

# Work Package 2 Report - Cyber resilience for the shipping industry

**Sahay, Rishikesh; Sepúlveda Estay, Daniel Alberto**

*Publication date:*
2018

*Document Version*
Publisher's PDF, also known as Version of record

# CyberShip Project
# Cyber resilience for the shipping industry
# Work Package 2 Report

Rishikesh Sahay, PhD
Daniel Sepúlveda Estay, PhD

April 4, 2018

**Abstract**

This report describes the current state of the research performed as a part of the CyberShip project for its Work Package 2. This work package aims at defining a CyberShip model and KPIs for cyber resilience. This is a project funded by the Danish Maritime Fund (DMF) with the objective of proposing a framework for improving the resilience of the shipping industry.

# Contents

# 1 Introduction

The CyberShip project, "Cyber resilience for the shipping industry", is aimed at proposing a theoretical framework to aid the decision making process for preventing and reacting to cyber-attacks in the shipping industry. This project is divided into six work packages that are developed sequentially. These work packages are:

- Work Package 1 (WP1): Project Management, to coordinate technical activities and assure quality of results
- Work Package 2 (WP2): Definition of Cyber Resilience KPIs, to define a specific cyber-ship model and cyber resilience key performance indicators (KPIs)
- Work Package 3 (WP3): Cyber-attack prevention measures, to define measures and tools at a strategic (design) level
- Work Package 4 (WP4): Cyber-attack response and recovery measures, to define measures and tools once and if the cyber-attack occurs
- Work Package 5 (WP5): Evaluation and application to specific case studies, to define and evaluate the case studies, and to propose recommendations for the shipping industry and regulators
- Work Package 6 (WP6): Dissemination, to link colleagues and stakeholders with the project and its findings and proposals

Currently, the project is developing Work Package 2. The second work package of the CyberShip project has two main objectives. First, it defines a generic cyber ship model through the identification of all systems, cyber components, and their communication requirements in a modern commercial ship. The resulting model defines what is understood as the "attack surface" of the ship. As such, a ship is seen as a system composed of several sub-systems that have individual and independent characteristics. Such a CyberShip model consist therefore of all systems and cyber components in a ship, their capabilities for computation and interaction with the environment, and the interactions between components in a modern ship.

Second, WP2 defines a set of Key Performance Indicators (KPIs) to measure the degree of cyber resilience performance of any ship system under investigation. These KPIs are qualitative and quantitative measures of the ship system's resilience towards cyber attacks. These indicators come from areas such as risk of cyber attacks, degree of resource redundancy, response and recovery times, and implementation costs.

# 2 Background

The widespread adoption of Information and communication technologies (ICT) throughout today's ships has led researchers to focus on security and resilience properties of a CyberShip to understand prevention, and reaction and mitigation to cyber-attacks. Focus on prevention is related to aspect such as how

security breaches within ship's technologies will result in variety of harmful impacts on ship operation and its crew members. The focus on mitigation and reaction is related with aspects such as how a system will continue to operate with an acceptable level of performance even when a cyber-attack is occurring.

A cyber- attack is defined in the context of this project as any attempt, successful or not, to gain illegal access to a computer or computer system for the purpose of causing damage or harm.

Within the technologies used to process information and control processes in a ship, Information Technologies (IT) and Operation Technologies (OT) can be identified.

Information technology (IT) relates to:

> "the entire spectrum of technologies for the information processing, including software, hardware, communications technologies and related services."

A relatively newer term is that of Operations Technology (OT), defined as:

> "the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise"

As a result of these definitions, IT and OT have different roles within the organization: OT is related to effects in the physical world, while IT is related to information processing. The need to differentiate between IT and OT can be explained through differences in aspects such as

- System Availability: OT systems are required to have a uch higher real-time availability, as these are affecting physical processes. In contrast, IT systems have regularly scheduled periods without service, as part of their maintenance strategy
- Dependence: while IT systems are dependent on technicians and administrators specialist in computer science, OT systems are dependent on the final users, i.e., those who are requiring the physical services these OT systems provide
- Access: OT has different ways in which it can be accessed, when compared with the TCP/IP interface of IT systems
- Knowledge: There is a lack of understanding of the physical processes enabled through the OT systems by IT specialists

# 3 Components of the cyber ship framework

The different components of the ship are shown in Fig. 1. It comprises of critical and non critical components. Critical components are essential for the safe operation of the ship. Below, we describe the critical and non critical components of the ship.

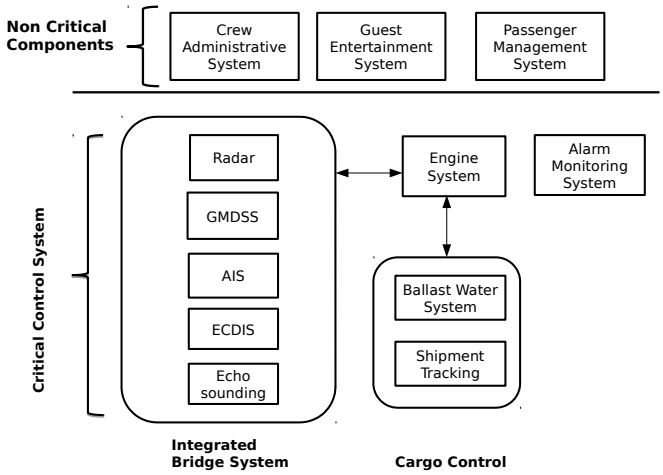


Figure 1: Critical and non critical components of the ship

- **Engine System:** It contains all the system related to power generation and propulsion [3]. It gathers the data related to speed, rudder angle, propeller. Moreover, it monitors the engine load, fuel consumption, water level in the ballast compartment. Depending on the information from the bridge control system it sends the command to propulsion control system to increase or decrease the speed of the ship. Furthermore, it also sends the command to increase or decrease the level of water in the ballast compartment depending on the information from the bridge system. However, the use of digital systems to monitor and control on-board machinery, propulsion and steering make such systems vulnerable to cyber attacks. The vulnerability of these systems can increase when they are used with navigation and communications equipment on ships using integrated bridge systems.

- **Automatic Identification System (AIS):** The AIS device transmits and receives data about a ship's name, type, size, status, position, heading, speed, cargo, next port of call as well as its IMO- and MMSI number [2]. The data is collected from the ship's sensors.

  AIS communications do not employ authentication and integrity checks. Hackers can send specially crafted messages that could mimic the location of an existing vessel, or even create a fake vessel and place it on its own virtual course. It is known as AIS spoofing.

  Attackers can capture and store AIS data and replay spoofed messages in specific time frame. Moreover, attackers can modify the AIS data such as location of position, port of call, estimated arrival time, etc. Additionally, attackers download the data of an existing ship, changing some of the parameters and submitting it to the AIS service. It is ship hijacking. As there is no authentication and integrity checks so AIS system is vulner-

able to attack traffic. Moreover, communication is made of RF. Anyone with cheap RF receiver can also listen to these messages.

- **Radar:** The purpose of the radar is to detect and monitor objects through the emission and reception of electromagnetic impulses [1]. The radar picture continuously and automatically processed to plot the acquired targets to determine distances and bearings towards that object. Moreover, the object's speed, course and position can be calculated, if ship's own data is available. Radar devices are vulnerable to jamming and DDoS attacks

- **ECDIS:** The ships which travel the oceans nowadays are obliged to be fitted with an ECDIS [2]. All ships should maintain nautical charts for route planning and monitoring for their voyage. ECDIS displays data related to selectable safety contour, isolated dangers, pre-planned traffic routes, distance to run, etc.

- **GMDSS:** It is an acronym for Global Maritime Distress System. Its aim is to ensure rapid and automated alerting in case of maritime distress. It transmits and receives the distress and safety messages through satellite links. Transmitted messages consists of ship's type, ship's MMSI number. The nature of distress message is generally related to sinking, grounding, flooding,fire explosion etc [1].

- **Echo Sounding Device:** The purpose of echo sounding device is to provide information related to depth of water under ship to aid in navigation specifically in shallow water [1]. It helps the `Engine system` to maintain the appropriate level of water in the ballast control compartment.

- **Cargo Management System:** Computer systems used for the management and control of cargo may interface with a variety of other system ashore [6]. These system may include shipment tracking details available to shippers via the Internet. Interfaces of this kind make cargo management systems and data in cargo vulnerable to cyber attacks.

- **Ballast water system:** It is a compartment within a ship that holds water, which is used as ballast to provide stability. Using water in a tank allows for the easier adjustment of weight. It also allows for the ballast to be pumped out to temporarily reduce the draft of the vessel when it is required to enter shallower water. In some ships, ballast water system is independent of the engine system. However, it relies on the model of the ship.

- **Alarm Monitoring System:** It provides visual and audible signals in the event of abnormal condition such as in fire explosion, flooding, collision, etc. It ensures that appropriate measures should be taken quickly to mitigate these extreme conditions. It is also known as Integrated Alarm and Control System [4].

- **Passenger facing networks:** Guest entertainment system and passenger's Internet access on the ships are public facing network [6]. If the Internet access to the passengers are provided through the same channel which controls the critical components on ship then t becomes easier for

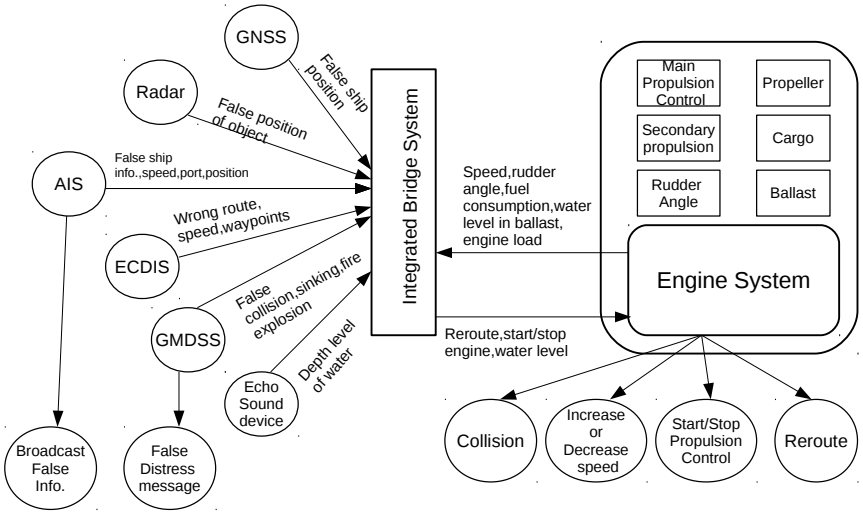


Figure 2: Impact of attack traffic on different components

the attackers to attack the control systems by attacking the guest entertainment system. These systems should be considered uncontrolled and should be segregated from the network of control system.

- **Passenger service management system:** It consists of the valuable passenger related data such as their personal identifier, transaction details related to bank etc [6]. Systems which is used to manage the passenger related data are themselves an attack vector as the collected data is passed on to other system.

# 4 Vulnerabilities and Impact of Cyber Attack on Ship

In this section, we discuss the impact of cyber attack on the different components of the ship and how it affects other components of the ship. Specifically, we focus on how attack on critical components can affect the normal operation of the ship. As shown in Fig. 2 `Integrated bridge system` manages all the bridge components. It provides the centralized access of the information from all the bridge components.

As we can see in Fig. 2, if AIS system is compromised by an attacker then it can be used to provide false information related to other ships to Integrated bridge system. Moreover, attackers can use the compromised AIS system to broadcast the wrong information and position of the ship itself. False information such as next port of call or speed of the ship can cause the Integrated

bridge system to send the control command to `Engine system` to divert the ship to longer routes or increase or decrease the speed of the ship. Moreover, false information such as position and speed of other ships can cause the collision of the ships.

Generally, AIS communications do not employ authentication and integrity checks. Hackers can send specially crafted messages that could mimic the location of an existing vessel, or even create a fake vessel and place it on its own virtual course. It is known as AIS spoofing. Attackers can capture and store AIS data and replay spoofed messages in specific time frame. Moreover, attackers can modify the AIS data such as location of position, port of call, estimated arrival time, etc. Additionally, attackers download the data of an existing ship, changing some of the parameters and submitting it to the AIS service. It is called ship hijacking. As there is no authentication and integrity checks so AIS system is vulnerable to attack traffic [5].

As discussed in Section 3 that `Radar` provides the information about the objects in the ship. Radar is vulnerable to jamming and DDoS attack. These devices provide wrong information about the object because of the false echoes caused by extraneous radar waves. These false information may cause the collision of the ship with the object. Collision of ship with objects can cause delay in offloading of cargo materials at the port and also it can sink the ship which can cause the loss of lives and cargo.

ECDIS is used as a replacement for the paper chart for the pre planned routing of the ship. Computer systems used for the ECDIS is vulnerable to malware attacks. Attackers can compromise these devices and replace the original chart with their own electronic chart. As a consequence, `Integrated bridge system` can issue control command to `Engine system` to reroute the ship to longer or shorter route. Rerouting of the ship to a prohibited area or through a longer route causes a delay in reaching the destination port, which can affect the offloading of the cargo materials. Even, if the ship reaches early to the destination port it can affect the offloading of the cargo materials because of the port operation (e,g., people on port may be busy in offloading of other materials). So, in both of the cases it will affect the supply chain management. Moreover, it can cause the ship to stop at different port contrary to what was planned by the crew members.

Global Maritime Distress System (GMDSS) is used to broadcast the distress messages related to collision, flooding, sinking, fire explosion, etc. If GMDSS is compromised by the attackers then it can be used to broadcast false distress messages to other ships or to the shore control center. Moreover, if the engine system is compromised by the attacker then it can send the false information regarding fire explosion, flooding, sinking, collision to `Integrated bridge system` which provide these alerting message to be broadcasted by GMDSS.

Global Navigation Satellite System (GNSS) is also vulnerable to cyber attacks. Signals and data of GNSS can be spoofed which in consequence can provide the wrong position of the ship. Spoofing of data from GNSS can cause the attack on ECDIS system as well. Since, the ECDIS system used GNSS data to upgrades the routes and position. As a consequence,`Integrated bridge system` can issue control commands to reroute the ship to other routes and it may lead to collision.

As we have surveyed in Section 3 that `Engine system` comprises propul-

sion control system, propeller, cargo control, ballast control. Engine system is also vulnerable to cyber attacks. Specifically, the computer systems involved in the `Engine system` is vulnerable to cyber attacks specially through malware. If the `Engine system` is compromised by the attackers then it can be used to send the false information related to speed, fuel consumption, engine load, water level in ballast compartment to `Integrated bridge system`. This can cause the AIS and GMDSS system to broadcast the false information related to ship. Moreover, by hacking into the `Engine system` attacker can issue the control commands to divert the ship to different routes, to start or stop the main propulsion system. Moreover, by issuing the control command to increase or decrease the water level in `Ballast control compartment` attacker can also sink the ship. It can delay the ship's arrival at the destination port which can affect the offloading of cargo. Moreover, attackers can also sink the ship near the port, which can affect the operation of the port for few days which in consequence affect the supply chain of shipping companies.

Moreover, cargo management system managed by the `Engine system` is also vulnerable to attackers. By getting access to these systems attackers can damage the data related to rates, loading, cargo number, date and place. Because of this no one can know where containers were, whether they had been loaded or not. Even after the recovery of the data, it will lead to significant disruptions in operations and resulted in sending cargo to wrong destinations which causes severe financial loss. Generally, attackers email malware to the port authorities or shipping companies. Then they broke into the facility housing cargo handling computers allowing wireless access to the key strokes and screen shot of computer screen. Jammers are a common tool for cargo theft by organized crime. Moreover, attack on cargo management system can cause the theft of cargo and delay the supply chain management of the cargo materials to the shipping companies. Furthermore, compromise of the cargo management system can cause the damage to the ship. For instance, after compromising the cargo management system hackers can close ventilation which cause the fire explosion on the ship because of cargo material.

Apart from the attack through outside of the network, ship can also be damaged by compromising the bridge system or engine system by rouge crew member. For instance, rouge crew member can use the USB key to update the ECDIS system and the USB key may contain the malware which can compromise not only the ECDIS system but can also affect the other components on the ship. Even rouge crew member can bridge the segregated networks which manages the control system (bridge and engine) on the ship with the crew management system which can cause the attack on the bridge or engine system.

Finally, human factors also have to be considered in a cyber-ship model, as only in highly automated shipping systems there is no expected interaction between human operators and the shipping system. Examples of human factors that can have a disruptive effect through cyber-attacks include evets such as unauthorized system entry (software level) or rewiring (hardware level).

## 4.1 Risk Templates

Table 1 shows the vulnerabilities in the different components of the ship. It provides the risk likelihood, planned controls which can be enforced quickly

to reduce the impact of the attack. Moreover, we also provide the KPIs which can be used to assess the performance of the mitigation mechanism to reduce the impact of attack traffic.

As can be seen in the Table 1 all the components are vulnerable to the attacks. Moreover, the impact of the attack traffic on the ship is very high, as it has been discussed in Section 4 that attack on the components of the ship may cause collision, sinking, and diversion.

Table 1 also provide the basic planned control to immediately mitigate the impact of attack traffic on the components of the ship. For instance, if the attack on the `Engine system`, `AIS system`, and `Radar` is detected then malicious traffic must be should be blocked at the border router of the network to reduce the impact of the attack traffic. However, if the traffic is suspicious in nature then it should be redirected to middleboxes or firewall for further processing. Additionally, response mechanism is assess through the metrics such as mitigation time and recovery time. ECDIS system can be protected using strong passwords and by continuously updating the anti-virus system. If the malicious traffic is found accessing the ECDIS system then it blocked by the firewall right away. Ballast compartment is vulnerable as it can be used to sink the ship by the attacker. If it is attacked then then immediate measures to reduce the impact is to either increase the level of the water or decrease the level of the water depending on the threshold value defined based on the depth of the water level depending on the position of the ship in the sea. Metrics used to evaluate the response mechanism is mitigation time and recovery time. As it is mentioned in the Section 3 that cargo management system contains the details of the cargo such as name, type of the cargo and shipping details. It is vulnerable to the attacker as it provides the financial gain to the attackers. Basic measures to protect the cargo management system is to deploy the Intrusion Detection System (IDS) and firewall which continuously process the traffic accessing the cargo management system. Metrics used to evaluate the effectivenss of the mitigation mechanism are mitigation time and recovery time, i.e. how quickly impact of the attack traffic can be mitigated.

# 5 Key Performance Indicators of Cyber Resiliency

A search of relevant literature revealed a series of Key Performance Indicators (KPI's) that could be applied to characterize the cyber resilience on a ship. These indicators have been divided into behavioral, structural and financial indicators.

## 5.1 Behavioral indicators

The behavioral indicators are related to the process times related to resilient behavior as well as indicators of the performance of the shipping system during the resilient response. The behavioral indicators related to time, are those that describe the dynamic response (behavior over time) of the system when reacting to a cyber attack. The resilient response of a system was already described in dynamic terms by Prof. Yossi Sheffi and Prof. Jim Rice in 2005 [10], and is represented by a "disruption curve" as can be seen in Figure 3.

This curve represents the evolution over time for some measure of performance in the system, such as accuracy or reliability of communication, for example. When a cyber-attack occurs, the performance represented by this curve, will initially decrease, up to a point where recovery will start to occur. In this point of inflection, the decrease in the performance will stop and a gradual return towards the previous level of performance will start. The performance level that is reached after the recovery efforts, will determine the long term impacts of the attack. The phases in a disruption that have been identified by Sheffi & Rice are:

1. **Preparation**, present in the cases where the organization can foresee and prepare for a disruption, to minimize its effects.
2. **Disruptive event**, when the disruptive events actually takes place
3. **First response**, aimed at controlling the situation, the protection or safeguarding of life, and shutting down or isolating the affected systems to prevent further damage
4. **Initial impact**, represents some of the immediate effects of a disruption. In the case of cyber attacks, it may be felt as the immediate decrease in customer service level or machine availability
5. **Full impact**, represents the medium to long term effects of a disruption, such as market effects, or longer effects in the available customer service, for example.
6. **Recovery preparations**, these preparations often start with the first response or even before the disruptive event if this has been anticipated. These may include measures of flexibility, i.e.., the redirection of existing organizational resources, or redundancy, i.e., the involvement of additional resources such as alternate IT systems, or service suppliers, for example
7. **Recovery**, Represent the process of getting the performance back to normal levels.
8. **Long Term impact**, representing the long term performance levels after the recovery measures have been implemented.

These phases are represented in Figure 3.

Each of these phases can include a number of indicators related to the times in which each of these phases is activated, for example:

- **Impact time**: The time it takes a cyber attack to cause a disruption in the system it is attacking
- **Detection time**: The time it takes a system to identify that an intrusion has taken place. This might be longer than the time it takes for this intrusion to disrupt the performance. It would be surprising if the Detection Time is longer than the Impact time, for example.
- **Total disruption time**: Total time it takes an organization to return to acceptable levels of performance, from the time of initial impact

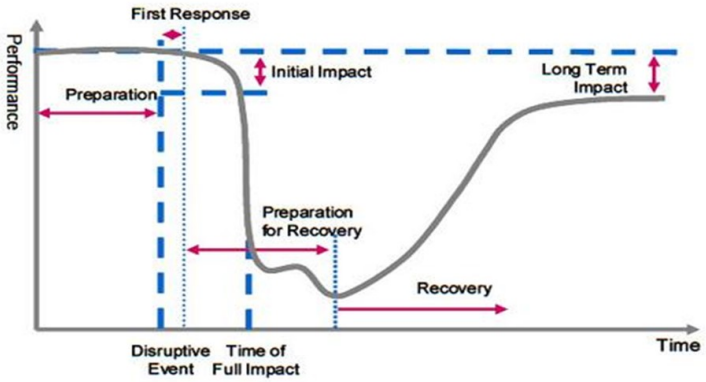


Figure 3: Disruption curve [10]

- **Time to initial impact**: Time from the Disruption time to the initial impact is detected
- **Time to recovery**: Time from detection to the lowest point in performance due to the disruption,
- **Time to deploy redundant resources**: measure of time from the detection of the attack to the activation of additional resources. These additional resources may originate both from pre-existing option contracts with external providers of resources, from internal sources of redundancy, such as parallel systems, or from external resources acquired and engaged only after cyber attack has been declared
- **Mitigation time**: Time from the detection of the attack to the moment whn the performance measure has returned to acceptable levels.
- **Restored level of performance**. The aim is to restore the performance of the critical function to normal level after disruption caused due to attack. Higher values are better as it means that the ship is restored to the normal functioning level.

## 5.2 Structural indicators

The structural indicators are related to the parts of which CyberShip system is composed, and how these parts relate to each other. An analysis of failure based on structure has been proposed by Leveson in 2007 [9] and her team. This approach considers understanding a system starting from the effects it wants to avoid, to then work deductively towards the structures and decisions (unsafe conditions) present in the system that currently allow it to present these unwanted effects.

It is similar to a fault tree analysis, as it considers the definition of the system that is under threat, the identification of a fault tree, the qualitative description of the tree and finally the quantitative description of the tree. However, a systemic analysis identifies unsafe conditions in a structured way, and also

considers unsafe conditions however indirect these may be to the causal chain that leads to a negative effect.

In the case of a cyber-attack, the unwanted effect would be for example, the interruption of customer service, due to the customer information system being out of service due to some type of cyber attack. The analysis would then proceed to identify the structure of the system, this is, the agents and communications present in the system. Then the control actions present in the system would be identified. These control actions are then tested for ways in which they can lead to an unwanted effect. This analysis results in structural recommendations that make the unwanted less likely or unfeasible.

This structured analysis begins by considering a system such as an IT system as a series of control feedback loops, where a controller oversees a controlled process though the use of sensors that pick up the state of the process and actuators that influence the state of the process. This configuration is the basic control feedback loop, as shown in Figure 4.

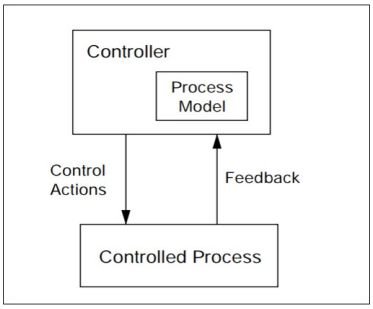


Figure 4: Basic control loop structure

Once the components of the control structure are identified, the different ways in which these components and their interactions can lead to an undesirable event, can be explored in a structured way. Examples of ways in which these components and interactions can fail, are shown in Figure 5

The process followed by the STPA method, as applied to cyber-risks, is shown in Figure 6.

This control loop can then be analyzed according to the types of failures that it can contain, some of these being related to the components themselves, but other related to the way in which these components communicate with each other through logic flaws, for example. This leads to indicators that have to do with the make up of the system that create the potential for failure as a result of how the system is structured. some of these indicators include:

- **Number of Unsafe Control Actions**: represents the ways in which the execution or non-execution of a Control Action designed into the system can lead to an unwanted effect.
- **Proportion of Unsafe Control Actions Per Hazard**: represents the number of Unsafe Control Actions that can lead to a specific condition of risk that given the correct environmental conditions can lead to an unwanted effect

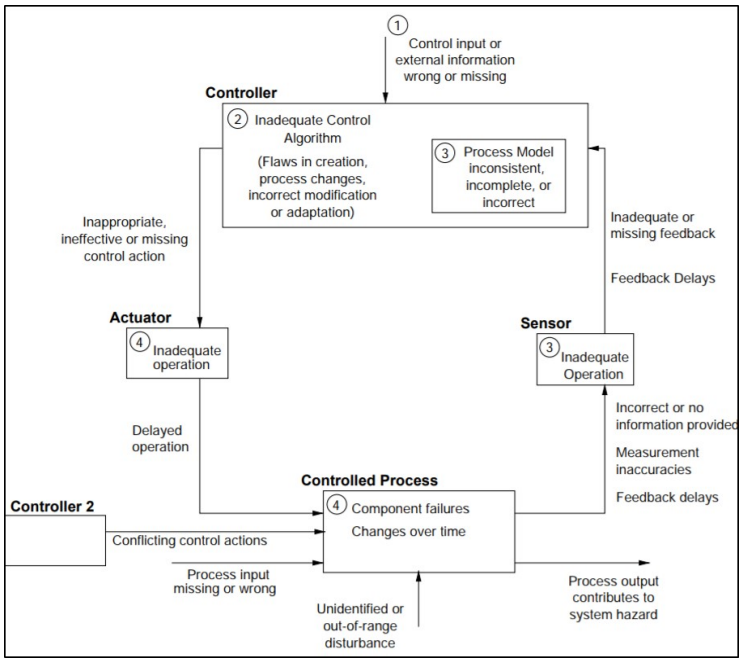


Figure 5: Control structure failure examples

- **Proportion of Unsafe Control Actions per Accident**: represents the number of Unsafe Control Actions that can lead to an unwanted effect

Additional to this, structural measures can be derived from the analysis of the control loops present in the existing systems, for example:

- **Number of open control loops**: related to the identification of desired control structures that do not have an active control loop in the current system structure
- **Number of redundant control loops**: related to the identification of desired control loops that have more than one active control loop in the current structure

Finally, structural indicators can be related to the structure of the attacks, particularly to the characteristics of the data transfer, such as:

- **Number of attempted intrusions stopped at a network perimeter:** The objective is to prevent and continue the operation of the ship. Higher number of intrusions stopped are better. Intrusions or attacks can be on the critical components of the ship. These attacks or intrusions can affect the proper functioning of the ship. Higher number of intrusions stopped are better since it signifies that the intrusions have been stopped which allows proper functioning of the ship.
- **Number of attempted intrusions deflected to a honeypot:** The objective is to prevent and continue the operation. Higher values are better.

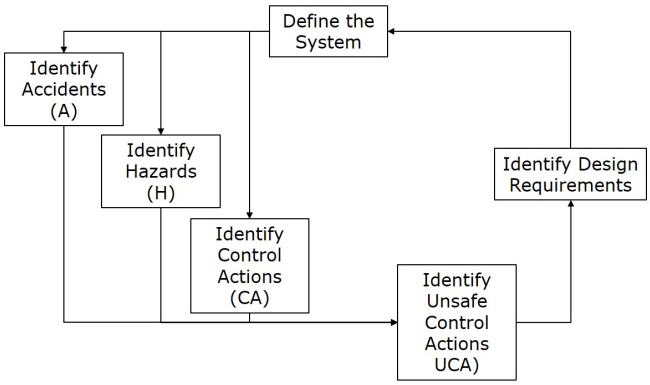


Figure 6: STPA process diagram

- **Length of time between an initial adversary act and its detection:** The objective is to prevent the attacker from compromising the system. Lower values are better, since if the attack is detected early then mitigation can be performed quickly which can prevent any damage caused to the normal operation of the ship. For example, it can prevent the ship from getting diverted to a longer route which can impact the arrival time of the ship at the destination port as well as the offloading of the cargo which can result in a delay in supply chain management of the shipping companies. This metric assumes that the initial adversary act can be identified.
- **The Number of Data Bytes in Command and response Packets:** Depending on how the components communicate the size of command and response packets may vary. By extracting the number of bytes in command packets we can know the pattern of communication between different components during normal traffic connections. This pattern can be matched continuously to monitor the state of the system.
- **Inter-packet time interval:** The inter-packet time interval for normal traffic traffic dataset and attack dataset can be measured. From the difference in the time interval, we can infer the that the inter-packet time interval could be used as a classification feature to detect the attacks.

## 5.3 Financial indicators

The financial indicators are related to the economic effects of a disruption, before, during, after a disruption from a cyber event and for the overall disruption event.

- **Cost of disruption**: this indicator reflects the total monetary cost of a disruptive event
- **Cost of mitigation**: this indicator reflects the monetary cost of containing the disruptive event from the time it is detected until the recovery

operations start

- **Cost of recovery**: this indicator reflects the monetary cost of recovering the performance level after a disruptive event, and from the point when all the mitigation measures were implemented.
- **Implementation costs - preventive**: this indicator reflects the monetary cost of applying measures before the disruptive event takes place
- **Implementation costs - upgrade**: this indicator reflects the monetary cost of applying the upgrade measures derived from the disruptive event.

# 6 Future Work

This section will summarize important information needed to complete Work Package 2 (WP2), and will detail the future work in the project that follows as a result of completing WP2.

## 6.1 Pending information

As a result of the research process, number of relevant areas have been identified where information has been either incomplete or absent from the literature that has been gathered as part of the work package.

- **Management and Operation of Integrated Bridge System:** Despite the relevance of the Integrated Bridge System in the ship, as it gathers the information provided other systems in the ship (See Figure 2), little information was found about how this Integrated Bridge System is designed, the format of information that is transmitted to and from the Engine System, which organization is in charge of its update and repair, and also which organization is therefore expected to react in case of an emergency.
- **Interaction between the Integrated Bridge System Components:** Despite the identification of the different systems that contribute information to the Integrated Bridge System (e.g., GNSS, Radar, AIS, ECDIS) little information was found about how these systems interact with each other directly.
- **Interaction between the Engine System Components:** Despite the identification of the different systems that constitute the Engine System (e.g., propeller system, ballast system, and propulsion control) little information was found about how these systems interact with each other directly.
- **Cross-interaction between System Components:** Little information has been found about the data that is accessed from across aggregated systems. For example, what information is accessed by systems such as the GNSS or AIS from the Engine system? In the same way, which data is accessed by the propeller or Ballast systems from the Bridge systems?

### 6.2 Next steps

This work will include the insider threats as part of the CyberShip model. Additionally, this work proposes to focus on the relationship between the Bridge systems and the Engine Systems, according to:

- **Data type enforcement:** The safe and complete transmission of information between systems is related to the standardization of these signals, since the result of such a standardization is a more effective detection of abnormal signals and/or patterns.
- **Software Defined Networks (SDN):** The use of Software Defined Networks as a way of automating response to attacks. Appendix 7.2 provides an initial description of such an approach.

Finally, this approach will be included in the next Work packages that are being developed in this project, i.e., Work Package #3 that focuses on prevention and Work Package #4 that focuses on response and recovery from cyber attacks.

## References

[1] Process map for Autonomous Navigation. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network, 2014.

[2] Final Report:Autonomous Bridge. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network, 2015.

[3] Final Report:Autonomous Engine Room. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network, 2015.

[4] Marine Systems Guide:Integrated Automation Solutions. Technical report, CMR Group, 2016.

[5] Cyber Security in the Shipping Industry. Technical report, Deloitte, 2017.

[6] The Guidelines on Cyber Security Onboard Ships. Technical report, BIMCO, 2017.

[7] R Kowalski and M Sergot. A logic-based calculus of events. *New Gen. Comput.*, 4(1):67–95, January 1986.

[8] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, Jan 2015.

[9] Nancy Leveson. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011.

[10] Yossi Sheffi and James B Rice Jr. A supply chain view of the resilient enterprise. *MIT Sloan management review*, 47(1):41, 2005.

# 7 Appendix

## 7.1 Towards SDN-based Mitigation Framework for CyberShip

The contribution of this paper is proposing a framework to mitigate the cyber attacks against the components of the cyber ship and to trigger the proper defense actions to countermeasure the identified attacks. We consider the following principles in the design of this framework. First of all, the design should be able to provide the defense in an automated way and the crew members of the cyber ship should not be burdened with such heavy tasks of implementing the security policies to mitigate the attacks to protect the systems. Typical crew members often lack enough expertise and vigilance to secure a network and components of the cyber ship, which often pose heterogeneous architectures and varying degrees of security properties. To address this challenge, we propose employing SDN technology as it provides the possibility for dynamic and automated deployment of defense mechanism.

The second design objective is that the framework should be resilient. The framework should ensure that the components of the cyber ship should not be impacted too much because of the attacks. It should be able to recover from the attack quickly to so that the ship can operate properly and should not cause any delay.

The third objective is the efficiency of the framework. The mechanism should incur low communication and computation overheads on the router and switches. It should limit the volume of the network traffic that needed to be mitigated and analysed. For instance, if the mitigation method requires rules for the traffic of a particular protocol or a specific source or destination IP address, appropriate filters must deployed automatically.

Last but not the least, the framework should consider scalability. Novel technologies are incorporated within these emerging devices to provide a wide variety of capabilities. This trends leads to a great degrees of heterogeneity in their architectures and in turn could create different types of security exposures. To cope with this challenge, the framework needs to support the new coming devices and technologies at a large scale.

To substantiate our claim, we propose an SDN enabled cyber ship framework. It aims to provide defense to the cyber ship framework in an automated and dynamic fashion. The defense mechanism is placed on the top of SDN controller, consists of key modules: Shipboard control system, Device Manager, Mitigation module, Detection module, Device Manager.

## 7.2 SDN Enabled CyberShip Framework

In this section, we propose a SDN assisted cyber ship framework. It combines the critical components of the ship with the SDN technology. It provides a cross control layer between the critical components of the ship and between the cyber layer of the communication network. Using this cross layer it is possible to integrate the the physical and cyber countermeasures in order to provide adaptive and automated mitigation to maintain the resilience of the cyber ship.

### 7.2.1 Components of the Framework

Fig. shows a framework of SDN assisted cyber ship framework. The framework contains different components of the SDN technology and th ship. Firstly, we describe the physical and data plane components of the framework and then we describe the control plane components.

The physical and data plane components of the framework is mainly comprised of SDN switches and the physical layer devices managing the different components of the ship. The components are as follows:

1. **Shipboard sensors and actuators:** These devices are used to control the physical components of the ship. These devices communicate with the shipboard control system to manage the components of the ship.
2. **SDN switches:** These are the programmable switches deployed in the data plane of the framework. These switches can be controlled by the SDN controller dynamically through the southbound API. This dynamic control enables us to manage the network and improve the resilience of the framework.

Next, we describe the components in the control plane of the framework.

1. **SDN controller:** It is a software platform deployed in external entity able to provide the network abstractions needed to manage the network [8]. It provides centralized intelligence and global visibility to manage the network. Southbound API in the SDN controller enables us to deploy the rules in the switches through a centralized location based on the need when it arises.
2. **Device Manager:** Our framework incorporates a database to simplify the management of a list of all known cyber physical devices. This database in general contains: (1) an ID associated with the cyber physical device, (2) features to create rules to redirect the traffic towards these devices, or to redirect the traffic towards security devices such as firewalls for processing, (3) location of the devices in the network i.e. through which switch and port the devices are connected.
3. **Detection Engine:** The framework employs a detection engine to examine the network traffic to identify suspicious activities. The programmability of the SDN technology enables the framework to deploy any detection mechanism such as machine learning algorithm for detecting anomalous traffic. Because of the modular design of the framework, security or the network administrator have the ability to deploy the detection algorithm according to their requirements. Once a suspicious or malicious traffic is detected, the detection engine in the framework identifies the attack source and the target of the attack traffic. This module then raises a security alert and forward these information to the mitigation engine.
4. **Mitigation Engine:** It aims to take appropriate countermeasures to protect the critical systems on the ship from attacks. It contains security policies defined in high-level language to mitigate the attacks to restore the system from the impact of the attack traffic. Based on the security alert from the detection engine security policy in the mitigation engine is instantiated to mitigate the suspicious or malicious traffic. The security policies are translated into low level OpenFlow rules for the deployment in the switches in an automated way.
5. **Shipboard control system:** The framework integrates the shipboard control system with the SDN controller. It periodically analyses the data from the shipboard sensors to detect any faults in the physical components of the shipboard system. In case, of faults or malfunctioning of the physical devices of the ship it sends an alert information to mitigation engine to redirect the traffic to other physical device or to block the traffic going towards that physical device.

### 7.2.2 Operational Workflow of the Framework

As shown in Figure 7, the framework integrates the SDN technology with the component of the ship. In the Figure 7 it shown that it is integrated with the propulsion control of the ship. The operational workflow is described as follows:

1. Propulsion control is registered with the device manager. The configuration is provided with the device ID, switch and port information through which propulsion control is connected.

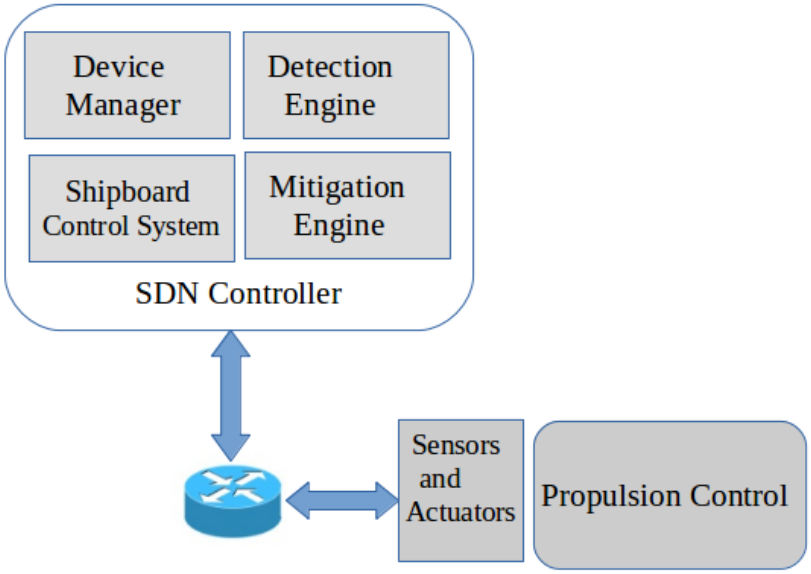


Figure 7: Framework of the CyberShip

2. The shipboard control system monitors the network activities on the propulsion control or other components of the ship. It sends the command to propulsion control system to adapt according to current status that it gather from the sensor elements of the propulsion control. It performs the logging on network activities associated with the critical components of the ship.
3. Detection engine collects and analyses the traffic statistics from the switch. In case, of suspicious traffic it sends an alert information to the mitigation engine.
4. Based on the alert information from the detection engine, mitigation engine deploy the low level rules in the switch to either redirect the traffic to another path towards redundant resource. Moreover, if the traffic is malicious in nature then mitigation engine deploy the rules in the switch to block the traffic.

## 7.3 Security Policy Specification:

In this section, we first describe how the high-level policies are expressed in the mitigation engine module of the framework. These high-level policies are translated into low level OpenFlow rules for the enforcement in the switches when the need arises. The automated policy deployment eliminates the need for manual policy enforcement.

### 7.3.1 Grammar of High-level Policy

```
1 <Policy>=<PolicyID><DeviceID><Rules>
2 <Rules>=Set(<Rule>)
3 <Rule>=<Event><Conditions><Action>
4 <Event>=<Attack_Type>|<Fault_Type>
```

```
<Conditions>=<Condition><Connective><Condition>
<Condition>=<Field_Name><Comparison_Operator><Value>
<Connective>=And|Or
<Comparison_Operator>=less than|equal to|greater than
<Action>=Block|Redirect
```

Listing 1: Grammar for the High-level policy language

The high-level policy syntax provides the guidelines to the security administrators to define the abstract policy. To do that, we need to define a grammar and formats. It enables the network operator to express the network and security policies into an easy to understand language without getting into low level implementation details.

In the framework, we use Event-Condition-Action (ECA) paradigm for policy specification [7]. The reasons for choosing ECA is two-fold: (1) it allows to specify a wide variety of events which can trigger conditioned actions; (2) it enables to define an asynchronous notification mechanism to react on these events. Our policy grammar shown in Listing 1 provides the syntax to define the security and network policies in a human readable format. The high-level policies are defined by the network operator in a simple way through the northbound API of SDN controller.

In particular, our policy is composed of a `PolicyID`,`DeviceID` and a set of `rules`. The `PolicyID` helps in uniquely identifying a policy in the mitigation engine module. The `DeviceID` specifies the device for which policy should be enforce. Each `rule` is composed of an event, some conditions and an action. Event represents what triggers the rule. In Listing 1, we exemplify events, such as attack and fault type. However, it is not limited to these events, other types of events can also be defined using our policy language. A network operator only needs to specify the corresponding conditions to define new events.

When an event is triggered, the associated parameters are checked against the condition specified in the policy. Condition is generally a boolean expression which can be evaluated to true, false or not applicable. Not applicable represents that no condition is specified for the event. In our grammar shown in Listing 1, Condition is specified with the field name and a value. Field name contains the name of the condition and value represents the parameter specified for the condition.

Action specifies the high-level decision which should be enforced when the conditions are met for the event. In Listing 1 two actions have been specified. High-level action `Block` is enforced when it is confirmed by the `Detection Engine` or `Shipboard control system` that traffic is malicious in nature. `Redirect` action is enforced when there is suspicious activities confirmed by the `Shipboard control system` on `Propulsion control` or by the `Detection engine` in the network.

## 7.4 Use Cases:

In this section, we demonstrates how the security policies can be deployed to mitigate the attack in the CyberShip framework.

**Blocking of the malicious traffic:** When a new physical device is added in the network then it is registered in `Device Manager` module. A table in the `Device Manager` module maintains the list of physical devices with unique deviceID, device location to divert the traffic towards the redundant resources in the network. For instance, Table 2 shows the the list of physical devices its unique ID, location of the device in the network i.e., through which switch and port number the device is connected.

In the use case, we assume that attack is launched by the attacker (A) on the propulsion control system. The
tt Detection engine detects the attack traffic. In the use case, we assume detection is performed based on the packet threshold. However, sophisticated detection algorithm can be deployed in the detection engine for detecting the attack traffic. Once, an attack is detected then detection engine sends the security alert information to the
tt Mitigation engine module. Security alert information consists of attack type, flow information, flow class, and switch ID. Type of attack includes any attack type such as DDoS attacks, malware attack. In this case, the flow informations are:10.0.0.1,10.0.0.2,IP, switch ID is 1 and attack type is UDP flood attack. Flow class specifies whether flow is malicious or suspicious. Flow which is confirmed as an attack traffic is classified under malicious class while flow which is not confirmed as whether it is malicious or legitimate is termed as suspicious flows. In this case, flow from source IP(10.0.0.1) to destination IP(10.0.0.2) is triggered as a malicious flow from the detection engine.

`Mitigation engine` then checks its policy database to enforce the action to mitigate the attack. In the framework countermeasures policies are defined in the XML format. An example policy is shown in Listing 2. PolicyID in the example policy specifies that policy is defined for mitigating the attack traffic. Listing 2 shows that if attack type is UDP flood and the flow is classified as malicious then block action should be enforced for the concerned flow. After getting the high-level action `Block` from the policy database, `Mitigation engine` enforce the block action in the flow table of the switch S1 for the flow from sourceIP (10.0.0.1) to destination IP(10.0.0.2). `Mitigation engine` module also contains a python script which takes sourceIP, destinationIP, switchID, port information, and protocol as inputs to deploy the low-level OpenFlow rules. Python script in the `Mitigation engine` module is triggered based on the high-level action which needs to be enforced.

```
1  <Policy PolicyID="Mitigation">
2          <Event Type = "UDP␣Flood␣Attack">
3      </Event>
4          <Condition>
5         <flow class="Malicious"/>
6         %<Impact severity="Low"/>
7      </Condition>
8      <Actions action="Block"/>
9      </Actions>
10 </Policy>
```

Listing 2: Policy to block malicious traffic

**Redirection policy to reduce the impact of attack:** In addition to simply blocking policy our framework also provide more sophisticated actions such flow redirection for the purpose of security and in case of fault or too much load on a critical physical component. Shipboard control system module analyzes the data from from the sensors of the `Propulsion control`. Shipboard control system can use some detection method such as based on watermark to analyze the status of propulsion control devices. If it finds some faults or attack on the propulsion control engine then it can sends alert information to mitigation engine module. Alert information from the `Shipboard control system` consists of the sourceIP, destinationIP, port, and protocol. Along with the alert information it also sends the high-level action Redirect and the location of the redundant `Propulsion control` to forward the traffic from the shipboard control system to start the operation of another `Propulsion control` engine. Device location information

consists of the switchID and the port information to forward the traffic. After receiving the information `Mitigation engine` module instantiates the python script in its module to forward the traffic from shipboard control system to redundant `Propulsion control` engine.

Another interesting application of the framework is to redirect the suspicious traffic to middleboxes which are traversing to `Main Propulsion control` engine for processing. A basic white-list of authorized traffic can also be created for the different components of the ship towards the `Main Propulsion control` engine and redirect all other traffic to middleboxes or firewall deployed for further inspection. A policy table is maintained as shown in Table 3 for the traffic from the different components of the ship to propulsion control. Policies are defined for the different components accessing the main propulsion control based on the context of the message forwarded by the components to the main propulsion control. For instance as we can see in Table 3, if the context of the message from the bridge device is to increase or decrease the speed of the propulsion control then it is redirected to the firewall for further inspection before being forwarded to the main or secondary propulsion control. However, if the traffic is traversing from `Shipboard control` to propulsion control system the it is allowed. Besides that traffic from other components to propulsion control with the context of the message to increase or decrease the speed of the propulsion control is blocked.

Table 1: Risk Template

| Risks | Risk Likelihood | Planned Controls | Impact | Action priority | KPIs for Assessment |
|---|---|---|---|---|---|
| Engine system | High | 1.Malicious traffic should be blocked at the border router 2.Redirect suspicious traffic to middleboxes. | Very high | High | Mitigation time, restored level of performance |
| AIS systems (Replay attack, communication system) | High | 1.Block the malicious traffic at the edge routers. 2.Redirect suspicious traffic to middleboxes | Very high | High | Mitigation time, recovery time |
| ECDIS | High | Strong password protection, define access rights for the different hosts | Very high | High | Number of attempted intrusions stopped |
| Radar(Jamming, DDoS attack) | High | 1. DDoS traffic should be blocked at the edge router. 2.Suspicious traffic should be deflected towards honeypot or middleboxes. | Very high | High | Mitigation time, Recovery time |
| Ballast Water System | High | 1. If the water level rises above a defined threshold: Close the compartment and decrease the water level. 2. Increase the water level if the water level reduces the defined threshold. | Very high | High | Mitigation time, recovery time |
| Cargo Management System | High | 1.Traffic should be processed through the IDS before accessing the system. 2.Antivirus and malware analysis tools should process the traffic accessing the cargo system | Very high | High | Mitigation time, recovery time |

Table 2: List of Physical Devices in Device Manager

| Physical Device | Device ID | Device location | Attributes(SourceIP, DestinationIP, Protocol,Port) |
|---|---|---|---|
| Main Propulsion Control | Propulsion_1 | SwitchID_1:2 | 10.0.0.1,10.0.0.2,IP,2 |
| Secondary Propulsion Control | Propulsion_2 | SwitchID_1:3 | 10.0.0.1,10.0.0.3,IP,3 |

Table 3: Policies specifying actions for flow from different components

| Flow | Context | Policy Action |
|---|---|---|
| Bridge to Main Propulsion Control | Increase/Decrease speed | Redirect Firewall |
| Bridge to Secondary Propulsion Control | Increase/Decrease speed | Redirect Firewall |
| Shipboard Control to propulsion control | Increase/Decrease speed | Forward |
| All other devices to propulsion control | Any | Block |