Cyber Resilience of Automated and Autonomous Ships

Enrico CARRARA[1]
RINA Services S.p.A.

Abstract. Modern automation systems on-board ships perform a variety of complex tasks, offering a great range of options for optimizing ship operation. Interaction between on-board computer-based automation systems and between on-board systems and remote monitoring or control stations has become a key factor for successful and economical ship operation, yet demanding high integration, connection, communication, and control of the interacting components. Complexity and interconnection of computer-based systems on ships however open the possibility for cyber-attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment. It is then necessary to safeguard ships and shipping in general from current and emerging cyber threats adopting countermeasures to make ships cyber resilient. With the advent of unmanned and autonomous ships (Maritime Autonomous Surface Ships - MASS), several tasks and functions traditionally carried out by humans are becoming blurred. While in conventional ship operation seafarers play a role in all functions and interact with ship's systems and the environment, MASS technologies bring changes in how tasks are carried out and how duties and responsibilities are assigned. Partially or totally replacing the human element e.g. in decision making processes and/or interaction with traditional automation systems and the environment, MASS technologies bring new specific cyber-resilience and safety challenges that need to be addressed and require new approaches to risk management. In this article, minimum requirements for cyber resilience of traditional ships are described, based on the work carried out by the International Association of Classification Societies (IACS) and new cyber-related challenges posed by MASS technologies are outlined.

Keywords. Autonomous ships, ship automation, cyber resilience

1. Introduction

Industry has been very active for many years in proposing to shipyards and shipowners advanced automation systems and solutions for the optimization and improvement of ship operations. Nowadays, it is undoubtable that on-board automation is pervasive and shall be considered an essential part of the ship.

Ship automation applies to almost all on-board systems, either essential or not, such as power generation, propulsion, dynamic positioning, cargo and ballast management, navigation, etc., performing analysis, monitoring and control functions. Indeed, there is a trend towards more and more automatic and integrated control of vessels: as an example, navigation systems on modern ships integrate traditional

[1] Enrico Carrara, RINA Services S.p.A., Via Corsica 12, 16128 Genova, Italy; E-mail: enrico.carrara@rina.org.

autopilot with automatic tracking control systems, sophisticated weather routing and weather planning systems, docking systems, etc.

Consequently, complexity has been also increasing with a variety of solutions consisting of stand-alone systems, partly integrated systems to fully physical and functional integrated systems, implemented via proprietary solutions with a limited number of vendors intermixed with open-source solutions, communication protocols and networks.

Moreover, the use of low-cost off-the-shelf computers not originally designed for ship automation purposes has also become more and more frequent. This trend is driven by the need to have more cost-efficient solutions yet creating new issues for design and specification of on-board systems that shall reconsider compatibility and integration aspects, specific failure analysis and test methods, adequate to ensure fault-tolerance in the overall system.

Besides increasing complexity, interaction among on-board computer-based automation systems and between on-board systems and remote monitoring or control stations demands higher integration, connection, communication, and control of the interacting components.

Thanks to standardization of communication protocols, it is relatively easy to connect various sub-systems into a networked integrated system. Integration of computer-based systems via standardized communication protocols ensures connectivity of devices and integration of controllers with operator stations, resulting in very interdependent configurations and network topologies that may include real-time field bus network communication on low level between devices and controllers, real-time control networks connecting controllers and operator stations, and office plant networks comprising various office systems and information management systems.

2. Key Factors for Cyber Risk of On-board Computer-based Systems

Complexity and interconnection of computer-based systems on ships open the possibility for cyber-attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment. It is then necessary to safeguard ships and shipping in general from current and emerging cyber threats adopting countermeasures to make ships cyber resilient.

2.1. Complexity

Complexity of on-board computer-based systems and networks makes traditional identification of vulnerabilities and understanding the effects of cyber events very difficult. Indirect effects and out-of-design interdependencies bring risk analysis and management of complex cyber systems to another level.

Besides complex-by-design systems, sometimes complexity is the result of uncontrolled growth. Typical cases of uncontrolled growth are continuous hardware or software fixes; forcibly ensuring backward compatibility; building new applications on top of legacy systems; merging separate systems of different companies into one almighty system; building byzantine architectures and processes, etc.

Complexity is related to uncertainty, as a state of limited knowledge concerning deviations from what is designed, planned, or assumed. As an additional source of uncertainty, complexity of on-board systems is per-se a source of vulnerabilities.

Vulnerabilities enter systems as they grow more complex. Indeed, some systems are so complex that they defy a thorough understanding.

The ability to develop new theoretical tools and methodologies to understand and engineer increasingly large and interdependent complex systems is required to mitigate cyber risk on-board.

2.2. Interconnection

On the other side, interconnection among computer-based systems on-board and to remote monitoring or control stations amplify the probability of occurrence of a cyber incident, due to the amplified set of possible points where an unauthorized user can access a system and extract data.

Connectivity has been considered for decades, with good reason, the main factor determining the attack surface of cyber systems. As such, most international standards and guidelines address network protection as one of the most important elements of cyber resilience.

In a scenario where fully integrated on-board systems with high demand for ship-to-shore connectivity for maintenance, monitoring, data collection etc. can be considered as normal, unauthorized access, misuse, modification, destruction, or improper disclosure of the information generated, archived, or used in on-board computer systems or transported in the networks connecting such systems are very likely and not difficult to be done.

In the historical approach to networking, a conceptual model was developed (the so-called ISO-OSI model) that partitions the flow of data in a communication system into seven layers, from the physical implementation of transmitting bits across a communications medium (layer 1) to the highest-level representation of data of a distributed application (layer 7).

Cyber risk factors affect each layer of the ISO-OSI model:

- Layer 1 - Physical Layer: vulnerabilities of layer 1 are typically related to loss of power or environmental control, physical damage or destruction of hardware, disconnection of physical links or interception of data. Cyber-attacks focus on disrupting this service in any manner possible, primarily resulting in Denial of Service (DoS) attacks.
- Layer 2 - Link Layer: vulnerabilities of layer 2 are typically related to spoofing MAC addresses, resulting in one node claiming the identity of another, or a node forcing direct communication with another. Attacks at this layer can focus on routing devices themselves. The majority of threats exploiting layer 2 vulnerabilities come from inside the organization itself. The goal of the attack is re-routing any traffic meant for the target host to the attacker's host.
- Layer 3 - Network Layer: vulnerabilities of layer 3 are typically related to route spoofing or IP addresses, that is a way to alter network topology or altering the identity of network resources. Attacks consist of packet sniffing and DoS attacks such as Ping floods and ICMP attacks. These types of attacks can be performed remotely over the Internet.

- Layer 4 - Transport Layer: many vulnerabilities of layer 4 come from poor handling of undefined conditions. Many transport protocols seem to have been implemented under the belief that they would be dealing with well-behaved communication from both the upper and lower levels. The most common attacks start with port scanning, a method by which vulnerable or open network ports can be identified.
- Layer 5 to 7 - Session, Presentation and Application Layers: typical vulnerabilities of these levels are weak authentication mechanisms, passing credentials in clear, leakage of information based on failed authentication attempts, poor implementation of encryption and decryption, compression, poor handling of unexpected input, uncontrolled use of application resources, insufficient application of least privilege criterion, backdoors, bypass of standard security controls, management of software exceptions, program logic flaws, etc. The greatest part of cyber-attacks affects layers 5 to 7, including virus and malware infection, buffer overflow, etc. They very often start from social engineering activities like phishing, scamming, etc.

Of course, networks can be protected at any layer. Defense-in-depth, an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network, can be implemented to reduce the extent of the attack surface and protect the network and the data within.

3. Cyber Resilience on Traditional Ships

In June 2017, the IMO Maritime Safety Committee (MSC) issued Resolution MSC.428(98) [1] recognizing, among other things, the urgent need to raise awareness on cyber risk, threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks.

Being able to perform a cyber security risk management is therefore a requirement by IMO. However, far from being just a tedious constraint, this should be seen as an opportunity to have a complete view of the Operational Technology (OT) and Information Technology (IT) systems on board ships, but also, and above all, to know which systems are critical, and how to implement the most effective measures to lower cyber risk to an acceptable level.

In Resolution IMO MSC.428(98), the IMO MSC explicitly mentions another seminal document, the MSC-FAL.1/Circ.3 “Guidelines on maritime cyber risk management” [2]. MSC-FAL.1/Circ.3 guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and introduce the functional elements that support effective cyber risk management: Identify, Protect, Detect, Respond, Recover.

These functional elements are de facto the “Core” part of the so-called NIST Cybersecurity Framework (“United States National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity” [3]). MSC-FAL.1/Circ.3 explicitly mentions the NIST Framework among the “Best practices for implementation of cybersecurity risks management”.

Even if the NIST Framework was not born for the shipping industry, it has been widely adopted in the shipping industry as the principal reference for the development of other guidelines and standards. In particular, the NIST Framework Core's five functional elements have been largely used since they provide an intuitive, high-level, strategic view of cyber security risk management.

IACS has been involved in addressing cyber resilience of ships since 2017, being the development of a set of technical measures for cyber resilience that support the safe operation of the ship one of the most significant outcomes.

Indeed, the primary goal of IACS work is to support safe and secure shipping, which is operationally resilient to cyber risks. To support safe and secure shipping resilient to cyber risk, in the IACS approach sub-goals for the management of cyber risk have been defined, based on the five functional elements of the NIST framework:

1. Identify: Develop an understanding of OT and IT on-board to manage cyber risk for systems, people, assets and data.
2. Protect: Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.
3. Detect: Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident on-board.
4. Respond: Develop and implement appropriate measures and activities to take appropriate actions regarding a detected cyber incident on-board.
5. Recover: Develop and implement appropriate measures and activities to restore capabilities or services necessary for shipping operations that were impaired due to a cyber incident

Functional/technical requirements are then given for the achievement of specific sub-goals of each functional element, organized according to a goal-based approach.

4. Automation and Autonomy

While in conventional ship operation on automated ships seafarers always play a key role in all functions and interact with ship's systems and the environment, MASS technologies bring changes in how tasks are carried out and how duties and responsibilities are assigned.

Even if not always obvious and sometimes blurred, the difference between automated and autonomous systems is relevant and important. Automation and autonomy are substantially different:

- Automatic (Αυτοματος) refers to a device or process working or acting by its own impulse, moving by itself. The word is a composition of αυτος (self) and a derivative of μεμονα (as adjective, to intend might, force, impulse)
- Autonomous (Αυτονομος) refers to something or someone who governs itself, lives by its own rules, independent. It is a composition of αυτος (self) and νομος (law)

Not in contrast with these definitions, IMO in [IMO MSC 99/WP.9] defined MASS as a ship which, to a varying degree, can operate independent of human interaction.

This definition has been widely criticized and will be revised in the future. Indeed, it is quite evident that this definition can be applied to both automated and autonomous systems, since it does not specify what "independent operation" really means, i.e. if system's actions are determined as a consequence of a deterministic processing of system's internal status and external environmental conditions, as in automation, or if they are determined by a decision taken by the system itself on the basis of its knowledge of the environment, the ship, the overall situation, and an evaluation of the possible consequences of such actions based on a set of "good/bad" criteria.

One of the key points of ship autonomy is the change of human role in ship operation, i.e., how humans interact with the ship and the environment. Autonomy implies changes in what are the actors involved in the accomplishment of a given task, what are the environmental elements the humans interact with, what are the systems, and how responsibilities are assigned.

The difference between automation and autonomy can be easily appreciated considering the so-called Data-Information-Knowledge-Wisdom (DIKW) pyramid. The DIKW pyramid, also known as the DIKW hierarchy, refers to a class of models for representing structural and/or functional relationships between data, information, knowledge, and wisdom. According to the DIKW pyramid, information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge.

In automated systems, the control loop is essentially based on acquisition of data from transducers, processing of such data to obtain information about deviations from the expected system behavior and computation of corrective actions to eliminate these deviations.

Conversely, in autonomous systems, the control loop is much more complex. While, as for automated systems, the control loop's starting point is acquisition of data from transducers, the amount and variety of data acquired is much greater and is aimed to achieve a complete situational awareness rather than simple information about system deviation from conditions established at design stage.

Situational awareness is the level of information required by autonomous systems to allow the next step, i.e., creation of knowledge. In the DIKW view, knowledge can be intended as the result of processing, organizing and structuring information and has to do with the capacity to understand, explain and negotiate concepts, actions, and intentions. Knowledge allows to organize information in models for reliving the past and anticipating or creating future. Knowledge has the potential of dynamically modifying the attitude to react to events and enables new behaviors to be envisaged.

Through knowledge, autonomous systems develop the ability to rank scenarios and recognize which is better and which is worse. In other words, the system makes judgments and decisions and selects the right things to do.

Another important feature of autonomous systems is their ability to evolve, thanks to the integration with technologies like artificial intelligence and machine learning. Evolving systems rely on emergent structures to generate new system behaviors, while fixed-design systems react badly to unexpected or changing environmental conditions.

Adaptation to changing conditions creates diversity. For fixed-design systems, diversity is usually seen as a source of unreliability. It is then clear that the criteria for achieving functional robustness for evolving vs. fixed-design systems are very different: where fixed-design systems rely on redundancy, evolving systems are characterized by a flexible/adaptable structure.

In safety management, diversity and uncertainty are seen as risk multipliers, and the prevailing paradigm tends to eradicate them through anticipation of all situations and predetermination of corresponding responses. But this safety strategy generates a vicious cycle of predetermination and vulnerability, more predetermination generating more vulnerability, which requires more predetermination, hence robust yet brittle

systems, less and less able to handle disturbances outside their envelope of designed capabilities.
Another approach to safety and risk management for autonomous systems is needed.

5. Cyber Resilience of Autonomous Ships

Among the new challenges posed by MASS technologies, transition from human to machine control of operational processes is for sure the most evident. As MASS technologies that permit electronics systems to make decisions are introduced, traditional assumptions around what crew are capable or required to do for the safe operation of the ship may become invalid, because the system awareness and/or the environmental situational awareness necessary for decision making is no longer maintained by the human as it was in traditional automated ships.

Ship safety is then achieved (or not) through the functions of equipment fitted on the ship rather than through human action, moving risks from the human element towards the equipment functions.

Autonomy does not simply change, or eliminate, tasks once performed by the human operator. It changes the task structure and creates new tasks that need to be supported, thereby opening the door to new types of risks, errors, and vulnerabilities. It is then clear that developing autonomous systems without consideration of a new approach to risk management related to the human factor may lead to new and more catastrophic failure modes. New forms of human error often emerge where, ironically, these technologies are introduced to eliminate human error.

Human errors and system vulnerabilities may also arise because the task structure changes in a way that undermines collaboration between operators. Effective system performance involves performing both formal and informal tasks. Informal tasks enable operators to compensate for the limits of the formal task structure; for example, with paper charts mariners will check each other’s work, share uncertainties, and informally train each other. Eliminating these informal tasks can make it more difficult to detect and recover from errors. In this sense, technology can disrupt the cooperation between operators.

Another substantial shift in the approach to cyber resilience of autonomous ships is due to their inherent complexity. More and more complex networks of sensors and actuators highly increase data collection needed e.g. for situational awareness and digital twins.

Complexity of autonomous systems brings emergent properties that are not directly related to any single component but are instead due to a context of use and interactions between different components, with or without human-system interactions. As a result, safety considerations at system integration level may become at least as important as safety at equipment design.

Attention to integration of systems should be improved in each of the stages of a vessel’s life. The lifecycle development of integrated systems needs to be well understood, as well as the involved parties, their roles and responsibilities.

In light of the above, cyber resilience of autonomous ships shall be reconsidered not as a simple extension of cyber resilience of automated ships, but as a process based on management of new types of risk and sometimes requiring new approaches to consideration of risk factors. This does not imply redesigning the principles of traditional cyber resilience. Rather, it is necessary to focus on the aspects characterizing MASS technology.

6. Concluding Remarks

In this article, several aspects of cyber risk related to computer-based systems on-board ships have been briefly presented, highlighting how the increasing level of complexity, integration and connectivity opens unprecedented opportunities for cyber-attacks. Cyber-attacks can target any layer of on-board networks, each having specific vulnerabilities and potential impact on the overall system performance.

International organizations such as IMO and IACS have recognized very quickly the urgent need to raise awareness on cyber risk, threats, and vulnerabilities to support safe and secure shipping resilient to cyber risks. A set of guidelines and standards has been produced to address cyber resilience of ships, such as the IMO Resolution MSC.428(98), the IMO MSC-FAL.1/Circ.3 and the IACS Unified Requirements on cyber resilience of ships.

The NIST Framework, even if not born for the shipping industry, has been widely adopted as the principal reference for the development of guidelines and standards. In particular, the NIST Framework Core's five functional elements provide an intuitive, high-level, strategic view of cyber risk management.

Maritime Autonomous Surface Ships (MASS) brought even more challenges to cyber resilience of ships, due to the differences between autonomy and automation. One of the key points of autonomy is the change of human role in ship operation, i.e., how humans interact with the ship and the environment.

Cyber resilience of autonomous ships shall be reconsidered not as a simple extension of cyber resilience of automated ships, but as a process based on management of new types of risk and sometimes requiring new approaches to consideration of risk factors. It is necessary to focus on the aspects characterizing MASS technology: transition from human to machine control of operational processes, increased complexity of systems, high connectivity of sensor/actuator subsystems, increased amount of data, increased diversity of workforce interacting with on-board systems, high system integration.

References

[1] Resolution IMO MSC 428(98), "Maritime Cyber Risk Management in Safety Management Systems", International Maritime Organization (IMO), June 16, 2017. 1 p.

[2] MSC-FAL.1/Circ.3, "Guidelines on Maritime Cyber Risk Management", International Maritime Organization (IMO), July 5, 2017. 4 p.

[3] "Framework for Improving Critical Infrastructure Cybersecurity", National Institute of Standards and Technology (NIST), version 1.1, April 16, 2018. 55 p.