IACS

Update on IACS' Cyber-related Work

Mr Anastasiou Panagiotis

IACS Cyber Systems Panel

IACS

IACS adopts new requirements on cyber resilience

- Recognising that cyber incidents on vessels can have a direct and detrimental impact on life, property, and the environment, IACS has steadily increased its focus on the reliability and functional effectiveness of onboard, safety-critical, computer-based systems.

- IACS identified at an early stage that, for ships to be resilient against cyber incidents, all parts of the industry needed to be actively involved, and so convened a Joint Working Group (JWG) on Cyber Systems which helped identify best practices, appropriate existing standards in risk and cyber security, and a practical goal-based approach.

IACS adopts new requirements on cyber resilience

- Building on this extensive collaboration, and utilising the experience gained from its existing Recommendations, as well as developments at IMO including, in particular, Resolution MSC.428(98) applicable to in-service vessels since the 1st of Jan 2021, IACS has adopted two new IACS Unified Requirements (URs) on the cyber resilience of Ships,

- Unified Requirements are adopted resolutions on matters directly connected to or covered by specific Rule requirements and practices of classification societies and the general philosophy on which the rules and practices of classification societies are established.

UR E26
Cyber resilience of Ships

UR E26 aims to ensure the secure integration of both Operational Technology (OT) and Information Technology (IT) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship. This UR targets the ship as a collective entity for cyber resilience and covers five key aspects:

1. equipment identification
2. protection
3. attack detection
4. response
5. recovery

UR E27
Cyber resilience of on-board systems and equipment

UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements:

1. for cyber resilience of onboard systems and equipment
2. relating to the interface between users and computer-based systems onboard
3. on product design and development for new devices before their implementation onboard ships.

UR E27 - Scope

- The requirements specified in this UR are applicable to computer based systems under scope of UR E26 “Cyber resilience of ships”
- Navigation and radio communication systems may follow IEC 61162-460 instead of the requirements in this UR.

UR E27 - Limitations

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware

- UR E22 for safety of equipment for the functionality of the software

UR E27 - Systems and Equipment

Systems and Equipment

A System can consist of a 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 - System Requirements

Table 1: Security capabilities are required for all computer-based systems as defined in UR E26. (Total 31 Requirements)

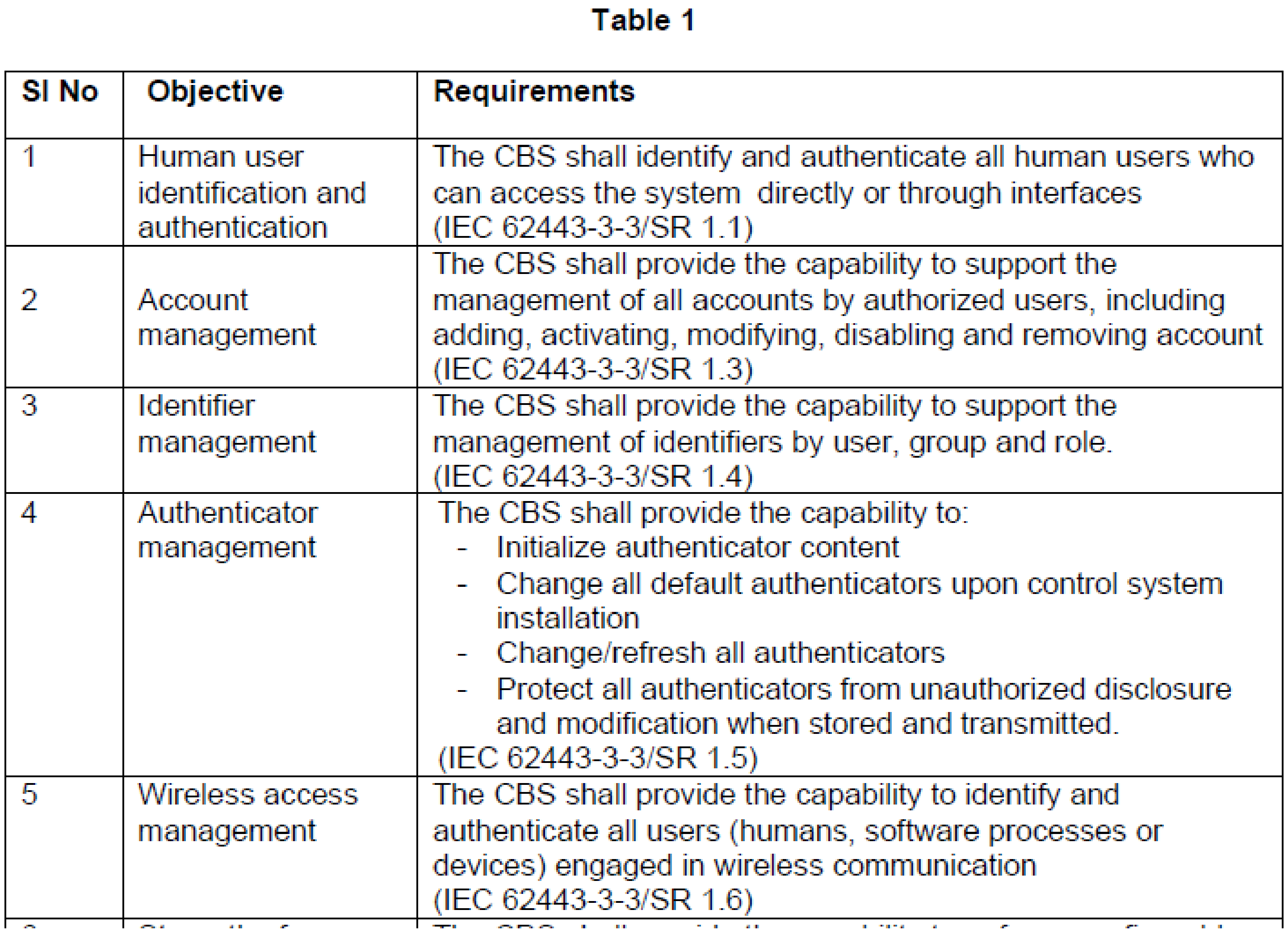

Table 1

Sl No	Objective	Requirements
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role. (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS shall provide the capability to: - Initialize authenticator content - Change all default authenticators upon control system installation - Change/refresh all authenticators - Protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6)

UR E27 - System Requirements

Table 2: Additional security capabilities are required for CBSs with network communication to untrusted networks i.e., interface to any networks outside the scope of UR E26. (Total 10 Requirements)

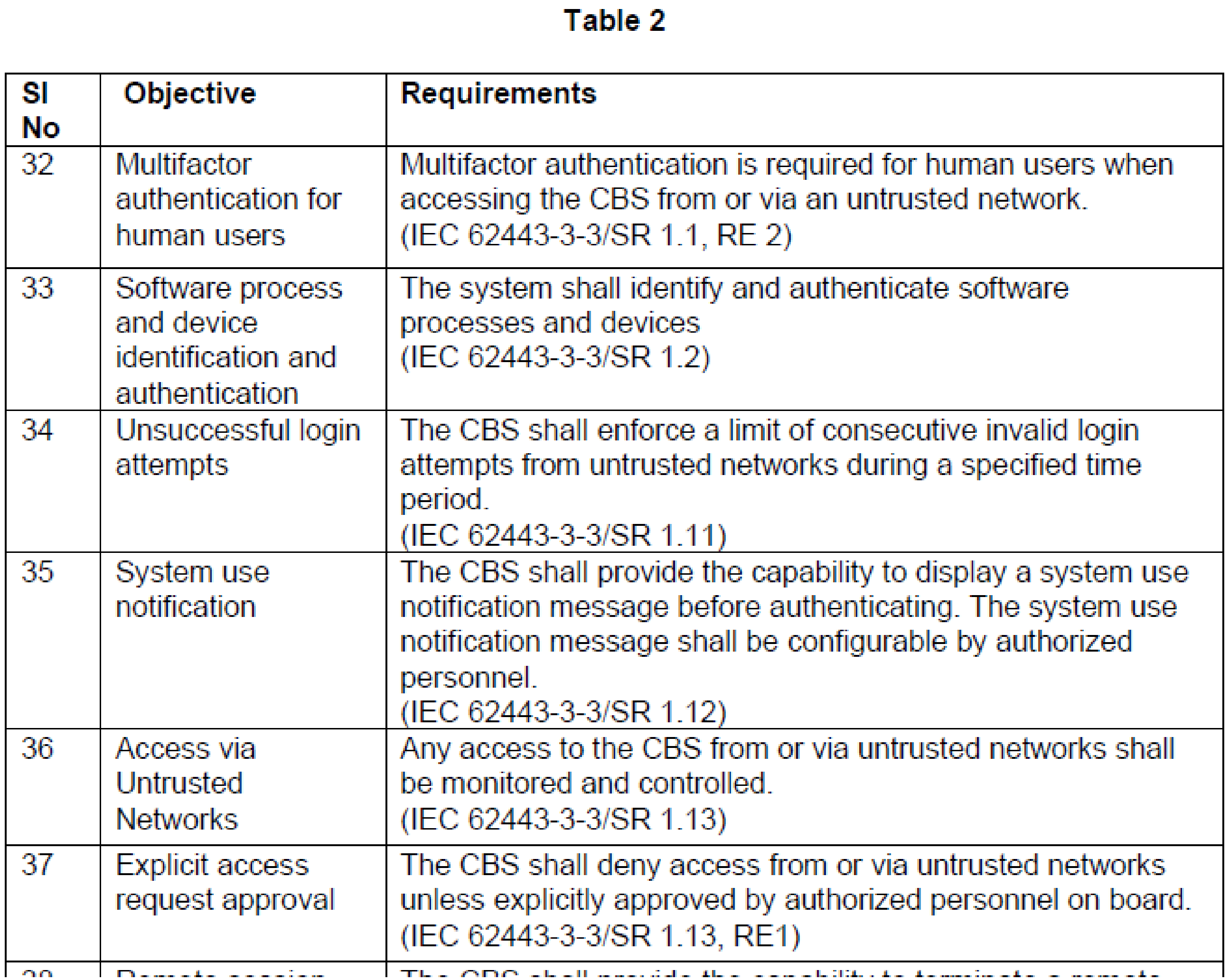

Table 2

Sl No	Objective	Requirements
32	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
33	Software process and device identification and authentication	The system shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
34	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
35	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
36	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
37	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
38	Remote session	The CBS shall provide the capability to terminate a remote

PTPC07
Unified requirements for verification of compliance with UR E26 and UR E27

- The new URs for cybersecurity focus on technical and procedural requirements. Classification Societies have agreed to ensure a harmonized approach for the application of the new UR's, during newbuilding and operational phases of the vessels and for that reason an additional UR is being developed to cover the verification activities to be performed by the Societies.
- Expected Summer 2023

תודה

Dankie

Gracias

Спасибо

شكراً

Merci

Takk

Köszönjük

Terima kasih

Grazie

Dziękujemy

Dėkojame

Ďakujeme

Vielen Dank

Paldies

Kiitos

Täname teid

谢谢

Thank You

Tak

感謝您

Obrigado

Teşekkür Ederiz

감사합니다

Σας

धन्यवाद

ขอบคุณ

Bedankt

Děkujeme vám

ありがとうございます

Tack