Tripartite 2019 – Tokyo

Session 3 ‘Digitalisation’

George Reilly

IACS Cyber Systems Panel Chairman
Coordination of IACS Role

Owners
Insurers
Shipbuilders
Cargo owners
Manufacturers
Communications
Port Authorities
Flag States

August 2019
Recognition within IACS
Developing Recommendations

Functionally Arranged

Philosophy
Vessel System Design

Design for Robustness
- Physical Security
- Programmable System Equipment Inventory
- Procedure for Software Updates
- Integration
- Communication and Interfaces
- Remote Update / Access

System Resilience
- Network Architecture
- Network Security
- Data Assurance
- Contingency Post Failure
- Manual Backup

August 2019
SAFER AND CLEANER SHIPPING
IACS Recommendations Relationship with IMO and the NIST Framework

IMO Guidelines

- Identify:
  - roles and responsibilities
  - critical systems, assets, data and capabilities

- Protect:
  - risk control processes and measures
  - contingency planning against a cyber event
  - ensure continuity of shipping operations

- Detect:
  - activities to detect cyber events

- Respond:
  - plans to provide resilience
  - restore systems impaired due to a cyber event

- Recover:
  - measures to pack up and restore systems impacted by a cyber event

NIST Framework

- Identify:
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy

- Protect:
  - Access Control
  - Awareness Training
  - Data Security
  - Information Protection Mechanism
  - Maintenance
  - Protective Technology

- Detect:
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes

- Respond:
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements

- Recover:
  - Recovery Planning
  - Improvements
  - Communications

IACS Recommendations

- 161 - Inventory List of computer based systems
- 164 - Communication and Interfaces
- 158 - Physical Security of onboard computer based system
- 153 - Recommended procedure for software maintenance of computer based systems on board
- 157 - Data assurance
- 103 - Remote Update / Access
- 159 - Network security of onboard computer based systems
- 156 - Contingency plan for onboard computer based systems
- 154 - Recommendation concerning manual/local control capabilities for software dependent machinery systems

IACS UR E22

- 160 - Vessel System Design
- 155 - Network Architecture
- 162 - Integration
Cyber risks addressed in safety management systems (SMS)

Regulatory Background - IMO

- MSC.1/Circ.1526 was superseded by (MSC-FAL. 1/Circ.3) in 5 July 2017.
- This now has more prominence due to 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.’
paragraph 11 highlights that some agencies appear focusing their approach to Cyber Risk Management through the ISPS Code. However, the Committee also agreed that this should not be considered as requiring a company to establish a separate cyber security management system operating in parallel with the company SMS.
1.2 Plans and procedures

IACS Resolution MSC.428(98) identifies cyber risks as specific threats, which companies should try to address as far as possible in the same way as any other risk that may affect the safe operation of a ship and protection of the environment. More guidance on how to incorporate cyber risk management into the company’s SMS can be found in annex 2 of these guidelines.

Cyber risk management should be an inherent part of the safety and security culture conducive to the safe and efficient operation of the ship and be considered at various levels of the company, including senior management, shore and onboard personnel. In the context of ship operation, cyber incidents are anticipated to result in physical effects and potential safety and pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents. Company plans and procedures for cyber risk management should be incorporated into existing security and safety risk management requirements contained in the ISM Code and ISPS Code.

The objective of the IACS is to provide a safe working environment by establishing appropriate practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. The SMS should include instructions and procedures to ensure the safe operation of the ship and protection of the environment in compliance with relevant international and flag state requirements. These instructions and procedures should consider risk arising from the use of IT and OT on board, taking into account applicable codes, guidelines and recommended standards.

When incorporating cyber risk management into the company’s SMS, consideration should be given as to whether, in addition to a generic risk assessment of the ship it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. The factors to be considered include but are not limited to the extent to which IT and OT are used on board, the complexity of system integration and the nature of operations.

According to chapter 8 of the ISM Code, the ship is obliged to conduct a security assessment. This includes identification and evaluation of key shipboard operations and the associated potential risks. As recommended by Part B, paragraph 3.5 of the ISM Code, the assessment should address security plans and telecommunication systems, including computer systems and networks. Therefore, the ship security plan may need to include appropriate measures for protecting both the equipment and the connection. Due to the fast adoption of sophisticated and digitized onboard OT systems, the ship’s security procedures are as up-to-date as possible.

The Vessel Management and Security Assessment (VMSA) also require plans and procedures to be prepared.
Consolidation

Consolidation of the Recommendations into one Document

Stakeholder Needs & Expectations
Consolidation through the Goal Based Standards format

A format that is familiar to IACS and many stakeholders

Starting with a declared GOAL:
Ships should be designed, built, operated and maintained to be cyber-resilient

Using elements that are familiar to the stakeholders that are familiar to IACS and the Joint Working Group
Consolidation Steps

- Agreement of the defined goal and a set of Functional Requirements
- Review of existing (Recommendation) material and the feedback that has been received
- Consolidated document will address the criteria for technical elements relating to construction and not cover operational elements
- Industry Standards to be referenced for operational aspects
- Only new construction ships considered
- Identify how consolidated document address the 5 NIST Functional Elements (Identify, Protect, Detect, Respond, Recover)
While the most intense activity within IACS will revolve around the consolidation of the Recommendations, Cyber Systems Panel will be available to identify, prioritize and progress other related areas that will themselves become priorities that need to be in place before the January 2021 Deadline arrives.
Thank you for your attention!
Maritime cyber risk

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

The overall goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

IMO guidance

IMO has issued **MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management**.

The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The Maritime Safety Committee, at its 98th session in June 2017, also adopted **Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems**. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company’s Document of Compliance after 1 January 2021.

Other guidance and standards

Guidelines on **Cyber Security** on board Ships issued by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.


United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the **NIST Framework**).