MarineAI Ltd

Cyber Security & Autonomy

Report for National Oceanography Centre

MarineAI Team
6-29-2021

Table of Contents

Executive Summary

Introduction

With the advent of autonomous and remotely operated vessels, the maritime industry will continue its dramatic shift towards an ever-increasing need for robust digital communication and secure vehicle systems.

This report focuses on the potential cyber risks that pose a threat to the safe operation of autonomous vessels which is being increasingly utilised on commercial sea going vessels. The innovative technology that makes these vessels possible, such as highly interconnected vehicle systems and Ship-Shore telecommunications, increase the risk for exposure to cyber security attacks. By their very nature autonomous and remotely operated vessels are vulnerable to increasingly sophisticated cyber security risks. Fortunately, the maritime industry is not the only domain undergoing this dramatic shift towards autonomous systems. Although the maritime domain is partially nuanced, enterprise level security solutions and best practices are available and can be adapted to accommodate the special needs of autonomous maritime vessels.

The Current Term

Traditional systems have not been designed with cyber security in mind and have relied on simple intercommunications between devices in closed networks. Modern systems are no longer closed systems, and in many cases even provide a gateway to the Internet. As marine systems become more digitally sophisticated, a commensurate increase in cyber security protocols must be adopted.

Cyber security concerns are even greater in the context of autonomous ships, where system connectivity is more important than ever. There is a great risk of having to face attacks that have the intent of gaining control of the ship to modify its operation according to external malicious objectives. They may simply be disruptive actions or manoeuvres introduced to demonstrate the hijacking of the ship and its cargo to obtain ransom, but also groundings or collisions caused with the aim of causing damage to the environment. Autonomous vessels are also vulnerable to indirect attacks due to the modification of the AIS or GPS signals.

One approach towards addressing the required level of cyber security is to generalize the Shipboard systems in three broad categories as follows:

- Spoof-vulnerable support systems such as sensors and navigation systems
- Passive consumer capabilities such as vessel analytics and monitoring systems
- Security critical interactive systems such as communication, planning and control management systems

Although the entire vessel platform requires a comprehensive approach, it is useful to look at an example of each of these categories separately.

Spoof Vulnerability

GNSS and AIS spoofing is an attack in which the main goal is to override the true navigation information provided by these systems. These techniques can allow the cyber attacker to either deny availability of this information outright or more nefariously provide false and misleading information to the higher-level systems that depend on valid data from these navigation systems. Many of the core

navigation and sensor technologies, such as GNSS and AIS, have significant cyber weaknesses and are not designed to safeguard from spoofing, jamming or even hijacking with viral firmware.

Passive Consumer Capabilities

An Electronic Chart Display and Information System (ECDIS), which has replaced traditional paper charts on the bridge, is an essential aid to navigation, and has been identified as potentially vulnerable to attack. Not only the validity of information on the digital charts, from hazard location and bathymetry, but also the increasing sophistication of the systems used to display the charts themselves have significant influence on the safe operation of a vessel at sea. This dependence on the accuracy and credibility of the digital chart data combined with the distribution method of this information is only amplified in the context of autonomous and remotely operated vessels. Autonomous systems must be able to trust the integrity and availability of the information distributed by digital charts to ensure effective situational awareness and allow for safe operation at sea. As such, these systems must not only be safeguarded from corruption of data, but also be protected from tampering and denial of service attacks. This is further exacerbated by the future need to adapt the use of ECDIS for autonomous vessels. ECDIS are presently setup for human readability. The additional layer to make the information from ECDIS more consumable for an autonomous system may introduce an unknown vulnerability.

Critical Vehicle Systems

Vehicle management systems, such as propulsion control systems, collision avoidance systems and autopilots, are safety critical systems. Each of these systems are highly interconnected and require active monitoring to ensure uninterrupted availability and reliable authentication methods.

Maritime cyber risk arises when any of these critical navigation or vehicle management systems are compromised, corrupted, or lost, which can lead to operational, safety or security failures and directly impact the ability to safely operate the vessel.

Comprehensive Approach

As a very general guideline, the United States National Institute of Standards and Technology (NIST) has released the Cyber Security Framework Version 1.1 to assist businesses in their approach to evaluate risk assessments by helping them understand an effective approach to manage potential cyber risks both internally and externally. More applicably, the International Maritime Organization (IMO) has adopted resolution MSC.428 (98) to guide ship operators on how to manage the cyber risks unique to the marine domain. The resolution stated that a vessel should have an approved Safety Management System that considers cyber risk management in accordance with the objectives and functional requirements of the International Safety Management Code.

The Medium Term

Originally, swarm intelligence was inspired by the behaviour of birds, insects, and fish, and their ability to work in groups. Swarm agents attempt to mimic this activity and act like super organisms with intelligent behaviour. The very concept of the swarm offers a much higher level of resilience than stand-alone systems with the loss of a part of a swarm does not usually affect its overall activity.

Compared to isolated autonomous systems, swarms are characterized by the level of interaction between the different agents allowing them to maintain global perception of their environment. Each agent forms an integral part of the swarm and actively engages in a dialogue with its closest agent to define or redefine in real time the objectives of the current mission.

Swarming involves coordinating the operation of several systems to accomplish a particularly important or complex mission. Swarms are made up of several homogeneous systems or groups of (relatively few) devices and can be managed centrally or by a decentralized control algorithm. Generally speaking, swarms often rely on a small system with autonomous movement capabilities and using images and sensors to acquire information in an environment. Swarms can act on this information to manouvre and can communicate this information to other agents. Swarms also produce collective functional abilities and may present unplanned solutions that would not be obvious based on the characteristics of a single agent.

The same basic principles that govern the activity of a swarm are also potential candidates for cyber-attacks. Each element of the swarm must be able to conceptualize the proximity information around itself. The conceptualization of proximity information is subject to erroneous interpretation in the event of a contrary disturbance of the environment parameters by a third party. A temporary loss or jamming of communications or incorrect positioning values can jeopardize the overall balance of the swarm. The principle of stability which implies that the swarm does not change its operating mode at the slightest variation of its environment can also be easily put in jeopardy by a cyber-attack. To a lesser extent, other principles governing the activity of swarms such as the principles of adaptability, quality or various response can also be put at risk by cyber-attacks, thus disrupting the overall activity of the swarm.

Swarming requires both autonomous movement and management capabilities which both pose a cyber security risk. A centralised management authority would be a reasonable target for a cyber-attack, as access to or control of the authority would allow an attacker to obtain data about the swarm. Even decentralized management systems rely on extensive communications that could be attacked to help a malicious actor understand and control the system.

Technologies that support the communications required for swarms include radio frequency (RF) and Long-Term Evolution (LTE) network technologies, which both have established cyber-security issues associated with them. For example, LTE technology uses basic hardware and software that have known vulnerabilities. Interference remains an untreated threat capable of preventing successful transmission of RF and LTE signals. Specialized software would help mitigate vulnerabilities by facilitating dynamic detection and adaptation to the RF environment.

Some emerging technology trends could potentially help mitigate the risks associated with intrusion detection and tampering with system functionality. One of these trends is the use of Machine Learning (ML), Artificial Intelligence (AI) and tools to detect cyber-attacks in real time. The cyber-security intrusion detection problem is to identify usage and policy violations among those who use a cyber

system. Different technologies such as Neural Networks, Decision Trees, Support Vector Machines (SVM) have been applied with success to solve these problems.

However, the applications of these techniques or even a fair comparison between them is limited by the availability of reliable training data. Little data is available today to address the problem of intrusion detection because signature identification is based on a database of previously identified signals. A comprehensive methodology involves a combination of a rule-based system (to identify "signatures") and a neural network (to determine if there has been an intrusion). While this approach holds promise for detecting cyber-attacks, again, the lack of data for model training poses a challenge.

It is self-evident that autonomous systems must be equipped with defensive capabilities and measures to respond automatically and dynamically to accidental and deliberate tampering events. It is also logical to consider the fact that if a particular Machine Learning or Artificial Intelligence technique is widely used to detect intrusions: then attackers can develop strategies to deceive the technique and the defences that have been put in place.

In addition to the rate of technological innovation related to autonomous systems, emerging industry trends may also intensify existing threats. Trends that enhance the capabilities of autonomous systems also expose the risk of unauthorized elevation of privilege. At the same time, these trends have the potential to mitigate the threat. For example, as swarms are equipped with additional autonomous capabilities and human operators are removed from the loop, the risks of aberrant system behavior going unnoticed may increase, particularly if automated detection systems are not deployed. On the other hand, automated tools could be used to identify and respond to attacks.

The Near Future Term

The maritime industry is expanding its digital footprint on shipboard systems to take advantage of advances in compute power, analytics and decision-making systems. Although these advances are essential for the operation of autonomous and remotely controlled vessels, they are also increasingly prevalent on manned vessels. These new technologies provide cost savings and safety improvements that give shipowners and operators a competitive advantage. However, the increased connectivity required for these types of systems results in an increased vulnerability and increased cyber security risks.

For example, there is more data flowing between the original equipment manufacturers (OEMs) and their discrete components on vessel for support and maintenance. This new communication channel could be exploited in a cyber-attack originating from the OEM portal that could affect multiple vessels with the vulnerable component.

Additionally, autonomous ships will require a whole series of new equipment to compensate for the lack of crew on board. These systems will have the task of supporting the operations of the ships and making them permanently accessible to various types of remote systems. This situation has raised many questions regarding cyber security and its ability to effectively resist malicious attacks.

Protection against cyber-attacks requires the elimination of existing vulnerabilities, the implementation of effective intrusion detection and prevention measures and recovery plans in case the above measures have failed. We must also take into account that attackers are becoming increasingly more sophisticated with access to powerful tools, which implies that cyber security must continue to be dynamic and proactive.

For example, AIS and GNSS are identified as prime cyber targets in the maritime operational world and preventing external or internal sources from compromising the integrity and availability of this data requires strong processes in place to monitor, identify, respond to, and recover from any potential cyber security incident. The development of new predictive cyber security methodologies and processes now makes it possible to detect these types of threats in real time. By using threat detection and prediction-based risk models derived from the maritime domain, AI systems are able to proactively analyse massive amounts of data in real time and help detect cyber-attacks on these maritime systems.

Detection and prevention measures are essential to provide additional security protection. As the technologies evolve it is now easier and less complex to implement detection and prevention security measures relying on:

- The adoption and deployment of centralized and decentralized hybrid, lightweight and AI-based intrusion detection, and intrusion prevention systems, as well as antivirus mechanisms to trigger an automated response through constant and continuous monitoring. Such adoption can bring many advantages to the maritime domain especially in the IoT field.

- The adoption of AI-based detection using ML-based mechanisms to ensure a higher accuracy in a timely manner.

- Hybrid detection that includes the combination of signature-based, behavior based, and anomaly-based Intrusion Detection System/Intrusion Prevention System patterns to cover a larger variety of maritime cyber-attacks and threats.

- Constant vulnerability monitoring through a constant vulnerability check, assessment, and management of the up-to-date systems, applications, and security patches to ensure a higher level of detection and prevention.

- Advanced activity monitoring that allows the continuous monitoring of autonomous system's behavior over time and compares it to check whether the behavior threshold is different than the normal pattern.

- Easier deployment that ensures a better integration around the onboard systems, including networks, devices, software, firmware, and operating systems, to ensure a constant detection and protection.

- Enhanced access management which defines the right data classification and protection via enhanced authentication mechanisms such as a privileged account management, or via endpoint network encryption to secure maritime communications.

Although a comprehensive cyber security approach is necessary, each of the lower-level systems in an autonomous system should be capable of managing a basic level of cyber security self-awareness without relying on the aforementioned, higher-level functionality to enable safe operations. Safe autonomous operations depend on computer systems and networks to conduct trusted system transactions and maintain unencumbered access to critical information and data. To achieve this, the definition, measurement, and monitoring of onboard system states is required. For example, an onboard Vehicle Controller in an autonomous vessel is the primary control system, responsible for the identification of:

- Communications State (the receipt of normal or emergency messaging)
- Autonomy State (whether the vessel is operating as autonomous or semi-autonomous)
- Vessel Control State (the functionality of the onboard control systems for propulsion and steering).

The base level of cyber security for the Vehicle Controller would require authentication of incoming messages; repudiation of invalid messages, self-checks to ensure tamper free operation and authorized possession and control of lower-level systems to act on required operations.

The Ship-Shore communications channel represents the primary attack vector from a shore-based third party. This communication pathway typical involves a single shore-based Command Information Control (CIC) and multiple vessels.

It is essential for the communication architecture to secure both the shore and ship-based aspects to secure the vulnerabilities exposed by the increased reliance on ship-to-shore communications used be current day autonomous systems. Any compromise of these systems to a cyber attack, could affect the data integrity and overall performance of the autonomous vessel. More significantly any breach within a cloud-based CIC could be exploited to affect all vessels managed by the compromised CIC.

Towards this end, a security model approach adopted by autonomous vessel operators follows the standard security model known as Confidentiality, Integrity, and Availability (CIA). This three-tiered model is a generally accepted component to assessing risks of sensitive information and establishing security policy at an enterprise level:

- Confidentiality Sensitive information must be available only to a set of pre-defined nodes. Unauthorized transmission and usage of information should be restricted. For example, confidentiality of information ensures that data moving to or from an autonomous vessel is not obtained by an unauthorized node for malicious purposes such as asset theft (maritime piracy) or damage (navigation plan alterations).
- Integrity Information should not be altered in ways that render it incomplete or incorrect. Unauthorized nodes should be restricted from the ability to modify or destroy sensitive information either onboard a vessel or for shoreside users of the CIC.
- Availability Information should be accessible to authorized nodes any time that it is needed. Availability is a warranty that information can be obtained with an agreed-upon frequency and timeliness. This is often measured in terms of percentages and agreed to formally in Service Level Agreements (SLAs) used by network service providers and their enterprise clients.

The aim of a comprehensive security model is to implement a valid, CIA-aligned, set of Physical, Technical and Administrative controls to protect the vessel platform.

Physical controls for autonomous vessels relate to the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of autonomous vessel physical controls are:

- Closed-circuit surveillance cameras
- Locked access hatches
- Locked jetty access

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Autonomous ship technical controls are far-reaching in scope and encompass such technologies as:

- Encryption
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software

Administrative controls define the human factors of security. They involve all levels of personnel within an organization and determine which users have access to what resources and information by such means as:

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting

The introduction of autonomous vehicles into the marine domain has been made possible by a confluence of technological innovations including low-cost sensors, edge computing, and machine-to-machine communications with data processing, analytics, and artificial intelligence. Fortunately, the

security needs of these new systems have also been progressing as these digital advances have transformed other industries such as manufacturing.

At this point it is useful to reframe the operation of a remote vessel and monitoring with a shore-based CIC as an enterprise level Internet of Things system. This architecture essentially characterises autonomous vehicles as edge nodes in an enterprise level system.

Enterprise systems are now all cloud or hybrid cloud systems and already have best practices in place for cybersecurity. Leveraging enterprise level industry best practices and applying them to the nuances of the maritime domain in this context provides a significant level of security.

Data integrity and high-availability are critical factors in the success of edge-based computing capabilities supporting core business needs, and this is no different in the marine domain. These same critical factors are required for fleet asset safety management and protection against black hat exploitation, such as piracy. For edge-to-core data exploitation, the availability and trustworthiness of data can mean the difference between success and failure.

As a platform with multiple edge devices intermittently connected to a centralized cloud-based CIC, an autonomous or remotely operated vessel has multiple entry points for hackers and security breaches. These are essential concerns for enterprise level security solutions based on the Internet of Things approach to system architecture.

Traditional systems, including those in the maritime domain, have previously maintained security in part by deploying to an air-gapped environment. Given the connectivity requirements, this is no longer possible with autonomous or remotely operated vehicles. The edge devices must be available for monitoring and control. Thus, at a fundamental level an edge-based system must conform with the following list of security requirements:

- Ability to check the integrity of the edge device by comparing the current software against an official state.
- All communication between an edge device and the shore side CIC must be signed and encrypted. Furthermore, cryptographic signing key pairs should be implemented and regularly cycled to maintain the highest level of protection
- The software running on an edge device must be verified against an official release to check for tampering.
- The software running on the edge device must be able to self-regulate connectivity between the CIC and other edge devices running locally.

There are many industry-level best practices available that provide the technical underpinnings to support these security requirements. For example, the configuration management and deployment of software running on edge devices can be very closely controlled through the simple use of Docker containers.

The Future Term

Cyber security is not just about preventing hackers from gaining access to systems and information, which could lead to loss of privacy and / or control. It is also about maintaining the integrity and availability of information and systems, such as the data corpus used for the building of computer vision models, ensuring business continuity and the continued usefulness of digital assets and systems.

For example, particular care must be taken in the classification of data and their encryption, identification, authentication, and authorization of users. Data protection against unauthorized use, protection of data integrity, connectivity protection, recording and auditing of activities are examples of cyber security methods to be put in place to ensure the overall integrity of systems.

Achieving this requires not only protecting ship systems against physical attacks and other unexpected events, but also ensuring that the design of supporting systems and processes is resilient and that backup and restore modes are appropriate and are available in the event of a compromise.

Artificial Intelligence (AI) plays a key role in this space and is gradually transforming the traditional operational process of the maritime industry. This transformation is reshaping the maritime industry, offering new opportunities to improve productivity, efficiency, sustainability. However, there are increased risks of cyber-attacks with catastrophic results.

AI's ability to analyse massive amounts of data at high rates means that security threats can be detected in real time, or even predicted based on risk modelling. Along with real time data analytics, AI aims to solve some of the near term and future cyber security issues. For example, reducing the potential attack surface and the number of attack vectors by safely managing connected edge devices with massive amounts of moving data are just some of the issues to be solved.

Looking towards the future, AI -powered, self-learning cyber security management systems should be able to solve many of these challenges. Analysed data used to correlate patterns among millions of attack-relevant signals is now a viable response to analyse and defeat cyber security threats. Just as AI can model normal behaviour and learn how users interact with systems, how to recognize vulnerabilities and malware, and how to understand what constitutes an emerging threat, it can also learn when alerts are effective. As the cyber security management dataset grows and receives more feedback on its decision-making, it can gain more experience and improve in the task of defending existing infrastructure.

Furthermore, these automated AI based tools will be able to not only detect cyber intrusion and but also provide strong encryption for communication and data. Generally speaking, countering future global cyber security threats to autonomous vessels, including those found in the marine domain, will be increasingly dependent on the deployment of well-defined processes and strategies that will inherently rely on Machine Learning and AI.

Conclusion

The marine world is experiencing the dawn of a new age of autonomy that has been made possible by the confluence of advances in machine learning and artificial intelligence and the massive increase in computing power of edge devices for smart sensor systems. Additionally, the connected nature of onboard vehicle control systems now allows all aspects of the vessel to be controlled by either a local high-level autonomy system or a remote operator. The innovations that have provided these capabilities also expose this new breed of vessels to significant risks due to cyber-attacks. Existing marine autonomous systems are highly dependent on a robust and reliable exchange of data between all the constituent devices. Future systems will become increasingly reliable on these trusted and authenticated data pathways.

By adopting a high-level system architecture in alignment with other industries that are currently deploying edge devices in an enterprise environment, the marine domain will not only be able to benefit from the technological advances these systems offer, but also the commensurate advances in cyber security.

Although the marine domain requires a nuanced approach to the design and deployment of these systems as edge devices, there is no need to deviate from standard industry best practices. In fact, it would be detrimental to attempt a system design approach that is not supported by industry standards for edge technology.

The fundamental cyber security issues are not unique to the maritime domain. These risks are shared by many other industries in an increasingly connected world. Aligning the requirements of the marine domain with these industry partners will ensure a cyber security solution that is scalable and resilient to future changes.