White Paper

Aperio Cybersecurity FAQ

APERIO

EMERSON

In this White Paper

In the modern maritime industry, cybersecurity is not just an option—it's a necessity. As shipping companies worldwide look to reap the rewards of advanced shipboard technologies to support digitalization, decarbonization, and crew welfare initiatives, data usage is soaring. The increasing digitalization and interconnection of the maritime industry presents opportunities to enhance onboard safety, operational efficiency, and environmental sustainability.

Emerson's Aperio system is designed to securely integrate control and monitoring functions on any type of ship and application, e.g. engines, generators, switchboards and other service systems. The system offers remote connectivity that connects the dots through E27 compliant cybersecurity. Aperio provides reliable integrated control and monitoring to assure safe, efficient, reliable, sustainable, and E27 cybersecure operations. With the Aperio system, you are securely connected to systems on board and on shore, enabling you to be compliant.

This document aims to provide an overview of the key cybersecurity capabilities of the Aperio system using an FAQ format. If more detailed descriptions of the individual security capabilities are needed, please contact the Emerson Aperio team.

Table of Contents

1. The Aperio system

Aperio is a computer-based system developed for tank monitoring, valve and pump control and alarm acquisition in marine applications. It is a marine management solution suited for several systems such as:

- Ballast tanks
- Bilge wells
- Service tanks
- Cargo tanks
- Bunkering
- Fuel oil consumption
- Machinery and service systems
- Other systems

Aperio can be combined in an integrated control and monitoring system (ICMS). The Aperio marine integrated control and monitoring system is a general system developed to solve any automation task onboard. Ongoing development of the system has led to today's system, with thousands of vessels in service worldwide. The operation of the system can be done from different sizes of operator panels, for example from a small operator panel of 10" (inch) that can be used for local control and accommodation alarm panel or a workstation with 24" wide screen. The same user interface is used on all sizes of workstations.

2. What are UR E26 and E27 and why are they important?

As shipping companies worldwide look to reap the rewards of advanced shipboard technologies to support digitalization, decarbonization, and crew welfare initiatives, data usage is soaring. The increasing digitalization and interconnection of the maritime industry present opportunities to enhance onboard safety, operational efficiency, and environmental sustainability. However, it also leaves vessel networks susceptible to cyber threats – and with cyber incidents growing in frequency, sophistication, and severity, ship owners and ship managers should prioritize integrating security into their connectivity strategy.

To reduce the occurrence and impact of maritime cyber incidents, the International Association of Classification Societies (IACS) has issued two unified requirements (URs): UR E26 – 'Cyber Resilience of Ships' – and UR E27 – 'Cyber Resilience of Onboard Systems and Equipment'. The URs aim to establish minimum requirements for the cyber resilience capabilities of newbuild vessels and their connected systems, respectively (See figure 1).

While E26 is mainly focused on ship builders and ship owners/operators and the E27 on the individual system component vendors, it is important to see the two standards as a whole (see table 1) when assessing a complete ship's cybersecurity profile.

Aperio and E27

Aperio is a complex system installed in the heart of a ship and is a natural candidate for an E27 certification. Aperio has been in the market for several years and has undergone significant changes to bring it up to the E27 standards. As a result, all Aperio 6 systems and forward will be secured according to the E27 standard, while older legacy Aperio systems (Aperio 3-Aperio 5) will not.

The updates to harden Aperio 6 to E27 standards is not the ultimate goal. Instead Aperio will continue to evolve through new initiatives to harden the solution against emergent cybersecurity threats.

One of the challenges with implementing strong cybersecurity solutions around products or services is that the solutions, if not implemented correctly, are often so disruptive to the crew and operations staff that they find practical workarounds. To minimize disruption, Emerson's Aperio team is constantly communicating and collaborating with shipowners and operators to find solutions which strike a balance between a reasonable and effective cybersecurity posture and ease of operation.

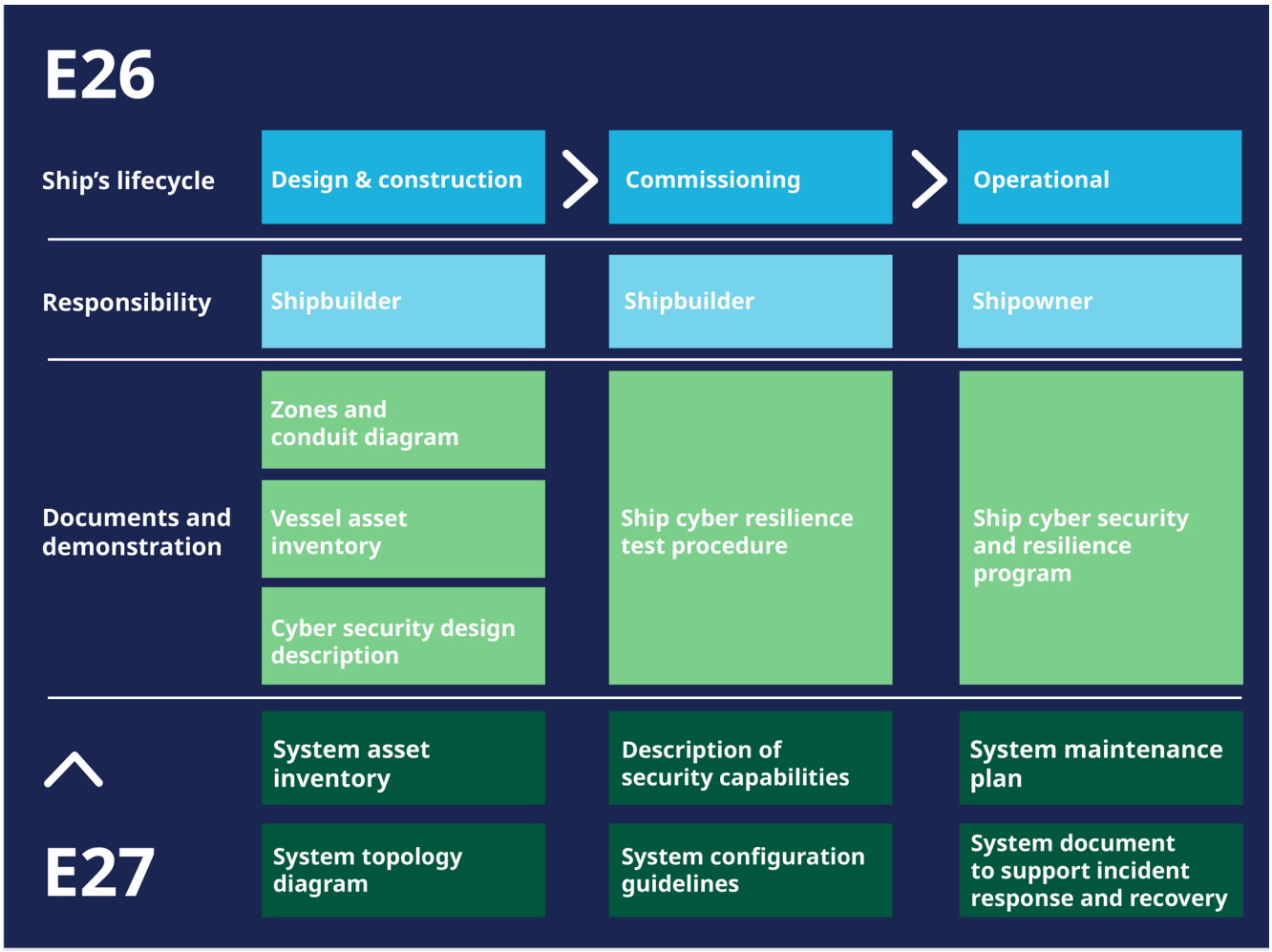

Figure 1. IACS E26 and E27 model overview

3. What is the top level cybersecurity approach of an Aperio system?

Aperio uses a multilayer security paradigm based on 'zero trust' concepts. The first layer protects the entire solution and anything inside. This zone is called Security Zone. See Figure 2 and Figure 3 for a graphical representation.

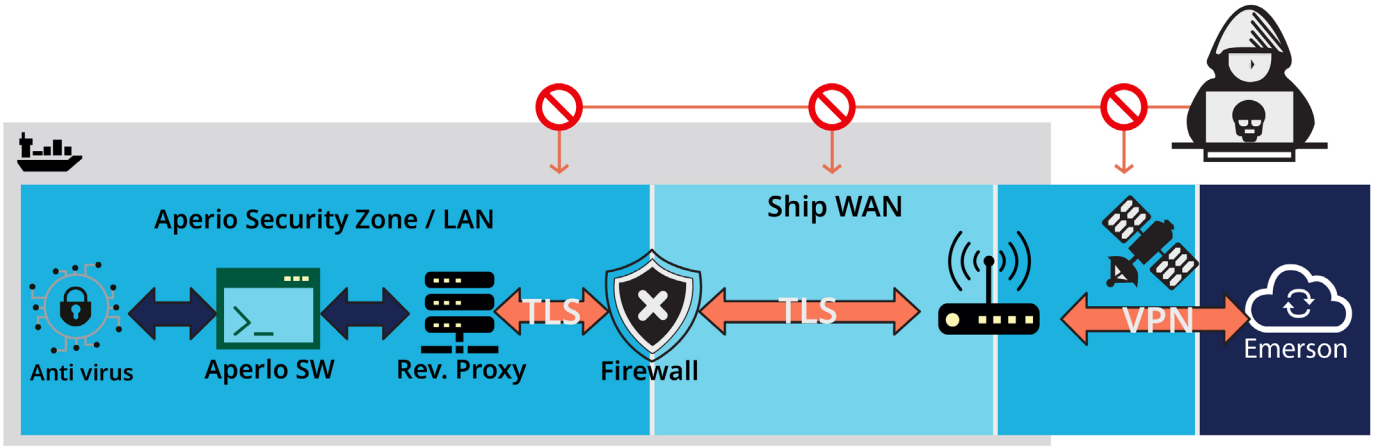

Figure 2. Aperio multilayered Security Model

The Aperio Firewall

The Aperio firewall components are responsible for segregating and protecting the Aperio system Security Zone and the firewall has four main functions:

- **Switch**: Allows for IP routing and segregating the internal LAN vs the exterior WAN (outside Security Zone)
- **Firewall**: Enforces various firewall rules, protecting internal endpoints, etc.
- **Manage**: Enables the component to be updated and restored.
- **NTP Client/Server**: Synchronizes all internal component times, enabling the Aperio system to get its time from a central NTP server on the ship.

Reverse Proxy

All controllers inside the Aperio Security Zone are set up with a reverse proxy which delivers several important functions.

- Protects internal IP/port traffic between components inside the Security Zone
- Encrypts all communication to the outside of the Security Zone using a TLS certificate.
- Validates X509 certificates which can be used to authenticate connections to IPs outside the Security Zone. This is an optional function.

Code Signing

All software components (applications, firmware, configuration, etc.) deployed to the system are both encrypted and code signed which ensures that the software cannot be altered and that it originates from the Aperio software team.

User Authentication

The Aperio system deploys and OIDC compliant user authentication and authorization scheme which is enforced in all user interactions with the Aperio system.

Threat Monitoring and Detection

In the unlikely scenario that a threat actor can get inside the Aperio Security Zone, there are measures in place to identify and log suspicious events using antivirus software and other monitoring services.

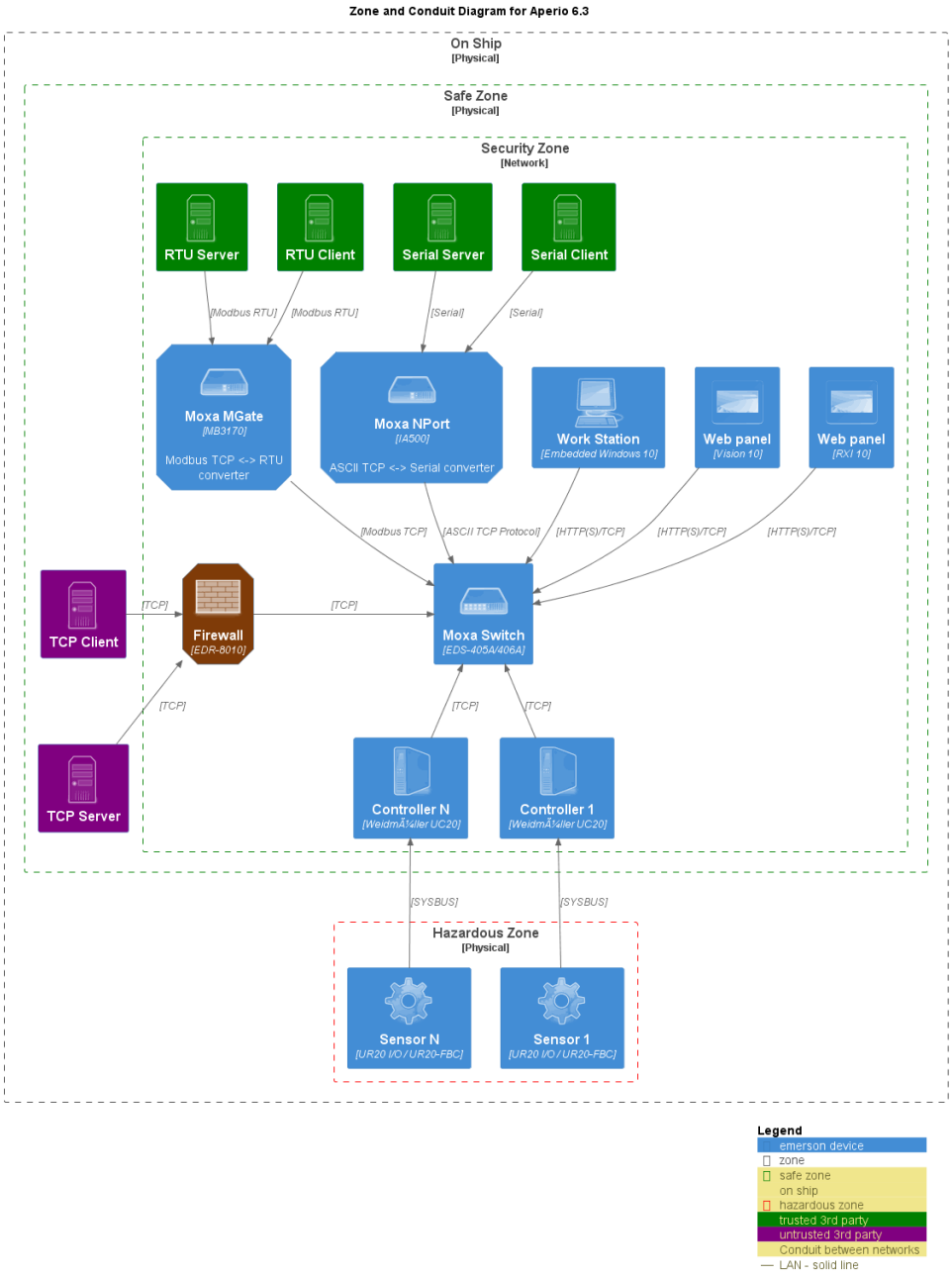

Figure 3. Aperio top-level System Layout

4. How does Aperio secure Remote Connections?

As described above, Aperio applies a 'zero trust' model which treats all IP communication with any computer outside the Security Zone as 'remote.' The Aperio E27 certificate will encompass components inside the Aperio Security Zone. However, in most implementations the E27 certificate is needed to connect the Aperio system with computers elsewhere on the ship or remote (off ship) computers. This is also why the Aperio system always includes a central firewall (see figure 2 on page 6).

For connection to a computer off a ship, Emerson recommends installing a VPN/router for example a Secomea box connected to a WAN port on the Aperio firewall. The VPN/router has its own (TLS / VPN) solution in place to ensure the remote connection is encrypted and terminates with a known computer/server (i.e., the VPN/router gateway server). Internet connection to the VPN/router can be made via the ship's satellite system or via a dedicated modem solution.

5. How does Aperio manage users and passwords?

Aperio employs a role-based user management solution based on the OAuth2/OIDC standard. To access secure functions from any Aperio Human Machine Interface (HMI), users need to log in from either an Aperio workstation or an Aperio web app. The login process requires users to be authenticated with a username and a password.

Each user is assigned a role, which defines their authorizations. Adding or modifying users is done on the ship with the Maintenance Manager app. Access within the Maintenance Manager app depends on the user's role. The Maintenance Manager app can also be used to log users out or completely disable them.

To modify an installed Aperio system, an Emerson engineering workstation needs to be physically connected to the system. Aperio Engineering workstations are authenticated towards the onboard Aperio system using public/private keys and the engineering workstation itself can only be accessed by an authorized and authenticated Emerson service engineer.

6. How does Aperio handle secure SW updates?

By default, only an Aperio engineering workstation can connect to and trigger updating of software components on an installed system. An Aperio engineering workstation could connect from a remote service location via the VPN/router option.

To update software to an Aperio system users must first access an authenticated endpoint and once authenticated, download the new software. Aperio software is always both encrypted and code signed and the first thing the Aperio system does after it has received new software is to check its encryption and code signatures.

The actual deployment of software packages is done locally on the controllers after the software updates have been downloaded and validated. If a software update process fails, the Aperio system will roll back to the previously installed version.

7. How does Aperio handle restoring system components?

Only Aperio engineering workstations, which save all ship installation and configuration data in project archives on a secure backend server, can fully restore a complete system.
For restoring individual system components on a ship, the Aperio system keeps backups of all installed components and can use the backups to restore any managed component in the Aperio system. For security reasons, all application backups are not file-copies but are copies of the original installation files. This means that if an application is hacked, it will not be copied to the backup and when the system is restored the original app is re-installed.

Emerson's aim is to enable ship crews to restore most Aperio system components locally. However, restoration of critical Aperio system components often requires a full system diagnostics/test that typically needs to be performed by an Emerson service engineer due to complexity and for cybersecurity reasons.

8. How does Aperio security handle web applications?

The Aperio system hosts several web applications which can be accessed internally (from inside the Security Zone) or externally (from outside the Security Zone). No sensitive information is stored in the Web Apps themselves.

Data encryption
All data between web app and central security zone is encrypted with TLS certificate.

User Authentication
Even if a web app is properly authenticated, users still need to be separately authenticated using username and password. A logged-in user is given a set of permissions based on the assigned role for that user. Permissions determine which system services users can access regardless of which Aperio web app the user is using.

Firewall and Reverse Proxy
All Aperio web apps communicate with a specific set of Aperio endpoints which are protected behind both a firewall (if the web app is called from outside the Security Zone) and a reverse proxy. As such, each Aperio endpoint is protected with both user-role authentication and various guardrails provided by the firewall and reverse proxy components.

9. How does Aperio handle cybersecurity incidents?

Aperio System Security Backlog

The Aperio System has a robust task and bug management system and utilizes an IEC-62443 compliant DevOps process (see Figure 4). All bugs are registered based on severity and impact and some bugs require an (unplanned) patch release. When releasing both full releases and patch releases, release notes explain the changes and fixes and any special instructions. As with a bug, a cybersecurity threat is registered and evaluated in terms of risk and impact and entered the general release planning process.

Because of the strong protection of the Aperio Security Zone, most identified cybersecurity risks will be mitigated when the system software is updated the next time an Emerson service engineer is on site. In the rare case of a critical cybersecurity threat, the fix can be deployed remotely but in close cooperation with the ship owner.

Backoffice Threats

The Aperio system is part of Emerson's Product Security Incident Response Team (PSIRT) scope. This is important because Emerson deploys a multitude of devices across many industries and continuously monitors threats across a very large industrial automation base. When a PSIRT incident is received, the Aperio team evaluates whether the threat affects any components of an Aperio system. If so, the threat is reported back to the Emerson central PSIRT system and it is added to the backlog.

The Aperio DevOps process also includes its own cybersecurity tests and if any threats are identified, they are added to the backlog.

Network Threats

The Aperio system network is built to withstand most cybersecurity-related threats, like network traffic flooding and other attacks. The firewalls protecting the Security Zone also have multiple mechanisms in place to mitigate various network attacks, like DoS attacks. All controllers feature a two-layer defense that is achieved by deploying a robust reverse proxy, which is also set up with various protection mechanisms, like IP endpoint rate limiting.

Security Zone Threats

While the Aperio system relies heavily on strong boundary protection, threats might make it through. Therefore, all computer/controller devices run their own threat detection and isolation (antivirus) solutions. If an internal threat is identified it will be logged and communicated in an alert.

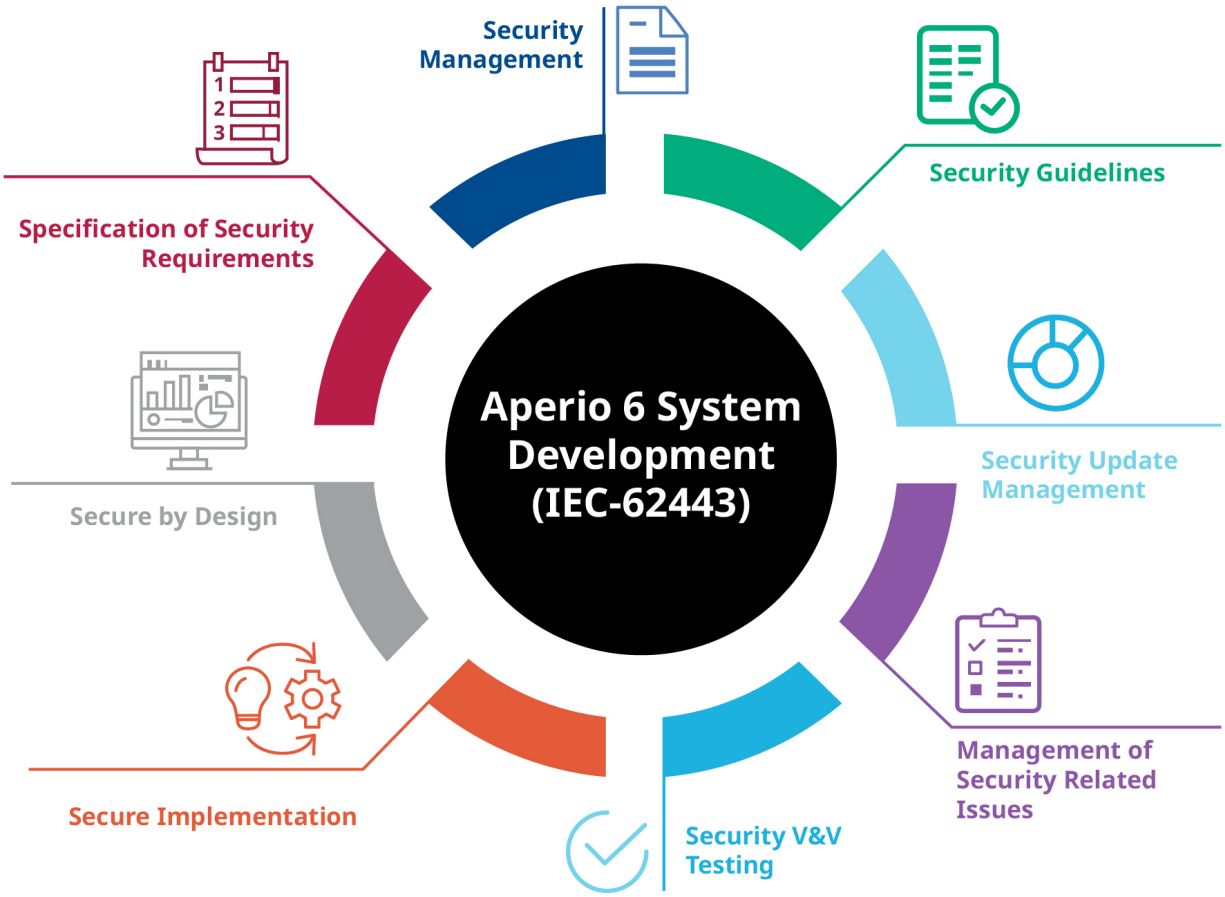

Figure 4. Aperio Software Development according to IEC62443 standards

For additional information, visit:
Emerson.com/marine

00870-0200-2827 Rev AA, January 2025