Active Shipbuilding Experts' Federation

ASEF

Define and assign roles in management of cyber resilience for new ships

ASEF/TWG/SWG5

for MASS and related issues

Wang xingchen/Engineer

MARINE DESIGN AND RESEARCH INSTITUTE OF CHINA

Tripartite Meeting in Seoul on 11-12 Oct. 2018

Background

- In Tripartite 2016, BIMCO gave stakeholders a question, “Ships should be built with cyber secure networks/components, and use contemporary software. And who will be responsible for it?”
- In Tripartite 2017,
  - ASEF gave the opinions on, “What can be considered by Shipbuilders to secure cyber security?”
  - In conclusion, one of the Intersessional work items for ASEF was, “**Define and assign roles in management of cyber resilience for new ships**.”
- A Sub Working Group was established to cope with the issue in ASEF, which is **TWG/SWG5** “MASS and related issues”:

✓Task I: **Cyber Resilience**	- related to JWG/CS by IACS
✓Task II: MASS	- related to IMO
✓Task III: Smart shipping	- related to ISO/TC8 WG10

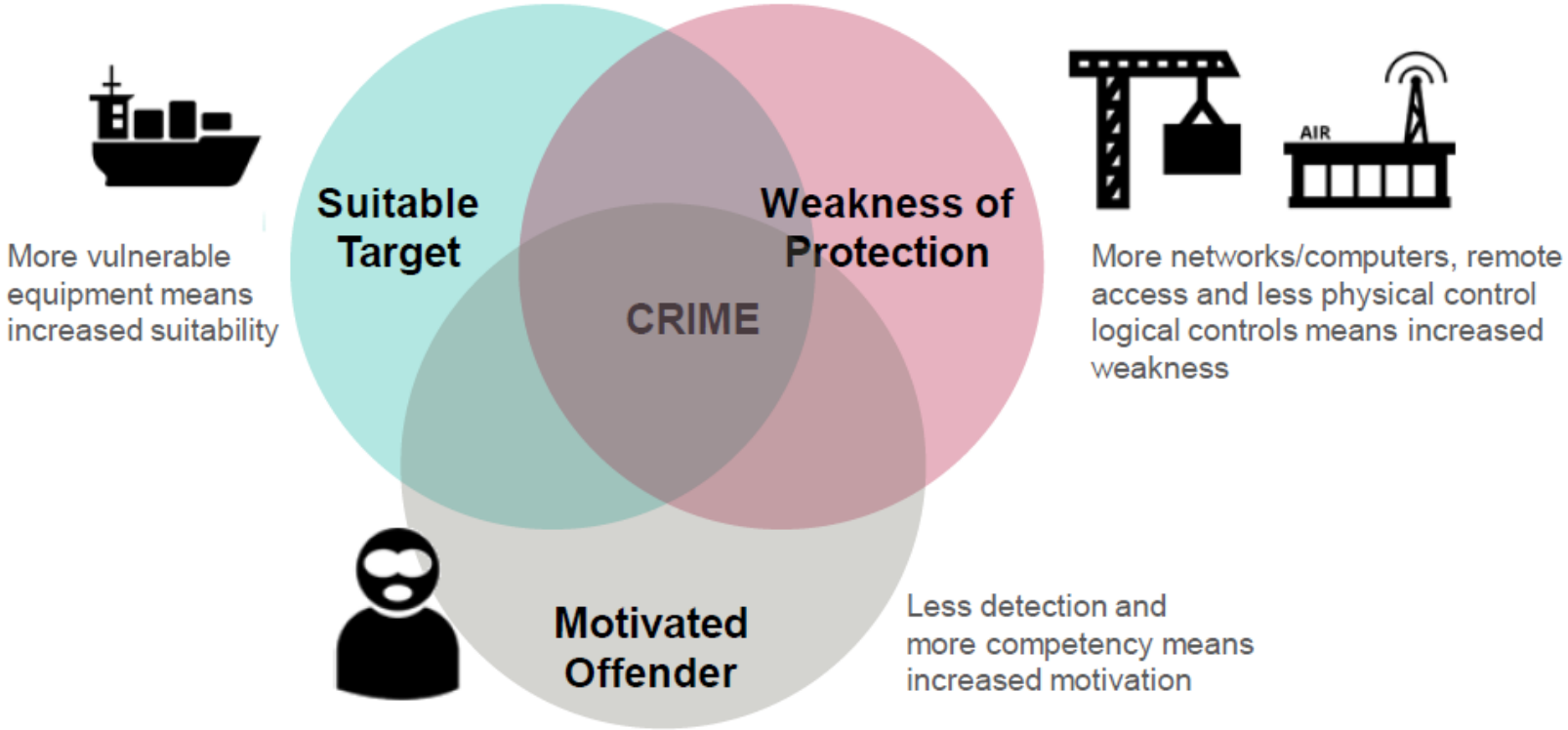
Background : Definition

- In MSC-FAL.1/Circ.3 on "Guidelines on maritime cyber risk management":
  - "*maritime cyber risk*" *refers to a measure of the extent to which a technology asset is 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*.

- In ASEF's opinion,
  - Maritime cyber risks vary with the development of onboard computer based systems. Higher levels of autonomy or automation might brings higher threat.
  - Maritime cyber risks vary with time. Virus and malware are growing at a faster pace.

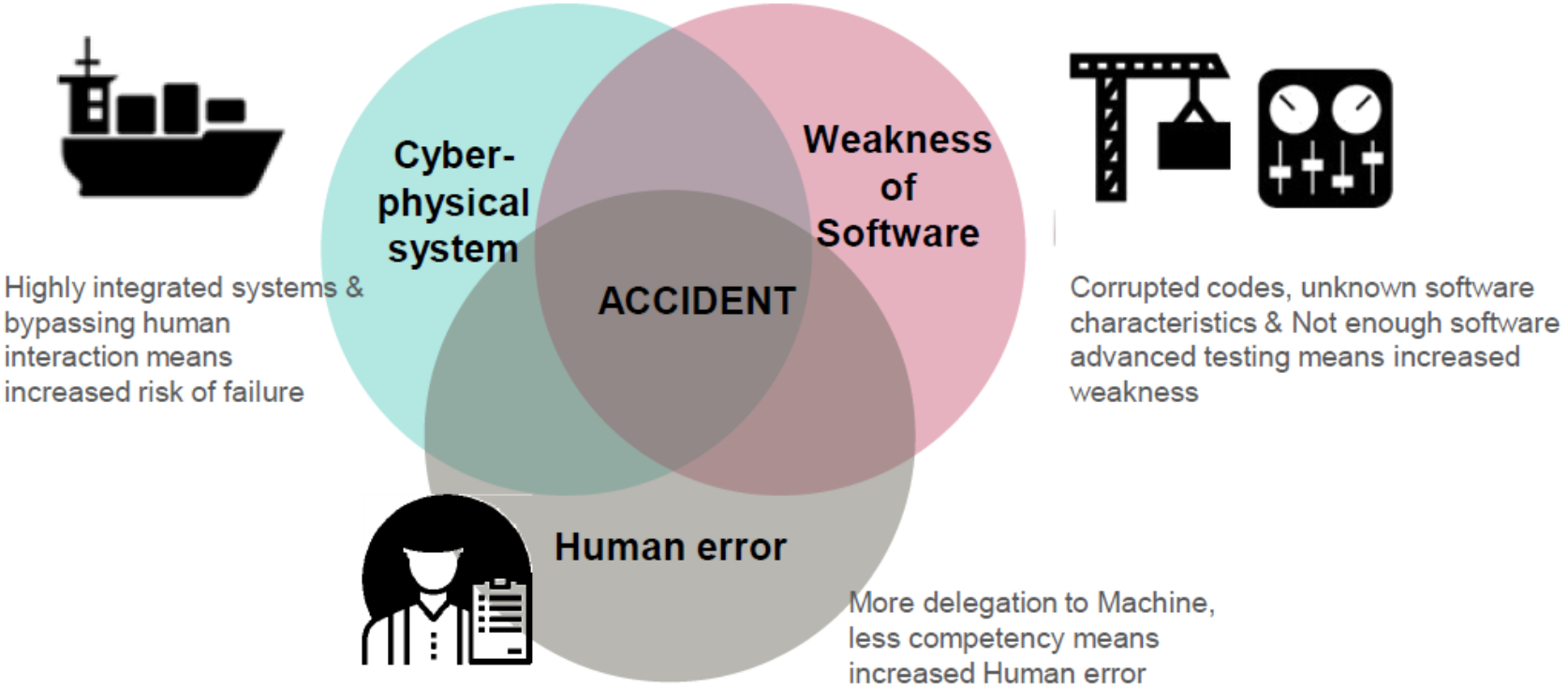
Background: Definition

- What's the definition for Cyber security?
  - In "The Guidelines on Cyber Security Onboard Ships" by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI: *"Cyber security" is concerned with the protection of IT, OT and data from unauthorized access, manipulation and disruption.*
  - Opinion from some Classification Societies: "*Cyber security*" is to prevent intentional malicious actions (cyber attack) .



Background: Definition

- What's the definition for Cyber safety?
  - In "The Guidelines on Cyber Security Onboard Ships" by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI: *"Cyber safety" covers the risks from the loss of availability or integrity of safety critical data and OT.*
  - Opinion from some Classification Societies: *"Cyber safety" is to prevent involuntary accidents and mistakes (system failure)*

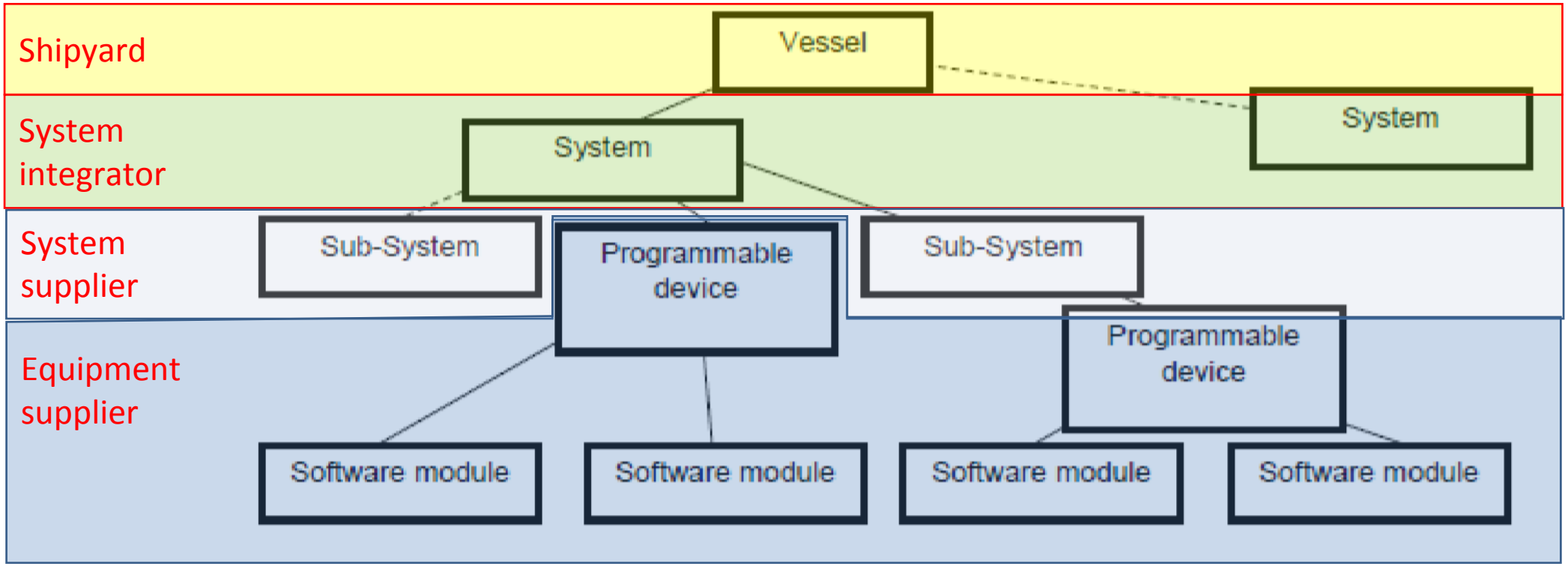


Background: Cyber resilience = Cyber security + Cyber safety

- A cyber resilience system can not only prevent intentional attacking and unintentional accident or mistake but also persist in recovering from the cyber malfunction situation for minimizing any kinds of consequential damage. But **countermeasure may be finite not infinite (imperfect)**.
- Although there are general countermeasures against on-the-ground cyber security with growing use of the state-of-the-art technology such as AI, internet of things (IoT) and autonomous systems, etc., **the detailed countermeasures are not clear**.
- For a more complete consideration of resilience, it is necessary to consider not only cyber (hardware and software) aspects that may be dealt with by **Class** but also to address human elements and training which will require consideration by **Owner**.
- To solve the problem of cyber resilience, include cyber security and cyber safety, is a common question of all industries.

Stakeholders of cyber resilience

- The stakeholders of cyber resilience may in general include Designer, Shipyard, System integrator, Equipment Supplier, System Supplier, Class and Owner. **Shipyard or system supplier may perform as designer and/or system integrator as the case maybe**.



Principles to define and assign roles for cyber related activities

- The activities for cyber resilience can be divided into 5 stages:
  - **Spec. define or contract**
  - **Design**
  - **System product**
  - **Ship building**
  - **Operation & Maintenance**

Before delivery

→ **After delivery**

- Principles to define and assign roles in management of cyber resilience:
  - Who in charge of the activity shall be responsible for it and take **the main responsibility**.
  - Who participate in the activity shall also take **the secondary responsibility**.

Activities in Spec. Define or Contract stage (before delivery)

Activities		Stakeholder						
		Designer	Shipyard	System Integrator	Equipment Supplier	System Supplier	Class	Owner
Spec. Define Or Contract	Decide the level of cyber security for order ship	☆	☆				☆	★
	Decide assets to be certified	☆	☆				☆	★
	Define the criticality of assets for cyber security	☆	☆				☆	★

★: main ☆:secondary

Activities in Design stage (before delivery)

Activities		Stakeholder						
		Designer	Shipyard	System Integrator	Equipment Supplier	System Supplier	Class	Owner
Design	Propose the requirement of system performance	★						★
	Propose the design of system performance	☆		★		☆		
	Confirm the design of system performance	☆		★		☆	★	☆
	Identify the risk of cyber system	☆		★		☆	☆	
	Take measures to reduce the risk	☆		★		☆		☆

★: main ☆:secondary

Activities in System product stage (before delivery)

Activities		Stakeholder						
		Designer	Shipyard	System Integrator	Equipment Supplier	System Supplier	Class	Owner
System product	Hardware manufacture				★			
	Hardware test			☆	☆	☆	★	
	Software coding				★			
	Software performance test			☆	☆	☆	★	
	Software safety test			☆	☆	☆	★	
	System integrate			★	☆	☆		
	System performance test			☆	☆	☆	★	
	System safety test			☆	☆	☆	★	
	System security test			☆	☆	☆	★	

★: main ☆:secondary

Activities in Ship building stage (before delivery)

Activities		Stakeholder						
		Designer	Shipyard	System Integrator	Equipment Supplier	System Supplier	Class	Owner
Ship Building	System install		★	☆	☆	☆		
	Authorization settings					★		★
	Mooring/Onboard test	☆	★	★		☆	☆	☆
	Sea trial	☆	★	★		☆	☆	☆
	Information transfer	☆	★	☆	☆	☆		★

★: main ☆:secondary

Activities in Operation & Maintenance stage (after delivery)

Activities		Stakeholder						
		Designer	Shipyard(1)	System Integrator(2)	Equipment Supplier	System Supplier	Class	Owner
Operation & Maintenance	Training			☆	☆	★		★
	System Maintenance		☆	☆	★	★		★
	Software Update		☆	☆	★	★		★
	Operation							★

★: main ☆:secondary

Notes:

(1) Shipyard is responsible for system maintenance and software update during warranty period.

(2) After delivery, Owner or some party assigned by Owner shall perform as System Integrator.

Define and assign roles in management of cyber resilience [1]

- **Designer** shall recognize and propose the requirement of cyber security/safety of a ship based on specifications specified by Owner and Class Rules, and instruct/assist Supplier and/or System Integrator to appropriately address and account for risks.
- **Shipyard** shall ensure the system installed correct and ensure intended functional performance of systems during mooring/onboard test and sea trials of the ship. If yard is a System Integrator at the same time, yard shall take the role of system integrator.
- **System Integrator** shall be responsible for system integration test before installation onboard & final integration and onboard testing, **recognized by Shipyard, Owner (and Class)**. The detailed and concrete procedures for planning and testing of the integrated system, however, **shall** be developed as an **indispensable element** by IACS to ensure the leveling of cyber security/safety/resilience of ships**. The responsibility for System Integrator specifically contracted/assigned by Shipyard should be clarified and agreed by Owner**. Otherwise, the role of system integrator shall be taken by either the Shipyard or depending on contract.

Define and assign roles in management of cyber resilience [2]

- **Equipment supplier** shall be responsible for the safety of software and hardware. All software shall meet the requirement of UR E22 by tests. All hardware shall meet the requirement of Classification Society by tests.
- **System supplier** shall be responsible for the cyber security/safety related performance of the equipment and system. It's also their duty to update the system in warranty of the ship, and to provide technical support in all life cycle of corresponding equipment and system, if applicable. They shall set authorization management to prevent misoperation by irrelevant person, and train the operators.

Define and assign roles in management of cyber resilience [3]

- **Class** shall be in duty bound to recognize the ongoing cyber threat and prescribe clear or specific requirements and standards for risk assessment, tests and verifications, including what should be done and to what extent as far as practical. To clarify the conditions to be satisfied at the time of delivery, Class may give suggestions, recommendations or guidance to Owner.

- **Owner** shall be in charge of the practical implementation of the procedures onboard including defined responsibilities and software change management during operation & maintenance stage. After delivery, the cyber security/safety issues including upgrades shall be under Owner's or Operator's responsibility.

Conclusion

- To ensure cyber health/performance for shipping industry, cyber resilience, including cyber security and cyber safety, need more attention.
- ASEF will invite comments by other Tripartite partners, on the current roles defined and assigned in management of cyber resilience for new ships.
- ASEF believes that common requirements for “Cyber Type Approval” by IACS would be necessary. With the standardized requirement for the equipment or system that deals with external/common interactions, the roles of each stakeholders will actually become more clear and easier.

Active Shipbuilding Experts' Federation

ASEF

Thank you for your attention.

ASEF/TWG/SWG5