Autonomous Shipping and Cybersecurity

Buques autónomos y ciberseguridad

DOI: https://doi.org/10.25043/19098642.185

Jaime Pancorbo Crespo [1]
Luis Guerrero Gómez [2]
Javier González Arias [3]

Abstract

Currently, as a result of new communications technologies, autonomous ships are even closer to our seas than we could think. But, besides undoubted advantages, it gives rise to uncertainties and challenges in several aspects, which include those related to the fields of cybersecurity and legislation, in relation to international regulations and national laws. The aspects of autonomous shipping are included in the information regulations of Bureau Veritas, and additional specific tags have been created to collect the cybersecurity/cyberprotection aspects of such ships.

The objective of this article is to present the current status and the foreseeable evolution of the regulations on autonomous shipping from the point of view of a Classification Society, as well as the current evolution of the methodologies concerning cybersecurity.

Key words: Connected ships, Autonomous ships / unmanned vehicles, Cybersecurity, IT/OT, Additional tags (Cybersafe/Cybersecure), Current research.

Resumen

Actualmente, y gracias a las nuevas tecnologías de las comunicaciones, los buques autónomos están aún más cerca de nuestros mares de lo que pudiéramos pensar. Pero, al igual que ventajas indudables, generan incertidumbres y retos en varios aspectos, entre los que destacan los relacionados con los campos de la ciberseguridad y legislativos, en lo referente a normas internacionales y legislación nacional. Los aspectos de los buques autónomos están recogidos en el reglamento informativo de Bureau Veritas, así como se han creado notaciones adicionales específicas para recoger los aspectos de ciberseguridad/ciberprotección de dichos buques.

El objetivo de este artículo es dar a conocer el estado actual y la evolución previsible de las regulaciones sobre buques autónomos desde el punto de vista de una Sociedad de Clasificación, así como la actual evolución de las metodologías concernientes a la ciberseguridad.

Palabras claves: Buque conectado, Buque autónomo/buque sin tripulación, Ciberseguridad, IT/OT, Notaciones adicionales (Cybersafe/Cybersecure), Investigaciones actuales.

Date Received: January 13th 2019 - *Fecha de recepción: Enero 13 de 2019*
Date Accepted: March 13th 2019 - *Fecha de aceptación: Marzo 13 de 2019*

[1] Marine Engineer. Bureau Veritas Spain and Portugal. Madrid, España. Email: Jaime.pancorbo@es.bureauveritas.com
[2] Marine Engineer. Bureau Veritas Spain and Portugal. Madrid, España. Email: Luis.guerrero@es.bureauveritas.com
[3] Marine Engineer. Bureau Veritas Spain and Portugal. Madrid, España. Email: Javier.gonzalez-arias@es.bureauveritas.com

Introduction

The new technologies and the inexorable advance towards the Industry 4.0 has introduced the maritime industry into a new field of possibilities in the development of the business:

- Increased security, such as the decrease in the possibility of human failures, etc.

- Reduced environmental impact, due to lower emissions and lower spill probabilities

- Reduced OPEX, given the possibility for a smaller crew, as well as improved ship performance that leads to lower fuel consumption, lower maintenance, etc.

- Optimized shipping management, basically due to integrated logistics, integrity management and continuous controls, monitoring and verification.

But although this "digitalization" process will bring numerous benefits and opportunities, it also entails new threats and challenges for the industry, from several points of view, which are highlight below:

1. Technology: Systems cybersecurity, connectivity, remote access, artificial intelligence.

2. People: Training, misuse of systems, corruption, etc.

3. Processes: Supply chain and Cyber Response Plan.

4. Legal: who is responsible for unmanned vehicles?

It is important to make a distinction between what is known by cybersecurity and cybersafety, which will help us better understand the problem:

- Cybersecurity (it is the protection against the intentional attack to a ship's systems, which would be also known as Cyberprotection).

- Cybersafety (the intrinsic safety of systems, *i.e.* reliability). As the independence of human intervention becomes more important, the reliability, both of the system's own equipment and the redundancy thereof, becomes fundamental.

Currently and as result of new communications technologies, unmanned vehicles are even closer to our seas than we could think. But for the existence of autonomous ships, we must not only provide the technical means to make feasible its materialization, but also cover legal aspects, regulations and the issues indicated above.

Current situation and Cybersecurity

In the results of the survey published by the specialized marine magazine IHS Fair play among 300 participants, 34% of them acknowledged that they had suffered cyber attacks in the previous 12 months (we must bear in mind that these participants are only those who were aware of being attacked!!!). Regarding these attacks, the greatest vulnerability was represented by the workers of companies, which accounted for 47% of them, while suppliers represented 19%.

The attacks have caused companies to consider the need to train their workers, both in preventive aspects as in how to react upon any risk or attack. 51% of companies have trained their workers in this regard, but only 23% are certified.

The following case is an example of what cyber attacks represent today: in June 2017, Maersk was attacked by malware as part of a global attack. The virus stopped the company's operations in ports such as Rotterdam, Los Angeles and Auckland and interfered with operations worldwide. Maersk reported losses close to 250-300 million dollars as a result of the operations that took place in July and August.

But as mentioned above, most cyber attacks are carried out by company personnel: an example of this is the cyber attack suffered in a MODU oil rig with a dynamic positioning system. A worker on the platform, completely unintentionally, introduced a malware through a USB stick inserted into a computer. This caused a loss of dynamic positioning and made the platform go adrift, so for security reasons, the well had to be temporarily closed. This could have resulted in a disaster not only for the workers but also for the environment!!

A final example would be that of the Clarksons magazine, in which the attackers gained unauthorized access to their computer systems and to the information contained in them, to then request a ransom for that information under the threat of disclosing it. The company's shares fell 2.71%.

This situation makes nonnegotiable the need to increase the security of the systems against external attacks and system failures due to reduced crews.

Autonomous Shipping

Autonomous ships should not be confused with unmanned vehicles. The definition of both is the following:

1. Autonomous ship. A ship that is capable of making decisions and executing actions with or without human intervention in the chain of decision. An autonomous ship can be manned with a reduced crew or no crew.
2. Unmanned vehicle. A vehicle that does not physically contain human life on board and is capable of executing controlled movements.

Internationally, autonomous ships are known as MASS (Maritime Autonomous Surface Ships).

To define their degree of independence with respect to human beings: data collection, data interpretation, decision assistance or completely autonomous, Bureau Veritas classifies autonomous ships according to who executes each step in the decision-making process (see Fig. 1).

It is important to emphasize that the previous classification is not homogeneous internationally, and different organisms represent the current situation in more or less levels, but the philosophy is common.

The aspects of autonomous shipping are included in the specific information regulations Bureau Veritas NI 641 "Guidelines for autonomous shipping" *(December 2017 Edition)*, and additional specific tags have been created to collect the cybersecurity aspects of such ships.

This process of autonomy and independence from human interference leads to different benefits, such as:

- Reduced crew costs

Fig. 1. Bureau Veritas classification of autonomous ships

Category	Level of Autonomy		Manned?	Control Method
Conventional	0	Human operated	Yes	Manual or automated operations under human control
Smart	1	Human assistance	Yes/No	Support in decisions. Humans take actions and decisions
Autonomous	2	Human delegated	Yes/No	Humans must confirm decisions
	3	Human supervised	Yes/No	The system awaits confirmation. Human are always informed of decisions and actions
	4	Completely autonomous	No	The System does NOT await confirmation. Humans are only informed in case of emergency

- Reduced human errors (let's remember that almost 80% of incidents/accidents are caused by human errors!)

- Reduced ship weight, by eliminating human support weight in superstructures

- Reduced fuel consumption (6%)

- Increased spaces dedicated to cargo

- Reduced construction costs (approximately 5%)

But there are other aspects to be taken into account and that have not been resolved yet, such as:

- Increased system reliability, which will result in a redundancy of many systems, increasing construction CAPEX by 10% for this reason.

- Technology. The current state of the art does not allow considering fully autonomous ships without the evolution of artificial intelligence systems, etc.

- Legal aspects. We must take into account the legal responsibilities that these ships represent, since they lack crew, and above all, the highest authority on the ship: the captain

- Regulatory aspects: the current rules assume the existence of an onboard crew and must adapt as the industry develops in this direction, taking into account the possible solutions to the problems that will be faced. Some of the regulations to take into account are the following:

    o STCW. Crew training. The treatment of the new "crew" of the vessel and its training should be appropriate to this new situation.

    o COLREG. The prevention of boarding attacks becomes even more important in the case of unmanned ships. Surveillance and identification systems must be increased.

    o SOLAS. Security of Human Life at the Sea... without crew? Firefighting safety systems must be installed in those places that are subject to fire risks, or automatic extinguishing systems that replace manual systems.

    o ISM. There must be a communication channel between the Company and the people onboard the ship.

Cybersecurity

Given the current trends of increasingly "connected" ships, it is essential to provide protection given the possibility of cyber attacks. Such protection is even more important, if possible, when taking into account the possibility of increasing the autonomy of ships.

With respect to cybersecurity, it is worth highlighting two widely used regulatory standards:

a) On the one hand, the international regulations of the International Maritime Organization (IMO), through MSC 428 (98), adopted in 2017. It is titled "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS". In this MSC, it is indicated that cyber risks must be correctly taken into account before the first annual visit for the issuance of the Company's Compliance Document, after January 1, 2021. In addition, this item must be included in the ISM.

b) On the other hand, the regulations of the European Union, which have two sources:

b.1) EU Directive 2016/1148 (This Directive concerns the security of information networks and systems). It is called NIS Directive. It includes the ports but not the ships.

b.2) The GDPR Directive (corresponds to EU 2016/679). This directive is already applicable (since May 2018) and includes ships.

It is important to highlight the creation of a specific cybersecurity-dedicated agency in the European Union, which is called ENISA (EU Cybersecurity Agency).

Another widely used standard, which is not in any case in the field of regulation, is the benchmark framework established by NIST (NIST = National Institute of Standard and Technology, part of the US Department of Commerce).

They are a very important reference framework, and are based on the current BIMCO guidelines (which acronym stands for "The Baltic and International Maritime Council").

Among the standards indicated by NIST, it is important to highlight that it establishes a series of parameters that must be solved sequentially in order to provide proper security. These parameters are the following:

a) Risk Identification. Among the corresponding categories, it should be emphasized the need to conduct risk analyses, not only for the formalization of the system used but also for its execution, affecting the entire company's logistics chain.

b) Protection of systems in the event of a cyber attack. This section includes all the protection related to maintenance, the formation of teams, data protection, etc.

c) Attack detection. The detection process must be taken into account, as well as the consideration of possible anomalies and a continuous monitoring system, in order to be able to detect an attack early.

d) Response to the attack. The purpose is to stop the impact of the incident, and involves actions to plan the response, plan correct communications, as well as the analysis of the attack, including mitigation systems and improvements.

e) Recovery of systems/data/etc. To this end, planning should be done on the possible recovery of information and systems, as well as on any improvements.

Other standards correspond to ISO, IEC, etc.

Once the problem has been identified, it is important to make a distinction about which ship system is being attacked. This division will be defined according to whether it will affect an IT or OT system of a ship:

a) *IT (Information Technologies).*
When an attack takes place on the IT systems of a ship, in which the financial and commercial aspects will be mainly affected, from the point of view of the reputation lost.

An example would be electronic mail systems, electronic certificates, etc.

b) *OT (Operation Technology)*
In this case not only monetary and commercial aspects are affect, but human life, the ship or platform are endangered and there is a possibility of environmental con-tamination.

The following are some examples of OT systems: ship navigation systems, dynamic positioning systems, etc.

Solutions of Bureau Veritas

The solutions found consists of additional tags that will provide additional benefits in terms of security and reliability.

a) Regarding the reliability of systems, the safety thereof is affected by three terms which together may cause an accident. These terms are: Systems, Software and Human Intervention. To deal specifically with these aspects, it is worth highlighting 2 additional tags in this regard:

a. SW-Registry. Software registration and maintenance.

b. HWIL (Hardware In The Loop), for

testing complex systems. It is developed through regulations Bureau Veritas NR 632 and NR 467.

b) Regarding cybersecurity, it is also affected by the intersection of 3 systems: Objective, Protection and Attacker.

To solve this issue, Bureau Veritas has created 2 specific tags, both included in Regulatory Note 659 (NR 659) (Cyber Managed and Cyber Secure), but without leaving aside the importance of certifying the logistics chain, which is established in Regulatory Note Bureau Veritas 642.

The CYBER SECURE tag is especially directed to newly built ships and affects both equipment (and their certifications) as well as the design of all aspects related to a possible cyber attack (physical access, such as cables, etc., as well as remote accesses both onboard and onshore). This tag not only affects the shipbuilder, but also equipment suppliers, shipyards and the systems integrator. Security control is carried out by means of automatic software. Equipment can be certified or not depending on the level requested in this same tag (certified equipment can be requested or not).

The CYBER MANAGED tag has been created especially for ships that are currently in service, and for those in which a design evaluation cannot be carried out, since it has not been taken into account in construction. In this tag, the roles of each one of the participants are detailed and explained. Likewise, the procedures used will be taken into account. Crews must receive adequate training on issues against a cyber attack. The organization must have a change management policy to ensures the proper management in terms of IT and OT systems. Similarly, through this tag, an adequate response must be given to incidents (both locally and remotely) and the status of vulnerabilities must be monitored. In this case, security control is achieved through manual procedures, unlike in the CYBER SECURED tag.

Furthermore, Bureau Veritas has created the SYSCOM tag, which is directly aimed at the prevention of malicious attacks. It is also a voluntary tag that protects data exchanges onboard and onshore.

Current research on Autonomous Shipping

Currently, Bureau Veritas is participating in the development of projects, both financed by public bodies and by industry consortia, in the field of unmanned ships. The following are currently the most important:

Bourbon Smart Ship Program

The consortium formed by the shipping company Bourbon, the manufacturer of dynamic positioning systems Kongsberg and Bureau Veritas, is developing a program that increases the automation level both in operations and in processes.

It allows a ship to transmit data onshore so that it can be analyzed and resolved, which translates into a reduced crew and reduced time onboard.

A pilot system is being developed and implemented on the ship Bourbon Explorer 508 (you can consult the website https://youtu.be/tCXe1eXJElM).

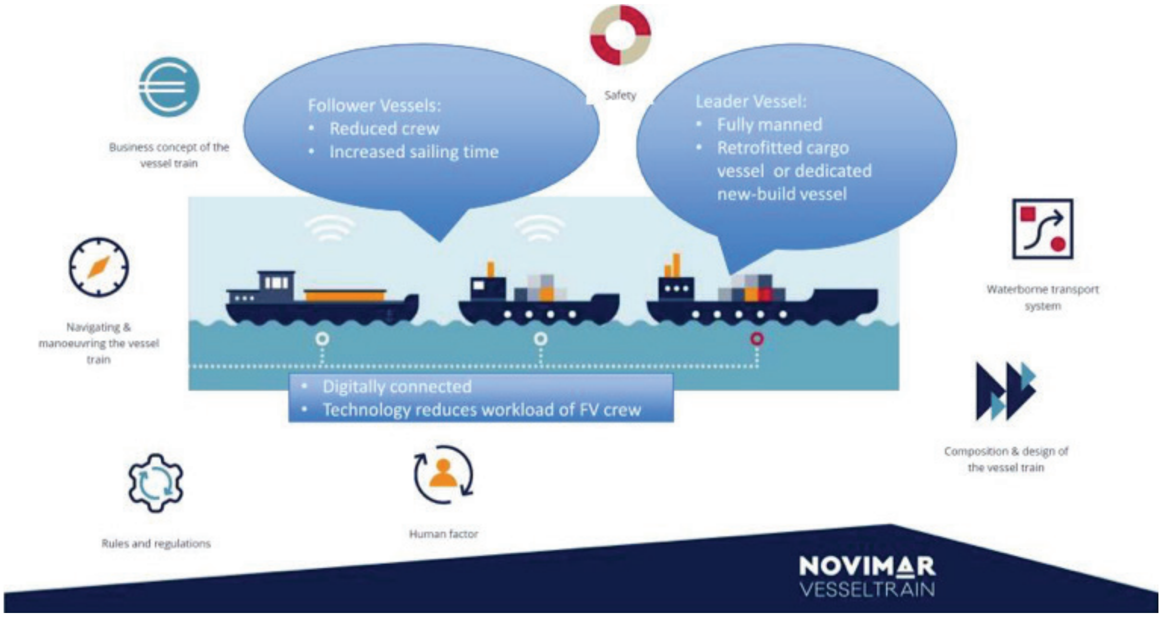
The next steps in this project will consists of the development of continuous testing and remote verification systems in relation to the ship's dynamic positioning system.

NOVIMAR Program

The NOVIMAR project is a H2020 European project with EU funding. It consists of the development of a new concept of marine transport called Vessel Train (see https://vimeo.com/263869758). The vessel train consists of a leading ship (L) followed by a series of ships with reduced crew and digitally connected to the leader, which are called follower ships (F).

This concept will reduce operational costs and increase economies of scale due to its use of existing infrastructures.

Fig. 2. NOVIMAR Concept


Safety
Business concept of the vessel train
Follower Vessels:
• Reduced crew
• Increased sailing time
Leader Vessel:
• Fully manned
• Retrofitted cargo vessel or dedicated new-build vessel
Waterborne transport system
Navigating & manoeuvring the vessel train
• Digitally connected
• Technology reduces workload of FV crew
Composition & design of the vessel train
Rules and regulations
Human factor
NOVIMAR VESSELTRAIN

Source: NOVIMAR Webpage.

Twenty-two companies participate in this Consortium, from logistics operators, industry, public and research agencies belonging to 7 EU countries and two associated countries.

Autonomous shipping JIP

The Dutch marine cluster, according to its planning, will carry out a first test of an autonomous ship in 2019. The vessel will be an existing offshore operation ship facilitated by SeaZip Offshore Services and built at the Dutch shipyards Damen. The demonstration will be part of a much more extensive 2-year program that includes a consortium of 17 members, which includes, in addition to Bureau Veritas and Damen, the Marin Channel, the Dutch University, TU Delft, etc.

This project is co-financed by the Ministry of Economic Affairs of the Netherlands.

Conclusions

Completely autonomous ships, to this day and in spite of the pilot projects created with small ships, seem a utopia in large ships, but which will be reached as the technology develops. What is sure and more immediate is the possibility of reducing crews given the current technology, although the equivalence of safety aspects with respect to minimum crews must be verified.

Cybersecurity is a fundamental aspect not only for the development of autonomous shipping technology, but also a navigation need, to accommodate the increased vessel connectivity, or through increases in automation with smart aids for operations such as the monitoring of various parameters and remote assistance to solve problems and incidents, while providing protection against attacks to both systems and communications.

Cybersecurity, together with the development of unmanned vehicles and autonomous ships, is a great opportunity for our entire sector and offers many different R&D opportunities in different aspects that will surely be implemented in the maritime sector.

References

BUREAU VERITAS. NR467 Rules for Steel Ships, July 2018.

BUREAU VERITAS. NI641, Guidelines for Autonomous Shipping, December 2017.

BUREAU VERITAS. NR 659 Rules on cyber security for the classification of marine units , December 2018.

BUREAU VERITAS. NR 642.Cybersecurity Requirements for Products to be installed On-Board Naval Ships. July 2018.

BUREAU VERITAS. NR 462, Hardware in-the-loop testing, January 2016.

Guidelines on Maritime Cyber Risk Management , IMO (International Maritime Organization), June 2017.

NIST (National Institute of Standards and Technology), Framework for improving Critical Infrastructure Cybersecurity, April 2018.

The guidelines for cyber security onboard ships, version 3, BIMCO, CLIA, INTERNATIONAL CHAMBER OF SHIPPING, INTERMANAGES, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL.