POSITION PAPER

Cyber Systems

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 steadily increased its focus on the reliability and functional effectiveness of onboard, safety critical, computer-based systems.

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.

Most of the maritime industry welcomes the experience of Class Societies regarding the implementation of requirements related to design and construction of onboard Cyber Systems.

Advice in this respect may represent a technical baseline on which to develop their own procedures relative to ISM Code requirements

Such recommendations would contribute towards a cyber-resilient new ship on delivery and contribute to owner's compliance with above said IMO resolution.

EU

The EU are active on several Digital and Cyber fronts that may have an impact on vessels operating in Europe. As initiatives develop, IACS will continue to consider the influence of EU initiatives on the industry, and its own position. Conversely, the EU have 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.

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 life 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 direct 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 will continue to proceed carefully in 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 will be progressing in steps

Continues >>

and encouraging feedback at each stage before delivering the recommendations. This includes:

- design, testing and survey criteria that will provide the necessary foundations for industry to use as the basis of their through life operations and procedures to counter cyber threats.
- preventative or precautionary measures that will 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 that developed requirements are demonstrably in support of identified objectives IACS is using 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 ships whose resilience can be maintained throughout their life-cycles.

Cyber resilience means capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, 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 is intending 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 original set of 12 Cyber Recommendations (153-164) available on the IACS website are the first tangible product of the IACS work. These represent good practice and can be considered as an indication of the way forward. Current IACS activities include the consolidation of these recommendations into a style and format that is easier to assimilate. The resulting single Recommendation will focus on design and construction aspects, contributing to achieving compliance with IMO resolution MSC.428(98) on delivery of a new ship. Future steps will be influenced by the ongoing feedback that is received.

UNIFIED REQUIREMENTS

It is recognized that a large part of the industry has a strong preference for IACS to move beyond Recommendations and develop Unified Requirements (URs) regarding Cyber. Acknowledging this preference and appreciating how URs should support greater consistency, IACS will continue to keep this under review. A final decision will be made when industry feedback on implementation of the Recommendations indicates that the topic is sufficiently mature.

Please note if you're reading this paper in hard copy the most recent version is available at www.iacs.org.uk/about/iacs-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.

International Association of Classification Societies Permanent Secretariat, 4 Matthew Parker Street, Westminster, London SW1H 9NP, UK

E: permsec@iacs.org.uk T: +44 (0)20 7976 0660 www.iacs.org.uk