Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering

Henrik Larsen

Cyber security alerts in remote operation center

Master's thesis in Information Security
Supervisor: Prof. Stewart James Kowlaski
December 2022

NTNU
Norwegian University of
Science and Technology

Henrik Larsen

Cyber security alerts in remote operation center

Master's thesis in Information Security
Supervisor: Prof. Stewart James Kowlaski
December 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering

NTNU
Norwegian University of
Science and Technology

Acknowledgment

I would like to thank the following persons for their great help during the work to finalize this master's thesis:

- The three captains from the norwegian shipping company. For contributing in the focus group interview by adding good and helpful solutions.
- The three cyber security analysts from a norwegian security operation center.For contributing with their expertise during the focus group interview.
- Kongsberg Maritime as my working place and my possibility to work with systems relevant to this topic. This has helped me with having a good understanding of the remote/autonomous concept.
- Product Cyber Security Manager Kenneth Solberg in Kongsberg Maritime for highlighting this problem and contribute with inputs.
- My supervisor Prof. Stewart James Kowalski for good guidance and inputs for the process to finish this thesis.

Thank you all so much for the contribution to make me able to finish this master's thesis.

Abstract

The next era of maritime systems will have to deal with remote and/or autonomous vessels. This includes that vessels need to be monitored and/or remotely control from shore. This will make the vessels more inter-connected and the cyber-surface will increase and lead to a higher risk of cyberattacks. Due to this it is desired to have better cyber security awareness through cyber security alerts. In this study we create mock-ups of how cyber security alerts may be displayed in a remote operation center. It was also made mock-ups for how different actors in a remote operation center can communicate to handle a cyber security alert. These mock-ups were displayed to a focus group of three captains and three cyber security analysts to receive input and feedback. The results of these focus group sessions are used to produce and improve mock-ups for human machine interface and playbook for handling cyber security alerts. In the end we give a recommended mock-up for the human machine interface to display cyber security alerts together with safety alerts. We also give a recommended playbook on how the different actors in a remote operation can handle a cyber security alert. This playbook aims to know if the cyber security alert is a real cyber threat and if an incident handling response need to be engaged.

Contents

List of Figures

List of Tables

1 Introduction

The next era of maritime systems will have to deal with remote and/or autonomous vehicles. In this project we focues in particular on remote and/or autonomous operated vessels. To make these vessels remote and/or autonomous will required that they are even more interconnected and also connected with a connection to a remote operation center that enables monitoring and control of the remote and/or autonomous operation. This will create from a cyber security perspective a larger attack surface towards these remote and/or autonomous vessels. It will also be harder to know if what you monitor and see in the remote operation center is manipulated by a malicious actor or not. In that matter it will be desired to have an option to monitor the cyber security state of the remote and/or autonomous vessels, just as vessels already receive alerts and indicators in regard to the the safety state of the vessel. The challenge with this is that vessel operators might not have the desired knowledge of cyber security to be able to assess the risk of an cyber security alert. This may increase the load of the operators cognitive capacity and human-errors could occur. Since safety alerts have been part of vessel operators workflow for decades, we have in this project focused on the cyber security alerts and how to present these alerts for the operator without challenging the operators cognitive capacity.

Research problem :
How should cyber security alerts be integrated with current safety alerts in a remote operation center without overloading the cognitive capacity of In section operators?

This paper is divided into ten chapters. In the second chapter we will give some background to the topic and relevant work. In chapter three we will outline the social and technical aspects concerning cyber security alerts in the context of remote operation of remote and/or autonomous ships. In chapter four we will go through the different methodologies used for interviews, information analysis and creating mock-ups. Further we will in chapter five establish some initial mock-ups for human machine interface for diaplying alerts and cyber security alert playbook for handling the alerts. Then in chapter six we will go through the data collection. In chapter seven we will give the results for the human machine interface design and in chapter eight we will give the results for the cyber security alerts handling playbook. In chapter nine we will go through the discussion including future work. In the end in chapter ten we have the conclusion.

1.1 Definition of terms

- **Remote and autonomous operations:** Remote and autonomous operations are two different types of operations. Remote operations are when a captain is remotely steering a ship from shore. When it comes to autonomy there are certain levels of autonomy. SAE International has released a definition of these six levels of driving automation. Level 0 defines as no automation and level 6 is defined as full automation. According to the SAE International all the levels are defined as following [8, 9, 10]:
    - Level 0: No Automation - In this automation level there is no technologies that provides any kind of assisted or automated driving of the specific vehicle.
    - Level 1: Assisted Driving Automation - At this level there is some kind of technology implemented in the vehicle that provide any kind of assisted or automated function. Examples of this can be parking sensors and automated adjustment of speed.
    - Level 2: Partial Automation - In this level there is multiple technology that provide an assistant or automated function and these multiple technology can work together simultaneously. Examples of this level is when a vehicle can determine the distance to an object or the traffic ahead and adjust the speed or steer the vehicle based on this information.
    - Level 3: Conditional Automation - The vehicle can do limited automation driving at certain conditions. Since it is just in certain conditions a human-being has to be standby in the vehicle to make sure that the vehicle is behaving safely at all circumstances. So if a ship is going to sail a specific route that includes certain conditions somewhere but not elsewhere. This ship needs to be controlled at certain points during the route.
    - Level 4: High Automation - In this level the vehicle has the capability to drive with full automation at certain conditions. Conditions in this matter can be like how the weather is and how the terrain is around the vehicle. In these scenarios a human will be a passenger on-board until the weather is too foggy for the sensors or a ship is going to pass through a really small passage, which the vehicle is not trained to do.
    - Level 5: Full Automation - The final level is full automation and in this level the vehicle is expected to get no human assistance at all. In this scenario the human interface may not be present at all in the vehicle.

  In an autonomous operation it is considered to use level 3-5 as described above.
- **Remote operation center(ROC):** This is an operation center at shore which is in command of all remote and/or autonomous operated vessels that are connected to this remote operation center. From this operation center the operation crew are able to monitor and control remote and/or autonomous vessels to make sure that operations goes as planned [6].
- **Cyber security alerts:** Cyber security alerts are alerts generated based on the status of the cyber security in a system or network. Mainly such alerts are generated by intrusion detection systems(IDS), anti-virus software(AV) and/or vulnerability assessment tool. IDS generates alerts when suspicious or malicious behaviour is detected in network traffic or in system logs

[11]. AV is generating alerts when finding files on a system that matches certain known signatures and/or patterns [12]. Vulnerability assessment tools are software that scans systems for known vulnerabilities and alerts upon them if found [13].

- **Vessel operators:** This is the captain of a ship or vessel. This operator is responsible for the operation of a certain vessel or ship. This person can take remote control of a remote operated vessel, but also monitor the operation of an autonomous operated vessel.
- **Security operation center(SOC):** This is operation center responsible for detect, analyze and respond upon security threats and other aspects. The SOC will mainly monitor cyber security related information and this can be information from either their own organization but also a customer which the SOC is supporting [14].

2 Background

2.1 Autonomous and remote ship

2.1.1 Autonomous ship specific environment

The uniqueness of the autonomous environment for ships are that we need to have a connectivity link back to a control center at shore to monitor the states of these autonomous ships. We will call this control center for ROC - Remote Operation Center. What information and data that is needed to be sent back to the ROC, depends on the level of autonomy to the ship as outlined in table 1.

Table 1: Autonomy level - Information to the ROC [7]

Autonomy level	**Information to and from ROC**
Level 0	Nothing will be sent over to shore.
Level 1	May receive some information to shore.
Level 2	Receive all information applicable for monitoring the remote and/or autonomous operation (only one-way communication, from vessel to shore)
Level 3	Receive and transmit information applicable for monitoring and remote control of the remote and/or autonomous operation (override control over the vessel from shore if applicable)
Level 4	Receives and transmits information relevant for autonomous operations (override control of vessel only when necessary).
Level 5	Receives information relevant for monitoring fully autonomous operations, but transmits only commands and no remote control is applicable.

For the vessel to send sufficient amount of information over to shore in close real-time perspective the environment depends on the connectivity systems between the vessel and shore. As shown in figure 1 we see an illustration of an architecture for vessel to shore control and monitoring. In this figure we find both satellite and LTE-mobile connection as connectivity carriers. This architecture may differ from which systems are going to get implemented into the environment and with what latency and bandwidth these systems depends on. It is also expected that most of the systems on the vessel will also be installed in the remote operation center(ROC) on shore. This is to be able to receive and process the same sort of information equally on both sides [1, 10].

2.1.2 Cyber security of autonomous vehicles

In a study of cyber security of autonomous vehicles by Yağdereli, Gemci and Aktaş it was delibrated upon several types of cyberattacks towards this concept of autonomy. This were cyberattacks like:

- Eavesdropping: Where an attacker intercepts data from the autonomous vehicle.

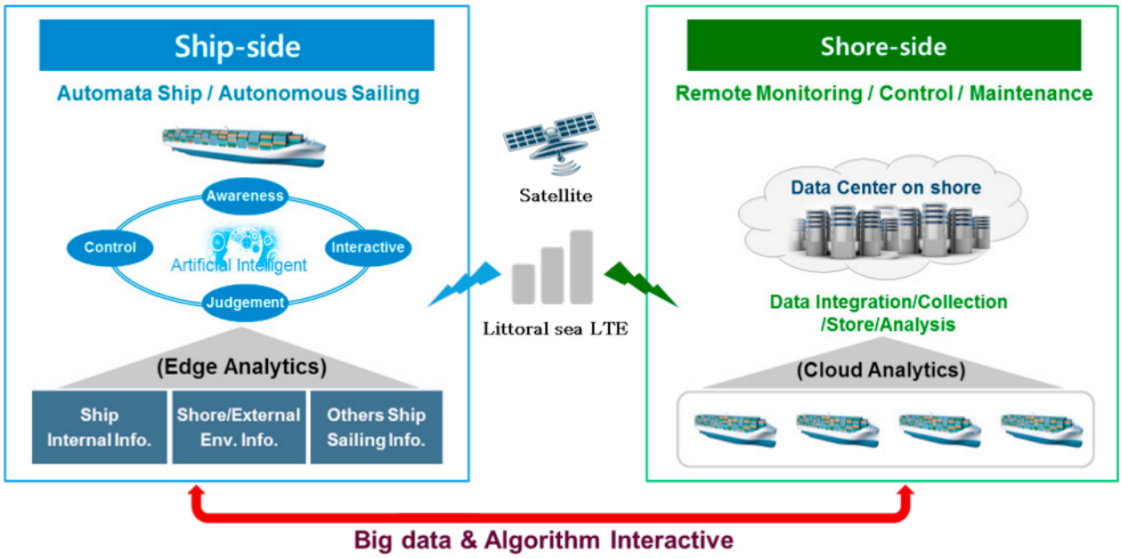


Figure 1: A high-level architectural environment to an autonomous ship operation [1]

- Traffic analysis: Here the attacker uses the traffic transmitted by the autonomous vehicle to analyze it and to find information that normally would not be easily accessible.
- Masquerade: This is where an attacker grants authorized access to a system by impersonates someone else. This attack can breach all kind of security.
- Replay: In autonomy, messages and commands will be sent back and forth between a command and control center (remote operation center) and the vehicle. These messages and commands can be intercepted by an attacker and replayed to perform the same command at a later point of time. This can make the attacker able to fraudulently control the vehicle.
- Message modification: This attack is similar to the replay. Here the attacker will use the intercepted message and modify it to give the vehicle another command than the one intercepted. For example a command for the vehicle to drive to a different location.
- Denial-of-service: This attack occurs when the attacker makes the system not available for a period of time. This can be overloading the bandwidth or shutting down any kind of system.

In the same study it was found several methods to cope with these cyberattacks and to avoid them:

- *Using reliable distributed programming tools and techniques:* This is a method depending on the developers of autonomous vehicles to develop secure, reliable and resilient systems.
- *Including cyber security requirements in the requirement analysis phase:* This means that the development of autonomous vessels need to include cyber security requirements into their requirement-database for their developments.

- *Using multi-agent system architecture:* Here the autonomous vessel is consider to have software agents in a distributed real-time systems where this will bring the capability to give status remotely to identify cyber-attacks.
- *Redundancy:* Here it will cope with the term "single-point of failure" where if a system goes down it will recover by using another system capable of the same features as the lost one.
- *Diversity:* This is when a single system is compromised it can not compromise other systems.
- *Defense-in-depth:* By this term it says that you should secure systems in several layers so that if the attack comes through one layer it still need to penetrate the next.
- *Authentication:* To make sure that no unauthorized get access to the system it is crucial to have accountability to make sure that authentication of authorized users is implemented into the systems. This can also be controlled in audit logs to keep track of any suspicious authentication situations like multiple failed logins and such.
- *Using micro-kernel:* Embedded software should use micro-kernels to avoid supervisory rights in the system and to discover any weaknesses before deployment.

When it comes to the risk of cyberattacks on autonomous ships, Jan Erik Vinnem and Ingrid Bouwer Utne has done study on this [15]. In this study they focusing on the risk related to environments around and not necessary only the ship itself. They mention that unmanned autonomous ships may be hijacked and used to ram into infrastructure systems as well as the ship getting lost which is a huge cost for the ship owners. Together with this it is mentioned that the unmanned autonomous ship should not be a cruise ship with thousand of passengers, since this can lead to harm of a lot of people. These risks are essential to managed in a good way to avoid such huge harm to people or infrastructure. Therefore it will be important to follow up the cyber security related to autonomous and remotely controlled ships.

2.1.3 Regulation and cyber security of autonomous ships

In a study performed by Henrik Ringbom [2] it was researched on how the regulation of autonomous ships would get regulated by for example the International Maritime Organization (IMO) and which challenges will get fronted. In this study it was found that depending on the degree of autonomy like explained in subsection 2.1.1 it would at fully manned but with monitored autonomy be no challenges regulation wise. As soon as the concepts exceeds this this it would start to be legally challenging for today's regulations. This is also explained by figure 2. It was also found that fully autonomous ships may not be accepted by the regulation in short or even medium period of time [2]. Cyber security will also be one of these challenges for the regulatory to accept autonomous ships. Anyhow when it comes to cyber security there is conducted some regulations and standards for autonomous shipping. In a study on "Autonomous shipping and cyber security" it was found that Bureau Veritas has found a solution towards this challenge. This solution is splitted into two different classification tags named "cyber secure" and "cyber managed". "Cyber secure" is a certification level of new built ships and is ensuring that the installed equipment onboard is at a acceptable level of "cyber secure". For "cyber managed" this is a concept where the ship is already in service. Here the cyber security is conducted through training and policies to ensure that the ship

will have less probability of cyberattacks. Together with this there is also found three widely used regulatory standards towards cyber security in the maritime sector[16]:

- "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS" by IMO through MSC 428 (98).
- GDPR directive by the European Union
- EU Directive 2016/1148(called NIS Directive). This is a directive on the security of information networks and systems. This is mainly for ports and not the ships.

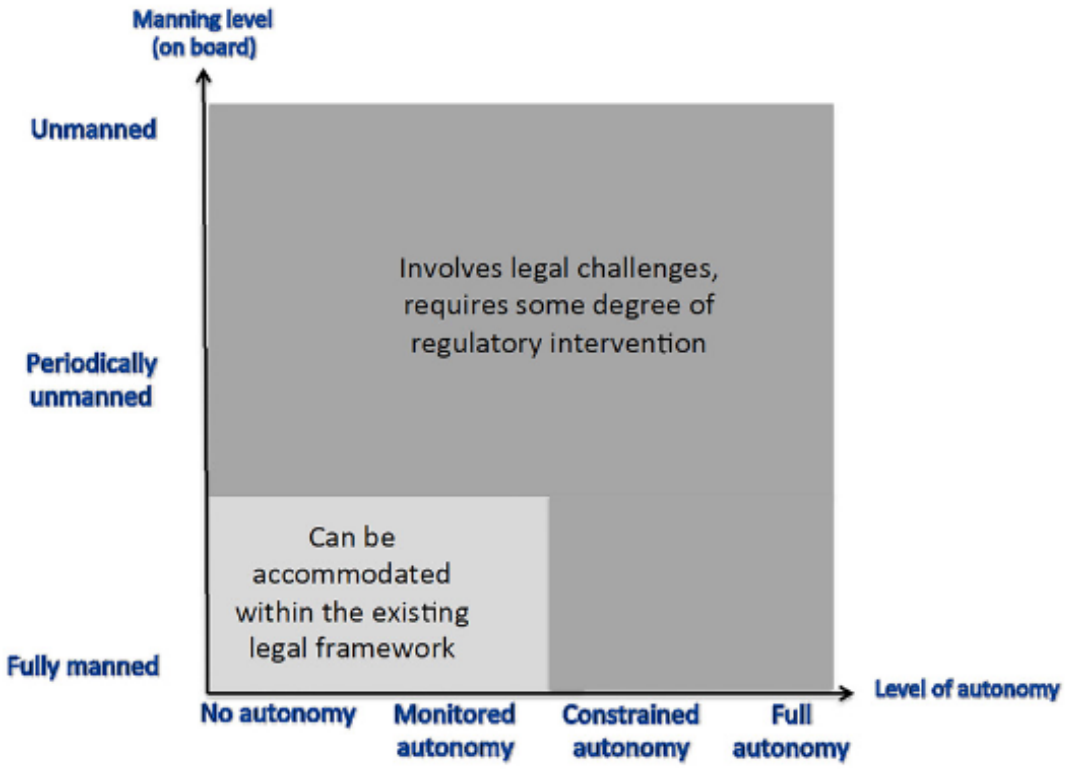


Figure 2: Nature of the legal challenge [2]

2.2 AUTOSHIP

Autonomous shipping Initiative for European Waters, also called AUTOSHIP, is an initiative with the focus on making the transition from today's generation of ships to the next generation of ships which is autonomous ships. This focus is mainly for the European Union, but may also affect the whole autonomous ship industry. The goal for this initiative is to convert 30 percent of the road transportation over to a multimodal solution by 2030 and even 50 percent in 2050. Multimodal

focuses on using more than one element to accomplish the same result, and in this case this means that they will use both autonomous ships together with the old generation of road freight. The ambitions of the different projects in this AUTOSHIP initiative is to make advanced Key Enabling Technologies, solid industrial investments and business worldwide, along to deliver the first autonomous ship technology on the market. There are a total of 11 experienced partners that participate in this initiative which are [17]:

- Ciaotech S.r.l - PNO Group
- Kongsberg Maritime CM AS
- Kongsberg Maritime AS
- Kongsberg Digital AS
- Kongsberg Norcontrol AS
- Sintef Ocean AS
- University of Strathclyde
- Eidsvaag AS
- Blue Line Logisitics NV
- Bureau Veritas
- DE VLAAMSE WATERWEG NV

AUTOSHIP will enable two significant test demonstrations which may make a difference in the next five years in the perspective of converting the road transportation to a multimodal solution. These two demonstrations are [17]:

- The Inland Water Way - This demonstration will be testing an remote/autonomous catamaran, more precisely a Class2 Pallet Shuttle Barge. This catamaran will have the job to transport goods on pallets up to 350 tons in the major EU port of Antwerp.
- The short-sea Shipping - This demonstration will be testing remote/autonomous transportation of fish feed to fish farms along the Norwegian coast.

2.3 YARA and ASKO

Yara Birkeland is a vessel that has the goal to be the first autonomous and zero-emmission container vessel. This is a project between Yara and the technology company Kongsberg. Kongsberg is here responsible for the technical solution to make Yara Birkeland. This includes systems and technology that makes the vessel able to perform remote controlled and autonomous operations. Yara Birkeland went into operations spring 2022. The vessel is for now not fully autonomous but will gradually be fully autonomous depending on the progression from Kongsberg [18]. Kongsberg has also in co-operation with Massterly the task to make two vessels that are autonomous and have zero-emission. This task is given by Asko which is a grocery distributor in Norway. As with Yara Birkeland Kongsberg has the task to deliver the technology making these vessels autonomous together with a remote operation center. The remote operation center is going to be used by Massterly to perform ship management and safe operations from shore [19].

2.4 Cyber security alerts in SOCs

Security Operations Center(SOC) is a center mainly used by large organizations as a part of their security strategy. In this center it combines processes, technologies and people to manage the overall security to an organization. This includes having several rather complex set of systems to provide situational awareness regarding the security posture. This situational awareness create a possibility to detect and mitigate a cyberattack. Security Information and Event Management(SIEM) is an essential part for many SOCs around the globe. This is a system responsible for collecting all security-relevant data and to display this in a analytically manner. This supports cyber security analysts with the analysis and are able to correlate events accross systems. Together with this it enables enrichment of context data, normalizing heterogeneous data, reporting and more importantly for this project alerting [20].

In a paper called AlertVision: Visualing Security Alerts it states that the best practice towards having Threat Intelligence is to use several IDS/IPS systems and correlate the alerts these generates [21]. When alerts are correlated it enables a capability to identify high-level patterns of current cyberattacks. This process can often be called alert correlation and can be used to find zero-day attacks in the future (cyberattacks that is unknown). A challenge in alert correlation is to find a automated way of vizualize these correlated alerts and is not been broadly researched for now. AlertVision is a product used to visualize security alerts. This product groups alerts firstly based on their property and then produces several sets of alert sequences. Each sequenced group represents certain cyberattack categories, such as an attack source IP or a target service. The system then scans for similarities between these sequences and visualize their correlations. This makes it easier to see that two different sequences that is quite different can relate to the same cyberthreat.

2.4.1 Risk management of autonomous ships

Since autonomous ships are a new concept and might include unmanned ships there needs to be assessments and regulations of such concept before getting into operations. Susanna Dybwad Kristensen has done a study on this in the paper "Risk Acceptance Criteria for Autonomous Ships". In this study it was developed a risk acceptance criteria (RAC) which were used in two different case studies for an autoferry and a cargo ship. Both case studies showed that they were not inside the acceptance criteria level, but it is worth mentioning that this was the RAC for existing vessels. The reason for this was also elaborated on and might be due to the new ship requirements that has been established by IMO the latest years. The risks mentioned in this paper can elevate when cyberattacks are included into the scenario since that may affect the probability and consequences of safety risks as well. [22]

2.5 Cogntive Capacity

During a study of cognitive task load in naval ship control centre it is stated that due to the increase of deployments of information and communication technology in such control centres there is even more information to be processed which will increase the cognitive task load of operators [23]. In this study they used a model that focuses on three different load factors: time occupied, task-

set switching and level of information processing. During the study they had 13 teams to perform eight different scenarios with different high and low levels of the different factors mentioned above. The results of the study showed that there were both under- and overload situations with negative effects on the performance to the operators. For our project the information processing level is the cognitive factor which will be one of the focus areas of our study. In this study it was shown that there was a huge difference of cognitive load when going from low to high level of information processing. This shows that the amount of information is a crucial factor towards the cognitive load to an operator .

Naveen Kumar and Jyoti Kumar did a study of design of control panels depending on cognitive load [24]. Due to control panels containing more and more information and are getting more complex. Should such information get display analogously, digitally or graphically, that is part of the study. To study which kinds of design is suitable for control panels they used measures of cognitive load. It was found that digital designs provoke higher cognitive load than analogue and hybrid designs.

In a study of the cognitive load of operators of the longest inter-connected electrical network placed in Australia [25]. These operators have a workstation with seven screens with a large co-ordination screen to display information and enables collaboration with other control centers. This study assessed the cognitive load both during a training scenario and in the regular control room. This measures the integration of the subjective and the physiological factors. In this study it was found that the cognitive load varied depending on different events, different participants of the same session and during different periods of the same session. During critical situations the operator collaboration with other control center was measured to high and the coordination screen was highly used. This screen and system was found to have some weaknesses and needed some improvements. This was also part of the conclusion where it was stated that layout strategies, potential combination of applications, redesign of certain applications, and linked views should be consider to get improved to minimize the cognitive load for the operators. Another factor of improvement was to improve the integration of procedures and linking of alarms to visual cues. This is directly relevant to this project and confirms that the design and workflow of alerts are a crucial factors towards lowering the cognitive load to operators.

During a study of the distributed cognition in a emergency co-ordination center it was found that the operators of this center had a fixed workflow [26]. This seem to delay the process of sending help. However it had its reasons. They uses recording of the calls to easier remember important information that is used to send help. This reliefs parts of the cognitive capacity for the operators. It was recommended to fix their procedure to include *situated co-ordination* that is more dynamic to be able to easier handle unforeseen situations. It was also found that all operators actively looked around at the other operators to see if any other operator needed assistance. Here it was suggested to add mutual awareness to be conscious on if another operator needed help or not. Mutual awareness has also been called the "cognitive empathy". Mutual awareness can also bring more timely co-ordination. Here it is also worth have the awareness about when it is the time for sharing information and advice to not overload the cognitive capacity.

Sarah Marie Brotnov has done a study on the cognitive ergonomics issues in the Norwegian Railway Operations [27]. In this study it is concluded with that the railway operations has a systematically variation of concentration and attention intensity. A positive factor is that the most demanding periods are often broken apart by less demanding periods which get the operator a possibility to not overload the cognitive capacity. In the paper it is also elaborated upon the railway infrastructure and how this affect the train operators. This can somewhat compare to informational screens for other kinds of operators in other sectors. In the study it was mentioned that there were found multiple context dependent signs and signals which would be more cognitive demanding and depend on the operators experience of the route. It was suggested to implement more context independent signs and signals in the future. When looking at accidents in Norwegian railway operations it was found that cognitive-related causes often was the main cause of the accidents. A sub-reason for this might be technical failures, unexpected events and/or task interruptions. So when the cognitive load already is highly demanding and then a technical failure comes into account this can elevated the risk, overload of the cognitive capacity of the operator and the probability of an accident rises. This technical failure can get compared to an cyberattack and this can be comparable to our topic.

In 2019 it was released a paper on "Self-Regulation and Cyber Agility in Cyber Operations" [3]. In this paper it was found that the demands and performance of cyber operators have both technical and human aspects and it is relies on skill-set of defenders to overcome attackers and the decision-making capabilities. Cyber operators need continuous updated technical knowledge which is changing continuously. They also need practical experience and training to make them quick learners and capable of adapting to novel and dynamic environments. Cyber agility is a term used in this paper and they define it as a construct of these three components:

- *Cognitive flexibility - agility to cognitively control and shift mental sets and overcome automatic or dominant responses.*
- *Cognitive openness - being receptive to new ideas, experience, and perspectives.*
- *Focused attention - ability to attend to relevant stimuli and ignore distracting ones*

During the study data was collected from self-regulation questionnaires where they self-reported their cognitive location in The Hybrid Space, defined as showed in figure 3. This data was collected during a cyber operation exercise of 4-days from 23 cyber cadets from the Norwegian Defence Cyber Academy(NDCA). The results from this study showed that there was a moderate positive relationship between self-regulation and cognitive agility. So by being self-regulatory you will expect increased cognitive agility [3].

2.6 SOC - Security Operation Center

Since cyberattacks have being increasing this has been affecting organizations with negative impacts like financial losses and denial of operations. However, security operation center(SOC) is something that is developed, sourced as a service and/or used by organizations to handle the impacts of cyberattacks. SOCs are design to detect, prevent and act upon cyberattacks which is crucial to limit the negative impact to the absolute minimum. SOC is staffed with roles like analysts, managers and

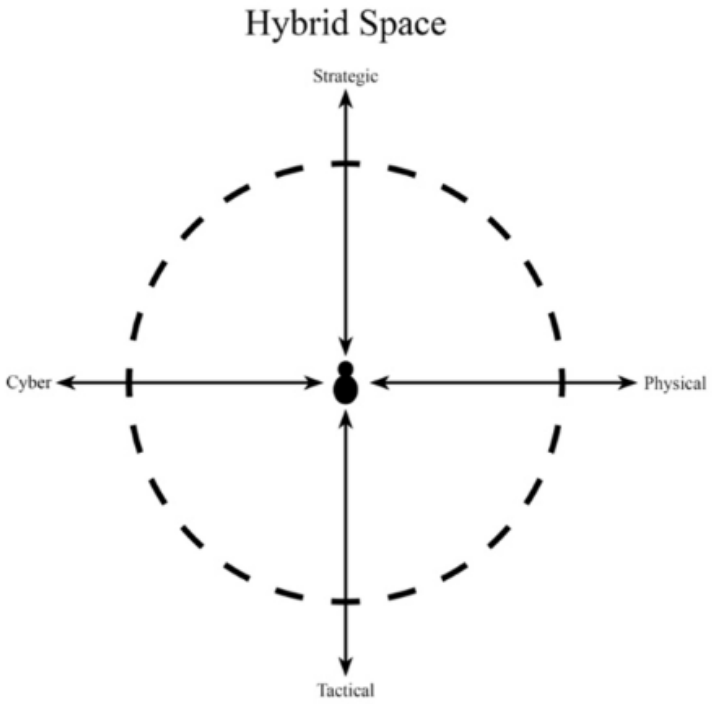


Figure 3: The Hybrid Space conceptual framework [3]

leaders. Their focus is to identify threats, anomalies and vulnerabilities. They will then respond to these depending on their interest. The response does often include many other parties depending on which organization that is affected by the threat. To be able to detect anything the SOC is dependent on receiving logging sources from various systems and equipment, which can include[28]:

- Routers
- Switches
- Firewalls
- IPS systems
- Web proxies
- Computers/Workstations
- Servers

These equipment need to be capable of forward all logs of interest towards the SOC, so the analysts can analyse the logs at a central point. The review and analysis of the logs are often done through a Security Information Event and Management(SIEM) system which is explained more about in sub-chapter 2.9 [28]. A SOC can look something like shown in figure 4, which is the SOC

of Telenor which is the largest telecommunication company i Norway.

Figure 4: Security operation center at Telenor [4]

In a study done on how to successfully develop and implement a SOC they have concluded with several different factors for successfully establish a SOC. These are displayed in figure 5 [5].

2.7 Control centers

Kongsberg Maritime is one of the companies that is focusing on getting autonomous ships a reality. They have created a conceptual illustration of how a remote operation center will look like in an autonomous ship environment [6]. This can be found in figure 6 and figure 7. Since this concept is so foreign for most of the stakeholders this illustration is meant to make an impression for the stakeholders to know what the remote operation center is all about. In a remote operation center captains can operate both remote and autonomous ships through the different remote control stations inside the remote operation center. So its two main functions are fleet monitoring and remote control. Fleet managers give tasks for remote control or monitoring to different captains. At the remote control stations captains verify status of the current ship when it comes to connectivity and critical vessel systems. From this station the captains can also communicate with all involved parties like the current port the ship is in for example. The captains can also adjust the ship's route plans and for example order it to go to an alternative port if required. For example when a ship has a failure on one of the systems or mechanical equipment it can be ordered to go to a specific port for maintenance. In the remote operation center they will also have fleet management stations to monitor autonomous ships at all times. Getting information of weather forecast and other crucial information related to each ships route. This makes it possible to manage many ships at once.

Factor	Basic Requirements
Human	1. Training 2. *Technical skills: a. Security monitoring b. Threat intelligence c. Incident management d. Forensic 3. Soft skills: a. Communication b. Teamwork *Depend on SOC functionality
Process	1. Define processes and procedures for all functions in SOC 2. Document the processes and procedures 3. Smooth and consistent operation
Technology & Elements	1. Management of log monitoring and collection 2. Analysis management 3. Incident management and response 4. Threat intelligence management 5. Forensic management

Figure 5: Basic requirements for humans, processes and technology [5]

2.8 Cyber-awareness in control centers

In control centers of any kind of operations it is important to increase the cyber-awareness to tackle the challenge with hackers and other cyber threats. In a study on "Real-time intrusion detection in power system operations" they established an algorithm on detecting cyberattacks. This algorithm was able to detect and alert upon 88 percent of the introduced cyber anomalies during the study. The algorithm used in this study was undeveloped and it is beleived that with even more testing and work with the algorithm it would be able to detect even more of potential cyberattacks. This shows that the use of intrusion detection systems with great algorithms will be able to increase and help control centers to detect and potentially act upon cyberattacks [29].

In operations of bulk handling ports it has also been done a study on cyber intrusion detection. The intrusion detection system will detect, process and analyze network traffic in the critical infrastructure and give alerts to the operators if anomalies are detected. In this study they have used machine learning to help with the intrusion detection. With the machine learning techniques it is dependent on real network traffic from the operations. In this study this was not conducted. However, the result in the study is still highly relevant for the control centers cyber-awareness. With the machine learning technique it is processing the real operational network traffic and defines what is normal. When the intrusion detection system then goes live in a production network it will gener-

Figure 6: An overview of the conceptual remote operation center created by Kongsberg Maritime. Image taken from their Youtube video. [6]

ate alerts when there is network traffic that deviates from what is defined as normal traffic. This is called anomaly detection of cyberattacks [30].

2.9 Information display

When it comes to cyber security it is normally used a SIEM to display information to a cyber security analyst. SIEM stands for Security Information and Event Management. In this study on SIEM it researched on the usage of SIEMs in critical infrastructures(CI). It was found that the security administrators in critical networks are dependent on gathering huge amount of data and also correlate these among the different CI systems. Due to this demand they often use SIEM to perform this collection and correlation of data. The problem to the current situation is that these SIEM solutions are not able to detect all the different cyberattacks relevant for the critical infrastructures. It was found that with the increasing number of different cyberattacks and their complexity, SIEMs can be a good solution to attack that challenge to help organization detecting mostly all types of cyberattacks. It is important to know that SIEMs need a lot and continuous work and improvement to be able to detect all kind of cyberattacks [31]. When it comes to information displays in maritime systems we often refer this to automation systems. K-Chief 600 delivered by Kongsberg Maritime is an example of such a system. This system is normally used in the control room of a ship and on the bridge of the ship. This system gives messages and alerts upon what happens in the systems

Figure 7: Conceptual remote control stations in the remote operation center. Image taken from Kongsberg Maritime's Youtube video. [6]

onboard. These alerts can get split into three different types. That is warnings, alarms and critical. These different types have their own dedicated color that indicates the urgency of the alert. These alerts can also get sorted into groups depending on their functionality onboard [32].

3 Sociotechnical perspectives

In this chapter we go into the socialtechnical perspectives of the systems in focus. Here we in detail describe which aspects are included into both the technical and the societal perspective and how these co-operate together.

3.1 Technical

In the concept of remote operation center we have several different systems integrated. For ships today and for the remote and autonomous ships safety sensors and safety alerts have been integrated to ensure the safety onboard. These systems gives output to several human interfaces used by the captain or operator of the ship. In comparison to this we believe that for remote and autonomous operated ships cyber security alerts will get integrated on a equally stage as safety alerts. In that matter the ship will have an intrusion detection system(IDS) to process, analyse and detect upon cyberthreats. When this IDS triggers an alarm it will display an alert in the remote operation center on the human interface used by the captain or operator of the ship. While that is in the ROC we also have the technical perspective extending into the SOC with much of the same information. The SOC will get the cyber security alerts just as the remote operation center, but will also be able to retrieve more logs and data to support with the analysis of the cyberthreat. This technical perspective may look something like shown in figure 8:

Table 2: Systems in focus

	Technical (figure 8)	**Social (figure 9)**
Above	Remote Operation Center (support from SOC)	Decision making
Focus	cyber security alerts (replicated to SOC)	Monitor alerts
Below	Intrusion Detection System	Cognitive capacity

3.2 Societal

Just as we have the technical perspectives there are several societal perspectives happen at the same time and in cooperation with the technical aspects. Like shown in figure 9 we have the high-level of the societal perspective as the decision making process. This process is the main objective when working as a captain or vessel operator. In regards to cyber security alerts or safety alerts the operator needs to monitor the alerts and process them to be able to perform decision making upon them. In some scenarios this task can be pretty rough when an overload of alerts happen at the same time. This may happen when the ship comes into an incident scenario, relevant to safety or cyber security. When this happen it will challenge the lower level of the societal perspective cognitive

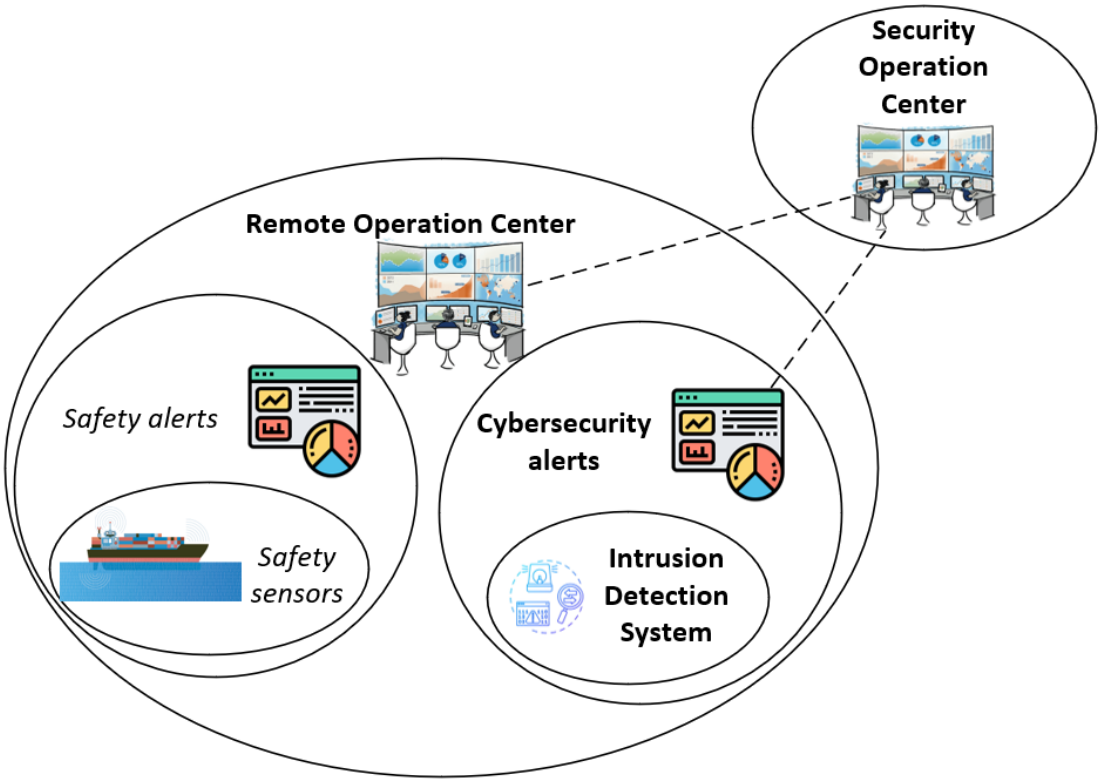


Figure 8: Systems in focus in the technical perspective

capacity. During normal operation this perspective might be not that loaded but then an overload of alerts will occur and an overload of the cognitive capacity may be the result of this. When the cognitive capacity gets overloaded human-errors are more likely to happen and bad decision can be made.

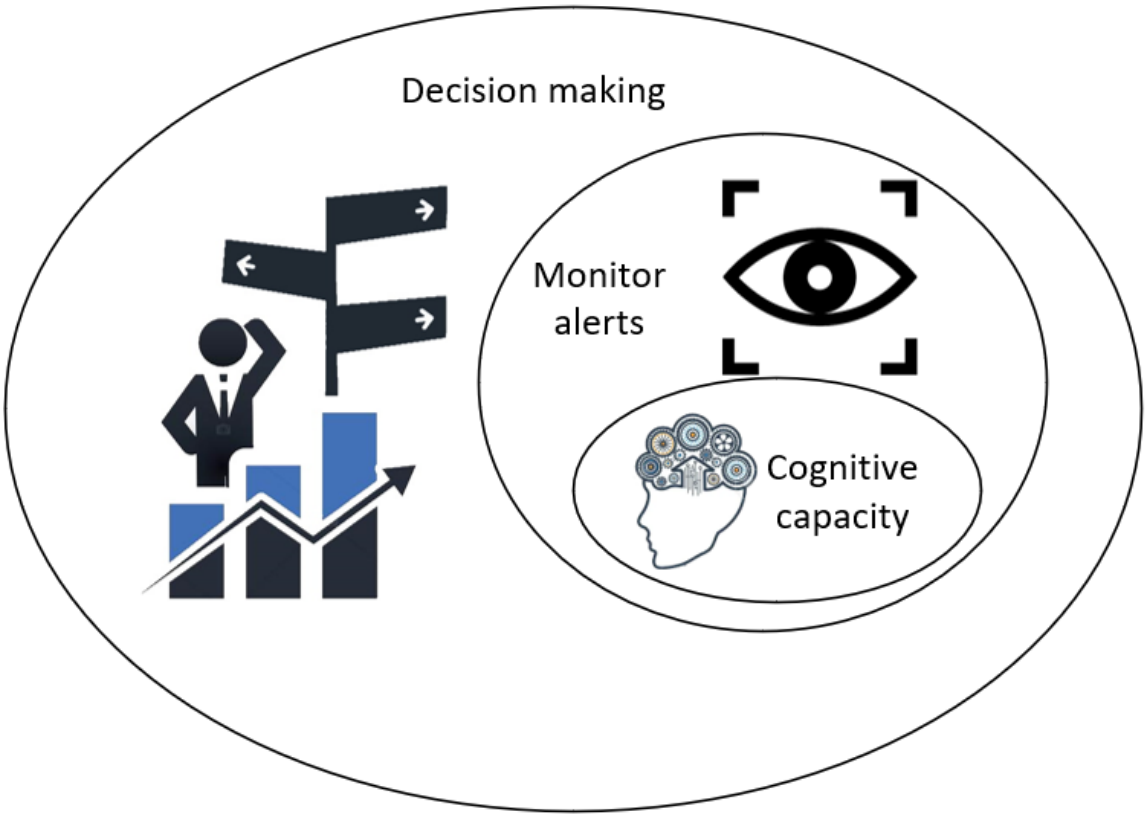


Figure 9: Systems in focus in the social perspective

4 Methodology

4.1 Focus group interviews

During the background literature analysis, no related work was found cyber security alerts in remote operation center and no work on merging of cyber security alerts and safety alarms into same alarm system. Given that the concept of merging cyber security alerts and safety alerts in a remote vessel is a new area focus groups research methodology was used to collect data on the product mock-ups. Focus groups are a method used when a researcher guides three to ten participants through open-ended questions about a certain topic. This method is a qualitative interview method where it focuses on the in-depth motivations and thought processes behind the participants experience [33]. Since this master's thesis is done towards systems related to ships and cyber security we have chosen to interview both captains and cyber security analysts. This has help us collect data on how captains make decisions using the tacit knowledge. Together with this we have learned how cyber security alerts should be formulated and how cyber security analysts may contribute and support a remote operation center. This has made the project having a "practical" and an user-centered perspective to the problem. As shown in figure 10 tacit knowledge is defined as [34]:

- Intuitive knowledge
- Know-how
- Knowledge rooted in context, experience, practice and values.
- Knowledge hard to communicate- since it resides in the mind of the practitioner.
- Knowledge that transfer during socialization, mentoring and etc.

4.2 Information analysis

A holistic approach is used to make an analysis of the qualitative data collected from the literature study and focus group interviews to analyze and come to a solution for the chosen research problem. Holistic approach is when you have one specific object/situation that you are observing and then take a step back to recognize the bigger picture around this object to understand the whole situation. This approach has its origin form the health care and specifically from Hippocrates that told people to stop focusing on single parts of the body or illness, and rather expand it to looking at the whole person. However in other industries this kind of approach is relatively new and not broadly used yet [35]. In research and problem solving a result may sometimes be correct when talk about it as a standalone perspective. However when having this research and problem connected with other parts the result may be weakened or rejected due to the effect the connected elements do to the focused research or problem. An example of this can be a bug in an information system. When the developer tries to fix this bug it may get fixed on a standalone system and everything

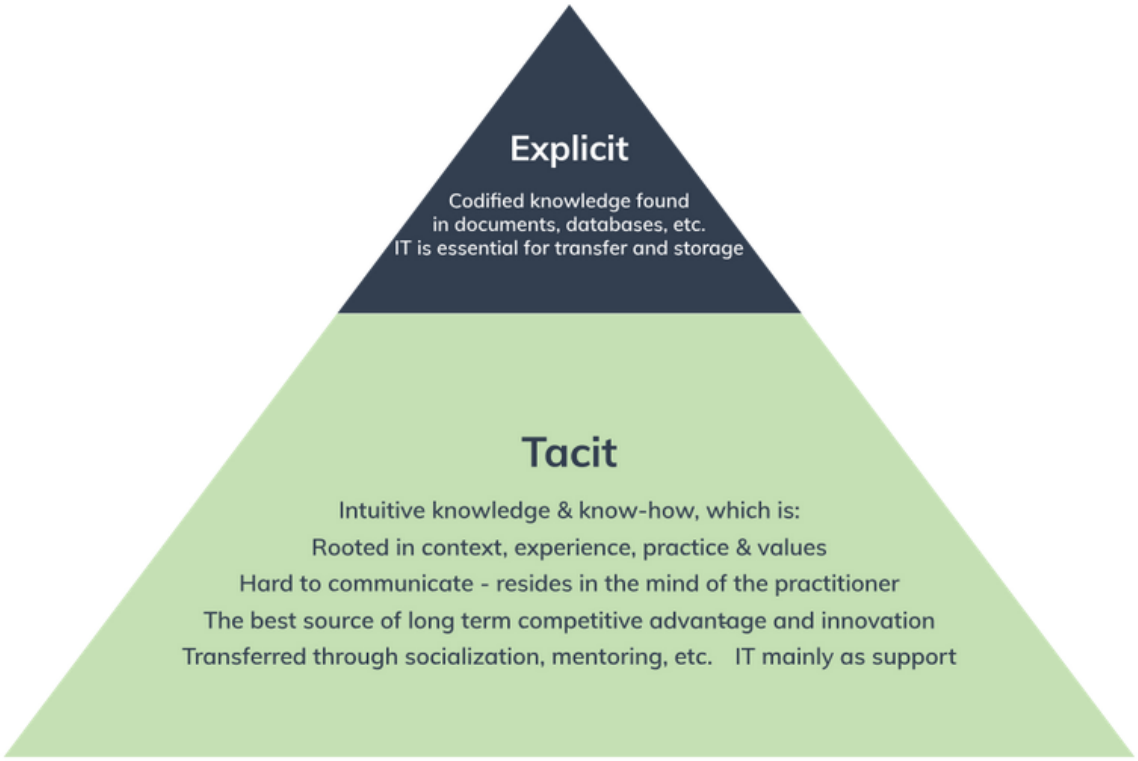


Figure 10: Definition of Tacit knowledge vs Explicit knowledge

seems to work correctly. However, when this information system gets connected to the enterprise network the bug is back. If the developer had done a holistic approach when solving the bug. The bug would get fixed when the information system was still connected to the enterprise network.

4.3 Create mock-ups

Based on the literature study also found in chapter 2 we have made alternatives to mock-ups for a human machine interface for displaying cyber security alerts together with safety alerts. Together with this we have made user-stories for how cyber security alert handling process might look like for the same alternatives from the human machine interfaces. Thereafter we have used this in the focus group interviews to have some concrete to discuss. Based on this qualitative and applied method we have used the knowledge learned to conclude with a proposed a human machine interface and cyber security alert handling process for the remote operation center.

5 Mock-ups

In this chapter we present mock-ups that will be used during interviews as reference. This will be models of how we potential consider how the human machine interface and cyber alert handling process might look like in a remote operation center concept.

5.1 Human Machine Interface(HMI) mock-up

Due to lack of time and resources we based this HMI mock-up on what was shown by Kongsberg Maritime as shown in figure 7. Together with this we added new idea to develop alternatives.

5.2 Alternative 1: Alert list

In the first alternative we consider a case where the captain is getting all the cyber security and safety alerts in one single list. The fleet management and the captain seat will conserve the same information but the fleet management is the one that is doing the main assessing of the alerts. This is also to decrease the amount of cognitive load for the captain. In this case the HMI might look something like shown in figure 11.

Figure 11: A mock-up of how HMI alternative 1: Alert list might look like

In figure 11, you can see at the right an alert list of the current alerts. Here you will find the latest alerts with the newest one at top, together with the severity. This alert list is merged with safety alerts.

5.3 Alternative 2: Status indicator and alert list in fleet management

In this alternative the captain will not receive the full list of alerts but based on the alerts there will be a status indicator of cyber security alerts with neutral, yellow and red status lights. The fleet management will as in alternative 1 get the full alert list and is the station that need to handle the alerts. They need to communicate with the captain to give the actual status of the cyber security on the ship based on advice from a Security Operation Center(SOC). In this case the HMI might look like shown in figure 12 through 14 based on which status it is indicating.

Figure 12: A mock-up of how HMI alternative 2 with status neutral

At the fleet management station they will find a complete overview of the status and all the different alerts. This needs to be used while requesting advice from the SOC and while communicating the status to the captain. How this will look like is not in scope of this paper.

5.4 Cyber security alert playbook

In this section we used the two different alternatives mentioned in last section and make a playbook on how to handle cyber security alerts between the different actors. To make this playbook we used user-stories and try to showcase how it would go on in a real scenario.

Figure 13: A mock-up of how HMI alternative 2 with status yellow (moderate)

5.5 Alternative 1: Alert list

In this first alternative we consider that we have two actors included into the handling of cyber security alerts. This is the captain operating the vessel and the supporting role of the cyber security analyst. The main activities included in this playbook for the captain is, operating the vessel and monitor and manage the alarm system which will display the cyber security alerts. In the rest of figure 15 we include all the tasks and iterations relevant for the situation right before and during the cyber security alert has triggered. The arrows visualize orders and communication lines between the different actors. At iteration 1 the actors performs the tasks during a normal state of their activities. From iteration 2 to 7 we find the different iterations and tasks that shall be done by the actors when a cyber security alert has triggered. In the last iteration we include the tasks done after the cyber security alert has been handled from the included actors. The rest of the incident handling process after iteration 8 is now handed over to the stakeholders and will not be included in this paper.

5.6 Alternative 2: Status indicator and alert list to fleet management

In the second alternative we added one more actor, the engineer, that will handle the main activity of monitor and manage alarm system. This task was assigned to the captain in alternative 1. All the iteration is the same, but with several new tasks which includes orders and communication between the different actors also visualized by arrows. The captain will in this alternative have less tasks relevant for the cyber security alert which will also decrease the amount of cognitive load.

Figure 14: A mock-up of how HMI alternative 2 with status red (severe)

You can find the whole playbook in figure 16.

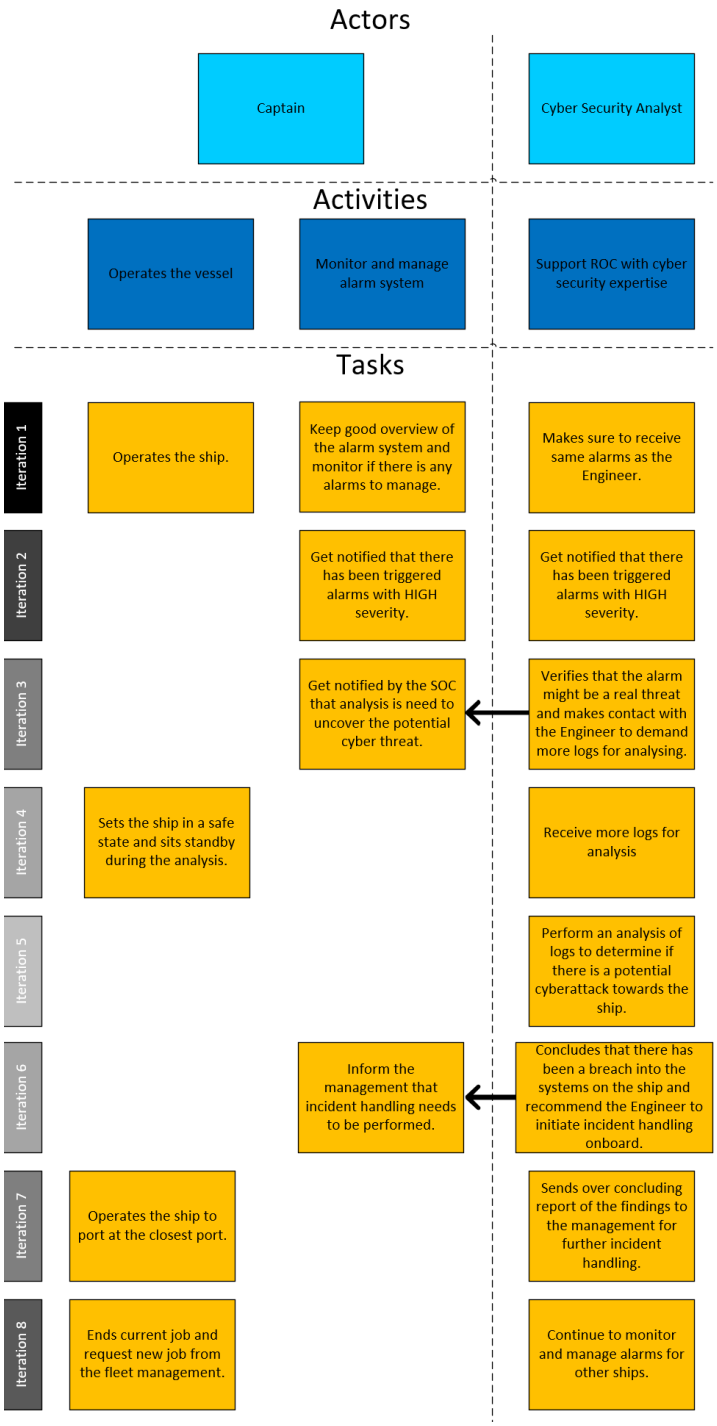


Figure 15: User-story of the cyber security alert playbook between captain and cyber security analyst.

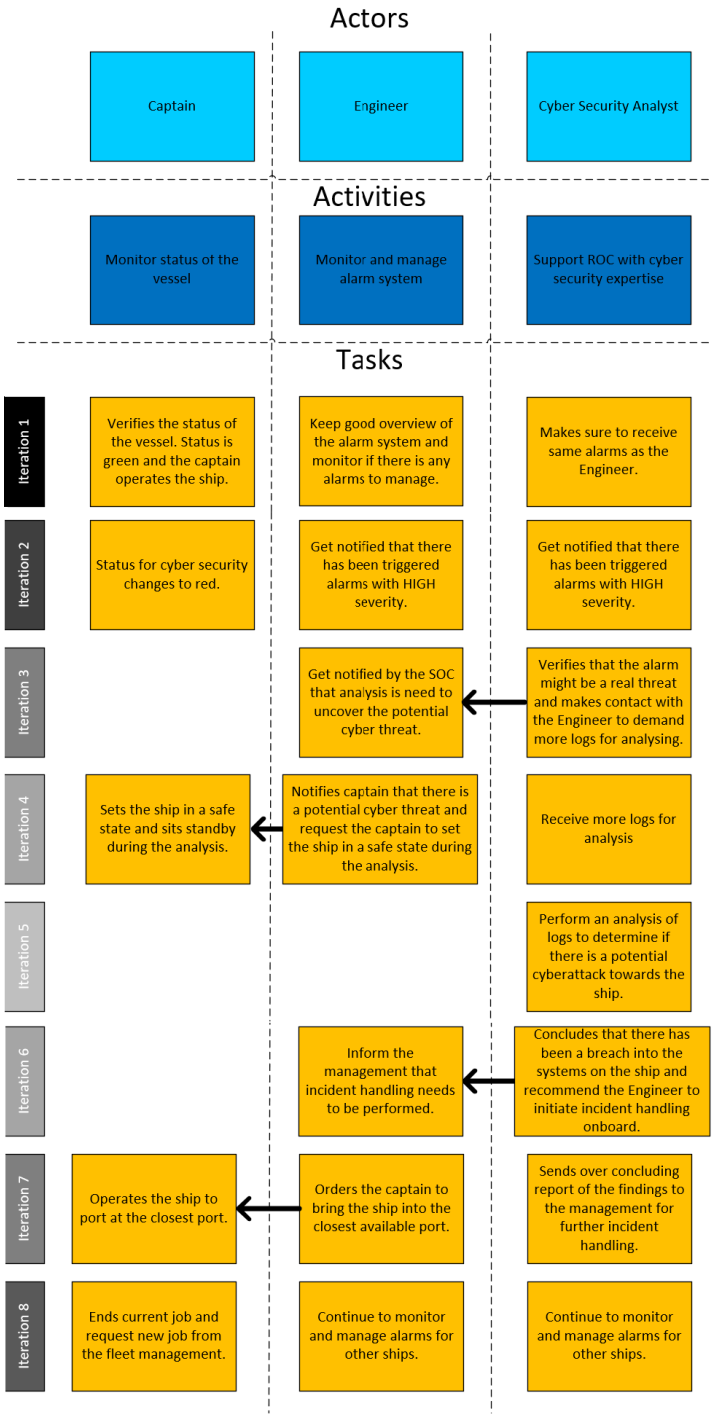


Figure 16: User-story of the cyber security alert playbook between captain, engineer and cyber security analyst.

6 Data collection

Since the concept is new we were only able to do some data collection from the parties expected to get included into this concept in the future. The goal with this is to collect tacit data on how the parties are working today and what they believe will be key points to include into the remote operation center concept. The main roles in these interviews were captains and cyber security analysts working in a SOC. During the literature analysis there was not found any other work done on merging safety and cyber security alerts into one alert system for a vessel operator. Due to this we want to perform a focus group interview, with three participants in each group. To gather as much of knowledge as possible through discussions and open-ended questions. This helped to get some of the tacit knowledge that is important in such a new topic. The interviews are performed in Norwegian. Both the Norwegian and English version of the questions can be found in appendix A and B.

6.1 Focus group interviews

6.1.1 Group: Captains

In this group we gathered three experienced captains as participants:
Captain 1:

- Job title: Captain
- Experience: 3,5-4 years
- Workplace: Norwegian well boat shipping company

Captain 2:

- Job title: Chief Officer
- Experience: 3,5-4 years
- Workplace: Norwegian well boat shipping company

Captain 3:

- Job title: Chief Officer
- Experience: 2,5-3 years
- Workplace: Norwegian well boat shipping company

All the questions for the captains were first made in English and then translated to Norwegian since all participants were Norwegians. They all got the questions for preparations together with this Youtube-video [6]. The interview took place at my house to establish a calm and comfortable context.

Summary of the interview with the captains:
Safety alert experience from the past:

- Not many safety alerts that goes of. It is more usual that other alerts goes of like machinery alerts and control system alerts.
- The alerts system triggers a lot of false positives and especially on new ships. These alerts is not always understandable why they trigger. False positives are getting acknowledge or silenced. These alerts get still shown until the engineer has verified that the alert is a false positive.
- Several different alerts have time requirements depending on sensors detecting the property it is alerting upon. How these alerts look like and are displayed to the captains are based on specification given from the supplier of the alert system. These descriptions are very general and not always good described. This makes the captain uncertain how to handle different alerts.
- To have an alert expert for general alerts existing today would not necessary help on the cognitive load for the captains. When it comes to cyber security alerts the captains desired that they needed a cyber security alert expert for support. This is due to minimal cyber security expertise in their role today.

Merging safety alerts and cyber security alerts into same system (mock-up of alert system in ROC):

- Cyber security alerts were highly desirable by the captains. They see the increase of interconnectivity and cyber security alerts may fit into their already existing alert systems. It was discussed that when cyber security alerts are integrated to already alert system this may lead to even more false positives. This can again lead to more cognitive overload and lack of focus to the main objective for the captains. The captains could also benefit from a separate screen with only cyber security alerts to just verify the status of the cyber security once in a while. The captains said that they sometime have missed some information regarding the status of the network or cyber security of the system onboard and especially when they receive mails regarding cyberthreats that have been detected for several days ago. They would benefit from knowing that while it happens.
- The captains desirably wanted cyber security alerts with information on which system that is under a cyberattack and said that this is the main key for them regards to cyber security alerts. It might be beneficial with information in regards to possible mitigation like when to shutdown systems that is not crucial for the specific operation for example.
- When alerts get triggered it should just get triggered once per event and not periodically. This would lead to too many alerts and might have lead to cognitive overload for the captains.
- The captains do not have any kind of cyber security related training today.
- The captains would like to just have status regards to cyber security alerts and safety alerts and having someone else to analyze and advice regards to the actual alerts. This would give

them higher cognitive capacity, due to not looking at alerts and assessing the situations based on these alerts.

Support from Security Operation Center(mock-up of cyber security handling process):

- To get support from a Security Operation Center would be desirably both in their operations today and for the remote and/or autonomous concept.
- When potentially working in a remote operation center it may be more wanted to have alternative 2 (figure 16) where the engineer is talking directly to the captain and the cyber security analyst. For the captains to have a direct communication line to the cyber security analyst would be too much information and less focus on the main objectives.

Thoughts on the mock-ups:

- The captains really like HMI alternative 2 (figure 12 to 14). One of the captains said that they also would like to have a hybrid solution between alternative 1(figure 11) and 2(figure 12 to 14). In that case the captain can be able to click on the status indicator and then get the list of the alerts generating the yellow or red status. In that case the captain will get the needed information if desired instead of stay more uncertain in situations where the engineer has trouble or having a huge job assessing the current situation.
- The captains liked the communication lines in alternative 2 16 but see that there should be done a job making playbooks of how to handle different scenarios. They did not like the idea of having to communicate with a cyber security analyst directly. The captain pinpointed that the most important in regards to cyber security analyst is to know which systems that is affected by a potential cyberthreat. So they know which system they can use or not and to know how to mitigate as much as possible when it happens.

6.1.2 Group: Cyber security analyst

In this group we we gathered three experienced cyber security analysts as participants:
Analyst 1:

- Job title: Cyber security engineer
- Experience: 6 years
- Workplace: Norwegian SOC

Analyst 2:

- Job title: Cyber security analyst
- Experience: 3 years
- Workplace: Norwegian SOC

Analyst 3:

- Job title: Cyber security analyst
- Experience: 2 years
- Workplace: Norwegian SOC

All the questions for the cyber security analysts were first made in English and then translated to Norwegian since all participants were Norwegians. They all got the questions for preparations together with this Youtube-video [6]. The interview took place at their workplace when I was on a visit.

Summary of the interview:
How is your working process today:

- An alert goes of and an indicator is found to narrow down the further analysis. The first part of the analysis goes on if the alert is a false alert or an actual threat. If it is an actual threat the goal is to find some indicators of compromise that ensures and proofs that a cyberthreat is real. During the log analysis it is also useful to use information from one log to correlate with other logs to describe an overview of what has happen on different systems. We can use dashboards of data to structure this data to see correlation and unusual behaviour. For example if you see unusual high network traffic towards one system.
- It is situation specific if the SOC-team helps with incident handling or not. It is also dependent on the party getting the support if they are paid to perform the incident handling or not. If it is a larger and more severe cyberthreat the supported party often establish an incident handling board that hires in technical incident handling teams that performs the low-level technical analysis of the cyberattack. However, the SOC needs to continue to monitor alerts regards to new potential cyberthreats. This may be different from SOC to SOC.
- The most important parts to know about is assets, trigger context of alerts and detailed descriptions on the alerts and logs. Together with this it is very usual to have hash values on files and malware related to the cyber security alerts. It is also dependent to have relevant logs to a specific cyber security alert, instead if having just a huge bunch of logs and you need to categorise these before an analysis can be done.
- Since our SOC is mainly monitoring IT system alerts and analysis are not very real-time dependent and it can take hours and days before receiving the alerts without problems. As long as the logs are standardize and common it is the most effective. And it is not necessary to receive logs that is just a bunch of encrypted data or logs from a temperature measurement system which has no importance to the cyberattack.

Support remote operation center (mock-up of the human machine interface):

- That a cyber security alert goes of. A common challenge is false positives and then we talk about a lot of false positives. This may disturb the operator in the remote operation center. Another problem is that if you implement more logging and alert triggers into a system there might be even more false positives. The remote operation center needs to be aware that false positives will happen.
- Asset-name, criticality of the system and description of how this system behave in normal operations.

Communication with operator at remote operation center (mock-up of the cyber security han-

dling process):

- To effectively communicate the cyber security incident to the remote operation center the ships are desired to be standardize when it comes to how the systems are onboard. It may also be desired by the SOC to have several system architecture experts in the SOC to support the other cyber security analyst. This is also due to the lack of knowledge regards to OT systems vs IT systems. We use to scale down the incident and more high-level description of the incident. We can advice them to not use a certain system but the most important message is to not shut it down when it is desired to keep logging on the certain system. In a remote operation center case it may be useful to give this information due to this is more related to OT systems. This is also dependent on the common knowledge regards to which system can get shut down and not.
- A possibility to call someone regards to OT systems and the system architecture on the ship may be desired. More knowledge regards to OT system is desire and also the difference between OT and IT systems to be able to switch mindset. For example the mindset that you now are supporting and analysing cyberthreat regards to physical systems where safety is important.
- Competence and knowledge around OT systems are desired. The analysis methodology may also differ from how we analyze today and this needs to be learned and experienced.

Thoughts on the mock-ups:

- The cyber security analysts assume that the HMI alternative 2 (figure 12 to 14) will work best as long as they now who to contact and communicate with and has confident that he/she will get the support and updated status as soon as possible.
- It is desire to have an engineer that have more knowledge about the ship and systems onboard to communicate and support the SOC in the analysis. It would be nice if this communication sequence would work in practice. But there may be a lot of this that needs to work to be able to have the communication sequence like this. A challenge here is the mandate to actually command a ship to go into a safe state and shut down operation which will include loss of income. Here it is needed to have a management leader that can perform and decide these decisions. This is also due to the management having a common understanding of the risk of shutting down the operation versus getting hacked and losing capability of continuing the operation. Here it is suggested to add an extra actor into the cyber security alert handling process to decided upon this.
- That extra logs is going to get downloaded from the vessel could be smart to do periodically, so that the SOC got some logs to start analyzing immediately and it may be found that a cyberthreat already was seen in the systems at an earlier stage. This periodically transfer of logs may be done at a time where the ship is at port for example. An extra point is to always send the logs to the remote operation center in case of the vessel to lose connection to the remote operation center. Then the logs can get retrieved from the remote operation center to

the security operation center. To analyze cyberattacks regards to OT systems are in our eyes not highly explored yet and there is much to learn around this. It may also be good to use the experience from IT cyberthreat analysis and reuse as much as possible into the OT analysis.

7 Human Machine Interface sketch design

Based on the mock-ups created as preparation for the focus group interviews and the interviews them self. We used this to elaborate on a recommended Human Machine Interface for displaying cyber security alerts in a maritime remote operation center. This is just recommendations and should be considered tested before used in production.

7.1 Recommended HMI

Since the mock-up was based on the illustrated HMI by Kongsberg Martime in figure 7. We used this HMI and add features to it to make it more suitable based on the feedback and inputs collected during the interviews.

During both focus groups it was agreed on that HMI alternative 2 shown in figure 12 through 14 may be the best alternative. In this alternative we are using the status indicator concept to visualize the status of the cyber security property of the remote/autonomous ship. This is visualized as a padlock symbol in the top right corner. If this padlock has no color, this means that the cyber security property has a neutral status and no cyber threat is present. When this padlock get colored yellow this means that it is found a moderate cyberthreat status based on the received cyber security alerts. If the status indicator turns red this means that the cyber security property status has changed to severe. In these cases the engineer at the fleet management level at the remote operation center will have the overall overview of the alerts and is responsible to assess the alerts with help from a security operation center. During the interviews the captains discussed a scenario where the cyber security status changes and the captains cognitive load gets affected by this. To cope with this situation the captains elaborated that this cognitive distraction may get relived by being able to get displayed and take a quick look at which cyber security alerts that generated the current status. A good example when this might get useful is when there has been cyber security alerts going of the last days that was consider to be false positives and these same alerts goes of again the following day. Then the captain can take a quick look at the alerts and do a quick assessment that this might be the same false positives as the last two days and just continue the operation without having the cognitive load being affected by these cyber security alerts. These points concludes our result for the HMI and can be found in figure 17 and 20.

Figure 17: Recommended HMI: Neutral status indicator (padlock symbol)

Figure 18: Recommended HMI: Yellow status indicator (padlock symbol)

Figure 19: Recommended HMI: Red status indicator (padlock symbol)

Figure 20: Recommended HMI: Red status indicator (padlock symbol) with alert list that can get shown on demand from the captain.

8 Cyber security alerts handling playbook

Based on the mock-ups created as preparation for the focus group interviews and the interviews them self. We used this to elaborate on a recommended cyber security alerts handling process with the intention of being a playbook on how the different actors are supposed to communicate and act upon a cyber security alert. This is just recommendations and should be considered tested before used in production.

8.1 Recommended playbook

As for the HMI we also used alternative 2 mock-up shown in figure 16. Both focus groups found the communication sequences as a good foundation as a playbook for them. They were not convinced that this would always work but that will time show during a potential test of this playbook. Anyhow the cyber security analysts said that they missed an actor that has the responsibility for the business continuity for the owners of the remote and/or autonomous ship. They as the supporting SOC will not be confident to order a ship out of operation just based on their cyberthreat assessment and recommendations. There should be some stakeholders that know the threshold for order a ship out of operation or not. We call this actor the business continuity manager and is a part of the fleet management team in the ROC. The captains were satisfied that someone at the fleet management has the responsibility to communicate to the SOC. This will stabilize the cognitive load around the cyber security factor. In other words, introducing cyber security alerts will not affect the captains workflow in a too huge matter if the fleet management handles this communication and assessment of cyber security. This concludes our result for the recommended playbook which can be found in figure 21.

8.2 Key factors for communication

Based on the focus group interview with the cyber security analyst we discussed and concluded on the following key factors for communication during a playbook like this:

- All actors knows the agreement of the support from the SOC. For example if the SOC just support with cyberthreat detection and advice. The ROC and the stakeholders need to be able to receive the advice from the SOC and use this to assess the situation if a incident handling team is needed or not.
- The cyber security analysts need to get familiar to the mindset of OT systems. Since analysts are mostly familiar with only IT systems.
- The cyber security analysts and the fleet management needs to have a common understanding of which systems onboard is essential and which are "fun to have"-systems.
- The trigger context of the cyber security alert is important to have the correct situational

awareness.

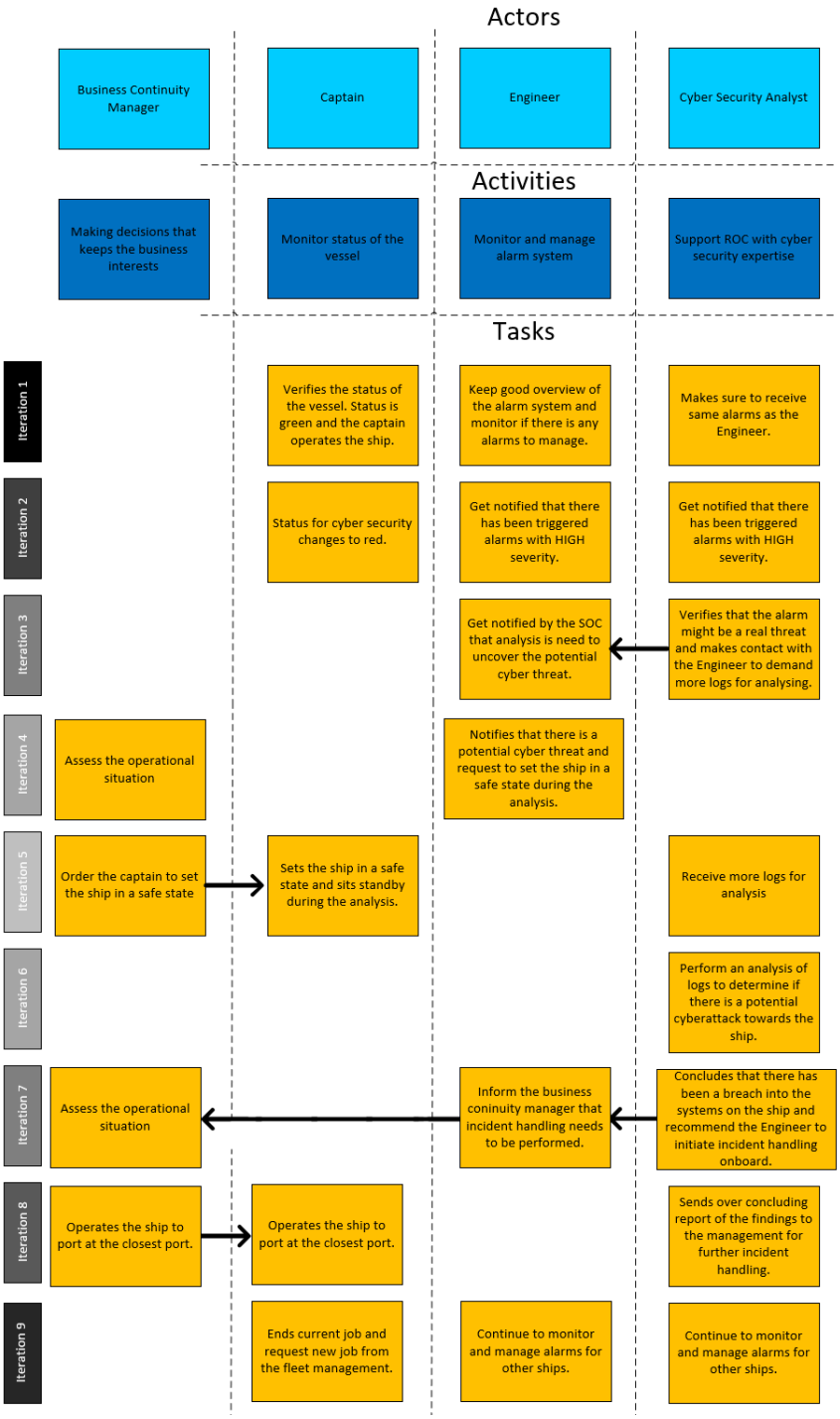


Figure 21: User-story of the cyber security alert playbook between business continuity manager, captain, engineer and cyber security analyst.

9 Discussion

We found early during the literature study that there is a limited amount of previous studies done on this subject. We consider the reason for this may be that remote operation center has not been commercially used for a very long time and that military drone remote operation centers are classified and therefore no public documents to find on this. We also found that maritime remote operation centers are an even newer concept where the huge marine technology company Kongsberg Maritime has not fully developed this concept yet for production on commercial ships. In that matter a systematic literature study was not the methodology used to answer the research question of this thesis.

However, we found that interviews of captains and cyber security analyst would fit better. It was first consider to be a big survey to collect data regards to remote operation center and the cognitive load working there. Here we found the same challenge as for the literature study that there is none to few maritime remote operation centers existing today. This made it hard to collect enough answers to the survey due to limited people working with remote operation center in a maritime context. It was here found that focus group interviews would fit better to do qualitative interviews with both captains and cyber security analysts. During the interview with the captains it was mentioned by one of the captains that well boats might not be done autonomous ever. This might be correct and we should have performed the interviews with captains of cargo ships instead.

To have some concrete material to discuss during the interviews we made some mock-ups. HMI mock-up work was simplified by using the concept shown in the Youtube-video provided by Kongsberg Maritime [6]. We wish that we could create a better representation of the HMI. However, due to time and lack of resource we considered this to be too much work and would fit better for someone that works with HMI and user-interfaces.

There was not done any measurement of the cognitive capacity and how demanding a remote operation center work process is during this thesis. This is also due to time and lack of resources to perform such study. We would also need a fully operational simulator for such a measurement. This was not something we were able to put together during this study but will be highly recommended for future work.

9.1 Remote Operation Center

A topic that has not been discussed in this thesis is that the remote operators of the ships may be expected to keep overview of multiple ships at the same time and how this affect their cognitive capacity. They may also be expected to move from remotely controlling one ship to another in a short amount of time. This may also be cognitive demanding. In the same scenario the fleet management need to monitor and have the full overview of all the different remote and/or autonomous

ships in their responsibility. Depending on how many ships they need to monitor the cognitive load will increase accordingly. We also consider that each shipping company that will use remote and/or autonomous ships will have one single remote operation center controlling and monitoring all their relevant ships. Another technical perspective is the connectivity between the ships and the remote operation center. This connectivity need to be robust and reliable to be able to avoid dangerous situations if something gets wrong in any of the systems onboard.

9.2 Cyber security alerts

For cyber security alerts to work in this context it is required that the ships have intrusion detection systems(IDS) that are able to understand OT and IACS systems. If this IDS solution goes too deep and are too complex this often results in a lot of false positives. This should be avoided as much as possibly in a maritime remote and autonomous context due to the cognitive load this can lead to when the opertors gets spammed with alerts. This can also lead to loss of confidence to the cyber security alerts and they will lose their effectiveness when a real cyberthreat comes present in the systems on a remote or autonomous ship. As discussed during the interviews the descriptions of cyber security alerts are a crucial factor. The challenge here is to create descriptions that are effective for both the captains and the cyber security analysts. The problem here is that a desired descriptions for the cyber security analysts may have too much information or use too complex terms for the captains to understand. And the same if we create too general descriptions with too little information for the captains this can make the cyber security alerts not useful for the cyber security analysts.

9.3 Support from Security Operation Center

The hardest part of the concept discussed in this thesis may be the connection between the cyber security alerts at the ship and remote operation to the Security Operation Center. To make this possible the correct technical infrastructure needs to be in place, both for the transfer of alerts and logs, but also for the communication line. The common knowledge should be synchronized between the alert expert at the fleet management in the ROC and the cyber security analyst in the SOC. When a cyberthreat gets present and depending on the size of the potential cyberattack the lead management to the ship owners need to have a good incident handling plan established and have agreements with an incident handling team that may be requested for the handling of the cyber incident onboard a ship. If this team needs to be shipped out to the ship while in a so called "safe state" or if the ship is able to port at the closest port is also questions that needs to get answered in another study. Due to this remote concept and the ship is on the other side of the world it makes the whole cyber incident handling process much more complex.

9.4 Future work

Since the maritime remote and autonomous ship concept is in early stages of development and testing. There are several things that can be studied on for future work. Some of them is listed below:

- Technical design on how to merge cyber security alerts into a status indicator.
- Perform cognitive capacity measures of captains working in a remote operation center.
- Perform cognitive capacity measures when captains uses the recommended HMI from this thesis.
- Perform cognitive capacity measures when captains and cyber security analysts uses the cyber security alert playbook recommended in the thesis.
- When ROC is in production: Perform a quantitative interview/survey to the same topic.
- When ROC is in production: Dig deeper into the possibilities and ideas on how to solve this research problem even better than in this thesis.
- Design and create a simple and effective HMI to show status indicators and/or alert lists for use in a remote operation center.
- How can cyber security alerts be described to be useful and effective for both the captains and the cyber security analysts.

10 Conclusion

The next era of maritime systems are going in a remote and/or autonomous direction. This includes that the ships will be monitored and remotely controlled from remote operation centers(ROCs). To make this happen the ships need to become more interconnected. This will lead to a larger cyber threat surface and the risk of cyber attacks may increase. To be able to cope with this challenge these remote operation centers will receive cyber security alerts from these remote and/or autonomous controlled vessels. Since cyber security alerts for the captains are unusual we need an effective way of introducing these alerts into the workflow for captains. We made mock-up of potential examples of how cyber security alerts may be displayed in a remote operation center. We also provide a mock-up playbook for the different actors to communicate when a cyber security alert gets triggered. These mock-ups were used under focus group interviews with both captains and cyber security analysts to receive inputs and feedback. In the end we connected the results of the interviews and the mock-ups to create recommended human machine interface(HMI) for displaying cyber security alerts and a recommended playbook to communicate between the actors to know if the cyber security alert is a real cyber threat and if incident handling response process need to be engaged in regards to this cyber security alert. The recommended HMI for displaying cyber security alerts includes a status indicator for the captains with a possibility to get an overview of the alert list to keep situational awareness if needed. The main responsible for the alerts will be the engineers sitting at fleet management and receive advice from the Security Operation Center that the cyber security analysts who produce the alerts along with other logs. Based on the cyber security alerts the cyber security analysts need to communicate recommendations and information regards to the alert to help the ROC to know if the cyber threat is real or not. If the cyber threat is present a decision will be made by the business continuity manger to decided if the operation should go into a safe state to handle the cyber incident or if the cyber risk is known but accepted. These sequences of communication and decisions are described in the recommended playbook for cyber security alert handling.

Bibliography

[1] I. Im, D. S. & Jeong, J. 2018. Components for smart autonomous ship architecture based on intelligent information technology.

[2] Ringbom, H. 2019. Regulating autonomous ships—concepts, challenges and precedents.

[3] Øyvind Jøsok, Ricardo Lugo, B. J. K. S. S. & Helkala, K. 2019. Self-regulation and cognitive agility in cyber operations.

[4] Telenor website. URL: https://www.telenor.no/bedrift/sikkerhetstjenester/sikkerhetssenter/.

[5] Majid, M. A. & Ariffin, K. A. Z. 2021. Model for successful development and implementation of cyber security operations centre (soc).

[6] Maritime, K. 2021. Kongsberg maritime - remote operation center. URL: https://www.youtube.com/watch?v=UPtdgiIrlJI.

[7] Organization, M. S. D. I. M. 2018. Autonomous ships view of the imo secretariat. URL: https://www.nmri.go.jp/study/contribution/WS_on_MASS/(0)%20Autonomous%20ships%20View%20of%20the%20IMO%20Secretariat.pdf.

[8] Sae international releases updated visual chart for its "levels of driving automation" standard for self-driving vehicles. URL: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles.

[9] Explanation of the 6 levels of driving automation. URL: https://blog.rgbsi.com/6-levels-of-driving-automation.

[10] Larsen, H. 2021. Cyber-risk assessment of remotely and autonomously navigated short-sea shipping vessels.

[11] What is a intrusion detection system? URL: https://www.barracuda.com/glossary/intrusion-detection-system.

[12] What is antivirus software? URL: https://www.webroot.com/ca/en/resources/tips-articles/what-is-anti-virus-software.

[13] What to know about vulnerability scanners and scanning tools. URL: https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/.

[14] What is a security operations center (soc)? URL: https://digitalguardian.com/blog/what-security-operations-center-soc.

[15] Vinnem, J. E. & Utne, I. B. 2018. Risk from cyberattacks on autonomous ships.

[16] Jaime Pancorbo Crespo, L. G. G. & Arias, J. G. 2019. Autonomous shipping and cybersecurity.

[17] Autoship - autonomous shipping initiative for european waters. URL: https://www.autoship-project.eu/.

[18] Mv yara birkeland. URL: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/.

[19] Kongsberg maritime and massterly to equip and operate two zero-emission autonomous vessels for asko. URL: https://www.kongsberg.com/no/maritime/about-us/news-and-media/news-archive/2020/zero-emission-autonomous-vessels/.

[20] M. Vielberth, F. Böhm, I. F. & Pernul, G. 2020. Security operations center: A systematic study and open challenges.

[21] J. Hong, J. Lee, H. L. Y. C. K. C. & Cha, S. K. 2019. Alertvision: Visualizing security alerts.

[22] Kristensen, S. D. 2021. Risk acceptance criteria for autonomous ships.

[23] M. Grootjen, M. A. N. & Veltman, J. A. 2007. Cognitive task load in a naval ship control centre: from identification to prediction.

[24] Kumar, N. & Kumar, J. 2019. Selection of control panel design using cognitive load parameters based on physiological data: An experimental study.

[25] U. Afzal, A. Prouzeau, L. L. T. D. S. B. A. L. & Goodwin, S. 2022. Investigating cognitive load in energy network control rooms: Recommendations for future designs.

[26] Artman, H. & Wærn, Y. 1999. Distributed cognition in an emergency co-ordination center.

[27] Brotnov, S. M. 2007. Railway driving operations and cognitive ergonomics issues in the norwegian railway: A systems analysis.

[28] Thompson, E. C. 2020. *Designing a HIPAA-Compliant Security Operations Center*. Apress, Dekalb, IL, USA.

[29] Jorge Valenzuela, J. W. & Bissinger, N. 2013. Real-time intrusion detection in power system operations.

[30] Kim Monks, E. S. & Moustafa, N. 2018. Cyber intrusion detection in operations of bulk handling ports.

[31] Gustavo González-Granadillo, S. G.-Z. & Diaz, R. 2021. Security information and event management (siem): Analysis, trends, and usage in critical infrastructures.

[32] Yunus Emre Senol, E. M. & Arslan, O. 2017. A novel approach to improve assessment process of simulator based emergency operations.

[33] Focus groups. URL: https://www.codecademy.com/resources/docs/uiux/focus-groups.

[34] Oragui, D. 2020. Tacit knowledge: Definition, examples, and importance. URL: https://helpjuice.com/blog/tacit-knowledge.

[35] BEYO. 2019. What are holistic approaches and why are companies using them? URL: https://beyo.global/thinking/what-are-holistic-approaches-and-why-are-companies-using-them.

A Focus group questions - English version

Questions for the captain:

Safety alarm experience from the past:

• How is your experience using alarm system when on duty?

• Do you experience a lot of false positives? If so, how do you handle these?

• Is there any time requirement to information and when to receive this kind of information? And how is this information conveyed for you?

• Do you think the alarms are informal and understandable for you to know how to act upon them?

• Do you think support from alarm experts would lower your cognitive load during your work?

Merging safety alarms and cybersecurity alarms into same system (mock-up of past and futuristic alarm system in ROC):

• Do you think cybersecurity alarms will fit into your already used alarm systems?

• When and if cybersecurity alarms will get integrated in a remote autonomous setting? How would you consider this to fit into your workflow when on duty?

• Which kind of information do you need to operate safely if a cyberincident happen? And how can this information get displayed?

• Is it desire to get information to be repeated in intervals or once as an event (when it happens)?

• Do you do any kind of cyberincident training in any form and if so, how?

• If you just get status of safety, connectivity, cybersecurity and other properties? While the analysis of each alarm is done by someone else? Do you think this will lower your cognitive load and make it easier for you to focus on your main objectives?

Support from Security Operation Center (mock-up of incident handling process):

• What do you think of getting support by a Security Operation Center, where a cybersecurity analyst gives advice of how to handle the different alarms and to **filter** out potential false positives?

• What do you think of the communication sequences modelled in the mock-up?

Summarizing question:

• As a summary, which of the human machine interface mock-up alternatives do you think will have the lowest cognitive load for you, but at the same time giving you the information you need?

• Do you think the incident handling process mock-up can provide you with a sufficient process to handle a potential, cyberattack against your ship?

• Any other suggestions to what we have discussed upon?

Question for the cyber security analyst:

How is your working process today:

• How are your working steps when analyzing logs?

• How are your procedure when an alarm is detected?

• Are you able to assist with incident handling? Or do you just give advice if a threat is detected?

• Which kind of information do you need to effectively assess that a cyberthreat is currently on a system?

• Is there any time requirement to logs and cybersecurity alerts and when to receive this kind of information? And how is this information conveyed for you?

Support remote operation center (mock-up of the human machine interface):

• How do you think you can be able to assist a captain of a ship when a cybersecurity alarm has been triggered in the remote operation center?

• Which kind of information from alerts do you need to be able to support the remote operation center?

Communication with operator at remote operation center (mock-up of the incident handling process):

• How will you communicate the effect of the cyberincident and what is needed to communicate to a captain so he/she knows what can't be done and what can be done?

• Which domain knowledge do you need to be able to help a captain to do the right operational decisions?

• How do you see your role in the scene of a cyberincident on a ship? And is there anything in your role that should be changed so there is an increased probability that you can stop a successful cyberattack?

Summarizing questions:

• Due to your experience of analysing alerts and logs. Which of the human machine interfaces alternatives do you think will perform best in a remote operation center?

• Do you think the incident handling process mock-up can fit into the concept of supporting a remote operation center when it comes to detection of cyberincidents and why?

• Any other suggestions to what we have discussed upon?

B Focus group questions - Norwegian version

Spørsmål til styrmann:

Erfaringer med sikkerhetsalarmer (safety):

- Hvilken erfaring har du med bruk av sikkerhetsalarmer når du er på vakt?
- Opplever du mye falske alarmer? Om ja, hvordan håndteres disse?
- Når det kommer til alarmer, har dere noe tidskrav til å få slike sikkerhetsalarmer? Og er der noe krav til hvordan disse sikkerhetsalarmene vises til dere?
- Føler du at sikkerhetsalarmene er forståelige og gir deg nok innsikt til å vite hva som må gjøres?
- Tror du å få støtte av en sikkerhetsalarmekspert ville bidratt til å få mer kognitiv kapasitet i ditt arbeid?

Knytte samme sikkerhetsalarmer og cybersikkerhetsalarmer i samme system (modell av tiltenkt konsept vil bli vist under intervjuet):

- Tror du cybersikkerhetsalarmer kan være til nytte og passe inn i allerede eksisterende alarmsystem om bord?
- Når og om cybersikkerhetsalarmer blir integrert inn i en fjernstyring og/eller autonomt skipsstyringskonsept? Tror du dette vil passe inn i arbeidet ditt, eventuelt hvorfor ikke?
- Hvilken type informasjon trenger du for å kunne operere skipet, når du for eksempel er under ett cyberangrep? Og hvordan tror du denne informasjonen kan best vises frem til deg?
- Er det ønskelig at slik informasjon blir vist én gang, per gang det oppstår, eller bør det periodisk bli gjentatt i alarmsystemet?
- Utfører dere noen type for cybersikkerhetstrening? I så fall hvilken?
- Om du til enhver tid fikk status om tilstanden til sikkerhet, cybersikkerhet, forbindelser og lignende faktorer? Mens en annen tok seg av analysen av hver enkelt alarm? Tror du dette vil øke din kognitive kapasitet i ditt arbeid, slik at du kan fokusere mer på dine hovedoppgaver?

Støtte fra Security Operation Center (SOC) (modell av kommunikasjon til SOC vil bli vist under intervjuet):

- Hva tror du om å få støtte fra et Security Operation Center (SOC), hvor en cybersikkerhetsekspert gir råd om håndteringen av de ulike cybersikkerhetsalarmene og for å filtrere ut falske cybersikkerhetsalarmer?
- Hva tror du om kommunikasjonssekvensene vist i denne modellen?

Oppsummerende spørsmål:

- For å oppsummere, hvilken av «human machine interface»(HMI)-modellene tror du vil gi deg mest kognitive kapasitet, men samtidig gi deg den informasjonen du trenger?
- Tror du modellene for hendelseshåndtering kan gi et godt utgangspunkt for hvordan man håndterer et mulig cyberangrep sammen med en SOC?
- Har dere noen andre forslag til det vi har diskutert?

Spørsmål til cybersikkerhetsanalytiker:

Hvordan er arbeidsprosessen din i dag:

- Hvordan jobber du når du analyserer logger?
- Hvordan er prosedyren din om en alarm oppstår?
- Støtter dere med hendelseshåndtering? Eller gir dere kun rådgivning når en cybertrussel er oppdaget?
- Hvilken informasjon trenger du for å effektivt kunne vurdere at en cybertrussel eksisterer på et system?
- Har dere noe tidskrav til logger og cybersikkerhetsalarmer? Og er der noe krav til hvordan disse loggene og cybersikkerhetsalarmene skal vises til dere?

Støtte remote operation center (modell av hvordan alarmer kan bli vist til remote operation center vil bli vist under intervjuet):

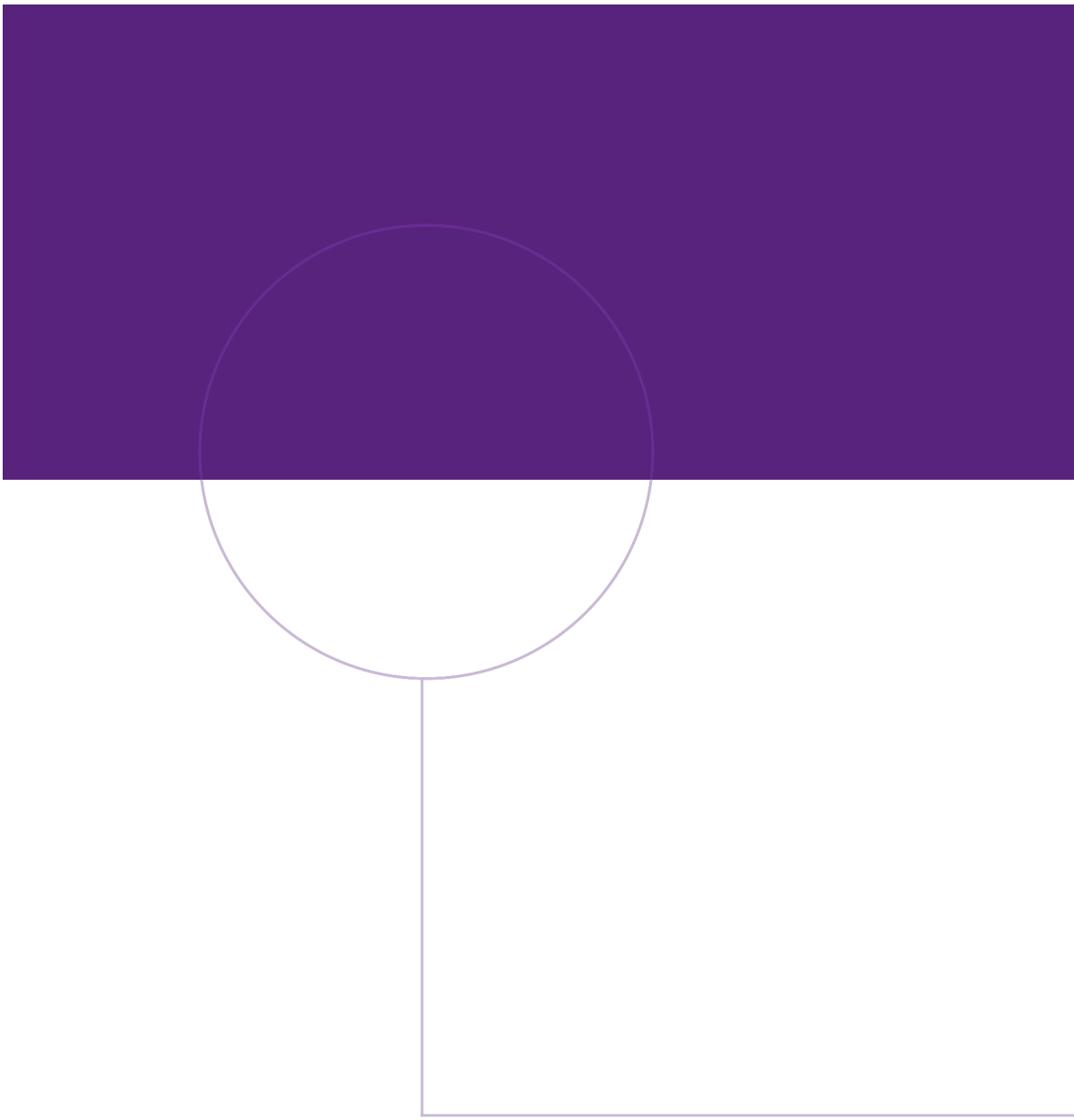
- Tror du at dere kan støtte en styrmann når en cybersikkerhetsalarm oppstår i remote operation center?
- Hvilken informasjon krever dere for å ha mulighet til å støtte remote operation center?

Kommunikasjon til styrmann i remote operation center (modell av kommunikasjonssekvensen til styrmann vises under intervjuet):

- Hvordan vil du kommunisere effekten en cybersikkerhetshendelse har, og hva må kommuniseres til en styrmann for at han/hun skal vite hva som kan gjøres og hva som ikke kan gjøres under en slik situasjon?
- Hvilken kunnskap og kjennskap til systemene om bord i et skip trenger dere for å hjelpe en styrmann til å gjøre de riktige valgene?
- Hvordan ser dere på deres rolle når en cybersikkerhetshendelse oppstår på et skip dere støtter? Og er der noe i din rolle i dag som bør endres for at du skal ha en større sannsynlighet for å kunne stoppe et vellykket cyberangrep?

Oppsummerende spørsmål:

- Ut fra din erfaring når det gjelder analyse av logger og alarmer. Hvilken av «human machine interface»(HMI)-modellene tror du vil passe best i et remote operation center?
- Tror du modellene for hendelseshåndtering kan gi et godt utgangspunkt for hvordan man håndterer et mulig cyberangrep sammen med en styrmann?
- Har dere noen andre forslag til det vi har diskutert?



NTNU

Norwegian University of
Science and Technology