

**WEBINAR**

# **IACS URs E26 & E27:**

Bridging the gap between  
regulation and implementation

**Wednesday 19 June • 08:00-09:00 BST**

Brought to you by

MARITIME  
**OPTIMISATION**  
& COMMUNICATIONS

In association with **inmarsat** 

# PANELLISTS



**Makiko Tani**


Deputy Manager, Cyber Security Team  
**ClassNK**

## **IACS URs E26 & E27:**

Bridging the gap between  
regulation and implementation

In association with **inmarsat**



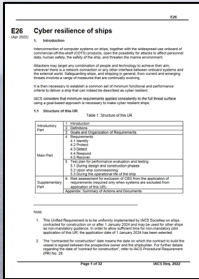


IACS URs E26 & E27:  
Bridging the gap between  
regulation and implementation

**From compliance to advantage**

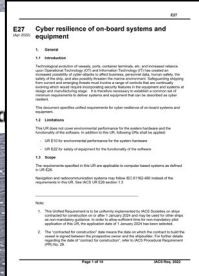
Makiko TANI  
Cybersecurity Team  
ClassNK





E26

E26: Cyber Resilience of Ships  
(For shipbuilders/integrators/designers)



E27

E27: Cyber Resilience of  
on-board Systems and Equipment  
(For systems/equipment manufacturers)

Mandatory for **all new builds**  
**contracted for construction from 1 July 2024**



## Guideline for Cyber resilience and on-board systems and equipment (Edition 1.0)

Issued on 2 Nov. 2023

- Application scope
- Approval process
- Explanation of requirements
- Items to be confirmed during document reviews and surveys
- Type approval process



## Guideline for Cyber resilience of ships

Scheduled to be issued in July 2024

- Application scope
- Explanation of requirements
- Items to be confirmed during document reviews and surveys
- Explanation of exclusions from the application of relevant requirements based on risk assessments

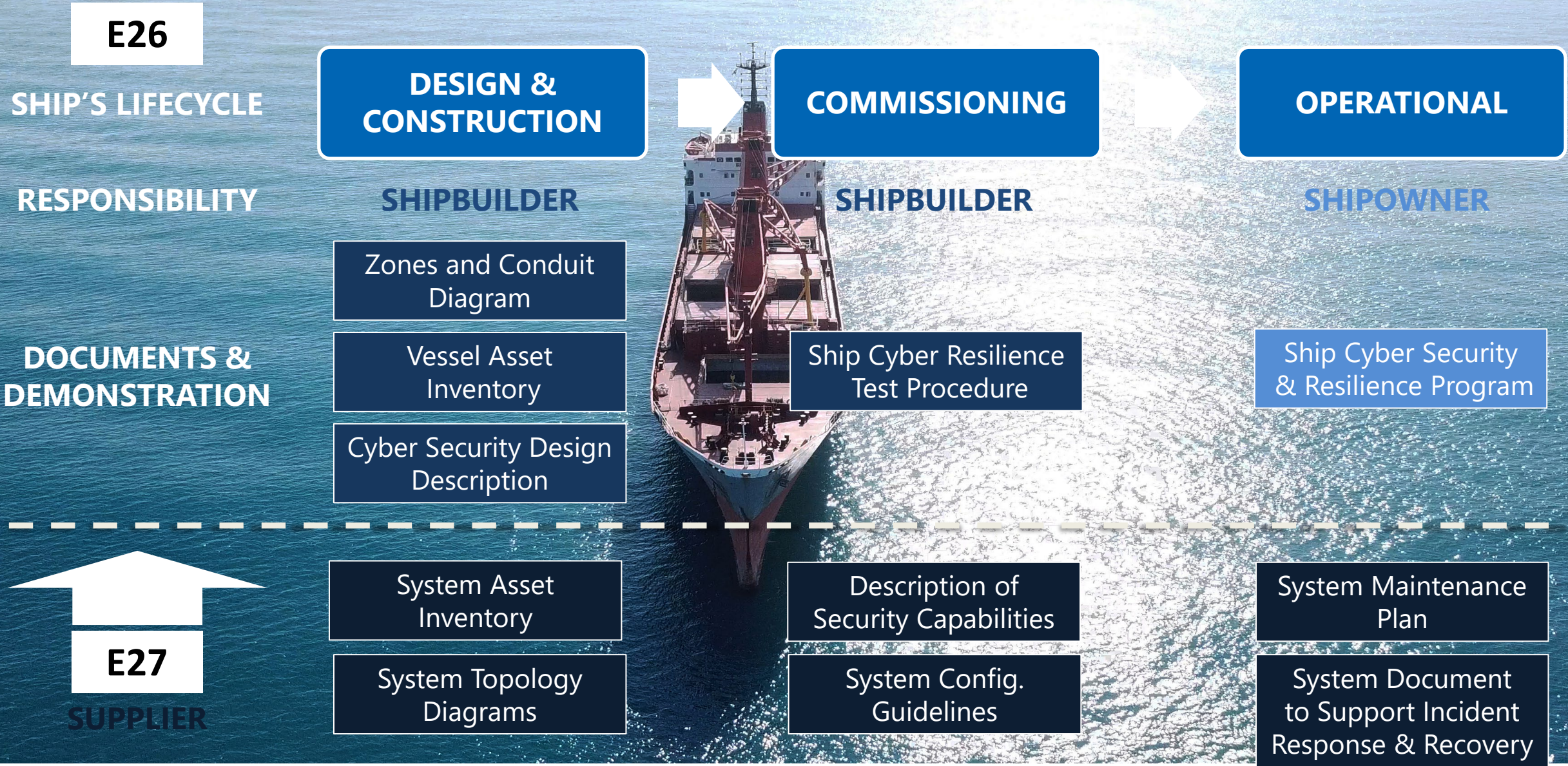


- “Guidelines for Cyber Resilience of On-board Systems and Equipment” supplements Chapter 4, Part X and UR E27(Rev.1)
- “Guidelines for Cyber Resilience of Ships” supplements Chapter 5, Part X and UR E26(Rev.1)
- Both guidelines include references to the Rules for the Survey and Construction of Steel Ships and correspond to its requirements.





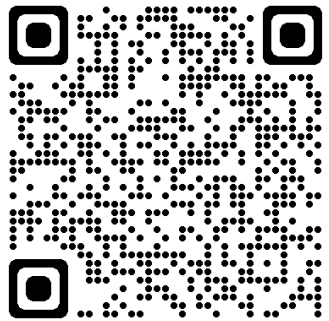
# Key submissions







Thank you!





# PANELLISTS



**Laurie Eve**  
Chief of Staff  
Inmarsat

## IACS URs E26 & E27:

Bridging the gap between  
regulation and implementation

In association with **inmarsat**

# IACS URs E26 & E27: Bridging the gap between regulation and implementation

Connectivity Solutions Provider  
Perspective

Laurie Eve  
Chief of Staff, Inmarsat Maritime  
[Laurie.Eve@inmarsat.com](mailto:Laurie.Eve@inmarsat.com)





# Key Recommendations

## People & Culture

- > Phishing remains most common initial access vector
- > User training and awareness programme to reduce human error
- > Ensure user privileges correctly assigned
- > Invest in QMS and standards like ISO 27001
- > Assess your suppliers' risk management practices
- > Cyber security in blue chips

## Network Connected Systems & Services

- > Increasing attack surface represents significant risk
- > Cost, time and resource considerations
- > Recommend a risk-management approach
- > Identify onboard assets, assess the risks and set the risk appetite
- > Decide which areas need investment and implement security measures accordingly
- > Key areas for investment: 24/7 SOC, Physical network separation, Cyber security solutions with multi-layer security
- > Maintain Situational Awareness and intelligence on evolving threats

## Incident Response Plan (IRP)

- > Assume will be breached
- > Robust response plan to reduce cost and impact of a cyberattack
- > Invest in incident management policy
- > Investment in terms of team responsibilities, facilities, back up data and systems
- > Importance of review, training and rehearsal

# Layered Security Posture to Support UR E26 & E27

	ENDPOINT SECURITY	UTM	SECURE EMAIL
GOVERN	<ul style="list-style-type: none"> <li>• IT Policy function</li> <li>• Risk Assessment Reports</li> </ul>	<ul style="list-style-type: none"> <li>• Risk Management</li> </ul>	
IDENTIFY	<ul style="list-style-type: none"> <li>• IT Asset Management</li> <li>• Teyla Scanner</li> <li>• Dashboard and Automated Alerts</li> </ul>	<ul style="list-style-type: none"> <li>• IT &amp; OT Asset Management</li> <li>• Dashboard and automated alerts</li> <li>• Network Discovery</li> <li>• Captive Portal</li> </ul>	
PROTECT	<ul style="list-style-type: none"> <li>• Malware / Ransomware protection</li> <li>• Endpoint-level firewalling</li> <li>• Crew Awareness Training Module</li> <li>• IRIS</li> </ul>	<ul style="list-style-type: none"> <li>• Intelligent AV</li> <li>• Intrusion Prevention</li> <li>• Application Control</li> <li>• Web Content Filtering</li> <li>• DNS Watch</li> <li>• Data Loss Prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Triple Engine AV scanning of all messages</li> <li>• Phishing and Spam filtering</li> <li>• Advance Threat protection against zero-day threats.</li> <li>• Quarantine mgt</li> </ul>
DETECT	<ul style="list-style-type: none"> <li>• Security / OSMO Reports</li> <li>• News/ Insight Section</li> <li>• Automated Alerts</li> </ul>	<ul style="list-style-type: none"> <li>• Security reports</li> <li>• Threat Hunting</li> <li>• Automated alerts</li> </ul>	
RESPOND & RECOVER	<ul style="list-style-type: none"> <li>• 24/7 SOC</li> </ul>	<ul style="list-style-type: none"> <li>• 24/7 SOC</li> </ul>	<ul style="list-style-type: none"> <li>• Data backup function</li> <li>• 24/7 Support</li> </ul>



# Mapping Fleet Secure Solution to Support UR E26 & E27

IACS Regulation	NIST Function	Requirements	FS UTM / Endpoint Function	Description
E26 Cyber Resilience of Ships	Identify &Protect	Ships must have the capability to identify and protect against potential cyber threats	Firewall and Intrusion Prevention Systems (IPS)	Fleet Secure UTM monitors and controls network traffic to prevent unauthorized access and detect malicious activity
			Gateway AV	Regular scanning and real-time protection against viruses and malware ensure the ship’s systems are secure
	Detect	Ships must be able to detect cyber incidents in a timely manner	Real-time Network Monitoring /SOC	Continuous monitoring of network activities helps in the early detection of suspicious activities or potential cyber threats
			Intrusion Detection Systems (IDS)	This function alerts operators about unauthorized access attempts or unusual network behaviour
	Response &Recovery	Ships need to have measures in place to respond to and recover from cyber incidents	Automated Alerts / Incident Response (SOC)	Predefined response protocols (such as alerts), automate the mitigation of detected threats, reducing response times and minimizing damage. 24/7 SOC helps with timely incident response
E27 Cyber Resilience of On-board Systems and Equipment	Identify &Protect	On-board systems must use secure communication protocols to protect data integrity and confidentiality	User Authentication (Captive Portal) and Access Control	Role-based access control (RBAC) ensures that only authorized personnel can access network and critical systems
		Implement strong access controls and authentication mechanisms to restrict access to critical systems		
		Conduct regular security assessments and keep systems updated to mitigate vulnerabilities	Advanced Security Reporting	Regular vulnerability scans via reports identify and prioritize security risks/updates

# PANELLISTS



**Kostas Grivas**  
Information Security Officer  
**Angelicoussis Group**

## **IACS URs E26 & E27:**

Bridging the gap between  
regulation and implementation

In association with **inmarsat**

Bridging the gap between regulation and implementation

# IACS URs E26 & E27

Kostas Grivas  
Information Security Officer



# New IACS requirements

- UR E26. Cyber Resilience of ships
- UR E27. Cyber Resilience of on-board systems & equipment

## Benefits of the recommendations

- Uniform application by All Classification Societies
- Description of minimum functional & performance criteria
- Responsibility spreads among more stakeholders. Suppliers, Shipyards/Ship designers, System Integrators, Shipowner/Company, Classification Society.

# Systems in Scope

All Computer Based Systems, where CBS is *"A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, use, etc. of information. CBS include IT and OT systems. A CBS may be a combination of subsystems connected via network"*

Indicative List:

- Propulsion
- Steering
- Electrical power generation and distribution
- Cargo handling system (limited to safety-related elements)
- Bilge and ballast systems, loading/unloading control systems, loading computer
- Scrubber control system and other systems for compliance with regulations to prevent pollution to the environment
- Any other OT system whose disruption or functional impairing may pose risks to ship operations (e.g. LNG monitoring and control system, relevant gas detection system etc.)



## UR E26 (Ships)

### Primary goal

- The primary goal is to support safe and secure shipping, which is operationally resilient to cyber risks.  
Safe and secure shipping can be achieved through effective cyber risk management system.

### Sub-goals

- **Identify**: Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.
- **Protect**: Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.
- **Detect**: Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.
- **Respond**: Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.
- **Recover**: Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.

## Summary of Actions and Responsibilities

The table presents in brief each stakeholder's responsibilities per element.

UR E26  
(Ships)

Element	Supplier	Shipyard / System Integrator	Shipowner / Company	Class
Identify	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Protect	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Detect	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Respond	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Recover	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Perf. Eval. & Testing	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check
Risk Asses.	Provide	Maintain & Provide	Maintain & Make avail.	Approve, Info & Check

\* for more information refer to the UR E26 Appendix.

\*\* Vessel's lifecycle phases are: Design, Construction, Commissioning, Operation and Survey



## UR E27 (O/B Systems)

### Purpose

- This document specifies unified requirements for cyber resilience of on-board systems and equipment.

### Definitions

**A System** can consist of group of hardware and software enabling safe, secure and reliable operation of a process. Typical example could be Engine control system, DP system, etc.

**An Equipment** may be one of the following:

- Network devices (i.e. routers, managed switches)
- Security devices (i.e. firewall, Intrusion Prevention System)
- Computers (i.e. workstation, servers)
- Automation devices (i.e. Programmable Logic Controllers)
- Virtual machine cloud-hosted

## UR E27 (O/B Systems)

### Obligations

The UR requires the submission and maintenance of certain type of documents as well as specific capabilities and processes.

- System Documentation
- Inventory
- Software Inventory
- Security capabilities for the CBSs in scope
- Product Design and Development (SDLC)



## Indicative details

Some of the required details can be:

- ✓ For each equipment, the involved hardware shall be detailed (i.e. motherboard, storage, interfaces (network, serial) and any connectivity)
- ✓ Network or serial flows (source, destination, protocols, protocols details, physical implementation)
- ✓ Current Version of the operating system and embedded firmware (software version) and date implemented
- ✓ Version information, license information with expiration dates and a log of updates (for S/W)
- ✓ For CBSs in scope (IAM, Credentials, MFA/ACL, Session control, NetSec, etc.)

UR E27  
(O/B  
Systems)

# Implementation Considerations

Although the new URs contributes a lot to the Vessels Cyber Security posture, there are a few things to consider. Indicatively:

1. Are all requirements practical to apply to certain O/B systems?
2. How excessive is the cost and complexity involved?
3. Is the time provided sufficient for the stakeholders to follow the requirements?
4. Shall all the requirements be deemed as mandatory?
5. Can all stakeholders be capable to follow all the requirements?

# UPCOMING EVENTS

Asia Maritime  
Webinar Week

SINGAPORE  
SOLUTIONS

Container Shipping  
Webinar Week

CONTAINER SHIPPING  
& PORT TECHNOLOGY

OFFSHORE  
SUPPORT JOURNAL  
CONFERENCE ASIA

osj  
offshore  
support  
journal

MARITIME  
DECARBONISATION, EUROPE  
CONFERENCE | AWARDS | EXHIBITION

marine  
propulsion

CRUDE TANKERS  
& TERMINALS  
CONFERENCE | AWARDS | EXHIBITION

TANKER  
SHIPPING & TRADE

MARITIME HYBRID, ELECTRIC  
& HYDROGEN FUEL CELLS  
CONFERENCE

marine  
propulsion

LNG SHIPPING &  
TERMINALS CONFERENCE

LNG  
SHIPPING &  
TERMINALS

INTERNATIONAL BULK  
SHIPPING CONFERENCE

riviera )))

SCAN HERE TO SEE THE FULL EVENTS SCHEDULE

