POSITION PAPER

Cyber Systems

(Revision 3)

IACS

International Association of Classification Societies

Our Position

Cyber incidents on vessels can have a direct and detrimental impact on life, property, and the environment. IACS has a strong technical knowledge and experience to support cyber resilience of vessels and onboard systems and equipment and is committed to the development of rules and recommendations that support operational safety and regulatory compliance.

BACKGROUND

IMO

IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL. 1/Circ.3, 5 July 2017) were given prominence by adoption of IMO Resolution MSC.428(98) which encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

IACS contributed to the development of a new revision of MSC-FAL. 1/Circ.3 by its experience and technical knowledge both in the design and construction of onboard Cyber Systems and its guidelines relative to onboard procedures for maintenance of cyber systems.

IACS Unified Requirements for cyber resilience contribute towards a cyber-resilient vessel and contribute to owner's conformance with the new IMO recommendations.

EU

The EU is active on several Digital and Cyber fronts that may have an impact on vessels operating in Europe. As initiatives develop, IACS continues to consider the influence of EU initiatives on the industry, and its own position. Conversely, the EU has expressed an interest in the work of IACS in this area and it is hoped that the ongoing dialogue will facilitate coordination and result in many common aspects, and effective results. It is recognized that any discontinuity will increase the risks of differing approaches, with the result of increased burden for the industry.

The European Maritime Safety Agency (EMSA) published a guidance document on how to address cybersecurity onboard vessels during audits, controls, verifications, and inspections (MARSEC Doc. 9209). The document provides guidance on how the cybersecurity-related elements should be assessed during maritime security inspections on EU Member State flagged vessels.

Joint Working Group/Cyber Systems (JWG/CS)

The interest and support shown by JWG/CS and many other industry stakeholders has highlighted the expectation placed upon Class to lead and have a central role in formulating the industry's response to Cyber threats on vessels. Effectively integrating this role with the other supply chain assurance, and through lifecycle survey activities of the Classification Societies, provides continuity in existing industry relationships, while providing a durable basis to delivering solutions to Cyber Systems challenges. This collaborative approach can be extended across all stakeholders, and builds towards common criteria for equipment and construction, based on which operational procedures under ISM would be developed by Industry.

IACS POSITION

IACS acknowledges the high level of interest on this subject, from the maritime industry, OEM's, Shipyards, and regulators. It also recognizes the need to carefully balance the required rigour with the need to avoid inadvertently creating simplistic suboptimum requirements that could lead stakeholders to allocate resources in ways that do not deliver the most cost-effective results, or which do not achieve the necessary levels of safety. All of those involved have a part to play in addressing their own safety and also a shared responsibility in considering the safety of others who share the same sea lanes and environment. In this context IACS continues to proceed carefully in

Continues >>

developing common practical solutions, in particular developing a set of technical measures that support operational safety and regulatory compliance. A signature part of this care has been to progress in steps and encouraging feedback at each stage of Unified Requirements development. This includes:

- design, testing and survey criteria that provide the necessary foundations for industry to use as the basis of through lifecycle operations and procedures to counter cyber threats.
- preventative or precautionary measures that reduce the possibility of cyber incidents occurring in the first place
- means to support resilience in the event of cyber incidents, whatever their cause.

IACS APPROACH

In order for developed requirements to be demonstrably in support of identified objectives, IACS has used a Goal Based Approach in the structuring of its work. Having this in common with other IMO activities, together with the associated use of familiar language, should support a common understanding and assist uniform implementation across the industry.

The goal in terms of design and construction is to enable the delivery of cyber resilient vessels whose resilience can be maintained throughout their lifecycles.

Cyber resilience means capability to reduce the occurrence and mitigating the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a vessel, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

It is recognized that Cyber Security cannot be achieved solely through design and construction criteria and that all stakeholders need to contribute and collaborate. A significant consideration which is not addressed by IACS, and hence needs to be specifically addressed by other industry partners in their procedures, is operational aspects. IACS has intended to identify assumptions that are made in respect of operational aspects when developing its design and construction criteria.

SUMMARY OF WORK CARRIED OUT BY IACS ON THIS ISSUE TO DATE

From the start, IACS has actively supported stakeholder consultation and feedback. The first tangible product of the IACS work was the Recommendation 166 (dated April 2020) as the consolidated document of the original set of 12 Cyber Recommendations.

During 2021, the IACS Cyber Systems Panel worked on two main projects as identified and prioritised by its industry partners in its roadmap of development. The first project was to translate the appropriate portions of consolidated Recommendation 166 into a Unified Requirements (UR) for the cyber resilience of vessels. The second project aimed to establish a new UR for cyber resilience of onboard systems and equipment.

Continues >>

The objective was to establish the minimum-security capabilities for systems and equipment to be considered cyber resilient, when used for essential and critical systems on board.

During 2022, with an objective to provide guidance on cyber risk assessment, IACS published Recommendation 171 “Recommendation on incorporating cyber risk management into Safety Management Systems”, which considers the complexity of onboard systems and their interconnectivity within and external to the vessel. The Risk assessment methodology provided in this recommendation can be used as one of the possible methods to address cyber safety issues within the context of MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management.

Also, during 2022, the publication of the two new Rev.0 versions of the URs for cyber resilience marked a significant milestone in IACS’ work to support the maritime industry:

UR E26 (Rev.0 Apr 2022) «Cyber Resilience of Ships» aims to ensure the secure integration of this equipment into the vessel’s network during the design, construction, commissioning, and operational life of the vessel. This UR targets the vessel as a collective entity for cyber resilience and covers five key aspects:

Identify

Protect

Detect

Respond

Recover

UR E27 (Rev.0 Apr 2022) «Cyber Resilience of On-board Systems and Equipment» aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard vessels.

During 2023 and consequent to the publication of the above Unified Requirements the need for enhancement of the published requirements based on industry feedback along with a common approach to survey was identified as a necessary step towards successful implementation of the unified requirements. To address the challenges in implementation of new cyber requirements in smaller and non-conventional vessels, the scope of applicability of these URs has been categorised as mandatory and non-mandatory compliance depending on vessel types and sizes.

These improvements have resulted in extensive changes to the two URs and considering the fact that the earlier published URs had not yet entered into force, the two Rev.0 versions of the URs were withdrawn in 2023. The two new Rev.1 versions of UR E26 and UR E27 published in 2023, supersede the original URs. The implementation date of the revised URs is set for 1st July 2024.

In order to address the challenges of increased use of computer-based systems (CBS) onboard and to provide further clarification on the requirements during CBS life cycle, IACS revised the existing Rev.2 version of UR E22. The updated Rev.3 version of UR E22, now titled “Computer-Based System”, addresses activities related to the development and delivery of a computer-based system. The requirements also include activities related to change management of CBS in operational phase. The implementation date of the revised UR E22 is aligned with implementation date of the revised UR E26 and E27 and is set for 1st July 2024.

Throughout 2024, IACS is working on a project aimed to establish a new Recommendation for cybersecurity controls for vessels in service. The objective is to establish a minimum set of realistic Cyber Resiliency Controls, to mitigate cyber risks, irrespective of the vessel’s construction year. The recommendation will focus on vessels in service and will not replace any of the IACS published Requirements and Recommendations on Cyber Resilience applicable to new buildings. The recommendation is expected to be finalized by the end of 2024.

Please note if you’re reading this paper in hard copy the most recent version is available at www.iacs.org.uk/about-us/position-papers
For more information, contact IACS Permanent Secretariat on +44 (0)20 7976 0660, permsec@iacs.org.uk. This position paper was first published in January 2020.