IACS

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

Vincent LAGNY

Incoming IACS Cyber Systems Panel Chairman

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

IACS Cyber panel has worked during the last two years on a set of 12 recommendations which proposes an implementation of cybersecurity on new ships.

Rec 153	Recommended procedures for software maintenance of shipboard equipment and systems
Rec 154	Recommendation concerning manual / local control capabilities for software dependent machinery systems
Rec 155	Contingency plan for onboard computer based systems
Rec 156	Network Architecture
Rec 157	Data Assurance
Rec 158	Physical Security of onboard computer based systems
Rec 159	Network Security of onboard computer based systems
Rec 160	Vessel System Design
Rec 161	Inventory List of computer based systems
Rec 162	Integration
Rec 163	Remote Update / Access
Rec 164	Communication and Interfaces

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

IACS Cyber panel deliveries are in conformance with its mission of support to flags and shipowners. In this state of mind, the Cyber panel will continue to collect needs from industry and administrations in a flexible and structured approach.

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

Indeed if the IACS Cyber panel activity is executed in one hand with maritime stakeholders, in the other, it takes in due consideration IMO and industry guidelines, e.g. on maritime cyber risk management (MSC-FAL.1-Circ. 3) and guidelines on cybersecurity produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, ISO, IEC and NIST.

IACS

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

As a first achievement, in the next months, the IACS Cyber panel will issue a larger and consolidated document which will replace the current set of recommendations.

2019

2020

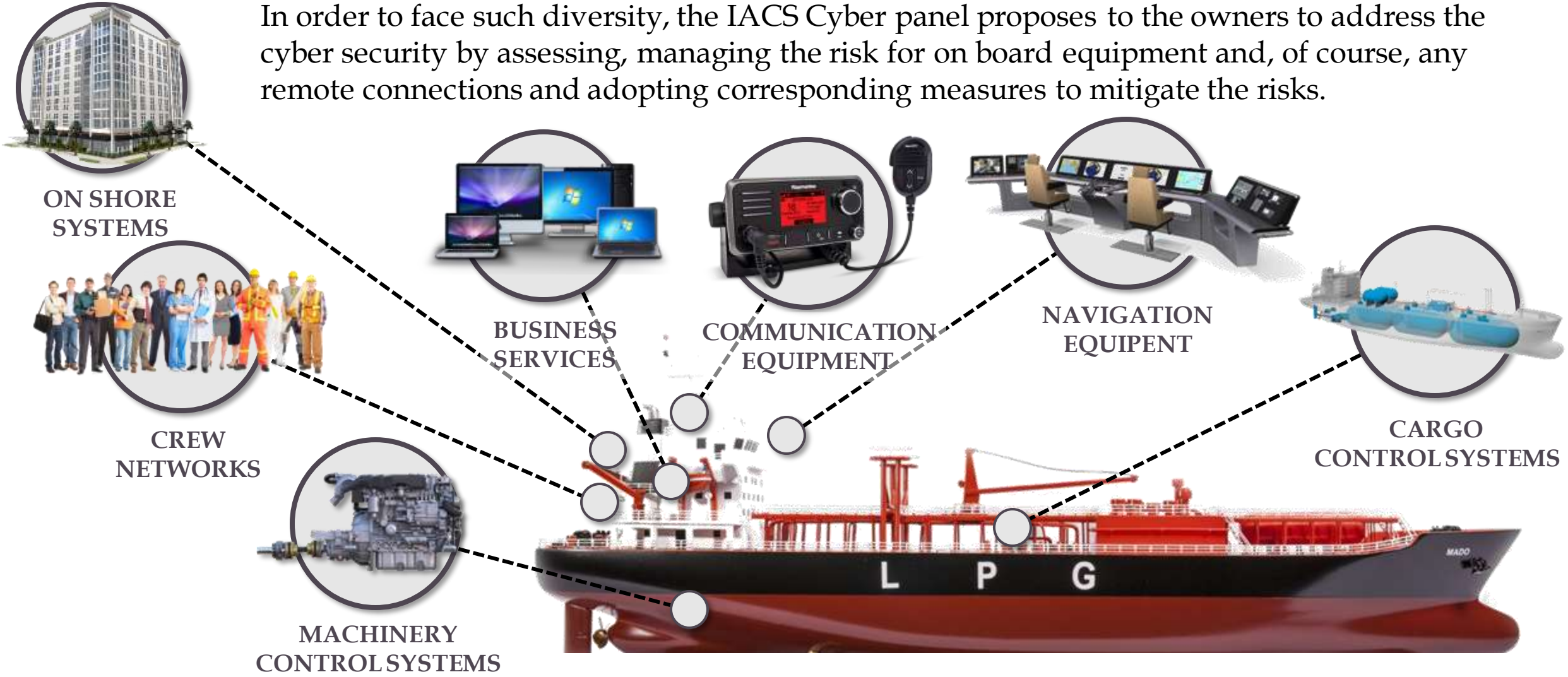
A way to understand the scope of the mission of the IACS Cyber panel is to have a detailed reading on the unusual environment of application of the cyber security the panel has to face.

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

Considering the existing fleet, we shall take into account a variety of ships from bulk carriers, passenger ships, oil tankers, gas carriers or cargos ships that is to be distributed in the 35.000 ships in service with an average age of 20 years old.

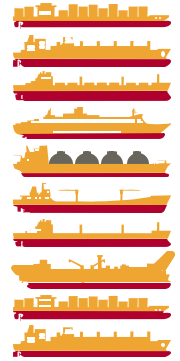
Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

In order to face such diversity, the IACS Cyber panel proposes to the owners to address the cyber security by assessing, managing the risk for on board equipment and, of course, any remote connections and adopting corresponding measures to mitigate the risks.



Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

For new constructions, we shall take into account the fact that cyber is a new topic for the shipyards and, moreover, most of them are not system integrators but are relying on system suppliers. With its publications, the IACS Cyber panel encourages yards to ensure cyber security by design and to endorse the responsibility of the cyber risk management for the integration of on board system.



+4%

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

If ship owners and shipyards have to consider this new challenge, we shall also help equipment suppliers to deliver assets in accordance with cyber security principles from a safety at sea point of view. Once more, the number of technologies talks by itself: communication systems, navigation equipment, machinery, cargo or ballast management and business networks are to be taken into account as they are both targets of attacks and sources of risk. Add to this scenario, the rise of new threats in operational technologies (ICS or industrial control systems), the lack of skills on the market and you will have a good view of the roadmap for the maritime industry.

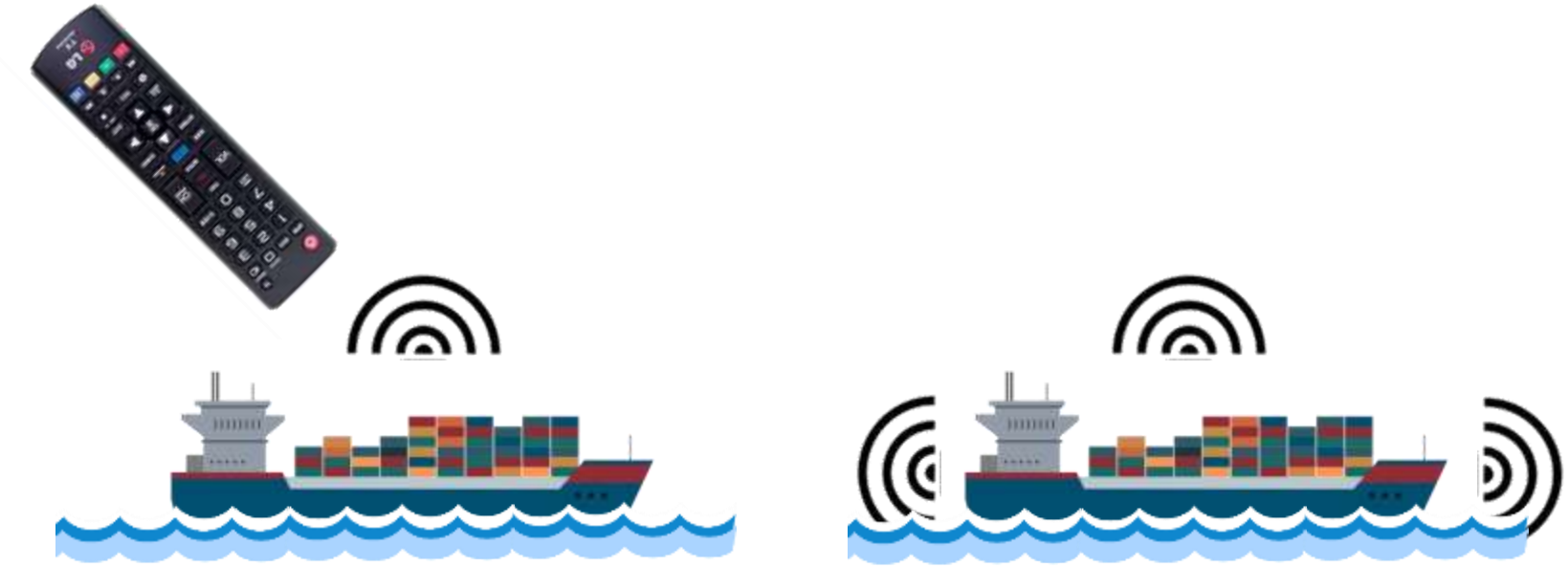
41% **of industrial control systems attacked in 2018**

Percentage of ICS computers attacked
H1 2017 – H1 2018

Source: Kaspersy Lab ICS CERT

Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

Last but not least, the shipping industry is naturally going from past and present vessels to remote controlled ships not forgetting upcoming autonomous systems and autonomous ships.



Introduction of IACS Activities related to Maritime Cyber Systems / Cyber Security

In conclusion, the maritime world challenge, and thus the IACS Cyber panel challenge, is to embrace past fleet and technologies, while accompanying contemporary construction and anticipating new usages at sea. To achieve those objective, and for the years to come, the mission of the IACS Cyber panel will continue to be a constant source of technical proposals for the safety at sea while ensuring the compliance with regulations for the maritime stakeholders.

Thank you!