infodas

connect more. be secure.

# Cyberthreats to the Shipping Industry and how to mitigate them

# Cyberthreats to the Shipping Industry and how to mitigate them

Dr. Fulvio Arreghini

When thinking about cybersecurity or cyberthreats, most people will have in mind server rooms full of blinking lights, SOCs where network operations are monitored by cyber teams or evil hackers wearing a black sweater trying to break into some kind of hi-tech datacenter. Nobody would ever think about one of the thousands of bulky, low-tech and sometimes rusty merchant vessels sailing around the globe.

Actually, cyberthreats to the shipping industry are a growing cause for concern of which operators are becoming more and more aware every day of the cyber risks costs and regulatory frameworks trying to define policies and guidelines to increase the cyber resilience of vessels.

When we think that 90% of the goods are now traded by sea, and we have a look to the increasing number of cyber incidents involving merchant ships and their actual or potential consequences, the compelling need of effective and efficient solutions for making current and future ships cyber resilient is more than evident. Here, after presenting current trends of the Shipping Industry's cybersecurity, the role of Cross Domain Solutions as an answer to this need is being analyzed.

## Container ships – a pillar of the global economy

Today, 90% of the goods are traded by sea and this trend is showing further growth. Containerized goods represent nowadays the most common mode of transportation and the great part of container travels, at least for the majority of their lifecycle, by sea. A quick visit to online maritime traffic trackers, such as Marine Traffic is enough to understand how many vessels are sailing around the globe. At the moment the screenshot below was taken, roughly 250 thousand vessels were being tracked. The green icons, representing cargo vessels, are notably in large majority, followed by tankers, represented by the red icons.

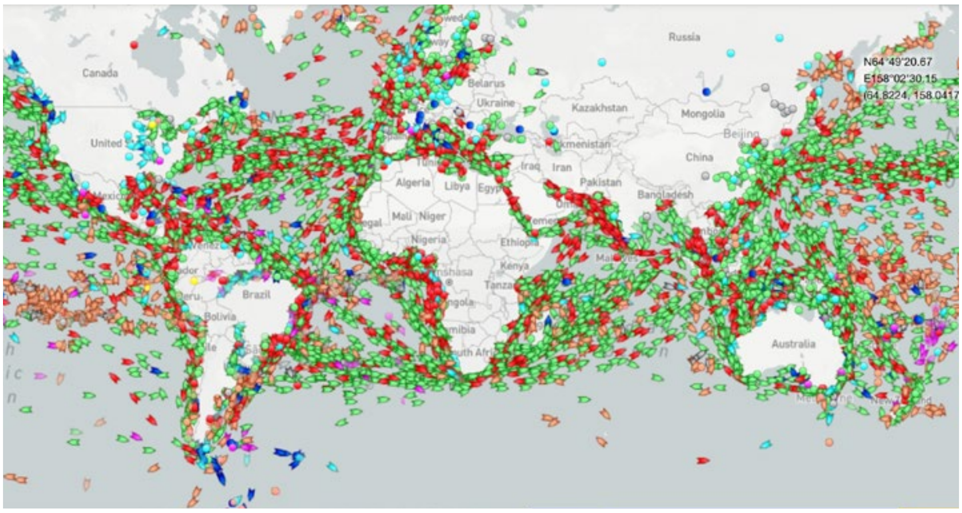

*Figure 1: Marine traffic screenshot*
*Source https://bit.ly/3B3Plgh*

Focusing at first on cargo vessels, most of them are carrying containers. The average size of a merchant vessel has doubled in the last twenty years and modern ships can carry up to 24.000 containers. The famous Ever Given container ship which blocked the Suez Canal was indeed carrying roughly 20.000 containers when the accident happened. This was a major *reveille* for many stakeholders as, despite the essential link of the trade supply chain the maritime segment represents, it had somehow remained invisible and been taken from granted.

The incident caused a damage estimated in 10 Billion USD. The infamous incident raised the attention not only to the potential disruptive effects of shipping accidents but also on the strategic importance of SLOCs (Sea Line of Communications) with particular emphasis on straits: it is estimated that 12% of the global shipping traffic is crossing the Suez Canal. Straits are well known as neuralgic points of the global maritime economy and their blockage is likely to cause severe consequences to the shipping economy.

On the other side, also disruptions in major ports/hubs can cause severe economic consequences, like the recent case of the decision from an important shipping operator to drop calls in the port of Hamburg due to its congestion and long waiting times. The functionality of port hubs depends on several factors like the planning of entrance/exit of ships, and of mooring, loading, offloading; and the scheduling of arrival of goods by other transportation means (e.g. rail, road). The complexity of the port activities relies on an accurate planning and execution and on the support of complex IT/OT infrastructures.

*Figure 2: Ever Given ship in the Suez Canal*
*Source https://bit.ly/3B5a7vX*

### Ships causing disasters: tankers and beyond

In the overall panorama of merchant vessels, tankers deserve a special mention. These vessels, besides carrying a significant value on their payload, also have a high potential to cause severe consequences to the crew, rescue operators and to the environment in case of accident. The collision of the Sanchi tanker is only one of the latest major disasters involving a tanker ship. It is furthermore interesting to note that the perception about the possible consequences of a tanker incident is widespread in the general audience, due to the high resonance that these kind of accidents always gain in the media, especially due to their immediately observable effects on the maritime environment. The perception of container ship accidents and their consequences on the marine environment is, on the other hand, less visible, even if the phenomenon is becoming, according to the experts, more and more relevant.

When an accident occurs to a merchant vessel, besides the immediate consequences like potential payload loss, casualties, costs for removing the wreck etc. medium-term consequences such as extensive pollution may have a huge impact on the global value chain. It is sufficient to think that an oil spill creating a pollution area will immediately affect the economy of the impacted environment and will produce immediate losses on the carrier company due to liability for damages and loss of reputation.

Here come the first set of handful conclusions:

- The shipping economy moves 90% of the goods.
- Each and every single merchant vessel is carrying a significant value (up to 24.000 containers).
- There are assets linked to the shipping economy, other than ships, like straits and major hubs, which can heavily impact the value chain.
- A merchant vessel can cause severe consequences in case of accidents which go well beyond the loss of part of their payload and can ultimately cause major losses to carrier operators.

### The cyber side of the shipping industry

The majority of merchant vessels in service are older than 15 years, with an average age just over 20 years across the fleet. Based on this data alone, it becomes easy to assume that a fleet composed mainly of old ships with legacy technologies onboard could be something that does not necessarily match the stereotypical interests of cybercriminals or hackers.

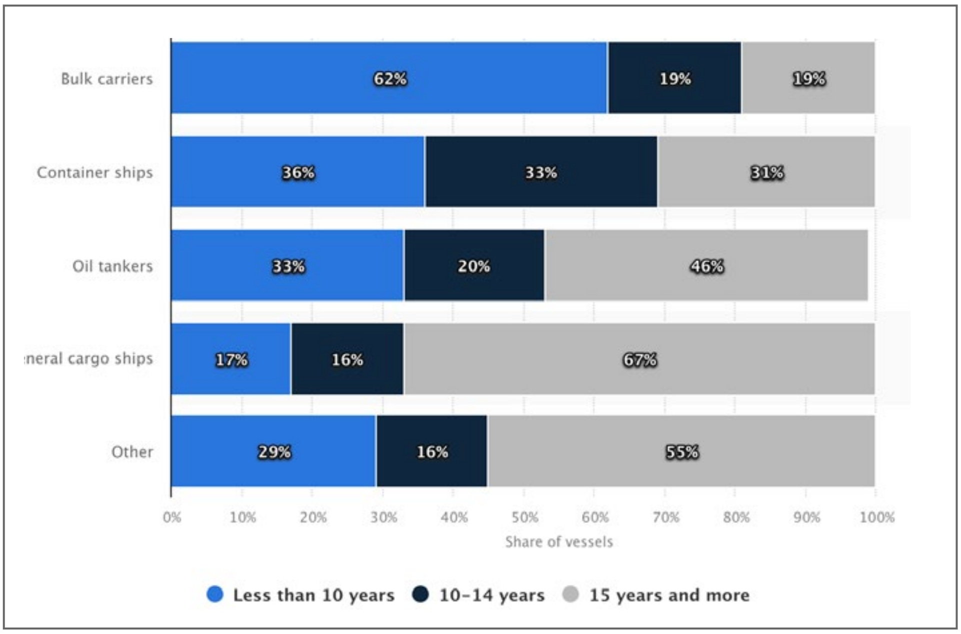

*Figure 3: average age of mer-chant vessels*
*Source https://bit.ly/3OYCGkf*

However, in reality, cyberthreats are becoming one of the major concerns for the Shipping Industry and the number of cyber-attacks targeting ships or ports is a phenomenon experiencing a fast growth with peaks of 400% at the beginning of the COVID pandemic.

Several initiatives have tried to analyze the reasons behind this, like the Cyber Resilience for the Shipping Industry (CyberShip) project. Among the major drivers for the increasing cyberattacks to merchant ships we are able to find:

## 01 Outdated technology

The great majority of merchant vessels IT and OT systems are based on outdated technologies and are not properly maintained/patched. It is not rare that the onboard IT systems are running on Operating Systems no longer supported (e.g. Windows 2000). This situation gets even more complicated in the OT branch of the ship: the control of many critical systems (ballast, propulsion, fuel distribution) runs on automation systems based on legacy protocols not designed for cybersecurity and often exposed to external attacks.

## 02 High dependencies on unsecured systems

Ships rely on several electronic aids, like ECDIS (electronic Chart Display and Information), GNSS, AIS which have not been designed with cybersecurity in mind, therefore, they are exposed to several attack vectors. Modern vessels designed to cruise with all these navigation aids are often running on autopilot. Consequences of an attack to these systems may go from the loss of situation awareness to the possibility to bring the ship out of its course and ultimately cause collisions with other ships.

## 03 Low awareness within the crew

The crews of most merchant ships do not include an IT officer and the introduction of cybersecurity awareness education programs for ship crews is quite recent. The crews of merchant ships, who spend significant time at sea communicates with homeland and the owner company using the Internet. The combination of low cyber awareness and significant time spent connected to applications like email services or web browsers, offers a wide surface for attack vectors leveraging on social engineering (e.g. phishing, spam emails).

## 04 Large window of opportunity

Ships spend great part for their time at sea and this circumstance alone offers a large window of opportunity to potential attackers. The isolated ship presents, in fact, high potential to Denial of Service attacks conducted by jamming its communication and positioning systems or to Man In the Middle attacks where these systems are hijacked to bring the ship off course.

## 05 High return on investment

The ship is by nature a HVT (High Value Target) for the reasons already analyzed in the first part of this article (value of the payload and potential to produce disasters). Considering the large number of ships in service and all other listed drivers, an attacker has a high potential of success even with simple, untargeted attacks, e.g. attacks not targeting a specific vulnerability of an onboard system (identified after a preliminary reconnaissance/fingerprinting phase) but just 'giving it a try'. This is the typical case of spam/phishing emails sent to a high numbers of recipients. Even with a relatively low hit rate (e.g. 1%) a significant effect can be achieved by the attacker.

## 06 High value of information

Besides the attacks vectors targeting the ship IT/OT to gain access to these systems as the first step of an attack chain usually intended to extorsion or demonstrative actions, attacks can be conducted to ships also to steal/leak sensitive information (e.g. financial information, data about the carried payload) and damage the carrier company's reputation.

Based on the above drivers, several attack chains can be imagined. These can be grouped into two broad categories: attacks targeting the ships as victims and attacks using the ship as part of a larger attack chain.

One summary of the typical cyberattacks observed in ships is presented in Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends from which Figure 4 is extracted.

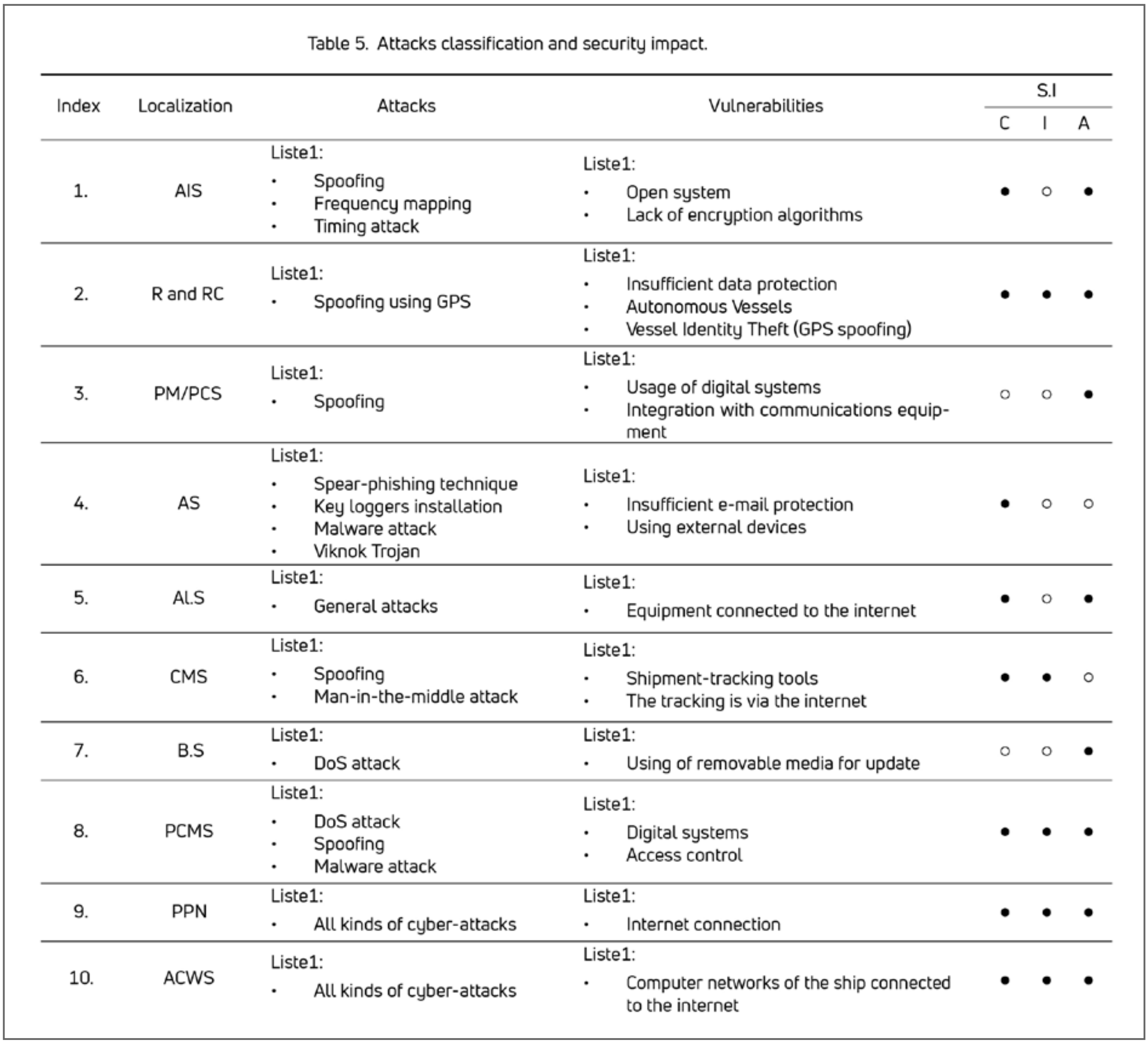

Table 5. Attacks classification and security impact.

| Index | Localization | Attacks | Vulnerabilities | S.I | | |
|---|---|---|---|---|---|---|
| | | | | C | I | A |
| 1. | AIS | Liste1:<br>• Spoofing<br>• Frequency mapping<br>• Timing attack | Liste1:<br>• Open system<br>• Lack of encryption algorithms | ● | ○ | ● |
| 2. | R and RC | Liste1:<br>• Spoofing using GPS | Liste1:<br>• Insufficient data protection<br>• Autonomous Vessels<br>• Vessel Identity Theft (GPS spoofing) | ● | ● | ● |
| 3. | PM/PCS | Liste1:<br>• Spoofing | Liste1:<br>• Usage of digital systems<br>• Integration with communications equipment | ○ | ○ | ● |
| 4. | AS | Liste1:<br>• Spear-phishing technique<br>• Key loggers installation<br>• Malware attack<br>• Viknok Trojan | Liste1:<br>• Insufficient e-mail protection<br>• Using external devices | ● | ○ | ○ |
| 5. | ALS | Liste1:<br>• General attacks | Liste1:<br>• Equipment connected to the internet | ● | ○ | ● |
| 6. | CMS | Liste1:<br>• Spoofing<br>• Man-in-the-middle attack | Liste1:<br>• Shipment-tracking tools<br>• The tracking is via the internet | ● | ● | ○ |
| 7. | B.S | Liste1:<br>• DoS attack | Liste1:<br>• Using of removable media for update | ○ | ○ | ● |
| 8. | PCMS | Liste1:<br>• DoS attack<br>• Spoofing<br>• Malware attack | Liste1:<br>• Digital systems<br>• Access control | ● | ● | ● |
| 9. | PPN | Liste1:<br>• All kinds of cyber-attacks | Liste1:<br>• Internet connection | ● | ● | ● |
| 10. | ACWS | Liste1:<br>• All kinds of cyber-attacks | Liste1:<br>• Computer networks of the ship connected to the internet | ● | ● | ● |

*Figure 4: List of cyberattacks to ships „Table 5: Attacks classification and security impact"*
*Source https://bit.ly/3B31FNF*

### Attacks to ships as victims

As already observed, the merchant ships are offering a high attack surface and a potentially high return on investment to an attacker. Attacks vectors like spam email, fake websites can allow the attacker to gain access to one or more ship's systems or to sensitive data. From that point on, depending on the attack strategy, the attacker could disrupt the normal operations of the ships (e.g. compromise the functionality of part of the IT/OT systems) or alter them 'under the hood' by, for example, bringing the ship off course by spoofing positioning systems data without being detected. Both these strategies could be the first step of a complex attack chain which could have as desired end state, among others:

- Extorsion: the attacker would request a ransom to restore the normal operation of the ship or to release the sensitive data (e.g. use of ransomware or threat of disclosure of data).
- Conventional attack: the attacked ship would be vulnerable to conventional attacks (e.g. piracy) leading to physical seizure of the ship or to theft of part of the payload.

### Ships as part of the attack chain

An attacked ship could not be the final target of the attackers. Given the high potential of the ship to cause damages, the attack could be planned and conducted to cause tangible effects to the organization related to the ship. Some examples of such an attack may include:

- Disruption of marine traffic, especially in areas like straits or ports: attacked ships could be used to block a bottleneck in the marine traffic producing disruptive effects.
- Environmental damages: a ship could be attacked to cause an environmental disaster. This kind of attack would have a high visibility and would produce a significant aftermath for the owning company. The vessel could be used to cause a large scale effect, as a demonstration/terrorist act or, the mere possibility of causing such a fallout can be used as a means of extorsion.

### Reducing the attack surface of ships

The increase of cyber resilience of ships and of the shipping industry environment has taken its first steps ahead only in very recent times. Several specialized providers now offer cyber risk assessment and mitigation or education/awareness programs for shipping industry operators. This is for sure the first and necessary step for the reduction of the attack surface of ships and the shipping industry; however, it's not a magic formula that will solve the problems in the blink of an eye. Assessment, planning and education take time and investment.

Simultaneously, it is very unlikely to see a massive modernization of the entire fleet to upgrade existing IT and OT systems to increase their security.

Diverse literature is available on thedefinition of policies and transfer of risk (i.e. insurances) against the cyberthreats in the shipping industry but it must not be forgotten that the cyber threats are exploiting human vulnerabilities and technical vulnerabilities, so a technical solution minimizing the exposure of systems and data and the possibility for the operators to compromise them even in case of unintended actions is probably the most effective and realistic solution in short and medium term.

Furthermore, even the fleet modernization alone is not likely to solve the security problems on its own. Firstly, the introduction of IT systems in merchant ships without a well conducted security planning is one of the causes that brought high vulnerability of the current vessels and this could be easily happen in the near future as new systems and more integration might further increase the attack surface for new threats. Secondly, the current trend of the shipping industry is headed towards autonomous ships, which are  posing significant challenges in terms of cybersecurity at different levels (technical and regulatory). Finally, it must be considered that, even if a modernization of the fleet occurs, a significant reduction of the cyber risk would be achieved only if the same modernization would be conducted in parallel to the port infrastructure, to which the ships are intimately connected.

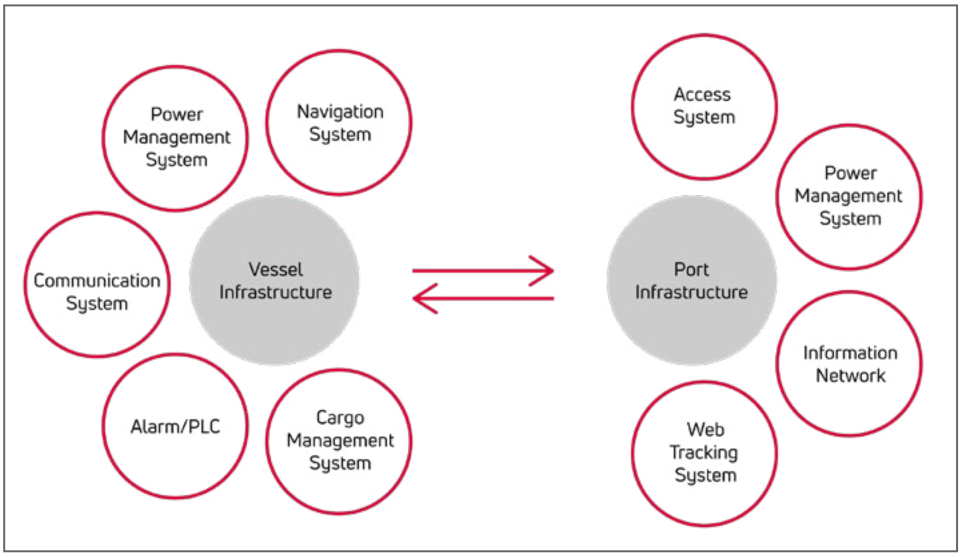

*Figure 5: vessel/port relationship*
*Source: Figure based on Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Belle-kens, X.; Information 2022, 13, 22. https://bit.ly/3XRDifO*

The already mentioned Cyber Resilience for the Shipping Industry (CyberShip) project suggests, among other mitigation measures, to increase the cyber resilience of ships by using SDN controllers associate to IDS/IPS systems to mitigate malicious content. These devices are for sure increasing the level of ship IT infrastructure, however, they they are still exposing the following limitations and disadvantages:

- They need a continuous monitoring (i.e. a SOC with trained operators) which is not likely to be implemented in many merchant vessels.
- They require continuous updates to be able to block upcoming attack vectors as they are in great part relying on the black list approach: general traffic is allowed whenever it is not explicitly forbidden.

A further contribution to the reduction of the attack surface of the shipboard IT/OT systems could come from Cross Domain Solutions (CDS). CDSs could be integrated in the existing IT/OT system on ships and at the port to protect the functionalities of critical systems like OT or navigation aids (IT/OT scenario), or to minimize the risk of unintended leak of information/data from onboard systems (Data Loss Prevention scenario). The inclusion of CDSs in critical points of the ship IT and OT architecture would allow the legitimate messages to be exchanged with other systems (onboard the ships and at the port) while preventing every other message which could eventually cause unintended operations or disruptions. The use of CDSs in this context is particularly suitable, as the great part of these systems are designed to exchange a limited set of well-formed messages for their intended operations. These messages being structured according to known formats, can be parsed automatically and filtered according to rulesets implemented in the CDSs, thus enforcing strict security policies. This scenario becomes particularly relevant in the already quoted situation of autonomous ships, in which some operations happen with no or minimal human intervention.

The added value of CDSs is their nature based on a whitelist approach compared to the one generally based on blacklist approach of firewalls: only explicitly allowed traffic/messages can pass through the boundary device, while every other data/message type is blocked. As the decision is based on a well-formed set of rules to identify the allowed traffic, the solution has null or very low sensitivity to potential new threats/malicious payloads as these are automatically blocked. In general, while solutions like firewalls or general internal networking devices are designed to allow general traffic to flow while trying to detect anomalies, in CDSs the approach is exactly reversed: only the traffic which is compliant to the security policies enforced by the configured ruleset will be allowed to cross the security domain boundary.

The main advantages of CDSs in a scenario like the one of a ship or port infrastructure are, among others:

- Once configured and deployed, CDSs require a minimum level of monitoring and no specialized IT skills.
- CDSs are designed to be failsafe: in case of failure, no traffic will be allowed to pass through so no risk of data loss/attack surface increase is generated.
- Strict security policies can be configured: this is particularly important in a context where the regulatory bodies, like IMO are trying to define policies and best practices to define a 'cyber secure ship'.
- CDSs benefit from a long experience in the military domain, including warships and are a matured and highly reliable solution already tested in the hardest operational conditions.
- CDSs have a minimum footprint on the existing network architecture and can be deployed and integrated easily with no or minimum alteration of the existing hardware and software.
- CDSs are extremely resilient to manipulation and possible human errors.

INFODAS has decades of experience in integrating CDSs in military ships and is actively supporting the digital transformation of several OT architectures.