Cyber Risk Management for Autonomous or Remote-Controlled Ships

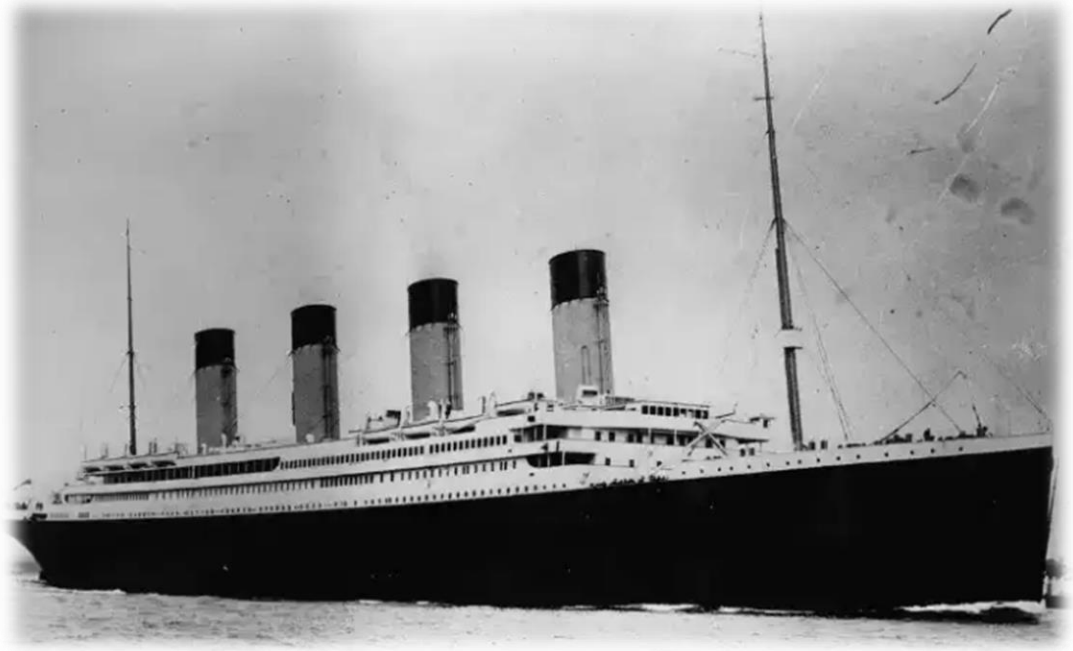
CDR Frank Strom – United States Coast Guard Office of Design & Engineering Standards

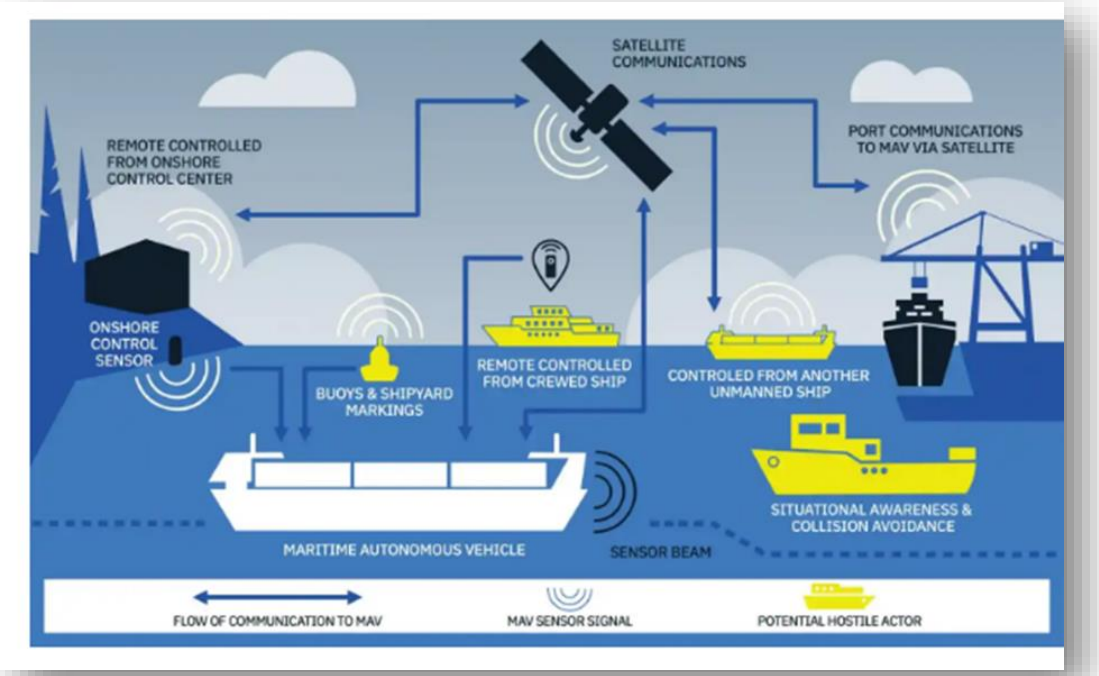
CYBER RISK MANAGEMENT (CRM) for Autonomous or Remote-Controlled Ships

AGENDA

- CRM to today's ships
- CRM for autonomous or remote-controlled ships
  - MASS Code development
- US CRM Efforts
- Cyber Related Standards and Guidelines

Ships as an Island vs. Ships as Part of a System





CYBER RISK MANAGEMENT – SHIPS

IMO – MSC/FAL Circ. 3 (May 2016) ***Guidelines on Maritime Cyber Risk Management*** **(previously MSC. Circ 1526)**	
Establishes high-level guidelines for a holistic, risk management approach to cyber	Aligns with NIST Cybersecurity Framework

IMO – Maritime Safety Committee Resolution 428(98) (June 2017)	
Affirms that approved Safety Management Systems should take cyber risk management into account	Encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems by 1 January 2021

Flag State Implementation (June 2017 – January 2021)	
USCG collaborating with industry to develop a clear path to compliance with MSC Resolution 428(98)	Development of industry standards, Company implementation, verification, and feedback through the SMS audit process

CYBER RISK MANAGEMENT – SHIP SMS

Standards Development

Appropriate standards will follow the Guidelines for Cyber Risk Management (MSC/FAL Circ. 3)

Incorporation of CRM into SMS

Company selects an appropriate standard and incorporates those practices into their SMS

Review of SMS by RO

Recognized Organization (RO) reviews SMS during annual review

New DOC issued

New DOC is issued in accordance with MSC Resolution 428(98) prior to **01 January 2021**

Evaluation during SMS audits

SMS audits will provide feedback and verification

CRM for MASS/ROC System

Cyber-Informed Engineering – Broad foundational structure that advocates for the inclusion of cybersecurity as a principle element of risk management

- Asset Inventory
- Supply Chain Vulnerability
- Network Segmentation

Draft MASS Code and CRM

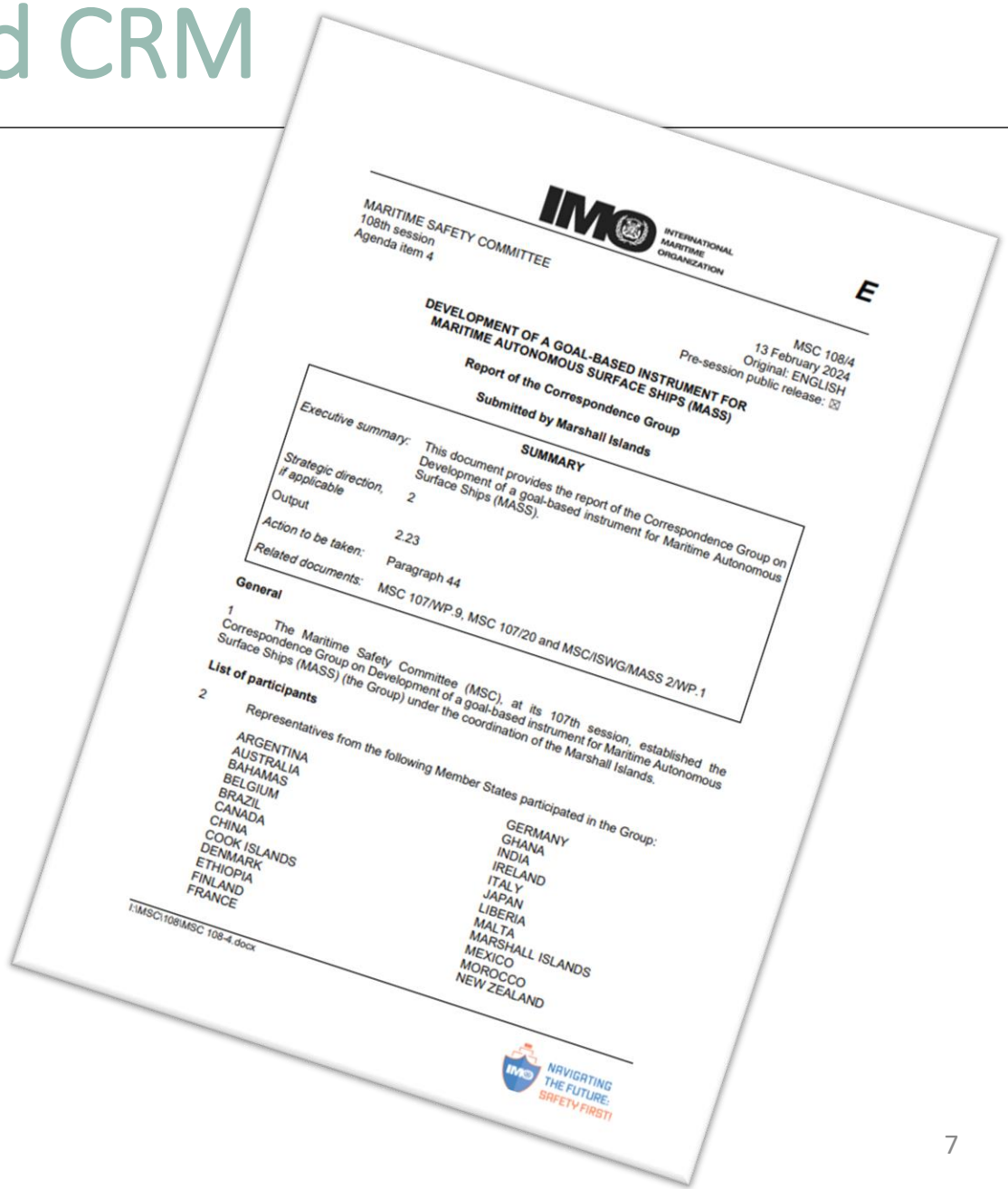
Chapter 3: System Design Principles

- *3.7 Security and Cybersecurity*: Security measures to protect the systems on the MASS and the ROC should be incorporated to prevent unauthorized access and cyber threats.
- 3.3 Robustness and Reliability
- 3.5 Redundancy and Fault Tolerance

Chapter 4: Software Principles

Chapter 5: Connectivity

Chapter 7: Human-Machine Interface



IMO INTERNATIONAL MARITIME ORGANIZATION

MARITIME SAFETY COMMITTEE
108th session
Agenda item 4

E

MSC 108/4
13 February 2024
Original: ENGLISH
Pre-session public release: ☒

DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

Report of the Correspondence Group

Submitted by Marshall Islands

SUMMARY

Executive summary: This document provides the report of the Correspondence Group on Development of a goal-based instrument for Maritime Autonomous Surface Ships (MASS).

Strategic direction, if applicable: 2

Output: 2.23

Action to be taken: Paragraph 44

Related documents: MSC 107/WP.9, MSC 107/20 and MSC/ISWG/MASS 2/WP.1

General

1 The Maritime Safety Committee (MSC), at its 107th session, established the Correspondence Group on Development of a goal-based instrument for Maritime Autonomous Surface Ships (MASS) (the Group) under the coordination of the Marshall Islands.

List of participants

2 Representatives from the following Member States participated in the Group:

ARGENTINA
AUSTRALIA
BAHAMAS
BELGIUM
BRAZIL
CANADA
CHINA
COOK ISLANDS
DENMARK
ETHIOPIA
FINLAND
FRANCE
GERMANY
GHANA
INDIA
IRELAND
ITALY
JAPAN
LIBERIA
MALTA
MARSHALL ISLANDS
MEXICO
MOROCCO
NEW ZEALAND

I:\MSC\108\MSC 108-4.docx

NAVIGATING THE FUTURE: SAFETY FIRST!

NIST Framework & DHS CISA Cybersecurity Performance Goals

The CPGs are intended to be:

- A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
- A combination of recommended practices for information technology and operational technology owners, including a prioritized set of security practices.

Cross-Sector Cybersecurity Performance Goals | CISA

US & CYBER RISK MANAGEMENT

FEBRUARY 21, 2024

FACT SHEET: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports

BRIEFING ROOM › STATEMENTS AND RELEASES

Today, the Biden-Harris Administration will issue an Executive Order to bolster the security of the nation's ports, alongside a series of additional actions that will strengthen maritime cybersecurity, fortify our supply chains and strengthen the United States industrial base. The Administration will also announce its intent to bring domestic onshore manufacturing capacity back to America to provide safe, secure cranes to U.S. ports – thanks to an over $20 billion investment in U.S. port infrastructure under President Biden's Investing in America Agenda. Today's actions are clear examples of the President's work to invest in America, secure the country's supply chains, and strengthen the cybersecurity of our nation's critical infrastructure against 21st century threats – priorities his Administration has focused on relentlessly since taking office.

CYBER RELATED STANDARDS AND GUIDELINES

International Standards:

- ISO/IEC 20000-1:2011 Information Technology – Service management system requirements
- ISO/IEC 27001:2013 – Information Technology – Information security management systems
- ISO/IEC 27002:2013 – Information Technology – Code of practice for information security controls
- ISO 28001:2007 – Security management systems for the supply chain
- ISO 31000:2009 – Risk management – Principles and guidelines
- ANSI/ISA-62443-4-2, Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components

Industry Recognized Standards:

- **National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity**

International Guidance:

- **Marine Safety Committee/Facilitation Committee (MSC/FAL) Circ. 3, *Guidelines on Maritime Cyber Risk Management***
  - *Up for Revision at MSC 108 – Agenda Item 6*
- **MSC Resolution 428(98) *Maritime Cyber Risk Management in Safety Management Systems***

Guidelines:

- International Association of Ports and Harbors (IAPH) Cybersecurity Guidelines for Ports and Port Facilities.
- International Association of Classification Societies (IACS) Recommendation on Cyber Reliance No. 166
- ASTM F3449 20 Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98) Cyber Risks and Challenges

White Paper on Cybersecurity Aboard MASS Submitted by France:

- MSC 108/INF.2 – Development of a Goal-Based Instrument for Maritime Autonomous Surface Ships (MASS)

THANK YOU!


U.S. DEPARTMENT OF
HOMELAND SECURITY


UNITED STATES COAST GUARD
SEMPER
PARATUS
1790