Ensuring Maritime Cyber resilience

R.Srinivas, Vice President, Indian Register of Shipping

The views expressed in this paper are the author's views and do not necessarily reflect those of his organization

Synopsis

The Maritime Industry**,** keeping in line with recent technological developments is moving from stand-alone computer-based systems to integrated computer systems. Be it a dynamic positioning system, integrated platform management system or integrated bridge system**,** critical process are getting automated and integrated. Though the technology presents numerous advantages, the risks and challenges faced by the industry especially in cyber security with specific focus on addressing the risks in new builds and existing vessels, needs special attention and in-depth analysis. For new builds cyber risks are to be assessed from design stage and require in depth risk assessment, resilient design and use of secured control systems. However**,** implementation of cyber security controls in existing vessels with legacy systems, is a challenge and require**s** specific methods, approach and strategies to address cyber risks.

Key words. Cyber security, Maritime cyber resilience, cyber risks

1.Introduction

New Technologies and developments in the field of artificial intelligence, blockchain, IoT and automation are resulting in increased digitalisation. With increased digitalisation, data is being used for real time control of process, decision support, monitoring and analysis. The stand-alone ship control systems for propulsion, power generation, steering etc. are being gradually integrated for better control and reduction in manpower.

Electronic Data Exchange through removable drives or internet has become the normal mode of data exchange between ship to shore and vice versa. The International Maritime Organisation (IMO) goals for decarbonisation and use of alternative fuels are also leading to increased digitalisation and automation. While shipowners have various options to meet the goals, the quicker measure would be digitalise the process and use data for increased operational efficiency. Though industry has been using cyber technology for its various operational systems, typically termed as Operational Technology (OT) systems for several decades, the focus was more on their usage, than on issues of cyber security, the latter term being generally associated with information technology (IT) systems. However, the vulnerabilities created by accessing, interconnecting or networking these systems either for data transfer, software updates, control, and for maintenance can lead to cyber risks, which are required to be addressed. Cyber-attacks on ship critical Machinery Control and Navigational systems can pose significant risk to vessels. The attack can affect safety of vessel, safety of personnel and of the environment.

The paper aims to bring out challenges in addressing cyber security aspects for ship control systems and initiatives taken to address these challenges for new builds and for existing vessels. The paper also highlights the challenges faced by implementers while trying to incorporate cyber risk mitigation controls in existing vessels equipped with legacy systems and discusses the strategies for effective management of cyber risks in such vessels.

2. IMO's initiative

Cyber security is high on the agenda of IMO and is being actively discussed at the Maritime Safety Committee (MSC) and at the Facilitation Committee. The Committee deliberated on papers submitted by the member States on the subject and in June 2016, the Maritime Safety Committee approved Interim Guidelines on Maritime Cyber Risk Management vide MSC.1/Circ.1526. These high-level guidelines present the functional elements that support effective cyber risk management. The Guidelines were superseded by MSC-FAL.1/Circ.3 which recommend a risk management approach to counter cyber risks and subsequently as per IMO Res. MSC 428(98) the cyber risk management is being addressed through safety management system.

Authors' Biography

Mr. R. Srinivas has 41 years of Maritime experience, spanning ship building, ship designs, maritime consultancy and Classification. He is working as Vice President & Senior Principal Surveyor at Indian Register of Shipping (IRS). Mr Srinivas was the Chairman of, IACS Cyber Systems Panel and IACS Joint Industry Working Group on Cyber systems. Presently he is IRS member of IACS Safe digital transformation panel.

 https://doi.org/10.24868/11173

3. Initiatives by the Indian Register of Shipping (IRS) to address Cyber Risks

For safeguarding ships from current and emerging threats, Indian Register of Shipping (IRS) has developed Rules for Cyber Resilience based on two unified requirements for cyber resilience published by International Association of Classification societies (IACS). The Rules for Cyber Resilience of ships specify the minimum requirements aimed to protect the vessel's cyber systems against cyber incidents. The requirements are mandatory for ships contracted for construction on or after 1st July 2024 and address the five functions 'Identify, Protect, Detect, Respond and Recover' to ensure cyber resilience. The Security capabilities of Systems and Equipment are to be designed and verified as per rules for Cyber Resilience of On-Board Systems and Equipment.

One of the key features of the new requirements is segregation of Computer Based Systems (CBS) into zones. All CBS in one zone have the same security requirements and can communicate with other zones only through conduits which have necessary data flow controls. The network housing all the CBS in scope are termed as Trusted Network and the rules specify additional cyber security requirements when CBS in trusted network(s) has to communicate with untrusted network(s).

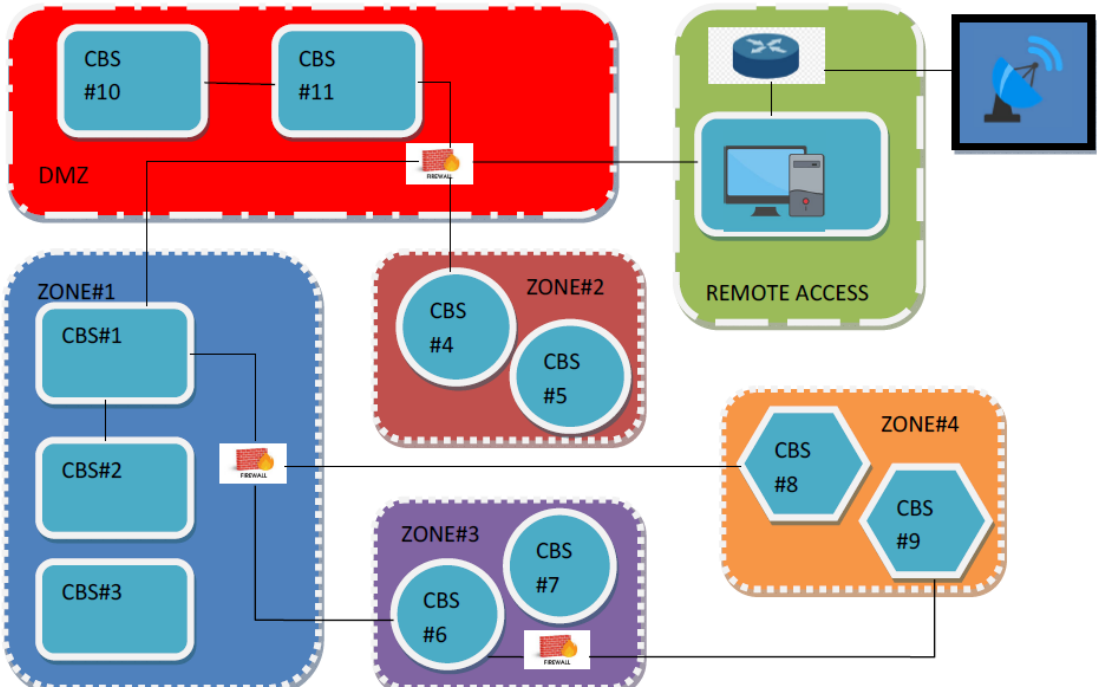

Figure 1: Zones

The requirements for Cyber Resilience of On-Board systems and equipment are applicable to computer based systems under the scope of the Rules for "Cyber Resilience of ships" which defines 30 Security capability requirements and a further 11 additional security capabilities to be complied with for CBSs which can communicate with un-trusted networks The requirements cover following areas**:**

- Identification and authentication controls
- Use control
- System integrity
- Data confidentiality
- Timely response to events
- Resource availability

To assist the maritime industry in identification of cyber risks and designing a suitable cyber risk management system for various types of vessels, both new build and existing, IRS published "Guidelines for Maritime Cyber Safety", based on IEC 27001, IEC 62443-3-3 and industry best practices. Further, for addressing the security requirements for control system components, IRS published classification notes on "Cyber Secured Control System components" which defines five levels of cyber security. Notwithstanding

 https://doi.org/10.24868/11173

the type of vessel, if any owner desires to protect the onboard computer based systems with additional cyber safety features, to address cyber risks due to increased system integration, including connectivity outside the vessel, additional Class notation as per guidelines can be assigned when requirements as stated in the IRS guidelines for cyber safety are complied with. For new construction ships which are not required to comply with rules, but the owners voluntarily intend to secure their vessel against cyber-attacks, a class notation to state that the vessel meets the minimum cyber security requirements as per Class rules will be assigned.

4. Addressing Cyber Security in New Build Vessels

All new builds, under the scope of applicability of the new rules**,** are required to comply with requirements of cyber resilience**,** which are to be implemented from design stage. For countering 'single point failures' a 'Defence in Depth' approach is encouraged whereby detection and protection measures**,** designed to prevent or slow down the progress of a hacker are implemented, thereby enabling an organisation to detect and respond to a cyber-attack. In cases where equipment and systems are not 'type approved', they can be certified 'specific to project', through review of manufacturer's documentation and witnessing of tests.

4.1 Compliance verification

The Class surveyor would verify compliance to the approved documents for following stages of ship life cycle

- Equipment product certification
- Vessel design phase
- Installation
- Commissioning before delivery
- First annual survey and subsequent annual survey
- Special survey

In the event a particular system does not meet the specified cyber security requirements, counter measures can be applied. Changes to hardware and /or software would require submission of updated plans and subsequent onboard verification.

4.2 Cyber Risk Assessment

Cyber risks can be defined as those risks that arise from the loss of confidentiality, integrity or availability of information in IT and OT systems, the consequences of which can severely impact an organisation and/or ship's critical operations. Ship-critical systems are to be designed, installed, tested and maintained to mitigate the risks arising out of use of such technologies. Therefore**,** evaluating the risks is essential for smooth operation of control and information systems. The National Institute of Standards and Technology (NIST) of the United States defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event. Risk therefore is a function of:

- Adverse impacts that would arise if the circumstance or event occurs, and
- Likelihood of occurrence.

4.3 Attack surface

One of the important aspects to be considered in assessing cyber risk is the 'attack surface'. An attack surface is typically the exposed area for cyber-attack and depends on the extent to which the system can be accessed either locally or from another location. For example, open USB ports on the PC give an easy access for the intended or unintended user to plug in a corrupted USB stick with virus. Similarly, when the system has provision for remote login the chances of attack increase as the asset can be connected from shore. The extent of attack surface available to the threat to exploit the vulnerability will determine the likelihood of cyber-attack on a particular equipment /system.

 https://doi.org/10.24868/11173

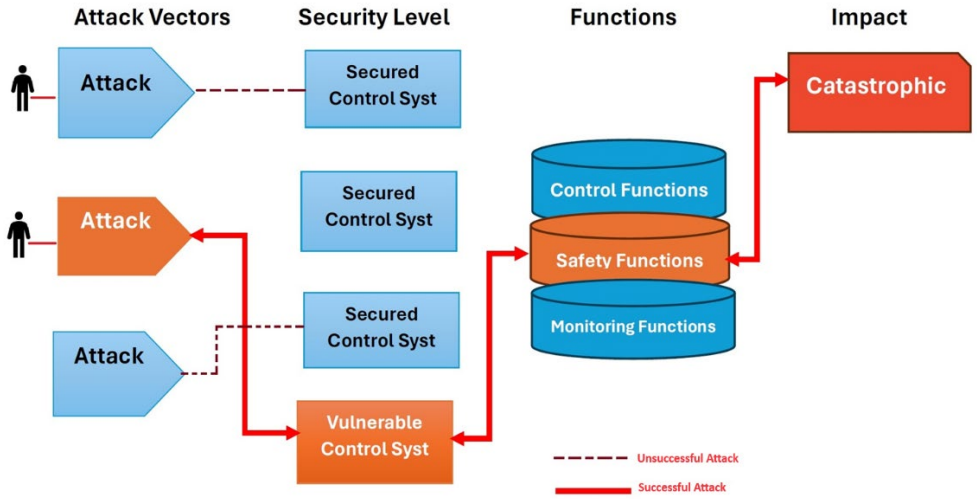

Figure 2: Attack Surface

For Ships built as per IRS guidelines, the yard /system integrators are required to provide a detailed risk assessment of ships IT and OT systems and a proposal for risk mitigation methods, which could be a combination of technical, procedural and managerial controls. The document is to be supported by network diagrams clearly identifying zones and conduits, vessel inventory and testing methodology towards verification of rule requirements.

Once identified, organizations should prioritize risks based on their potential impact and likelihood of occurrence. Based on the results of the risk assessment, organizations should develop and implement risk mitigation strategies to reduce the risk of successful cyberattacks. Vessel operators should view cyber risks along with the physical, human factor, and other types of risks. It is essential to protect critical systems and data with multiple layers of protection measures which should include role of personnel, procedures and technology. It is imperative to note that it is not a linear exercise and requires a holistic approach to protect critical assets, considering all interconnections, dependencies and upgradations.

5. Cyber Security in Existing Vessels

5.1 Challenges

While it is comparatively easier to implement the cyber security requirements for new builds, implementation of cyber security requirements for existing vessel i.e. vessels in operation**,** is a challenge. Some of the critical challenges are presented below**:**

5.1.1Outdated Hardware, Software

Legacy OT systems typically consist of outdated hardware and software which were not designed with security perspective**.** Hence, they may not support modern algorithms, communication protocols, encryption algorithms or secure communication protocols. These factors increase their vulnerability to cyber-attacks. Legacy OT systems may also use insecure communication protocols that can be exploited by attackers.

5.1.2 Lack of Security Awareness

Operators who manage the systems may lack security awareness and training, making them vulnerable to social engineering attacks. Social engineering attacks can be used to gain access to sensitive information or systems by exploiting human vulnerabilities.

5.2 Strategies for cyber risk management of existing vessel

To overcome the abovementioned challenges and especially to secure legacy OT systems, the following approach is suggested

5.2.1 Conduct Gap Assessment

Implementation of new controls would require a detailed analysis of existing systems and the Gap with respect to the desired security level.

 https://doi.org/10.24868/11173

Gap assessment should be aimed to identify gaps existing in technical and procedural controls and may be categorised accordingly in two groups; one group identifying Gaps in policies and procedures, while the second group identifying Gaps in controls. Identification of CBS in scope and review of available documentation /information on the CBS would be the first step in assessment of gaps in existing controls. Vulnerability of identified systems are to be assessed based on:

- Extent of connectivity i.e. integrated or stand-alone
- Number of systems with which asset is integrated
- Remote connectivity (ship-to-shore connectivity)
- Criticality of the equipment/system
- Software update methodology
- Possibility of remote operations / monitoring etc.

The above-mentioned activity would help in arriving at the risk level for each vulnerable system. Documentation verification and analysis is to be followed by onboard assessment of identified vulnerable systems. The methodology consists of verification of Policies, Procedures and Controls for each identified vulnerable system and interaction with concerned ship personnel. One of the objectives of the interaction is to ascertain their commitment and clarity in their roles and responsibility towards implementation of cyber risk management. Identified vulnerable systems are assessed towards compliance with requirements of following functional domains, as applicable. The requirements are broadly grouped into 2 groups.

Group A

- Governance
- Procedures
- Risk Management
- Training & Awareness,
- Reports and Review procedures

The requirements of above functional domains, generally require policies and procedures to be defined at Company level and implemented onboard and ashore.

Group B

- Access Control
- Network Security
- System Security Controls
- Software Configuration
- Backup and Recovery

Towards implementation of the requirements of the abovementioned controls, generally assistance of manufacturers could be required.

5.2.2 Conduct Risk Assessment

Risk assessment is the process of identifying, evaluating, and prioritizing risks to legacy OT systems. This includes identifying vulnerabilities, threats, and potential consequences of a successful cyber-attack. Once identified, organizations should prioritize risks based on their potential impact and likelihood of occurrence. Based on the results of the risk assessment, organizations should develop and implement risk mitigation strategies to reduce the risk of successful cyber-attacks.

Vessel operators should review cyber risks along with the physical and human factors, as well as other types of risks. It is essential to protect critical systems and data with multiple layers of protection measures which should include role of personnel, procedures and technology.

5.2.3 Enforce Access Control

Access control involves implementing mechanisms to control access to legacy OT systems. Access controls should include strong authentication, authorization, and accountability mechanisms. Organizations should limit access to critical systems only to authorized personnel with a legitimate need to access them. The first step in implementing access control is to identify the assets that need to be protected and the individuals or roles that require access. Access control policies should be developed to define the rules and procedures for granting and revoking access to these assets. Authorization mechanisms should be implemented to define what actions users can perform on the system and which resources they can access.

 https://doi.org/10.24868/11173

5.2.4 Carry out System Hardening

Hardening legacy OT systems involves implementing security controls to reduce the attack surface and improve the security posture of the systems. This could include implementation of firewalls, intrusion detection and prevention systems, access controls, and other security measures to limit the potential for successful cyber-attacks. In addition, unnecessary or unused services, protocols, and applications that could be exploited by attackers, should be removed. Disabling unnecessary ports, removing default accounts and passwords, and restricting access to critical systems and components, could be some of the methods. It is important to note, however, that hardening should be performed in a careful and deliberate manner, as any misconfigurations or errors can result in unintended consequences or downtime.

5.2.5 Conduct Training

Implementing security awareness and job specific training programs for OT systems is essential for reducing the risk of cyber-attacks caused by human error or oversight. These programs should include training on basic cyber security principles, regular cyber security awareness training, and clear policies and procedures for reporting potential security incidents or threats.

By establishing effective security awareness and training programs, organizations can improve the overall security posture of their critical infrastructure and reduce the risk of successful cyber-attacks. It is important to note that security awareness and training should be an ongoing process and that organizations should regularly review and update their programs to ensure that they remain effective in the face of evolving cyber threats and attack techniques.

5.2.6 Implement Change Management

System security can be maintained by regularly carrying the software updates and patches. Operating critical, essential system by outdated software and hardware, can make them vulnerable to cyberattacks. All the patches are to be tested prior to deployment and change management process has to be defined and documented. Procedures shall be implemented for testing the patches before deployment. Updation and patching of legacy OT systems can be challenging due to the potential for disruptions to critical operations and are to be carefully planned, taking into account the manufacturer's recommendations.

5.2.7 Implement procedures for Monitoring and Incident Response

Identification of incidents that are more likely to occur, would be the first step in development of Incident Response Plans. The Plan should outline the steps that should be taken in response to each type of incident. This plan should include procedures for detection, containment, eradication, and recovery. A desirable feature in vessels with increased integration and remote connectivity would to use tools and techniques to identify and respond to potential cyber threats and attacks in real time. This includes implementing network and system monitoring tools, intrusion detection systems etc.

5.2.8 Implementation of Procedures for Backup & Recovery

Implementing data backups and recovery plans is an important aspect of securing legacy OT systems. These systems handle critical data that is essential for vessel operations and a loss or corruption of this data could have serious consequences on the safety of the vessel. Organizations should develop a data backup and recovery plan to address the procedures for scheduled backups of critical data including testing of backup and recovery procedures. Procedures for Secured storage of backups and periodic testing to ensure that it can be recovered in the event of data loss or corruption are to be implemented.

6. Conclusion

Cyber-attacks are on the rise and it is important to address the cyber risks from design stage through a holistic approach. It is not sufficient to address the risks only through procedural controls and requires, in addition, that control systems components also have features to address cyber risks. Risk assessment forms a fundamental and important step in addressing cyber risks. A holistic approach addressing various threat actors and threat paths are to be considered along with the overall impact on the safety of the vessel and the environment when the subject system is compromised. Awareness and system specific training is essential for successful implementation of cyber risk management.

References

- IMO guidelines on Maritime Cyber Risk Management
- ISO/IEC 27001 standard on Information technology – Security techniques
- National Institute of Standards and Technology(NIST)

 https://doi.org/10.24868/11173

- IRS Guidelines on Maritime Cyber Safety
- IRS Classification notes on “Cyber secured Control system components”
- IEC 62443-3-3 Industrial Communication Networks - Network and System Security - Part 3-3: System Security Requirements Security Levels

Bibliography

- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Security (the NIST Framework).
- Code of Practice - Cyber security for ships by Department of Transport UK
- IEC 62433-2-1 Establishing an Industrial automation and control system security program
- NIST Special Publication 800-30
- ISO 31000 – Risk Management-Principles and Guidelines
- IRS Rules and Regulations for the Construction and Classification of Steel Ships
- IACS UR E26 Cyber resilience of ships
- IACS UR E27 Cyber resilience of on-board systems and equipment

 https://doi.org/10.24868/11173