INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
103rd session
Agenda item 20

MSC 103/INF.8
26 February 2021
ENGLISH ONLY
Pre-session public release: ☒

ANY OTHER BUSINESS

Update on IACS' work on requirements for cyber resilient ships

Submitted by IACS

SUMMARY

Executive summary:	This document updates the Committee on how cyber safety is being further addressed by IACS within the context of MSC-FAL.1/Circ.3, and describes the progress IACS has made on this topic and the work it is taking forward
Strategic direction, if applicable:	Not applicable
Output:	Not applicable
Action to be taken:	Paragraph 17
Related documents:	None

Introduction

1 The Facilitation Committee, at its forty-first session, and the Maritime Safety Committee, at its ninety-eighth session, having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in annex to circular MSC-FAL.1/Circ.3. The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

2 This paper provides information on IACS work in relation to that circular.

Discussion

IACS Recommendation 166 – recommendation on cyber resilience

3 On 4 May 2020, IACS was pleased to announce the publication of its Recommendation on cyber resilience (Recommendation 166). This single, standalone Recommendation consolidates IACS' previous 12 Recommendations related to cyber resilience (Recommendations 153-164). It applies to computer-based systems which provide

control, alarm, monitoring, safety or internal communication functions which are subject to the requirements of a classification society. Part of the objective in consolidating the 12 Recommendations was to define responsibilities, harmonize and simplify the language used therein.

4 Recommendation 166 has benefited from the valuable input of a wide range of industry partners contributing via the Joint Working Group on Cyber Systems and covers the constructional aspects of the 12 previously published Recommendations 153-164. It provides information on matters such as reference guidelines and standards, terms and definitions, goals for design and construction, functional requirements, technical requirements and verification testing.

5 The publication of this important Recommendation marked a significant milestone in IACS' work to support the maritime industry in the delivery of cyber resilient ships. The significant cross-industry cooperation that led to its development should be highlighted; the IACS Cyber Systems Panel looks forward to maintaining that dialogue.

6 Recommendation 166 is applicable to ship's computer-based systems using digital communication to interconnect systems within the ship, and ship systems which can be accessed by equipment or networks off the ship. This Recommendation is an important step in addressing cyber resilience from the earliest stages of ship's life.

7 Operational aspects which were included in the superseded 12 Recommendations 153-164 have been identified and grouped under a separate annex. Following the publication of this consolidated Recommendation 166, the earlier 12 Recommendations 153-164 have been officially withdrawn by IACS.

Setting a roadmap

8 During the second part of 2020, the IACS Cyber Systems Panel continued to work with its industry partners and looked for their feedback to confirm its roadmap of development. Three prioritised project teams were thus agreed and established by the IACS Cyber Systems Panel.

Project 1: unified requirements for cyber resilience of new ships

9 The first project team was tasked with translating appropriate portions of Recommendation 166 into unified requirements with the following objectives:

.1 building on the experience and knowledge acquired in the development of the consolidated Recommendation 166, produce a unified requirements document with minimum goal-based requirements for cyber resilience of new ships. The focus will be set on operational technology systems and cyber incidents resulting from any type of offensive manoeuvre which targets such systems, excluding system failures. The extent of requirements will be limited to the most common and effective cyber security barriers, feasible for a smooth implementation on all new ships. Such requirements will be mandatory for operational technology systems which, if compromised, could lead to dangerous situations for human safety, safety of the ship and/or threat to the environment;

.2 organize that unified requirements document to make it possible to implement the requirements therein uniformly and smoothly by classification societies and industry, and make it applicable to all ship types in such a way

that the requirements enable a minimum level of security and apply to all classed ships/units regardless of operational risks and complexity of operational technology systems;

.3 organize that unified requirements document to encourage its evolution and improvement to continuously provide answers to industry expectations on, for example, systems connectivity, digitalization and smart shipping, anticipating the needs of maritime autonomous surface ships (MASS) and supporting the effort of national and international authorities on cyber risk management.

Project 2: unified requirements for cyber resilience of onboard systems and equipment

10 The second project team aims to establish unified requirements for cyber resilience of onboard systems and equipment towards cyber security to determine which requirements are to be met to certify a cyber system equipment used for essential and critical systems on board. Indeed, in existing scenario, tests for such equipment are conducted only for an environmental test requirement, as per IACS existing documents, however those tests do not address cyber security aspects.

11 The project would focus on activities of cyber system equipment which includes design, requirements for cyber resilience towards cyber threats, validation, certification and change management.

12 The development of unified requirements for onboard systems and equipment is coordinated with the development of the unified requirements for ships mentioned in the above description of project 1, to ensure that systems and components have the required security capabilities necessary to comply with the requirements for the ship.

13 Input from the Joint Working Group on Cyber Systems will be considered during the development phase and the industry group will be involved in the review process.

Project 3: update of the unified requirement about onboard use and application of computer-based systems (unified requirement E22)

14 The aim of the third project team is to update the unified requirement about onboard use and application of computer-based systems (UR E22) to improve and clarify the requirements for the life cycle activities of computer-based systems for both suppliers and system integrators.

15 Indeed, during the evaluation of the current UR E22 by the IACS Cyber Systems Panel, it was agreed that an upgrade of UR E22 was needed. The objective is to provide a minimum set of requirements to suppliers and system integrators of software-based automation which ensures that both individual systems and the total integrated functionality are of high quality and safe for use.

Publication

16 Publication of these three documents containing new interconnected cyber focused unified requirements is planned during the second half of 2021.

Action requested of the Committee

17 The Committee is invited to note the information provided.