that traditional Deep Packet Inspection (DPI) in such firewalls only partially inspects the payload. However, it should be noted that from the time after this paper was published, several security companies claim to have OT-specific firewalls with DPI. Nevertheless, the paper proposes a new algorithm, Comprehensive Packet Inspection (CPI), that will perform more thorough inspection of data. This CPI technology is implemented using iptables in the Linux operating system. It inspects all meaningful fields and single bytes in the application content against predefined firewall rules. The paper also aims to solve the lack of compatibility between firewalls and proprietary industrial protocols. Proprietary Industrial Extension Algorithm (PIPEA) can add rules for proprietary industrial protocols into OT-specific firewalls. An additional algorithm is presented in the paper, i.e. Out-of-Sequence Detection Algorithm (OSDA). This algorithm is used to detect abnormalities within industrial operations. In summation, the technologies and algorithms CPI, PIPEA, and OSDA are what together constitute SCADAWall [LGZ+19].

2.4.6 Access Management

Access management (AM) is an essential part of a holistic remote access solution. In this thesis, AM will be used as an umbrella term, encompassing several different aspects, including access control (AC), user management (UM), and identity and access management (IAM). It is important to have a clear structure for how users should be added, removed, and escalated in privilege in day-to-day operations. This means that access management systems have to balance security versus simplicity. On the one hand, the system should be adequately secured: getting privileged access should be a process with strictly defined steps involving multiple security personnel and supervisors. On the other hand, if this process is too cumbersome, it will result in extra costs for the company because the effectiveness of workers will decrease. To further add to this problem, most OT environments have several separate systems that each need numerous different privileged users and authorization levels. This will also be discussed in section 4.1.

Recent research has been conducted to find better solutions for AM, for example, the paper *Application model for privileged account access control system in enterprise networks* by Sindiren E. and Ciylan B. [SC19]. This paper features a simplified model with only one type of privileged account, but the ideas can also be implemented in more complicated systems. The application designed, named *Privileged Account Access Control System* (PAACS), features two modules; one for directory service privileged accounts and one for local administrator accounts. To access any given IT assets as a privileged user, permission from both these accounts is needed.

In the paper *Access control for Cyber-Physical Systems interconnected to the Cloud* by Lopez and Rubio [LR18] several ways of managing access control for users are

discussed. Among these are Role-Based AC (RBAC), Attribute-Based AC (ABAC), Organizational-Based AC (OrBAC), and Risk-Based Access Control (RiskBAC). The latter was designed for highly dynamic environments involving multiple organizations and may be interesting to explore further. For example, when access to a system is requested, the risk of the demanded access is calculated as $risk = V\ x\ P$. In this equation, V is the value of the resource accessed (this reflects its criticality or sensitivity), and P represents the probability of unauthorized disclosure based on the trustworthiness of the entity requesting access. Lopez and Rubio argue that this is not an applicable solution because it is too time-consuming to analyze the criticality and probability of abuse for every system in a large network. However, in offshore installation, this work has already been performed (provided it complies with cybersecurity standards like IEC 62443 and has established zones and conduits with SL-T ratings).

In recent years, several papers have also discussed access control for Zero Trust Networks. For example, Vanickis et al. describe a policy enforcement framework for Risk Adaptive Access Control (RAdAC), named FURZE [VJDL18]. RAdAC is a concept that tries to aid in the trade-off between operational need and introduced risk when making access control decisions. The FURZE framework includes a general AC policy language and generic firewall rules aimed at Zero Trust Network (ZTN) implementations. In 2020, a paper by Ahmed et al. presented another model for AC in a ZTN [ANUT20]. This model aims to provide a policy for protecting sensitive data when requests are made from several different locations, both within the internal DMZ and remote locations.

2.4.7 Network Access Control

An important subset of Access Control is Network Access Control (NAC). This is a solution where a set of protocols implement a policy for how to securely access nodes inside a network when a new device is connecting for the first time. Before granting access to the network, these protocols will validate new devices by measuring their authenticity, integrity, and security posture. NAC is based on three functional areas; authentication/authorization, assessment of security posture, and quarantine and remediation [Ser10]. The two first areas are used for validation, while the last defines how devices not complying with security policy should be handled. NAC solutions can also be classified into two categories; clientless and client-based. For clientless solutions, no software is needed on the client to assist with the validation process. On client-based solutions, software used to assist the NAC validation has to be preinstalled on connecting entities.

Major network access control solutions today include Cisco's Identity Services Engine (ISE), Microsoft's Network Access Protection (NAP), Forescout Platform,

Aruba ClearPass, FortiNAC and, an open-source alternative Trusted Network Connect (TNC) [Gar].

In a paper by Muhammad et al., an enhancement of NAC is proposed [MAZ17]. This solution uses machine learning, based on behavioral patterns of device traffic, to develop an Intelligent Filtering Technique (IFT). The purpose of the research is to address challenges with BYOD environments, but the overall ideas could apply to all NAC areas. As mentioned previously regarding VPN, it is a problem that traffic coming into a critical system is encrypted, thus making traditional anti-virus, firewalls, and IDS ineffective. The IFT proposed by this paper uses Inter-Arrival-Time (IAT) features from TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) protocols to profile connecting devices. This enables it to filter out all with abnormal behavior from the network in real-time, even though the data is encrypted. The filtered-out devices are sent to an Access Control Security Manager (ACSM), which controls access to the system.

2.4.8 Remote File Transfer

In order to perform remote work on an ICS system, it may be necessary to transfer files from an external device into the internal network. For example, third-party vendor companies regularly need to transfer patch files and update systems they are responsible for. Transferring files to the internal network can either be done with a physical medium or by sending them over the internet using the RAS. However, both cases entail a clear challenge; bringing a file into the OT network introduces a security threat since the file may contain malware or other harmful content. This implies that a solution should be in place to handle this transfer in a secure way. The following section will investigate technologies for remote file transfer.

Sheep Dipping

The concept of sheep dipping is a method used to analyze files for malware before they are allowed into an organization's network. More precisely, this is performed when data is brought into an organization on a physically removable medium (e.g., an USB flash drive). The removable medium is inserted into an isolated environment where it is analyzed for malware and other harmful content. This environment could be a stand-alone computer connected to a network under strictly controlled circumstances. Sheep dipping makes it possible to discover malware before files are allowed into the internal network. It is important to note that sheep dipping is a physical process. It does not apply to files downloaded from the internet unless the downloaded file is transferred to a physically removable medium.

Sandboxing Security

Sandboxing is generally a term used for describing the isolation of an application from other system resources and running applications. A sandboxed application will only have access to resources contained within its sandbox. This provides the system with an additional layer of security and prevents potential malware from escaping the isolated environment. In the context of cybersecurity, sandboxing is often used to test files for malicious content in a controlled virtual environment. This is different from typical virus scanning as it gives the possibility to perform more rigorous analysis, such as executing suspicious files and analyzing their behavior. The sandboxed environment should be as identical as possible to the actual system so that the analysis is performed under similar conditions to those in the real environment [VGT14].

2.4.9 Intrusion and Anomaly Detection Systems

Defense-in-depth is a key concept in cybersecurity. If one barrier is penetrated, several other layers of security will still be in place. Following this analogy, if security methods such as the firewall and NAC have failed to prevent malicious data from entering a given system, the next security barrier would typically be an intrusion and anomaly detection system (IADS). This is a system that monitors either a host or an entire network looking for malicious activity and policy violations. The detection is generally categorized into two different approaches: Signature-based Detection (SbD) and Anomaly-based Detection (AbD). Signature-based monitoring use a database of patterns or strings corresponding to known attacks and will compare this with captured events to recognize possible intrusions. Anomaly-based detection, often using machine learning, will monitor a system for deviations from expected behavior, such as failed login attempts or processor usage. IADSs can also be categorized based on how and where they operate; host-based IADSs will monitor files and activity on a given device, while network-based IADSs will monitor traffic going in and out of a network [LRLT13].

In this search for emerging research into IADS, the focus has been on systems for the lower levels of the Purdue model. An IADS deployed on levels 4 are an equally important part of the layered defense, but as this are operating on an IT-only networks it is not the scope for this thesis. In the paper *Intrusion and anomaly detection for the next-generation of industrial automation and control systems,* published 2021, Rosa et al. provides a review of recent AbD techniques for SCADA systems and goes on to propose a complete framework for a new IADS [RCdF+21]. According to this paper, the latest research into IADS for ICS has focused on two main approaches; SbD using the most common SCADA communication protocols (e.g., Modbus, DNP3, CIP) and machine learning-based AbD. The former approach is likely to fail against unknown vulnerabilities, while the latter requires previous training and is usually

tuned for a specific process or protocol. Open-source network-based IDSs have been the focus in several recent research aimed at improving their support for SCADA systems. Among these are Snort, Suricata, and Bro [ZZTX10, WDSN17, LSDM+13]. Such IDSs are efficient solutions that can enforce communication policies at the network level and be a smart addition when designing improved RA solutions for ICS. For AbD, several papers have proposed solutions built on different machine learning methods. A complete overview can be found in the paper mentioned above by Rosa et al.

2.4.10 Unidirectional Security Gateway

A Unidirectional Security Gateway is a security device based on a one-way data diode. It is designed with two separate circuits, one transmit-only and one receive-only. This physically constrains the transfer of data to only allow one direction and provides a hardware-enforced perimeter, giving better security than other software-based solutions [KFG19]. The use of this technology seems to be increasing, and several academic papers are discussing such devices for securing critical ICS [HKKN16] [Gin13].

The Unidirectional Security Gateway is most commonly used to secure connections between a high-security and low-security network and can be used in two different ways. Firstly, the diode can be configured as receive-only: this will protect the *confidentiality* of the high-security network. Data could be transferred into the network, but no information is allowed to leave. However, in industrial systems, the most relevant case is when the device is configured in the opposite direction. With this, the *integrity and availability* of the high-security network will be protected. Data can be transmitted out of the system, but no data can be received. This is typically used in monitor-only solutions. However, it is important to note that this strict one-way communication is hard to implement in practice without additional solutions. This is because most data protocols, like Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and Modbus, require the recipient to acknowledge received data. Without this, it would not be possible to provide quality of service (QoS). Fortunately, this issue can be solved by introducing intermediate proxy servers, and often unidirectional gateway products have these servers built-in by default [KFG19].

Availability is essential in ICS, and Unidirectional Security Gateways is an attractive option since this device does not implement a complicated software ruleset. This means that traffic can flow through it without introducing any latency [Sco15] and it is, therefore, a possible replacement for network barrier technologies such as firewalls and whitelisting. However, compared to these options, the Unidirectional Security Gateway has a far higher capital cost [Sco15]. But on the other hand, it will

not have an equal need for maintenance and configuration as it is a device mainly based on hardware.

2.5 Cyberattacks Against ICS

As already mentioned, the number of cyberattacks towards ICS are increasing. However, a silver lining is that the growing number of ICS-related incidents also increases research on the topic. The saying goes, *know thy enemy*, and understanding how previous cyberattacks have been conducted helps the industry prepare for future incidents. A good list of such attacks is described by Hemsley and Dr. Fisher in *History of Industrial Control System Cyber Incidents* [HEF] and by Khorrami et al. in *Cybersecurity for Control Systems: A Process-Aware Perspective* [KKK16]. We have compiled a brief overview of the recent years' most relevant ICS-based cyberattacks and some discussion into important key takeaways from these papers.

2.5.1 Stuxnet

Probably the most widely known cyberattack of all time was aimed at OT, more specifically at SCADA systems. Stuxnet was a malicious computer worm, using four different zero-day flaws to infect Microsoft's Windows operating systems and then look for Siemens Step7 software[MRHM10]. The attack targeted Iranian nuclear facilities in Natanz, where Step7 software managed PLCs used in gas centrifuges for separating nuclear material. Stuxnet first monitored the systems to gather operational information and then used this to take control over several PLCs. Finally, the worm modified these devices and caused the centrifuges to spin themself into destruction while at the same time circumventing industrial safety systems by feeding false data back through the PLCs. The attack destroyed around 1,000 centrifuges, about 11% of Iran's total number installed at the time. In addition, it decreased the production of enriched uranium and likely caused chaos within the Iranian nuclear program [MY12].

While it is believed that the malware initially was injected into the system using USB flash drives, Stuxnet still used remote access capabilities. According to researchers from the Slovakian internet security company ESET, the Stuxnet malware communicated with a command-and-control (C&C) server over normal HTTP traffic [MRHM10]. The apparently harmless URL *http://www.mypremierfutbol.com/index.php?data=data_to_send* was used to send commands to the Stuxnet malware while it was running on infected systems. Data_to_send is the encoded message, encrypted with a custom algorithm. We have seen that several standards, frameworks, and academic papers highlight network monitoring as an essential feature. As much of what was infected were highly critical OT systems, a robust monitoring service ought to have registered this unusual traffic, for instance, an anomaly detection mechanism.

This indicates how mitigating security measures are very useful when an attack has already occurred.

Years later, in 2011, a new malware similar to Stuxnet was discovered by the Laboratory of Cryptography and System Security (CrySyS Lab). However, its nature had changed: instead of being a worm-like Stuxnet, it was now a Remote Access Trojan (RAT). It is believed that this malware has been used for espionage on PLC producers [VH15]. PLCs are used in every industrial process, one example being offshore installations on the NCS. There is an alarming tendency that cybercriminals go after hardware suppliers, and it is therefore vital that companies act carefully and demand strict security requirements when buying equipment from third-party vendors.

2.5.2 Ukrainian Power Grid Attack

On December 23, 2015, a Ukrainian regional electricity distribution company reported several service outages. This was caused by a third party's illegal entry into the company's SCADA systems and resulted in seven electricity substations being disconnected for three hours. In total, approximately 225,000 customers lost their power in various areas across Ukraine[EI16].

According to a whitepaper written in a joint effort by Electricity Information Sharing and Analysis Center (E-ISAC) and SANS Institute, this attack had the sophistication consistent with a highly resourced threat actor [EI16]. While such attacks are difficult to protect against, to say the least, understanding the methods used and how to mitigate them is of great importance. Additionally, this attack is a perfect example of how the increasing connectivity of ICS, even though secure VPN solutions, can cause physical harm to both equipment and people. First, the attackers used various techniques, including spearfishing, variants of the BlackEnergy 3 malware [KMM$^+$16], and manipulation of Microsoft Office documents to get the initial foothold into the electricity company's IT network. From there, they pivoted to the industrial network. The attackers had experience using OT infrastructure and were able to operate the ICS using, for instance, Human Machine Interfaces (HMI). The final attack was either performed over a VPN connection into the ICS using existing RA tools within the environment or by issuing commands directly from a remote station.

E-ISAC and SANS have compiled an extensive list with mitigations for the different attack methods used, and only selected topics will be discussed here. With regards to the VPN exploitation, the mitigation recommended is relatively simple; enable two-factor authentication. In addition, several aspects are mentioned to further increase the security of a VPN solution, including jump servers with NAC, use of DMZs, traffic monitoring, and anomaly detection. Also, split tunneling is

recommended to be disabled in the VPN solution. Furthermore, as mentioned above, part of the attack conducted from the company's workstation was accessed using a RAS. Mitigation methods to hinder these kinds of attacks include host-based application-aware firewalls, application whitelisting, and management efforts to identify changes to the operation of an asset. Another mitigating approach is to require a confirmation from an operator when performing changes to ICS, or the implementation of Area of Responsibility to limit what components a single authorized user can access.

There are clear similarities between the mitigations recommended in the whitepaper by E-ISAC and SANS and the best practice standards mentioned in the first section of this chapter. Consequently, even though defending against Advanced Persistent Threats (APTs) can be almost impossible, this attack would have been harder to perform and with limited effectiveness if the Ukrainian electricity company would have compiled with best-practice security standards.

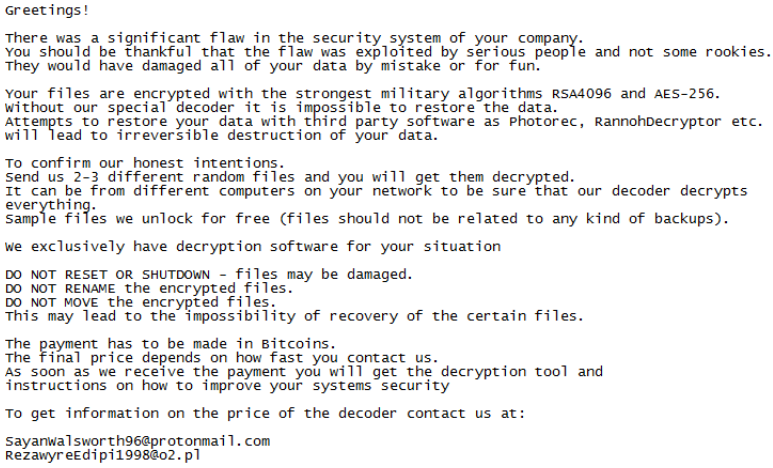
2.5.3 Hydro Ransomware Attack

A third example of cyberattacks towards industrial targets happened in March of 2019. Hydro, a major Norwegian aluminum and renewable energy company was hit by a targeted crypto-locking malware called LockerGoga. As previously mentioned, this type of attack, often referred to as ransomware, is increasingly targeting ICS. The outcome was that both office- and industrial Hydro-owned computers in 40 different countries stopped and became unusable. As a result, several plants went into manual operations, and the rest had to be completely shut down. Hydro has estimated the total cost of the attack to be between 550 and 650 MNOK [AS20].

LockerGoga first appeared when it infected computers owned by the French company Altran Technologies in January of 2019. It works by traversing the victim company's network while encrypting files and changing user passwords. After this, it leaves a text file on a desktop with a ransom note similar to the one in Figure 2.8.

According to an incident report published by Finnish researchers at Aalto University, the attack infected Hydro's Windows Active Directory (AD) server. It then used elevated admin permissions to reach all AD-managed endpoints [LAG19]. Because both enterprise- and industrial systems were affected, the networks likely used the same AD server for all access management. This is a significant security flaw and goes against all the previously discussed recommendations regarding the segmentation of different security zones. It is clear that if Hydro had better segmentation, for instance, an architecture based on Zero Trust, LockerGoga would not been that effective.

Furthermore, while LockerGoga operated, it definitely caused a large amount of



```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

SayanWalsworth96@protonmail.com
RezawyreEdipi1998@o2.pl
```

Figure 2.8: Ransom letter used by LockerGoga [Mal19]

unusual network traffic that would easily be picked up by a properly implemented monitoring system, especially one with machine learning-based anomaly detection. This once again highlights the importance of the *defense-in-depth* principle; even when the initial security barrier was breached, other security mechanisms should have stopped this attack or at least mitigated the damage caused.

2.6 Literature Review Summarized

The following tables summarize findings from the literature review. First standards and industry guidelines, then papers related to different RAS. Previous attacks towards the industry have not been summarized.

2.6.1 Standards and Guidelines Summarized

Responsible institution	**Name**	**Last revision date**	**Full Name**	**Comment**
IEC	IEC 62443 3-2	2018	Security risk assessment and system design	Details how to assess the risk of a particular IACS, and how to reduce risks to tolerable levels
	IEC 62443 2-2	2020	IACSs security program ratings	States how one can address the protection level provided by a holistic protection scheme of an ICS
	IEC 62443 2-4	2015	Security program requirements for IACS service providers	Includes a list of security requirements for RAS
DNVGL	DNVGL-RP-G108	2017	Cybersecurity in the oil and gas industry based on IEC 62443	Defines how the IEC 62443 series can be implemented in the petroleum sector
NOG	NOG 104	2016	Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems	Highlights the importance of a documented work process for RA. Features several well-defined access barriers, like ISBR-18 that details how to implement secure RA
	NOG 123	2009	Classification of Process Control, Safety and Support ICT Systems Based on Criticality	States that different ICS should have different acceptable access methods
Homeland Security / CPNI	-	2010	Configuring and Managing Remote Access for Industrial Control Systems	Features a detailed overview of roles associated with a RAS for ICS
SINTEF	SINTEF A1626	2007	The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems	Features a comprehensive list of cyber threats to RAS

NIST	NIST SP 800-46	2016	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	Gives recommendations on how to secure teleworks, RA, and BYOD technologies
	NIST SP 800-82	2015	Guide to Industrial Control Systems (ICS) Security	Provides recommendations for how to mitigate common threats to ICS systems
	NIST SP 800-207	2020	Zero Trust Architecture	Features the abstract definition of ZTA with general deployment models and use-cases
SANS	-	2015	Tactical Data Diodes in Industrial Automation and Control Systems	Explaining the use of Data Diodes (Unidirectional Gateways) within the IACS domain
HSD (The Hague Security Delta)	-	2019	Understanding the Strategic and Technical Significance of Technology for Security *The Case of Data Diodes for Cybersecurity*	Explaining Data Diode technology, with its strengths and weaknesses, and giving an overview of the current stakeholder landscape and new developments

Table 2.1: Summary of standards and guidelines

2.6.2 Emerging Technologies Summarized

Category	Developed / mentioned by	Technology	Comment
VPN	Nyakomitta et al. (2020)	Secure Remote Access Method (SRAM)	Prevention mechanisms to six named security threats, including session hijack and masquerading
	Jahan et al. (2017)	L2TP with IPSec	Compares different VPN protocols and find L2TP with IPSec to be the best choice
	Korhonen (2019)	Software-Defined Perimeter (SDP)	A security framework designed to micro-segment network access (based on ZT)
Zero Trust	Boumhaout et al. (yet unpublished)	ZTA for ICS	An approach to implement ZTA in an ICS environment
	Osborn et al. 2016	BeyondCorp ZTA	An overview of a ZTA solution by Google's BeyondCorp
	Qi An Xin Group / Gartner (2019)	Client-Initiated ZTNA	Enforce ZT policies using a client agent that requests access from an SDP Controller, and giving access through an SDP Gateway
	Waverley Labs	OpenSDP	An open-source Software-Defined Perimeter solution
DMZ	Ning et al. (2018)	A DMZ using dual-firewall	Provides better security and clear management separation in the DMZ
Firewalls	Li et al. (2018)	ScadaWall	A firewall for SCADA systems that can filter on SCADA protocol-specific packages
	Nivethan et al. (2016)	ICS Firewall	A firewall that uses iptables as an effective firewall for SCADA systems
	Gartner	Next-generation firewalls	Deep level packet examination to add application-level inspection of packets
	Mungekar et al. (2019)	ICS Firewall	ICS firewalls with NGFW capabilities and that can understand ICS specific protocols
Access Management	Sindiren E. and Ciylan B. (2019)	Privileged Account Access Control System (PAACS)	A model to enable the privileged accounts to be controlled, managed, and followed at minimum cost

	Lopez and Rubio (2018)	Risk-Based Access Control (RiskBAC)	Access control framework designed for highly dynamic environments, involving multiple organizations
	Vanickis et al. (2018)	FURZE (Fuzzy Risk Framework for ZTN	A policy management framework to implement risk-based AC in ZTN
	Ahmed et al. (2020)	AC Model for ZTA	A policy for protecting sensitive data when requests are made from both internal DMZ and remote locations
NAC	Muhammad et al. (2017)	AI-based Intelligent Filtering Technique (IFT)	Mainly focused on BYO. Use inter-arrival-time features to profile connecting devices, even when data is encrypted.
Sandboxing Security	Vasilescu et al. (2014)	Practical malware analysis based on Sandboxing	A virtual twin of a physical environment for executing and analyzing files for malware
IADS	Rosa et al. (2021)	Snort, Suricata, Bro	Open-source network-based IADSs with support for SCADA systems
Unidirectional Security Gateway	Heo et al. (2016)	UNIWAY	A Unidirectional Security Gateway that enforces reliability and security of transmitted data in ICS
	Ginter A. (*from Waterfall Security*) (2013)	Unidirectional Security Gateway for ICS	An explanation of how Unidirectional Security Gateway used in ICS work

Table 2.2: Summary of emerging technologies

** The author in this table only refers to where we found information about the technology or solution. In some cases, the author actually developed the solution, but in other cases, the technology was just discussed in their paper.

Chapter 3
Methodology

This chapter presents the research methodology used for the thesis. It starts by repeating the research question and describing the overall research design. Then the first section explains the approach used to answer our research question in light of the scientific method. The remainder of this chapter describes each of the four separate parts of this thesis. First, the literature review that was conducted and the rationale behind it, then the methodology used to define functional requirements and user stories. The following section describes how we identified threats and focus areas, and the final section explains the evaluation method used to develop the actual recommendations.

As previously stated, the overall research question is as follows:

> *How can new ideas and emerging technologies in remote access be applied in the development of improved remote access security recommendations for Norwegian petroleum companies?*

Figure 3.1 shows the research design for this thesis, with the four parts mentioned indicated by the outer boxes. The results from the literature review are presented in chapter 2, while the remaining three results are presented in chapter 4. The arrows between boxes are meant to show how we used earlier gathered data to produce later results.

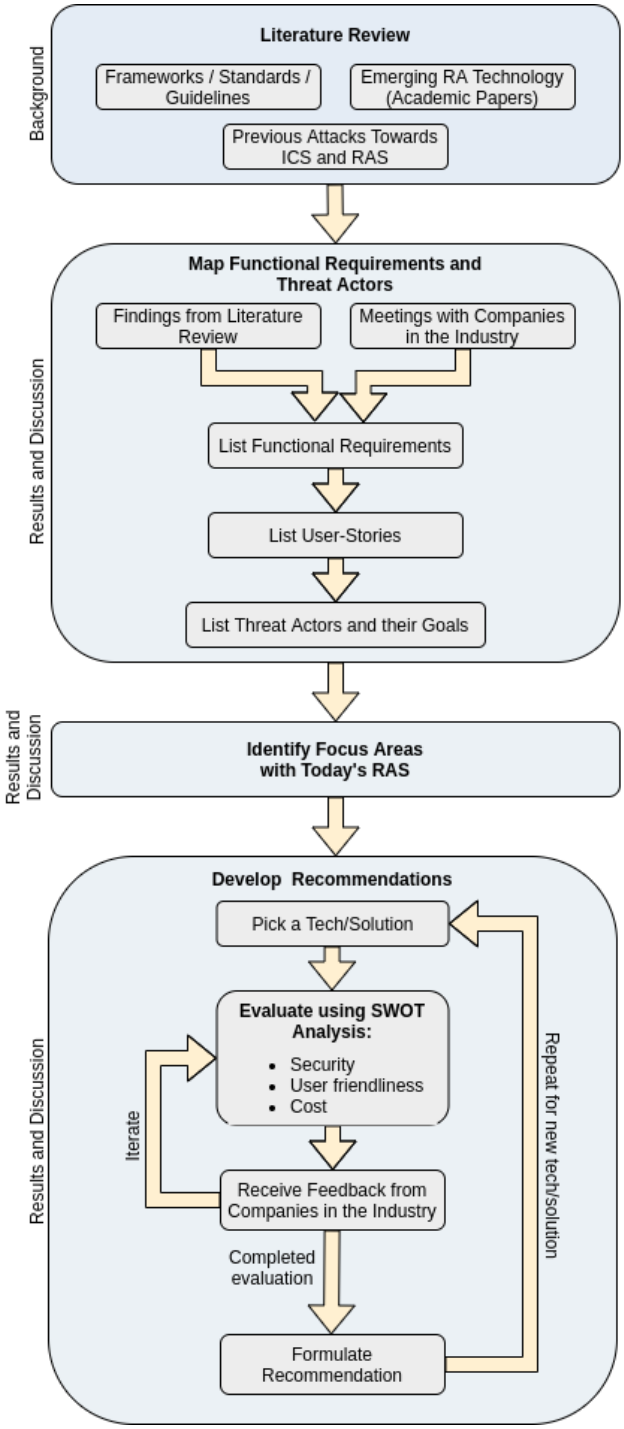


Figure 3.1: The overall methodology used for this thesis

3.1 Design Science

In the information system research cycle, design science is the process of creating and evaluating artifacts intended to solve identified organizational problems[HRM+04]. This differs from more standard research, which tries to explain or make sense of an existing reality. In short, the design science methodology can be summarized in the following three phases:

1. Identify a need/demand
2. Develop a solution
3. Justify/evaluate the proposed solution

A more thorough explanation can be seen in Figure 3.2. The figure is a modified version of the Design Science Information Systems Research Framework described by Hevner et al.[HRM+04]. It also highlights how this specific thesis relates to the design science methodology.

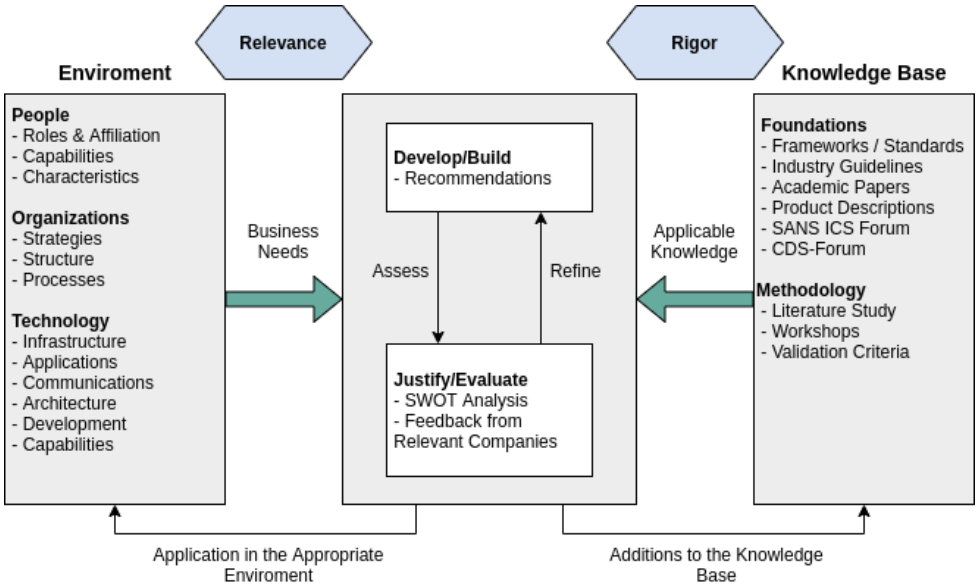


Figure 3.2: The Information Systems Research Framework, modified to reflect this thesis

Design science is inherently an iterative process. The final part of this research, with the actual development of improved solutions, will use The Generator-Test Cycle, as described by Herbert A. Simon[Sim19]. This will be further explained in section 3.5.

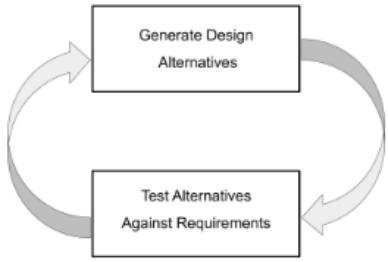


Figure 3.3: The Generator-Test Cycle

3.2 Literature review

At the start of this research, a literature review was conducted. As described by Christopher Hart:

> "*A literature review is an objective, thorough summary and critical analysis of the relevant available research and non-research literature on the topic being studied.*" [Har98]

The review was intended to give relevant background information into the chosen topic and provide the groundwork for the thesis's subsequent phases. Due to the nature of the topic area, the review was not restricted to academic papers. It also included frameworks and guidelines made by governmental institutions and private companies.

In the paper; *A Guide to Writing the Dissertation Literature Review*[Ran09], Randolph describes how conducting a literature review parallels the process for conducting primary research. With a few modifications to the well-known steps of the scientific method, the key components for a secondary research literature review are outlined as follows:

1. A rationale for conducting the review
2. Research questions or hypotheses that guide the research
3. An explicit plan for collecting data, including how units will be chosen
4. An explicit plan for analyzing data
5. A plan for presenting data

The rationale for performing the review and the project's research question has already been discussed. To ease the search process, we decided to divide the data

into different groups. This was done to better frame the search due to the large topic area needed to be covered. The first group consisted of standards, frameworks, and industry guidelines related to RA in ICS. Some of this is not publicly available, making the search dependent on industry contacts and access to proprietary sources. In the second and most important group, the focus was on emerging remote access technologies. Here the search was not strictly bound to industrial systems: we were also looking at innovative solutions used in different sectors. Finally, to better understand the current threat picture for ICS, the last group focused on papers describing previous cyberattacks towards industry networks, especially those where RAS were exploited.

Because the focus of this thesis lies on offshore installations on the NCS, we prioritized data related to this area. However, RA technology will have many similarities across different sectors and locations. Therefore this was not a strict exclusion criterion. For the data collection, the primary sources were Oria.no, Google Scholar, and ordinary Google searches. Data was also collected from sources not available to the public, like the SANS ICS Forum and Sintef's CDS Forum.

3.2.1 Groups for the Literature Review

Group 1 - Standards, framework, and industry guidelines: This group consists of relevant standards, frameworks, and guidelines focusing on cybersecurity in ICS. For this group, we did not use Google Scholar or Oria. The reason is that these documents are not normally found in academic databases. Frameworks are typically published by government institutions, commercial actors, or industry interest organizations. Furthermore, standards issued by institutions like IEC and ISO are often not freely available.

Group 2 - Emerging remote access technologies: For this group, the goal was to find new research and emerging technologies in the field of RA. Since the underlying principles have many similarities, the search was not restricted to studies exclusively on industrial systems. However, research with a focus on ICS tended to be prioritized. To simplify the search, we assembled a list of all relevant aspects within remote access and performed an independent literature review for each sub-category. While doing the review, new technologies were discovered, resulting in additional sub-categories added. The final list of topics was as follows:

- Virtual Private Networks
- Zero Trust and Zero Trust Network Access
- Demilitarized Zone
- Firewalls
- Access Management

- Network Access Control
- Sheep Dipping
- Sandboxing
- Intrusion and Anomaly Detection System (IADS)
- Unidirectional Security Gateway

Because the goal of this group was to find emerging RA technologies, a strict inclusion criteria when it came to the novelty of research was followed. Only research dated from 2013 and later was considered.

Group 3 - Cyberattacks towards ICS: In order to give guidance on how the security solutions for RA in ICS should be designed, it is necessary to understand how attacks have previously been conducted. For this group, the search was focused on previous cyberattacks towards industrial systems. Luckily, there are several studies dedicated to the mapping of such attacks, and compiling a list of relevant incidents was not difficult. Then, similar to the process for the previous group, we used this list to perform separate literature studies on each attack. The following topics were chosen:

- Stuxnet attack on the Iranian Nuclear Program
- Ukrainian Power Grid Attack
- Hydro Ransomware Attack

3.2.2 Backward- and Forward Snowballing

To further increase the number of relevant papers in our literature review, we performed limited backward and forward snowballing searches on interesting papers. As described by C. Wohlin[Woh14], backward snowballing is the process of going through the references of each paper found in the initial search to identify new papers. Accordingly, in forwarding snowballing, the method is to look for papers that have cited the papers already identified. However, this method was only relevant to the two last groups of the literature review.

3.3 Functional Requirements and User Stories

Having a clear understanding of the functional requirements tied to RAS is necessary for developing good security recommendations. These requirements will provide a frame for where the focus should be and what areas the proposed recommendations should prioritize. However, how to define such functional requirements is not a straightforward problem. A proposed solution is to structure this problem into the following five separate questions:

- Who needs access?
- From where is access needed?
- From what devices is access needed?
- What needs to accessed?
- What operations are needed upon access?

3.3.1 Initial Draft and Company Workshops

An initial first draft of functional requirements was defined based on these five questions. The standards, frameworks, and industry guidelines described previously were of much help in making this outline. For instance, Sintef report A1626 has a section describing different access modes, and both the IEC 62443 2-2 standard and DNVGL-RP-G108 define roles and responsibilities related to the operation of industrial systems. Here RA is divided into three coarse categories; no access, read-only access, and full read/write access. The CPNI report previously discussed features a comprehensive list of roles using a RAS. Furthermore, IEC 62443 and DNVGL-RP-G108 have detailed models describing the architecture of RAS to ICS.

Workshops with companies Alpha and Beta were then conducted to get feedback and initial thoughts on the draft for functional requirements. The workshops were structured as informal conversations. The rationale behind this was to make the attendees, who were security employees with leading roles in their respective companies, talk freely about issues with their existing solutions without the fear of being quoted. Based on input from workshops, the functional requirements were refined and somewhat shortened.

3.3.2 User Stories and Final Version

User stories are a popular method for representing requirements using a simple template such as; "*As a ⟨role⟩ , I want ⟨goal⟩ , [so that ⟨benefit⟩]*" [Coh04]. To further specify what functional requirements the RAS have, several such user stories were constructed. However, because these needed to answer all five questions mentioned above, their structure differed from the simple template formulated by Cohn. Therefore, to shorten the length of the constructed user stories, unnecessary words, such as "*as a*", were removed.

Together with corresponding user stories, the updated functional requirements were sent with a request for comment to the collaborators in companies Alpha and Beta. The final result is described in section 4.1.

3.4 Map Threats Actors and Identify Focus Areas with Today's Solution

In order to give security recommendations for the RAS used by Norwegian petroleum companies, it is vital to have a clear understanding of the threats the system faces. Therefore, in section 2.5 previous attacks against ICS were explored, with the reasoning "*know thy enemy.*" The same rationale holds here. Furthermore, to specify the thesis further, two focus areas were chosen. We first compiled a list of all potential threat actors and the goals they might have. After this, we identified two key aspects in the current RAS used by companies Alpha and Beta that will be the focus for the following evaluation.

The process of mapping possible threat actors and goals was split into two parts. First, we conducted a brainstorming exercise to map out every potential aspect related to this list. To not be influenced by outside factors, this was performed without using any sources other than our own knowledge on the subject. After this, we reviewed the outlined threat actors and goals in light of the results from several other academic papers and revised the original list. The final list is presented in section 4.2.

The focus areas were identified using the previously listed user stories, threats, and most importantly, feedback received in meetings with Alpha and Beta. The two key areas are described in section 4.3.

3.5 Development of Recommendations

In the final part of this thesis, the goal is to formulate recommendations for how RAS currently used by Norwegian petroleum companies can be improved. The first step of this process was to define what *improved* means and accordingly which criteria should be used to evaluate different solutions. Then, the next step was to break down the information gathered in the literature review and use this to identify the most promising technologies and solutions. This is the first part of the Generator-Test Cycle, named "*Generate Design Alternatives*" in Figure 3.3. The result of this was summarized in a set of tables. Below each of these tables follows a more thorough discussion of the elements listed. This discussion is meant to dive deeper into each solution's positive and negative aspects. It also serves as background information for the final part, where we use SWOT analysis and workshops with companies Alpha and Beta to evaluate the various solutions. This will be described in the following sections.

3.5.1 Criteria Used in Evaluation

To derive recommendations for the companies, we needed a method for measuring the usefulness of the previously explored technologies. For this, we chose to use a set of evaluation criteria. These were mainly chosen based on previous workshops we had with the companies Alpha and Beta and the two identified focus areas. It was essential to understand which aspects of a technology that was important to the companies in order to derive helpful recommendations. In the best way possible, the criteria are designed to evaluate whether specific new ideas or technologies better solve issues with existing RAS. In addition, the criteria will help assess the solution in its entirety, that is, how it facilitates the system's functional requirements while hindering the threats previously identified.

3.5.2 SWOT Analysis

In order to recommend one specific solution above another, a systematic and traceable process must be documented. The method is as follows; first, we formulate a possible recommendation, and then we perform an evaluation using a well-structured framework. For this, we chose a **S**trengths, **W**eaknesses, **O**pportunities, and **T**hreats (SWOT) analysis. This strategic analysis framework is meant to evaluate an organization's market position or an important business decision. Using SWOT analysis seems to be a good solution because it provides a framework for analyzing positive and negative aspects while at the same time identifying possible opportunities and threats. Academic papers have also used this method for evaluation related to cybersecurity in the past[RDRN$^+$20, FGG$^+$16].

For this SWOT analysis, it is important to explain how we chose to define the difference between strength/weakness and opportunity/threat. The former is defined as a well-established effect that is directly related to using one solution. For instance, a solution using a stronger encryption scheme directly affects the confidentiality of transferred data in a positive way and would therefore be defined under *Strengths*. The latter is defined as when a solution has secondary effects that might happen sometime in the future. For instance, an opportunity can be that the stronger encryption algorithm makes the company compliant with privacy regulations that might suddenly be posed on the industry in the future.

3.5.3 Workshops with Companies

After the initial SWOT analysis was completed, we scheduled meetings with security personnel in Alpha and Beta. The meetings were structured as workshops, and the aim was to get relevant feedback from actors in the field. Participants were high-ranking personnel working hands-on with the RAS and other aspects related to OT security in their respective companies. In the meeting, we presented different

technologies and solutions together with the related SWOT analysis. Then followed a discussion where the participants gave their initial thoughts and feedback. In addition, we used these meetings to clarify aspects that was unclear after reading the company's internal documentation regarding their specific RAS.

The SWOT analysis and company workshops formed the second part of the Generator-Test Cycle, named "*Test Alternatives Against Requirements*" in Figure 3.3. Here the various solutions or technologies were tested against our evaluation criteria and functional requirements. After the first workshop, as we used an iterative approach, the evaluations were modified and some solutions were added and removed. Then, we proceeded to do further evaluations and scheduled a final workshop with the two participating companies. Finally, modifications reflecting the received feedback were done, and a set of final recommendations were formulated.

3.6 Challenges and Limitations

This section addresses possible biases and limitations of the research in order to increase the research's credibility. It discusses the generalisability, reliability, and validity of the research that has been conducted.

A major part of our thesis is to look into academic research within the field of RA. Unfortunately, under the project's time constraints, it was not possible to conduct a systematic literature review. Accordingly, academic research that could have influenced our choices or presented new solutions may have been overlooked, thereby limiting the reliability of the results.

The other primary source of information for this thesis has been companies Alpha and Beta. They have provided insights into the industry through meetings and workshops, and given important feedback on our tentative recommendations during the iterative process. Having conversations with only two companies allowed us to have multiple in-depth meetings and understand specific needs and issues with their RAS. Under this thesis's time constraints, having such in-depth discussions with more companies would not be feasible. However, meetings with more organizations could have given a more comprehensive understanding of RAS on the NCS, highlighting different issues. This weakens the generalisability of this thesis and may affect the applicability of the recommendations and results to other companies working on the NCS.

3.7 Ethical Considerations

A significant ethical concern for this thesis is the possibility of leakage of sensitive information. This could expose companies Alpha and Beta to dangerous cyberattacks,

and therefore measures to protect their identity were taken. Firstly, each company was anonymized using pseudonyms (these companies are not actually named after greek letters). Secondly, before getting access to the companies' internal documentation and scheduling meeting we signed Non Disclosure Agreements with both companies. Finally, both companies received drafts before the thesis was delivered. In this way, they were able to ensure that no sensitive information had been disclosed.

Chapter 4
Results and Discussion

This chapter presents the findings that have been derived based on the information presented in the previous chapters and from meetings with company Alpha and Beta. First, section 4.1 presents the functional requirements and user stories. Next, in section 4.2, threats to the RAS are outlined, and identified focus areas with today's RAS are presented in section section 4.3. Then section 4.4 evaluates different solutions and discusses developed recommendations, and finally, section 4.5 presents the final recommendations.

Furthermore, we have chosen to combine results and discussions into a single chapter. This is because the results in this thesis are so dependent on the discussion and would not make sense standing alone. Therefore, this section both present the results and discusses the rationale behind them.

To reiterate, the research question of this thesis is:

> *How can new ideas and emerging technologies in remote access be applied in the development of improved remote access security recommendations for Norwegian petroleum companies?*

To answer this, we followed the method outlined in chapter 3. The sub-research questions helped us in the process and are therefore sequentially answered first.

4.1 Functional Requirements and User Stories

Functional requirements and user stories are seen as essential for deriving threats and further exploring improved solutions for remote access. The following section, and the next one, seeks to answer the sub-research question below:

> **Sub RQ A:** *What are the functional requirements and threats related to a state-of-the-art remote access solution for Norwegian petroleum companies?*

As previously explained, the functional requirements presented have been derived in an iterative process, with feedback from Alpha and Beta. They are intended to highlight different components of a RAS and what functionalities that are expected from the system. The functional requirements are divided into five categories, containing 22 requirements in total. Each category is assigned a unique color; this is meant to simplify the later construction of user stories.

4.1.1 Explanation of Terms Used in Functional Requirements

Regarding the actors in the *Who* part, *system operators* are defined as company employees that use the RAS to work on the platform. *Managed service providers* are any third-party suppliers that interact with the RAS, for instance, to perform updates on components they have delivered. *Field technicians* are on-site personnel, often involved in more physical labor. Finally, *system support specialists* are company workers that use the RAS to aid other personnel. They do not use the RAS to perform any actual work themself, but rather help others do their work if needed. They are not necessarily OT personnel; they can also be IT employees or general supporting staff.

From what contains four terms. Firstly, a *dedicated remote access desktop* is a computer located in a secure location within the corporate office of either the operating company or a third-party vendor. It is generally the most secure way of accessing any RAS. As described in the previously mentioned report by Homeland Security and CPNI[SC], this computer should solely be used for remote access. It is centrally managed and hardened with a baseline image specific for remote access needs. Furthermore, it should have appropriate cybersecurity countermeasures, like antivirus and host-based IADS. The next term, a *corporate computer*, is a computer owned by the operating company. Its security functions are configured and maintained by the organization, making it more secure than what can be expected from a *personal desktop*. This, as the name shows, is owned by personnel working in the organization and will have fewer restrictions in terms of what software can be installed. Lastly, a *personal tablet or phone* has similar characteristics to the personal desktop. However, these can often be more secure because of restrictions on installable software imposed by the Apple and Android operating systems. On the other hand, phones and tablets are more likely to get lost or stolen, which may cause security incidents as well.

The functional requirements in the category *From where* are divided up into four subcategories. *Offshore via remote access* means that the ICS are accessed from

within the offshore platform. The ICS can also be accessed from an *onshore control room*. This is regarded as the most secure remote connection point because the room is located within the organization's network and usually imposes strict access control. However, while relevant to include, these two access points are considered outside the scope of this thesis. The last two subcategories are *onshore, inside the corporate network* and *onshore, outside the corporate network*. These categories emphasize whether the ICS are accessed directly from the operating company's corporate network or if the client is connecting from outside this network, such as a home network or the network of a third-party vendor.

In the category *systems and zones to be accessed* the first system is the *platform industrial DMZ*. This refers to the industrial DMZ, serving as the gateway between the internal platform network and the corporate network. This zone is typically accessed if work or configurations has to be done on devices located within this DMZ. Additionally, all other traffic going to the internal ICS have to go through this zone. The *internal platform network* is a trusted network protected behind the IDMZ referred to as level 2 and 3 in the Purdue model. Here, engineer workstations are located, together with other services like the historian, domain controllers, and the application-, database- and IO servers. Next, *network switches* are devices on the data link layer responsible for forwarding packets based on MAC address. These are placed in multiple zones within the internal network and can normally be accessed via the RAS configuration. *Specific SCADA and DCS systems* refers to the several different SCADA or DCS systems that control and monitor industrial processes running on the offshore platform. This subcategory contains actual ICS that interact directly with devices managing physical processes. Nowadays, the distinction between SCADA and DCS has disappeared mainly because faster computers and bandwidth expansions allow even wide-area systems to handle large amounts of data[Bot16]. While industry experts still distinguish between the two (SCADA being centralized and data-gather oriented, and DCS distributed and process-oriented), they have been combined into a single subcategory in this thesis. Finally, *industrial safety systems* are different from the previous category in that they are not meant to control processes. Instead, these systems are solely meant as protection mechanisms that will securely shut down processes when a dangerous situation is imminent.

Read values using a controlled client/program refers to the case when a user has access to a client or program that displays monitoring values from the offshore platform. This allows users to get valuable system information, but at the same time, restricts the user from interacting any further with the internal system. *Support using read-only video* is when onshore personnel need to help employees on the platform with technical solutions or aid in some other way. This is performed through a read-only video stream so that the onshore employee sees the screen of the field technician to facilitate the assistance better. *Upload files* is when a user needs to upload a

file to a system on the offshore platform. This could be for software updates or, in other ways, configure a remote system. *Perform task via controlled client/program* is the case when personnel needs both read- and write access to perform a task. The controlled program is similar to what was previously mentioned. Finally, *perform task via full terminal access* is similar to the previous case, but now the user is not bound by a client or program. In this case, the user has full terminal access to the remote computer.

Who

- System operators
- Managed service providers (third-party suppliers)
- Field technicians
- System support specialists

From what

- Dedicated terminal desktop
- Corporate desktop
- Personal desktop
- Personal tablet or mobile

From where

- Offshore via remote access
- Onshore control room
- Onshore, inside the corporate network
- Onshore, outside the corporate network

Network to be accessed

- Platform industrial DMZ
- Internal platform network (Purdue level 2/3)
- Network switches (for SCADA, DCS, Telecom..)
- Specific SCADA and DCS systems
- Industrial safety systems

To do what

- Read values using controlled client/program
- Support using read-only video
- Upload files
- Perform task via controlled client/program
- Perform task via full terminal access (read/write/execute)

4.1.2 User stories

The following user stories were compiled from the above-listed functional requirements. They aim to describe different ways in which a RAS can be used. No considerations with regards to security were made in this process. For instance, user story 4, where the internal platform network is accessed from a personal computer outside the corporate network, might pose a greater risk than what should be allowed. There are 21 user stories, each compiled together using an element from all five categories of functional requirements. As aforementioned, the five different color codes are tied to the functional requirements.

1. A system operator wants to, from a dedicated terminal desktop inside the corporate network, access the critical safety systems, upload a patch file, and use a controlled client/program to perform a critical update.
2. A system operator wants to, from a dedicated terminal desktop inside the corporate network, access a specific SCADA- or DCS system and perform tasks via full terminal access.
3. A system operator wants to, from a corporate desktop inside the corporate network, connect to the internal platform network and perform tasks via a controlled client/program.
4. A system operator wants to, from his/her personal desktop outside the corporate network, access the internal platform network to perform tasks via a controlled client/program.
5. A system operator wants to, from his/her personal tablet or phone outside the corporate network, access a monitoring system to perform tasks via a controlled client/program.
6. A system operator wants to, from a corporate desktop outside the corporate network, access a monitoring system to perform tasks via a controlled client/program.
7. A system operator wants to, from a corporate desktop inside the corporate network, access the platform industrial DMZ to perform tasks via full terminal access.
8. A system operator wants to, from a corporate desktop inside the corporate network, access network switches to perform tasks via full terminal access.
9. A system operator wants to, from a corporate desktop inside the corporate network, access the platform industrial DMZ to perform tasks via full terminal access.

10. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access the critical safety systems, upload a patch file, and use a controlled client/program to perform a critical update.

11. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access a specific SCADA- or DCS system and perform a task via a controlled client/program to update some devices.

12. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access network switches and perform a task via a controlled client/program to update the devices.

13. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access a specific SCADA- or DCS system and upload several patch files.

14. A managed service provider wants to, from a dedicated terminal desktop outside the corporate network, access a specific SCADA- or DCS system and perform a task via a controlled client/program to update some devices.

15. A managed service provider wants to, from a corporate desktop outside the corporate network, access a specific SCADA system to perform tasks via a controlled client/program and check that systems are properly managed.

16. A managed service provider wants to, from a corporate desktop outside the corporate network, access a monitoring system to perform tasks via a controlled client/program.

17. A system support specialist want to, from a dedicated terminal desktop inside the corporate network, start a connection to any system on the platform for support using read-only video to aid people on the platform

18. A system support specialist want to, from a dedicated terminal desktop inside the corporate network start a connection to the internal platform network and perform task via full terminal access to help users with system management

19. A system support specialist want to, from a corporate- or personal desktop inside the corporate network, start a connection to a specific SCADA- or DCS system with read-only via video to aid people on the platform using a SCADA or DCS system

20. A system support specialist wants to, from a corporate- or personal desktop outside the corporate network, start a connection to the internal platform network and perform task via full terminal access to help users by performing access management

21. A system support specialist wants to, from a corporate- or personal desktop outside the corporate network, start a connection to a specific SCADA- or DCS system with read-only via video to aid people on the platform using ICS.

The process of writing user stories highlighted new issues with the existing functional requirement. With these in mind, an updated version was defined. Additionally, the user stories also made it apparent that the current scope was too broad. Therefore, some functional requirements will not be focused on in this thesis and were abandoned to narrow the scope further. These are seen as "grayed out" in the above list.

4.2 Threats Actors and Goals

This section briefly explains the actors that have been identified as potential threats to the RAS reviewed in this thesis. In order to give a better understanding, both the actors and their possible reasons for an attack are included. We followed the method described in section 3.4. This section presents the second part of the answer to sub-research question A. In order to provide the industry with valuable recommendations, it is essential to have a clear view of possible threats the industry faces. Understanding these aids in pinpointing which technologies would provide the best solution.

4.2.1 Explanation of Terms Used in Threats Overview

This section describes the type of actors that may conduct an attack on the RAS. *Nation-state* actors, often coined *advanced persistent threats (APTs)* in security settings, are typically a nation's intelligence service or an organization connected to a nation-state conducting actions on their behalf. They have highly skilled hackers and substantial resources at their disposal. On the other end of the scale, a *script kiddie* is a novice hacker that uses premade programs and scripts to conduct simple attacks. More professional hackers performing attacks for financial gain fall under the term *cyber criminal*. Furthermore, regarding insiders that may perform an attack there is the *unintentional insider* and *intentional insider*. The *unintentional insider* may mistakenly cause damage to a system with, for instance, a wrong configuration. An *intentional insider*, on the other hand, is an individual who performs an attack with actual intent. This can be because an employee, or third-party supplier with sufficient access rights, is in conflict with the company. *Competitors* are fairly self-explanatory. These are other companies in the industry willing to break the law to get a competitive edge. *Cyber terrorists* are individuals using the internet to cause others harm, either for political- or ideological gain. Finally, *cyber activists* are individuals, usually members of an organization, that work to achieve a political or

social change. Contrary to terrorists, they are most likely not willing to cause actual harm to other people.

There can be several motives behind a cyberattack, and the reasons are mostly tied to the type of actor behind it. Firstly, the goal of *financial gain* is fairly self-explanatory; the attacker wants to earn money. Ransomware attacks fall under this category. *Hinder production* is the act of making a system unavailable, or in other ways make it impossible for an organization to operate normally and generate revenue. Then, two goals connected to the exfiltration of information are *intellectual theft* and *intelligence*. *Intellectual theft* is the process of stealing high-value intellectual property that is not publicly available, whereas *intelligence* is when espionage is used to gather information about critical infrastructure or other information that is of relevance to the attacker. The next goal, *terrorism*, is when an attacker wants to cause harm, either for political- or ideological gain. Finally, *publicity* is a goal when the attacker just wants attention. This can be an activist move to promote a political cause or simply a hacker looking for recognition and media attention.

It is important to note that these categories are overlapping. For instance, ransomware will also hinder production, intellectual theft is often part of an intelligence operation, and terrorists also want publicity.

Who
- Nation-state (APT)
- Script kiddie
- Cybercriminal
- Unintentional insider
- Intentional insider
- Competitors
- Cyber terrorist
- Cyber activist

Goal
- Financial gain
- Hinder production
- Intelligence or intellectual theft
- Terrorism
- Publicity

4.3 Identified Focus Areas

To further specify the scope of our thesis, key aspects with the solution currently used by our collaborating companies needed to be identified. To address this sub-research question B asked the following:

> **Sub RQ B:** *What are the key focus areas with the remote access solutions used by Norwegian petroleum companies today?*

After a thorough evaluation of gathered information from literature studies, workshops with companies Alpha and Beta, and the structuring of functional requirements and threats, the following focus areas with today's RAS used by Norwegian petroleum companies were defined.

- The companies we collaborate with have issues with **access management** in their RAS. Work permit systems are cumbersome and manually managed, meaning that users have to be manually added and deleted. This leads to high costs because of wasted time and frequent use of technical support.
- According to companies Alpha and Beta **file transfer** is an important feature in the RAS. Especially third-party contractors use this periodically to update devices, meaning that personnel from outside the operating company regularly transfer files into OT environments. While working solutions exist, as this poses a major attack surface, there is still room for improvement.

User stories 1, 10, and 13 all revolve around transferring of files and the risk it introduces. None of the user stories deal directly with AM, as this is related to the management of the RAS and not a task performed with it.

4.4 Evaluation

The following section presents an evaluation of a subset of the technologies explored in chapter 2 Background. It was not deemed meaningful to evaluate all the solutions from the literature review independently, and some were instead integrated into other solutions. The choice of which solution to evaluate was taken based on workshops with companies Alpha and Beta and the identified focus areas. The evaluation has been divided into three sections: *network access security architecture*, *firewalls*, and *other solutions*, where the latter describes several solutions not directly related to each other. Each section features a summation of the different solutions with regards

to our evaluation criteria. Then follows a discussion, and finally an analysis to find the best security recommendation.

To reiterate, the sub-research question answered in this section:

Sub RQ C: *How can specific technologies improve existing remote access solutions with regards to the identified focus areas?*

In order to answer this sub-question, the method explained in section 3.5 was followed. Each technology is evaluated with regards to the focus areas presented in the previous section and on the following criteria: security, user-friendliness, and cost-effectiveness. With this, the aim is to understand how introducing a possible solution would improve the existing RAS. The following paragraphs give a brief definition of the criteria used in the evaluation.

- The *security* criteria revolve around how a given solution or technology realizes the CAIC model mentioned earlier, with the four goals (in decreasing priority): *control, availability, integrity, and confidentiality*. Due to our selected focus areas, we primarily look at how it increases the security of file transfers.
- *User-friendliness*, or *usability*, defines how a technology or solution makes the system easier to operate. The main focus is on making the system easier for administrators, and in this way, requires less AM. This definition means that a technology enabling automation has high user-friendliness because it removes the need for human interaction altogether. However, simplicity for end-users is also included when evaluating user-friendliness.
- The *cost-effectiveness* is simply how effective a technology or solution is with regards to keeping costs at a minimum level. This includes capital costs (purchasing a product), maintenance costs (internal employees or third-party support), and cost of implementation (installation and configuration). In addition, if a solution is hard to use, the cost is also increased due to less effective employees and frequent use of technical support.

4.4.1 Network Access Security Architecture

The first technology solution that will be evaluated relates to the overall network access security architecture used for the RAS. The solution chosen here affects both of the identified focus areas; a better access solution will simplify AM and make file transfers more secure. We found that companies Alpha and Beta both have a combination between ZTA and perimeter-based security; we have given this solution the term "*enhanced VPN*". This solution is part of a Commercial off-the-shelf (COTS) product delivered by a third-party vendor that will remain anonymous. The term

enhanced is used because the VPN solution is more than a simple tunnel. It features several security mechanisms such as client-NAC, MFA, and separate access rights (read/write).

During the literature review, several sources recommended abandoning the old perimeter-based approach and instead build an architecture based on the security principle of Zero Trust. This ZTA, with ZTNA/SDP as the access technology, might better solve the earlier mentioned focus areas and provide overall increased security and user-friendliness to the RAS. However, implementing such a system would need a complete rework of the network architecture, and this may not be possible for an offshore platform in-operation. Therefore the table also contains a hybrid option with a granular transition towards a ZTA without removing existing security infrastructure. The following section will evaluate whether a Zero Trust approach would improve the RAS used by Norwegian petroleum companies compared to the old perimeter-based enhanced VPN solution.

Solution	**Security**	**Usability / user-friendliness**	**Cost-effectiveness**	**Proprietary?**	**Novelty**
Perimeter-based with enhanced VPN	Single perimeters that defend different levels. VPN gives users access to resources on a specific security level. Can also be restricted to some degree. For instance to a subnet or workstation (using RDP).	A well-established technology/method that most people are familiar with.	Low capital cost	Both open-source and proprietary solutions exist.	Old idea, but new solutions are emerging here as well
ZTA-based with ZTNA	No single perimeter, rather protects separate micro-segmented resources within the network. Using RiskBAC and IADS with a wide array of data points. One centralized access control manager for all connections	Clearly defined IAM with a single access control engine. A new solution that might lead to additional administration and user support	High capital cost because of micro-segmentation and implementation of new technology	Most solutions are proprietary but open-source solutions also exist.	Relatively new concept
Hybrid ZTA-based and Perimeter-based VPN	Gradually migrating to ZTA starting with the most critical infrastructure	Give users time to familiarize themself with a new system	The longer migration process leads to a more gradually running cost	Combination	Combination

Table 4.1: Zero Trust Solutions Summarized

The actual VPN protocols (IPSec, L2TP...) used in the solution deployed by Alpha and Beta are state-of-the-art, based on data gathered in our literature review. They will therefore not be a topic for any further discussion. However, even using secure protocols, the principle of *least privilege* is still important. The perimeter-based and ZTA combination solves this to some degree; as explained in subsection 2.4.1, a VPN connection can tunnel a user to a specific subnet and restrict all access to the overall internal network. The network is horizontally segmented following the architecture of the Purdue model, and also have some degree of vertical micro-segmentation on each level. However, OT devices, like PLCs, often have little capabilities compared to devices found in IT networks. This makes it difficult to follow the Zero Trust principle, where every device is a separately segmented resource. Still, it should be

possible by using virtual separation methods such as Software-Defined Networking (SDN) and firewall rule sets.

As shown in user stories 1, 10, and 13, several different users, both company employers and third-party suppliers will access the RAS. This makes the concept of Zero Trust very helpful; if a third-party supplier needs to transfer patch files to a critical system, the access should be restricted to solely this one system, not the entire network. This means that, with regards to the Intentional insider threat actor described earlier, a Zero Trust solution with complete segmentation of every resource would provide better security.

There are, however, other aspects of Zero Trust that Alpha and Beta have yet to implement. Tenet 5 and 7 listed in NIST SP-800-207 described the use of continuous system monitoring and anomaly detection. In the case of leaked credentials or an exploited zero-day, a properly deployed IADS significantly increases the chance of detecting an attacker. This is especially important in the case with APTs like nation-state-backed hackers because these have the capabilities to circumvent other security barriers. The paper mentioned in subsection 2.4.9 by Rosa et al. lists several detection systems aimed at OT environments. Some are signature-based and run on protocols like Modbus and DNP3, while others are anomaly-based using machine learning. Anomaly-based systems will also be very effective in ZTA due to the large amount of data available for the ML algorithm.

Another aspect of Zero Trust is the well-defined access management mechanisms that can be helpful when several different clients use the system. As of now, both our collaborating companies use a work permit system based on NOG-088. This system is very generalized and used for anything from physical maintenance on the platform to remote monitor access. Its primary purpose is to maintain the continued safety of the offshore installation, for instance, by ensuring that a device is not remotely accessed while being used by an on-site engineer. This means that when issuing work permits for the RAS, cyber threats could easily be neglected compared to other more physical concerns. Therefore, a possibility with a ZTA is to separate cybersecurity from the other aspects of the work permit. Administrators manually issuing permits will then only need to think about safety and operational aspects. Cyber evaluations, such as checking the security posture of the client and the criticality of the requested resource, could be handled by an Access Control Engine, as described in the previously mentioned BeyondCorp architecture. This combination of role-based access control and risk-based access control is described in subsection 2.4.6, together with a discussion about two frameworks for enforcing access policies in ZTA.

When it comes to validating users connecting to the RAS, the system is dependent

on a network access control mechanism, as described in subsection 2.4.7. This is already implemented in the solution used by Alpha and Beta, where it is verified that a device has up-to-date antivirus before access is granted. However, ZTA sets additional demands to the NAC solution that are currently not implemented by our collaborating companies. For example, in ZTA, the NAC should analyze all available data regarding the behavior and environment of the connecting user/device pair. A big part of this requires behavior analysis where the NAC can detect suspicious actions by a connecting user. This would, for instance, be a user that normally only connects to the RAS during work hours, suddenly attempting to gain access in the middle of the night. If the connecting IP also originates from a different county, the NAC would most likely flag this as suspicious and raise an alarm. The machine learning approach for NAC proposed by Muhammad et al. in subsection 2.4.7 is interesting as this also addresses BYOD environments.

Regarding user-friendliness, one can argue that ZTA is more cumbersome for end-users because the principle of "*never trust, always verify*" could lead to a more frequent need for authentication. But this stricter policy may also positively affect the process of AM and thus increase the user-friendliness of the overall system. Employees in companies Alpha and Beta say they spend unnecessary much time with access management. The thorough process needed to produce work permits can partly explain this problem. This process is often handled manually and required before granting all new users access to the system. Even though a work permit system is integrated into Alpha- and Beta's RAS, this process still causes many delays and technical support costs. Assuming that the micro-segmentation of resources is sufficiently trusted, the case can be made that many situations would not need such a thorough review before a work permit is granted. If a new user needs access to a system with low criticality, in ZTA only this one system would be affected. Further assuming that the network is compliant with the IEC 62443 3-2 standard, all zones and conduits should have established Security-Level Targets defining the risk tolerated with accessing each system. This would drastically decrease the threat of granting access because, if a new user has malicious intent, lateral movement from the initial point of access would be impossible.

Furthermore, the ultimate goal would be to automate the entire cybersecurity aspect of the AM process. The agile methodology of Client-Initiated ZTNA, where the access boundary is created based on well-defined identity- and context parameters, could better facilitate such automation.

As a final point, it is interesting to see that even though both our collaborating companies' solutions use aspects from ZTA, their employees were, for the most part, not familiar with the Zero Trust model, nor was it ever mentioned in their internal security documentation. This shows that Zero Trust principles seem to be a

natural way forward for securing modern networks, even without following specific architecture frameworks such as Google's BeyondCorp. We also noticed this effect in current cybersecurity research. For instance, the RA VPN solution described in the previously mentioned paper by Nyakomitta et al. does not mention Zero Trust; however, it uses several of the same principles.

Migrate from the existing solution to a ZTA with ZTNA?

SWOT Analysis

Strengths		Weaknesses	
	Security • Microsegmentation limits lateral movement in the network • Protects against DDoS since internal network resources are hidden • RBAC and RiskBAC using large amounts of data points • Continuous monitoring and anomaly detection • Client-side NAC evaluating all available data (behavioral and environmental attributes) **User-friendliness** • A single network access controller • Less manual AM for administrators **Cost-effectiveness** • Simplified AM with fewer costs to administration and technical support		**Security** • Loss of availability during migration **User-friendliness** • System administrators not familiarized with the new system • High segmentation and frequent authentication affect the productivity of employees **Cost-effectiveness** • Capital cost of buying a new COTS product • High implementation cost (micro-segmentation, adding new tech, etc..)
Opportunities	• Facilitate further automation of AM • Simplify the movement into cloud-based solutions • Company gets recognition from being an early adopter of new technology • More attractive company for security- and other IT/OT personnel	Threats	• Misconfigurations when implementing a brand new architecture • Issues ending the contract with existing vendor (if they do not offer a ZT solution)

Table 4.2: SWOT Analysis ZTA

As shown in the above SWOT analysis, a ZTA has benefits over perimeter-based architecture with regarings to both security and user-friendliness. While the capital costs are higher, a simplified AM could make up for this with fewer expenses going

to administration and technical support. However, the major weaknesses are not coming from the architecture itself but rather the migration process. This was also reflected in feedback received from workshops with companies Alpha and Beta. Their employees stated that the complexity and cost of completely reworking the RAS architecture in a brownfield project are too large. In addition, the introduced risk during migration could also outweigh possible benefits. Especially when the existing solution already is, according to the majority of employees and company leadership, sufficiently secure.

Therefore, and because many of the Zero Trust principles are already implemented, the hybrid approach seems a better fit for this case. More segmentation can be performed gradually, and other ZT aspects not yet implemented can be added. This hybrid solution was proposed in NIST SP 800-207, where they resonated with the improbability of major enterprises being able to migrate into ZT in a single technology refresh cycle. The report also features steps explaining how to switch from perimeter-based architecture to ZTA.

We can now formulate our first proposed guideline to improve the RAS used by Norwegian petroleum companies.

To better the overall security, as well as simplify Access Management, Norwegian petroleum companies should use a hybrid approach between perimeter-based security and Zero Trust Architecture, where they continually add security barriers based on Zero Trust principles.

Additional Zero Trust security barriers that could be added:

- *Enforce system-wide continuous network monitoring in combination with machine learning-based anomaly detection. This includes support for monitoring OT-specific protocols.*

- *Integrate a risk and identity-based access management architecture as described above in order to remove workload from the work permit system.*

- *Upgrade the existing NAC mechanism to include user/device behavior and environmental factors such as client use patterns and IP geolocation.*

In summation, this recommendation highlights the security benefits that come with a Zero Trust model while at the same time recognizing that changing existing solutions on brownfield projects is a gradual process.

4.4.2 Firewall

The type of firewall deployed can affect both network security and the administration needed to manage the solution. A remote connection carries data, like packets part of a file transfer or OT protocol-specific messages, from the public internet into the internal IT- or ICS/SCADA network. In order to discover malware or malicious network traffic, it is crucial to have a firewall that inspects these packets properly and is able to uncover incidents that may compromise the security of the organization's network. In the literature review several, different firewall alternatives that would improve the security of an ICS were discovered.

The table below outlines the different firewalls presented in chapter 2, focusing on our chosen evaluation criteria.

Solution	**Security**	**Usability / user-friendliness**	**Cost-effectiveness**	**Proprietary?**	**Novelty**
Traditional firewall	Implement security policies that filter traffic going in and out of a network based on port, protocol, and source- and destination address. This can restrict the source and destination addresses to be within the addresses of the organization and third party.	Simple functionality and a well-known type of firewall	Well-established solutions and relatively cheap to implement Exist free community editions of open-source solutions	Both open-source and proprietary solutions on the market Open-source solutions for firewalls with filtering capabilities on layer 3 and 4 of the OSI model	Old concept

NGFW	Can perform filtering on the same criteria as traditional firewalls. Additionally, can set application-specific rules, thereby perform deep packet inspection and encrypted packet inspection. With NGFW, uploaded packages could be better analyzed. Several security tools are merged into one with NGFW.	Need skilled resources that can understand the complex ruleset syntax. To maintain the firewall. The complex firewall rules can introduce delays in the network. However, added complexity is on the administration and not the end-user.	A more complex solution that is more expensive to buy from vendors. Expensive to configure/operate as this type of firewall has more functionality. There are community editions on the market that offer some NGFW capabilities to open-source firewalls for a far cheaper price than the commercial editions [Inc20].	The underlying idea is not proprietary. But to our knowledge, there are no open-source NGFW.	Relatively old idea, but advances within machine learning and other modern technology has led to more sophisticated capabilities for this type of firewalls.
SCADAWall	Does not have all the functionality that NGFW comes with. However, it should be able to inspect SCADA commands and prevent intelligent attacks by using the three algorithms CPI, PIPEA, and OSDA.	Requires knowledge about iptables in Linux for configuration. It is not a commercial solution, which often leads to a more complex configuration/operation for the administration. Can lead to increased delay on the ICS network.	Open-source and free to use without any purchase. However, high complexity may lead to large implementation costs.	Open-source	Relatively new solutions

OT firewalls	OT firewall with NGFW capabilities. Can then perform filtering and DPI on OT-specific protocol messages. Makes it possible to whitelist allowed ICS commands. Can increase the system's ability to defend against attacks on the protocol.	Requires knowledge about how to configure/operate the firewall. The administrator needs to have an understanding of the OT protocol used.	The implementation of open-source solutions, such as iptables, requires both knowledge and money in the form of the time of the personnel that configures and operates the open-source solution. Commercial solutions are often expensive but require less time invested from the organization.	Both open-source and proprietary	Relatively new solutions

Table 4.3: Firewall Technologies Summarized

The capabilities needed from a firewall are dependent on its placement in the network. For example, internet-facing firewalls should be more focused on IT, while firewalls further into the industrial network should be more focused on OT protocols. However, for both of these, the capabilities provided by NGFW would significantly increase the security of the networks. The following section will give an analysis of NGFW in an IT environment.

It is essential not to be too narrow when recommending specific technology, as solutions regularly becomes updated, which again leads to outdated recommendations. However, something like NGFW is not a specific technology. Instead, it can be seen as the concept of inspecting packets more thoroughly than previous generation firewalls. Therefore, we can give a more precise recommendation when it comes to the capabilities a perimeter firewall should have.

Companies Alpha and Beta stated that file transfer was a focus area for them, as it poses a significant attack surface. The user stories 1, 10, and 13 revolve around uploading files into the internal network. A firewall that can discover security issues during file transfer is therefore highly recommended. As mentioned in subsection 2.4.5, NGFW is the most novel generation of firewalls. It combines multiple security

technologies and can inspect files better than previous generations. For instance, it has built-in capabilities of malware detection and intrusion prevention. This makes the system able to respond to security incidents faster than with a traditional firewall. Furthermore, the addition of DPI adds the ability to identify malicious software before it can infect the network. Therefore, it would be beneficial to use NGFW with DPI to improve the robustness of the network with regards to malware attacks as the result of a malicious file transfer.

However, NGFW has some disadvantages when it comes to cost-effectiveness and user-friendliness. Commercial NGFWs are costly, and the price increases with every capability added to the firewall. They also have a complex configuration process and can be challenging to operate. This makes NGFW prone to misconfigurations. It can also pose a threat if an organization does not keep personnel updated on the technology of the firewall. Fortunately, this added complexity does not affect end-users but only the personnel that is managing the firewall. However, the end-user can experience latency issues, as an NGFW can lead to an added delay in network traffic.

Start using Next-generation firewalls?

SWOT Analysis

Strengths	**Security** • Deep packet inspection provides improved malware protection • Reduced risk from all threat actors, especially *intentional insider* and *nation-state* • Provides multiple security technologies in one package **User-friendliness** • Widespread technology, well understood and with good documentation • Easier administration of merged security technologies **Cost-effectiveness** • Reduced cost from the centralization of several security technologies	Weaknesses	**Security** • None **User-friendliness** • Can lead to latency for end-users • Need for skilled personnel to operate **Cost-effectiveness** • Higher maintenance cost than more primitive firewalls • Higher capital cost than more primitive firewalls
Opportunities	• Expand the security tools deployed in the network • Can identify traffic by user and provide application control at an individual level	Threats	• Misconfigurations on implementation

Table 4.4: SWOT Analysis Next-generation Firewalls

Based on this analysis and workshops with companies Alpha and Beta, we can formulate the following recommendation regarding the usage of firewalls in the RAS used by Norwegian petroleum companies.

To better secure third-party file transfer, Norwegian petroleum companies should use a Next-generation Firewall with deep packet inspection and intrusion prevention systems at the network perimeter (Purdue level 3.5).

The above recommendation is specific for firewalls governing IT networks, and the next section will analyze the usage of NGFW in OT.

While bringing NGFW capabilities into an OT firewall gives several security benefits, it can also pose a big challenge. These firewalls govern traffic containing OT-specific messages and therefore need to understand OT protocols in order to implement NGFW capabilities. However, several major companies have over the last years developed NGFW for industrial systems. Additionally, as mentioned in subsection 2.4.5, SCADAWall is an open-source alternative that can perform DPI on OT-specific protocol messages. As these types of firewalls become more available on the market, it could be beneficial to implement them in the RAS.

As mentioned earlier, recommending a specific solution, such as SCADAWall, would not be sustainable in the ever-changing field of industrial cybersecurity. However, the general idea of having OT-specific firewalls at the perimeter of or inside the industrial network has great potential. These firewalls can protect the ICS against various attacks on OT-specific protocols, such as Modbus, DNP3, and CIP. Deep packet inspection also makes it possible to configure the firewall so it only allows specific protocol commands, which also can increase the user-friendliness of the solution. For example, a notification can be sent to end-users to inform them if they have performed an invalid command. As stated in NIST SP 800-82, firewalls in the OT environment can contribute to a significant increase in the security of ICS environments, as well as improve the responsiveness of the network.

NGFW capabilities brought to an OT firewall make it capable of stopping security incidents using IPS. Company Beta stated that a firewall with these capabilities could have prevented a security incident they previously had experienced. In addition, with the ability to detect and stop security incidents, companies could quickly gain the capital cost for buying such a solution.

We should also keep in mind that there are downsides to an ICS-specific firewall as well. Commercial OT firewalls are costly, and the price increases with capabilities added. It also has many of the same disadvantages as with IT NGFWs.

Start using OT firewalls?

SWOT Analysis

Strengths	**Security** • Defend against attacks on ICS/SCADA protocols • With DPI one can deny ICS commands that are not whitelisted **User-friendliness** • Send notifications to end-users on invalid commands • Easier administration of merged security technologies **Cost-effectiveness** • Reduced cost from the centralization of several security technologies	Weaknesses	**Security** • Stated that OT firewalls as of today do not perform DPI in a satisfactory manner **User-friendliness** • Can lead to latency for end-users • Need for skilled personnel to operate **Cost-effectiveness** • Higher maintenance cost than more primitive firewalls • Larger capital costs than with more primitive firewalls
Opportunities	• Can give feedback to personnel when not allowed ICS commands are performed	Threats	• Overestimation of the security provided by the solution • Misconfigurations on implementation

Table 4.5: SWOT Analysis OT Firewalls

Based on this analysis and workshops with relevant companies in the industry, we can formulate the following recommendations regarding the usage of OT firewalls. As mentioned above, Purdue level 1.5 is just a logical separation we have added to specify that this firewall should be located between level 2 workstations and the level 1 basic control domain.

To better secure third-party file transfer, Norwegian petroleum companies should have an OT firewall with NGFW capabilities at the industrial perimeter (Purdue level 1.5) that can operate on OT-specific protocol messages.

4.4.3 Other Solutions

Several of the systems running inside the OT environment are maintained by vendors other than the operating company. Some of the earlier identified use-cases show that these third-party actors need to transfer files into secure systems, such as industrial safety systems, to perform updates and other maintenance work. The security threat this poses has been handled differently by the companies collaborating with this thesis. Alpha does not allow any write access to such systems from locations outside the company-controlled premise, while Beta has given RA to a few selected third-party vendors. Considering the importance of patch management and the improved simplicity by allowing remote patching, is it possible, with enough security mechanisms, to allow this type of access?

Furthermore, with several different users and access levels, this selective process leads to a large amount of AM. Could new technologies, while at the same time help secure third-party file transfer, also simplify the AM associated with the RAS? The table below summarizes different methods that could both increase security and minimize the need for AM.

Solution	**Security**	**Usability / user-friendliness**	**Cost-effectiveness**	**Proprietary?**	**Novelty**
Dedicated remote access desktop (operating company provide a dedicated computer and only allow connections from this)	Can be preinstalled with hardening software specified by the operator's security personnel (the only ones with admin rights). Restricts how a third-party vendor could compromise the system, either voluntarily or accidentally. Can also be stripped of unnecessary software and disallow all other connections to the computer. For instance, this will hinder typical phishing attacks simply because the desktop cannot receive emails.	Users are very restricted, and work would take additional time. Need to go to a specific machine, most likely locked up somewhere in the office, every time a file transfer to the operator's network would be needed. Simplify access management structure as only users with physical access to this desktop should have access to the system.	Need to distribute physical hardware. Can be problematic with a large and dynamic number of vendors.	Not relevant	Not relevant

Sheep Dipping	Can perform antivirus scanning on a dedicated device without the consequences of altering a live system. This makes it possible to perform a more thorough antivirus scan than what can be done if the file is simply transferred into the remote system.	Decreases the user-friendliness of uploading files. In addition, the entire process of performing sheep dipping on a file makes it more time-consuming and complicated to transfer files.	Need for additional hardware, as well as time spent by personnel performing the sheep dipping task.	Not relevant	Not relevant
Sandboxing	File uploads can be tested for malware in a sandboxed environment. Rigorous malware analysis can therefore be done. By uploading files to a virtual OT environment, OT-specific malware and zero-day malware can be identified.	The rigorous analysis of malware can lead to an increased delay, and with this, decrease user-friendliness. Increased management would be needed, but the amount can be regulated by how the solution is implemented.	The sandboxed environment should be as similar as possible to the real environment. This increases the workload on technical personnel and implementation costs. There exist cloud-based sandboxes that are similar to ICS. These are more affordable as there is no need for creating an own solution.	Proprietary	Old concept

Unidirectional Security Gateway (one-way data diode)	Data can physically only be sent one way. Can assure that access is bound to read-only or (if used other way) protect any sensitive information inside the internal system from leaking out. Data can physically only be sent one way. Can assure that access is bound to read-only or (if used other way) protect any sensitive information inside the internal system from leaking out.	Decrease the possibility for QoS mechanisms (not possible to send ACKs etc..) Can simplify AM because different access levels can be secured in hardware. For instance, read-only access using a one-way data diode makes it impossible for the user to affect the internal system.	Very high capital cost.	The device itself is a simple hardware device. However, complete products are a proprietary combination of hardware and software.	One-way diodes are nothing new, but vendors are releasing new products based on this concept.

Table 4.6: Other Solutions Summarized

Dedicated Remote Access Desktop

The most secure way of remote accessing an offshore installation is using a designated control room. Companies operating platforms have such onshore rooms, with strict physical access control and often a dedicated connection to the platform. However, third-party vendors using the RAS will not have their own control room. To get some of the same security principles a dedicated desktop, as described in subsection 4.1.1, can be used instead. Since this desktop is managed by the operator company, not the third-party vendor, the operator knows that it complies with their security policy. In addition, it will not allow any other connections, including the vendor's internal network and the public internet. This drastically limits the attack surface because no malicious files could be accidentally or intentionally downloaded. However, while this is well suited to secure a regular workflow, it does not help with file transfers. Since all other connections are disallowed, personnel would have to download, for instance, patch files on another device and then physically transfer them into the dedicated desktop. This moves the security of file transfers one step backward without solving the issue.

However, there is a difference between user-friendliness for the end-user and simplicity in identity and access management. While dedicated desktops are cumbersome for the third-party end-user, they would be easy to handle from an AM perspective. The operating company can give one such desktop to every vendor with the need for remote access file transfers, and each vendor's identity could easily be connected to their respective desktop. Furthermore, the issues that company Alpha experienced, where legitimate users were denied access because of false positives with the NAC, would be less likely using dedicated desktops. This is because these computers are already configured to comply with every security policy imaginable.

Only allow third-party vendors to connect using dedicated remote access desktops?

SWOT Analysis

Strengths	**Security** • Ensuring that access is requested from a device complying with the company's security policies • Block all connections other than to the RAS **User-friendliness** • Simplified AM for operator company's administrators **Cost-effectiveness** • None	Weaknesses	**Security** • File-transfer security is just moved one hop back **User-friendliness** • Cumbersome for end-users • Files would first have to be physically transferred into this machine before uploaded to the RAS • Machines would have to be distributed to third-party vendors **Cost-effectiveness** • Cost of hardware • The cost of technical support now falls on the operating company
Opportunities	• Less technical support needed	Threats	• Desktop misconfigured • Desktop not properly handled by third-party vendors

Table 4.7: SWOT Analysis Dedicated Remote Access Desktop

Based on the above discussion and analysis, we will not make any recommendations regarding the use of dedicated remote access computers. While it could be argued that security is added, it does not solve issues related to the focus area of file transfer.

Furthermore, the cost and decreased user-friendliness seem to be larger than the added security benefit.

Sheep Dipping

Organizations can use sheep dipping to perform rigorous malware analysis on a physical removable medium, such as a USB drive. It has both clear advantages and disadvantages when applied to user stories 1, 10, and 13. As sheep dipping is mainly intended for removable mediums brought into an organization, in the case of file transfer over a RAS, the process needs to be modified. In this instance, the starting point is not a removable medium with content but a file that should be transferred over a RAS. This difference adds complexity for the end-user. An effective sheep dipping solution requires the development of a system that resembles the actual environment of the offshore installation in the best way possible. Creating such a solution could be time-consuming. However, if implemented correctly, it will give significant security benefits to the system.

Instead of directly sending a file to the remote location over the RAS, a user would have to go through a more cumbersome method. First, the file that should be transferred has to be moved to a physical removable medium. Then, the medium is inserted into the machine performing the sheep dipping. Lastly, the file is moved back to the computer and transferred over the RAS, or the medium is sent to the offshore location. This means that the process of transferring files would take more time and be less user-friendly. Furthermore, when it comes to cost-effectiveness, a company needs to have a physical or virtual machine where the file can be tested. This device could be made in-house or bought from vendors of sheep dipping solutions. The price of this is mainly dependent on the complexity of the sheep dipping solution. It is also stated in the guidelines DNVGL-RP-G108 and NOG 104 that transferring files over a RAS is preferred over this solution.

The main benefit brought by sheep dipping is improved security. Files can actively be scanned for malware in a secure environment. The level of protection brought is mainly dependent on the construction of the solution. Sheep dipping shares many similarities with sandboxing, as companies can decide themself how comprehensive the solution should be. The solution they create will then affect the security, complexity, and cost-effectiveness. Having a sheep dipping solution with an environment that resembles an ICS environment could help to discover OT-specific malware and protect against vulnerabilities such as zero-days. If the solution is a good representation of the actual environment, it could be used as a platform for testing and training personnel. This technique does not protect against intentional attacks by inside personnel, as the process would not hinder a person from changing the file after having performed the sheep dipping.

Use Sheep Dipping when transferring files into the ICS?

SWOT Analysis

Strengths	**Security** • Provide thorough malware analysis • Can discover attacks on ICS/SCADA specific protocols • Can potentially discover zero-days **User-friendliness** • None **Cost-effectiveness** • None	Weaknesses	**Security** • None **User-friendliness** • Delay for end-users • Cumbersome to use for end-users **Cost-effectiveness** • High cost on implementation if developed in-house
Opportunities	• Provide a platform for testing and training of personnel	Threats	• False positives blocks legitimate files

Table 4.8: SWOT Analysis Sheep Dipping

Based on this analysis, it is clear that sheep dipping is a solution that would increase the security related to file transfers. However, it would significantly increase the complexity, while at the same time decrease the cost-effectiveness of the system. Therefore, we will not make any recommendations regarding the use of sheep dipping. If a remote medium is brought into an organization (i.e. remote file transfer is not possible), sheep dipping should be done before inserting the remote medium into an organization's desktop. However, as this user story is outside the scope of this thesis, we will not make any recommendations for this specific case.

Sandboxing

Similar to Sheep Dipping, Sandboxing can also be used to perform thorough malware analysis on files transferred into the ICS. For this solution to work properly it requires the development of a sandbox that resembles the actual environment of the offshore installation. This could be both costly and time-consuming to create. Furthermore, sending files through such a pipeline could lead to delay for users trying to transfer files, and this will affect the overall user-friendliness of the RAS. However, an effective sandboxing solution, implemented correctly, would give significant security benefits to the system.

It is stated in DNVGL-RP-G108 that a file transfer solution should have two file storages; one temporary storage for malware scanning and a secondary storage where the files are available from the process control domain. A sandboxing solution could be implemented in such a temporary storage, but instead of just scanning files they will also be executed and ran in a virtual environment. In order to increase the effectiveness of the solution, the storage can be made to emulate the company's OT network. Thus, it would not only be able to discover malware but could also discover possible attacks on OT-specific protocols. For example, if an adversary has written a program that would cause the ICS to behave in an undesired way, running the file in the virtual sandbox environment could discover this. Then the file would be blocked and quarantined. This also makes sandboxing able to discover zero-day vulnerabilities that regular signature-based antivirus scans would miss. However, it is important to note that some malware has functionalities for detecting if it is being run in virtual environments and would therefore alter its behavior accordingly.

In terms of cost-effectiveness, an organization can adjust the cost and maintenance requirements themselves. For instance, it is possible to purchase COTS ICS sandboxes that exist on the market. In addition to decreasing the capital cost of implementing an own solution from scratch, this would also lower the administration needed as the whole process can be outsourced to a cloud-based solution. However, one downside with this type of solution is that the generic sandbox environment would not reflect the actual organization's ICS environment, limiting the effectiveness of running OT-specific programs. Furthermore, all files sent into the internal OT network would at some point be saved in the cloud, and sandboxing requires all files unencrypted to work correctly. This could cause problems if sensitive data needs to be uploaded through the RAS.

There are many ways to design a sandboxing solution. The simplest way, if not outsourcing, is to make an isolated virtual environment without any effort to resemble the actual network. This generic sandbox could scan files using standard antivirus software and run non-specific executable files. However, it is also possible to use a hybrid approach between developing a solution locally and outsourcing the sandbox to the cloud. With this solution, all files would be run locally, and based upon the result, they would either be allowed into the internal OT network or sent to the cloud solution for further analysis. If the internal network is sufficiently segmented, it is also possible to decide how thoroughly a file should be tested based on its target system's criticality. For instance, a file only tested in the local solution might not be permitted into the industrial safety systems but can be permitted into less critical parts of the internal network.

Start using Sandboxing to analyze files transferred into the system?

SWOT Analysis

Strengths	**Security** • Provide thorough malware analysis • Can discover customized attacks based on OT-protocols • Can potentially discover zero-days **User-friendliness** • Can be automated and performed behind the scene for end-users **Cost-effectiveness** • None	Weaknesses	**Security** • Third-party security and confidentiality issues if outsourced to the cloud **User-friendliness** • Delay for end-users **Cost-effectiveness** • High cost on implementation if developed in-house
Opportunities	• Provide a platform for testing and training of personnel • The sandbox platform can be used for security auditing and penetration testing	Threats	• False positives blocks legitimate files

Table 4.9: SWOT Analysis Sandboxing

Based on this analysis and workshops with companies Alpha and Beta, it is clear that a sandbox solution would drastically increase the security related to file transfers, especially those coming from third-party vendors. Just implementing the simple, generic sandbox described above is a low-hanging fruit that gives significant security benefits without large negative effects in terms of decreased user-friendliness and cost-effectiveness. From this, it is possible to develop the sandboxing to more advanced solutions. We, therefore, formulate the following recommendation regarding the usage of sandboxing to analyze file transfers.

To better secure file transfers to the offshore installations' internal networks, Norwegian petroleum companies should implement sandboxing, either locally, cloud-based, or in a hybrid solution.

Unidirectional Security Gateway

The usage of one-way data diodes, or *unidirectional security gateway* as security vendors prefer to call their solutions, is a way of being entirely sure that data only can be transmitted in one specific direction. This can be used to enforce either read-only or write-only in the RAS.

Unidirectional Security Gateways could simplify AM because they make it, given that they are implemented correctly, impossible for users with read-only access to elevate their privileges. The management of work permits is one of the most significant AM issues for companies Alpha and Beta. By implementing one-way data diodes to enforce read-only access, users who only need to monitor values (user stories 5, 6, and 16) can get access without applying for a work permit, which would save administration costs. This also applies for system support specialists that need read-only video access in order to assist offshore personnel (user stories 17, 19, and 21). In addition, this type of read-only access could protect legacy hardware in the OT environment, as attackers would not be able to communicate with the devices. One major downside, as described earlier, is that enforcing read-only may affect QoS and would make one-way data diodes unsuitable for systems with low tolerability for delay and errors. Some vendors claim to provide software-based unidirectional gateway products that do not affect QoS. However, these are fundamentally different as they are not based on the underlying data diode technology enforcing one-way traffic. Accordingly, they will not be considered for this recommendation.

One-way data diodes are not as effective when it comes to file transfers. In industrial settings, their primary purpose is to transfer data *from* a high-security network *to* a low-security network. For example, they can transfer SCADA sensor data from the ICS to the corporate network. In the identified issue with file transfer, however, it is the other way around. Files need to be transferred *to* a high-security network *from* a low-security network. Implementing one-way data diodes here to enforce write-only access may prevent a potential malicious actor from receiving responses when attacking a system. The attacker would therefore be completely blind. However, this would also be the case for legitimate users. Employees would, for instance, not get a confirmation whether a file is successfully transferred or not. As this affects user-friendliness too much, we will only consider data diodes that enforce read-only in this analysis.

A major downside with Unidirectional Security Gateways is that these devices are very expensive, with costs ranging between 30,000 - 150,000 EUR[KFG19]. Cheaper

options exist, but they often lack government approval or certification, making them a security threat on their own. In addition to this comes the cost of managing such devices. As it is relatively novel for ICS, getting personal with sufficient knowledge to maintain a solution could be difficult.

Start using Unidirectional Security Gateways to make a separate read-only access channel?

SWOT Analysis

Strengths	**Security** • Ensures read-only access with high certainty • Active attacks not possible • Hardware solution that removes the inherent weaknesses in software • Less prone to configurational mistakes • Improved security for legacy hardware in the OT environment **User-friendliness** • Simplified AM (because only read-access is ensured) • Less evaluation needed before granting access **Cost-effectiveness** • Low maintenance cost (hardware-based)	Weaknesses	**Security** • Only helps read-access **User-friendliness** • Limited QoS for transferred data • Need skilled personnel to implement • Several separate access methods needed **Cost-effectiveness** • High capital cost
Opportunities	• More people get access to relevant monitor data • Simplified AM lead to less administration costs • Recognition from being an early adopter of new technology	Threats	• Need technology, so might not be sufficiently tested

Table 4.10: SWOT Analysis Unidirectional Security Gateways

The above analysis shows positive effects for security and user-friendliness, while low cost-effectiveness is the main negative factor. This means that, because buying several such devices is too expensive, they should only be used for the most critical systems. Another option could be to combine data from several internal OT systems and send it through a single one-way data diode. Based on this analysis and workshops with relevant companies in the industry, we formulate the following recommendation regarding the usage of Unidirectional Security Gateways.

To simplify Access Management, as well as increase overall security, Norwegian petroleum companies should implement Unidirectional Security Gateways to enforce read-only access to critical systems.

4.5 Final Recommendations

In the previous section we have analyzed different security technologies and solutions in order to make educated recommendations to the Norwegian petroleum industry. In contrast to the many vague and generalized recommendations found in other papers, these are meant to be concise and easy to implement. Furthermore, even though the recommendations chosen were analyzed to have overwhelming positive effects, negative sides were also highlighted. This means that relevant security personnel should be able to make their own educated decisions when implementing the following recommendations.

First we will repeat the overall research question for this thesis.

How can new ideas and emerging technologies in remote access be applied in the development of improved remote access security recommendations for Norwegian petroleum companies?

In answering the above question, our thesis has resulted in the following final cybersecurity recommendations for the remote access solutions used by Norwegian petroleum companies operating offshore installations on the NCS.

1. *Use a hybrid approach between perimeter-based security and Zero Trust Architecture, where they continually add security barriers based on Zero Trust principles. Barriers to add could be:*

   - Enforce system-wide continuous network monitoring in combination with machine learning-based anomaly detection. This includes support for monitoring OT-specific protocols.

   - Integrate a risk- and identity-based access management architecture as described above in order to remove workload from the work permit system.

- Upgrade the existing NAC mechanism to include user/device behavior and environmental factors such as client use patterns and IP geolocation.

2. *Use a Next-generation Firewall with deep packet inspection and intrusion prevention systems at the network perimeter (Purdue level 3.5).*
3. *Add an OT firewall with NGFW capabilities at the industrial perimeter (Purdue level 1.5) that can operate on OT-specific protocol messages.*
4. *Implement a sandboxing solution to use with file transfers, either locally, cloud-based, or in a hybrid solution.*
5. *Implement Unidirectional Security Gateways to enforce read-only access to critical systems.*

Chapter 5
Conclusion and Future Work

This thesis has explored several remote access security solutions, ranging from well-known methods to emerging technologies not yet implemented by the sector. These solutions have been studied by reviewing academic and commercially published papers, information from security solution vendors, as well as through workshops with relevant personnel from the collaborating companies, Alpha and Beta. Our overall aim has been to formulate specific and easy-to-implement recommendations for how Norwegian petroleum companies, specifically the two companies collaborating in this thesis, could improve their remote access solution.

Sub RQ A *"What are the functional requirements and threats related to a state-of-the-art remote access solution for Norwegian petroleum companies?"* is answered with an overview of functional requirements and threats for a modern RAS together with related user stories. These two sections also include detailed explanations of the different roles and threat actors, respectively. Following this, the focus areas of the existing RAS have been identified in order to answer sub RQ B *"What are the key focus areas with the remote access solutions used by Norwegian petroleum companies today?"*. Finally, the answer to sub RQ C *"How can specific technologies improve existing remote access solutions with regards to the identified focus areas?"*, together with the recommendations that have been the overall goal of this thesis, are outlined and discussed.

Current developments in the industrial threat landscape, together with the increased demand for remote access connectivity, pose a significant danger to the industrial systems that manage every aspect of critical infrastructure in today's society. The ICS on the offshore installations owned by the companies Alpha and Beta are no exception, and the security of their RAS is of vital importance. However, their solutions are not only bound by security considerations. When implementing a secure remote access solution, user-friendliness and cost-effectiveness must also be taken into consideration. The results of this thesis do not provide a complete solution. However, the proposed recommendations provide easy-to-implement improvements

to current solutions. Regarding the combination of security, user-friendliness, and cost-effectiveness, they are intended to enhance the RAS being used by the Norwegian petroleum industry. Hopefully, these recommendations and the overall analysis in this thesis will be helpful for improving RAS in the future.

Future Work

There are several avenues for future work related to this thesis. Firstly, there are still many potential solutions that we were unable to include due to time constraints. For instance, the use of honeypots and different antivirus software. Thus, an area of future work could be to extend the analysis in this thesis to include a broader range of solutions.

Additionally, this work only extended to theoretical analysis. Accordingly, we did not perform any practical simulations with the different solutions and technologies. More accurate results could be obtained by evaluating how these solutions actually function in a simulated environment. However, creating a realistic virtual environment that reflects the network of offshore installations could be challenging.

This thesis only collaborated with two petroleum companies. Due to time restrictions, it was not possible to have an in-depth case study with a large number of corporations. However, such a study would provide more generalizable results and may yield better recommendations. Therefore, an area of future work could be to perform this type of thesis, using several different petroleum companies from sectors.

Finally, also due to time constraints, we were only able to perform a limited literature review. This means that a future study could extend the results of our literature review and conduct a systematic literature review of all available papers related to RAS for industrial systems. The feedback received indicates that the industry is very interested in this type of information.

References

[AA20] National Security Agency and Cybersecurity & Infrastructure Security Agency. Alert (aa20-205a). [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-205a, July 2020. (last visited: 2021-05-23).

[Aga04] Sarika Agarwal. Testing web security: Assessing the security of web sites and applications. by steven splaine. published by john wiley and sons, new york, u.s.a., 2002. isbn: 0-471-23281-5, 345 pages. *Software Testing, Verification and Reliability*, 14(4):284–285, 2004.

[ANUT20] Iftekhar Ahmed, Tahmin Nahar, Shahina Urmi, and Kazi Taher. Protection of sensitive data in zero trust model. January 2020.

[AS17] DNV GL AS. Cyber security in the oil and gas industry based on iec 62443. [Online]. Available: https://rules.dnv.com/docs/pdf/DNV/rp/2017-09/dnvgl-rp-g108.pdf, September 2017. (last visited: 2021-05-24).

[AS20] Hydro AS. Cyber-attack on hydro. [Online]. Available: https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack/, October 2020. (last visited: 2021-05-15).

[BD20] E. B. Boumhaout and A. Danielsen. Towards zero trust for critical infrastructure: Rethinking the industrial demilitarized zone. 2020.

[Bot16] Robert Botezatu. Cyber security for scada and dcs systems a summary of the current situation and key points to consider. [Online]. Available: http://www.icare-cybersecurity.com/assets/icare-ics-white-paper-.pdf, April 2016. (last visited: 2021-03-10).

[BRAA12] Thanh Bui, Siddharth Rao, Markku Antikainen, and Tuomas Aura. Secure it systems. 2012.

[Cam20] Mark Campbell. Beyond zero trust: Trust is a vulnerability. Technical report, October 2020.

[Che03] William R Cheswick. Firewalls and internet security : repelling the wily hacker, 2003.

[Clo] Cloudfare. What is a software-defined perimeter. [Online]. Available: https://www.cloudflare.com/learning/access-management/software-defined-perimeter/. (last visited: 2021-04-10).

[Coh04] Mike Cohn. User stories applied : for agile software development, 2004.

[DAKH13] Mohammad Dadashzadeh, Rouzbeh Abbassi, Faisal Khan, and Kelly Hawboldt. Explosion modeling and analysis of bp deepwater horizon accident. *Safety Science*, 57:150–160, August 2013.

[DCB18] Krati Dadheech, Arjun Choudhary, and Gaurav Bhatia. De-militarized zone: A next level to network security. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018.

[EI16] E-ISAC. Analysis of the cyber attack on the ukrainian power grid. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf, June 2016. (last visited: 2021-03-12).

[FGG+16] Angelo Furfaro, Teresa Gallo, Alfredo Garro, Domenico Saccà, and Andrea Tundis. Requirements specification of a cloud service for cyber security compliance analysis. In *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, pages 205–212, May 2016.

[FWD19] Filkins Filkins, Doug Wylie, and Jason Dely. Sans 2019 state of ot/ics cybersecurity survey. [Online]. Available: https://industrialcyber.co/wp-content/uploads/2020/05/Survey_ICS-2019_Radiflow.pdf, June 2019. (last visited: 2021-03-25).

[Gar] Gartner. Network access control (nac) reviews and ratings. [Online]. Available: https://www.gartner.com/reviews/market/network-access-control. (last visited: 2021-04-24).

[Gar17] Gartner. Next-generation firewalls (ngfws). [Online]. Available: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws, September 2017. (last visited: 2021-05-24).

[Gin13] A. Ginter. Unidirectional security gateways: Stronger than firewalls. [Online]. Available: https://accelconf.web.cern.ch/icalepcs2013/papers/thcoba02.pdf, 2013. (last visited: 2021-05-03).

[GJ07] Tor Grøtan, Martin Jaatun, Knut Øien, and Tor Onshus. The sesa method for assessing secure remote access to safety instrumented systems. [Online]. Available: https://www.sintef.no/globalassets/project/hfc/documents/sintef-a1626-the-sesa-method-for-assessing-secure-remote-access-to-safety-instrumented-systems.pdf, June 2007. (last visited: 2021-04-07).

[Gro19] Qi An Xin Group. Zero trust architecture and solutions. [Online]. Available: https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf, August 2019. (last visited: 2021-05-03).

[Har98] Chris Hart. Doing a literature review : releasing the social science research imagination, 1998.

[HEF] Kevin E. Hemsley and Dr. Ronald E. Fisher. History of industrial control system cyber incidents.

[HKKN16] Youngjun Heo, Byoungkoo Kim, Dongho Kang, and Jungchan Na. A design of unidirectional security gateway for enforcement reliability and security of transmission data in industrial control systems. In *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016.

[HPV+99] K. Hamzeh, G. Pall, W. Verthein, W. Little, and G. Zorn. Point-to-point tunneling protocol (pptp). [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2637, July 1999. (last visited: 2021-03-02).

[HRM+04] Alan Hevner, Alan R, Salvatore March, Salvatore T, Park, Jinsoo Park, Ram, and Sudha. Design science in information systems research. *Management Information Systems Quarterly*, 28, March 2004.

[IEC15] Iec62443-2-4. industrial communication networks - network and system security - part 2-4: Security program requirements for iacs service providers. Standard, International Electrotechnical Commission, June 2015.

[IEC18] Iec 62443-3-2. industrial communication networks - network and system security - part 3-2: Security risk assessment and system design. Standard, International Electrotechnical Commission, March 2018.

[IEC20] Iec62443-2-2. industrial communication networks - network and system security - part 2-2: Iacss security program ratings. Standard, International Electrotechnical Commission, March 2020.

[Inc20] Sunny Valley Cyber Security Inc. Installing next-generation firewall plugin for opnsense. [Online]. Available: https://www.sunnyvalley.io/post/opnsense-ngfw/, August 2020. (last visited: 2021-05-23).

[Ipt] iptables(8) - linux man page. [Online.Available: https://linux.die.net/man/8/iptables.

[IS16] Industrial Automation ISA99 and Control Systems Security. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99, December 2016. (last visited: 2021-05-03).

[JLYZ18] Ning Jiang, Hu Lin, Zhenyu Yin, and Liaomo Zheng. Performance research on industrial demilitarized zone in defense-in-depth architecture*. In *2018 IEEE International Conference on Information and Automation (ICIA)*, 2018.

[JRS17] Sohely Jahan, Md. Saifur Rahman, and Sajeeb Saha. Application specific tunneling protocol selection for virtual private networks. In *2017 International Conference on Networking, Systems and Security (NSysS)*, 2017.

[JWK21] Martin Jaatun, Egil Wille, and Stine Kilskar. Grunnprinsipper for ikt-sikkerhet i industrielle ikt-systemer. [Online]. Available: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id4-grunnprinsipper-for-ikt-sikkerhet_sintef-rapportnr-2021-00055-feb---signert.pdf, January 2021. (last visited: 2021-04-10).

[KFG19] Katarina Kertysova, Erik Frinking, and Gabriella Gricius. Understanding the strategic and technical significance of technology for security: The case of data diodes for cybersecurity. [Online]. Available: https://www.thehaguesecuritydelta.com/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf, August 2019. (last visited: 2021-05-02).

[KKK16] Farshad Khorrami, Prashanth Krishnamurthy, and Ramesh Karri. Cybersecurity for control systems: A process-aware perspective. *IEEE Design Test*, 33(5), 2016.

[KMM+16] Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir Sezer. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, pages 53–63, 2016.

[Koi] Waverley labs: Open source software defined perimeter.

[Kor19] Ville Korhonen. Future after openvpn and ipsec. Master's thesis, 2019.

[LAG19] Suvi Leppänen, Shohel Ahmed, and Robin Granqvist. Cyber security incident report—norsk hydro. 2019.

[LGZ+19] Dong Li, Huaqun Guo, Jianying Zhou, Luying Zhou, and Jun Wen Wong. Scadawall: A cpi-enabled firewall model for scada security. *Computers Security*, 80, 2019.

[LR18] Javier Lopez and Juan Rubio. Access control for cyber-physical systems interconnected to the cloud. *Computer Networks*, 134, April 2018.

[LRLT13] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 2013.

[LSDM+13] Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K Iyer. Adapting bro into scada: building a specification-based intrusion detection system for the dnp3 protocol. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, pages 1–4, 2013.

[Mal19] MalwareHunterTeam. [Online]. Available: https://twitter.com/malwrhunterteam/status/1105004059122032640, November 2019. (last visited: 2021-05-27).

[MAZ17] Musa Abubakar Muhammad, A. Ayesh, and P. B. Zadeh. Developing an intelligent filtering technique for bring your own device network access control. *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.

[MRHM10] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho. Stuxnet under the microscope. [Online]. Available: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf, September 2010. (last visited: 2021-02-20).

[MSR20] Abhishek Mungekar, Yashraj Solanki, and Swarnalatha Rajaguru. Augmentation of a scada based firewall against foreign hacking devices. *International Journal of Electrical and Computer Engineering*, 10:1359–1366, April 2020.

[MY12] Paul Mueller and Babak Yadegari. The stuxnet worm. 2012.

[NA] P. S. Nyakomitta and Silvance O. Abeka. Security investigation on remote access methods of virtual private network. *Global journal of computer science and technology.*

[NHC18] Kishan Neupane, Rami Haddad, and Lei Chen. Next generation firewall for network security: A survey. In *SoutheastCon 2018*, April 2018.

[Niv16] Jeyasingam Nivethan. On the use of open-source firewalls in ics/scada systems. *Information Security Journal A Global Perspective*, 25, April 2016.

[OA15] Norwegian Oil and Gass Association. Nog 088: Norwegian oil and gas recommended guidelines for a common model for work permits (wp). [Online]. Available: https://www.norskoljeoggass.no/contentassets/19cf6f3a9415400ebff20d0c40436f6a/088-recommed-guidelines-for-common-model-for-work-permits.pdf, June 2015. (last visited: 2021-04-01).

[OA16] Norwegian Oil and Gass Association. Nog 104: Information security baseline requirements for process control, safety and supportict systems. [Online]. Available: https://www.norskoljeoggass.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf, December 2016. (last visited: 2021-04-04).

[Osb21] Charlie Osborne. Colonial pipeline attack: Everything you need to know, May 2021.

[per] perimeter81. Software-defined perimeter. [Online]. Available: https://www.perimeter81.com/solutions/software-defined-perimeter. (last visited: 2021-05-17).

[Ran09] Justus J Randolph. A guide to writing the dissertation literature review. *Practical assessment, research evaluation*, 14(13), 2009.

[RBMC20] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connely. Nist special publication 800-207 zero trust architecture. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207, August 2020. (last visited: 2021-04-28).

[RCdF+21] Luis Rosa, Tiago Cruz, Miguel Borges de Freitas, Pedro Quitério, João Henriques, Filipe Caldeira, Edmundo Monteiro, and Paulo Simões. Intrusion and anomaly detection for the next-generation of industrial automation and control systems. *Future Generation Computer Systems*, 119, 2021.

[RDRN+20] Petar Radanliev, David De Roure, Jason Nurse, Razvan Nicolescu, Michael Huth, Stacy Cannady, and Rafael Montalvo. Future developments in standardisation of cyber risk in the internet of things (iot), January 2020.

[SC] Homeland Security and CPNI. Configuring and managing remote access for industrial control systems. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf. (last visited: 2021-05-22).

[SC19] Erhan Sindiren and Bünyamin Ciylan. Application model for privileged account access control system in enterprise networks. *Computers Security*, 83, 2019.

[Sco15] Austin Scott. Tactical data diodes in industrial automation and control systems. [Online]. Available: https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057, May 2015. (last visited: 2021-05-02).

[Sec] Pulse Secure. Next generation access architecture for protecting application infrastructure. [Online]. Available: https://www.pulsesecure.net/products/sdp-overview/. (last visited: 2021-05-17).

[Ser10] Gloria J. Serrao. Network access control (nac): An open source analysis of architectures and requirements. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 2010.

[SFSC19] Roberto Setola, Luca Faramondi, Ernesto Salzano, and Valerio Cozzani. An overview of cyber attack to industrial control system. *Chemical Engineering Transactions*, 77, January 2019.

[Sho] Shodan. [Online]. Available: https://www.shodan.io/. (last visited: 2021-05-28).

[Sim19] Herbert Simon. *The Sciences of the Artificial*, volume 3. John Wiley Sons, Ltd, 2019.

[SOMB16] Max Saltonstall, Barclay Osborn, Justin McWilliams, and Betsy Beyer. Beyondcorp: Design to deployment at google. *Login*, 41, March 2016.

[SPL+15] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. Nist special publication 800-82 revision 2: Guide to industrial control systems (ics) security. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, May 2015. (last visited: 2021-05-09).

[SS16] Murugiah Souppaya and Karen Scarfone. Nist special publication 800-46 revision 2: Guide to enterprise telework, remote access, and bring your own device (byod) security. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf, July 2016. (last visited: 2021-05-09).

[VGT14] Mihai Vasilescu, Laura Gheorghe, and Nicolae Tapus. Practical malware analysis based on sandboxing. In *2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference*, 2014.

[VH15] Jan Vávra and Martin Hromada. An evaluation of cyber threats to industrial control systems. In *International Conference on Military Technologies (ICMT) 2015*, pages 1–5, 2015.

[VJDL18] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, and Brian Lee. Access control policy enforcement for zero-trust-networking. In *2018 29th Irish Signals and Systems Conference (ISSC)*, 2018.

[WDSN17] Kevin Wong, Craig Dillabaugh, Nabil Seddigh, and Biswajit Nandy. Enhancing suricata intrusion detection system for cyber security in scada networks. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2017.

[Woh14] Claes Wohlin. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on evaluation and assessment in software engineering*, EASE '14. ACM, 2014.

[ZZTX10] Zhimin Zhou, Chen Zhongwen, Zhou Tiecheng, and Guan Xiaohui. The study on network intrusion detection system of snort. In *2010 international conference on networking and digital society*, volume 2, pages 194–196. IEEE, 2010.

Peder Grundvold & Jon Breivik Smebye

Remote Access Security Recommendations for Norwegian Petroleum Companies

NTNU
Kunnskap for en bedre verden