zenitel

EXIGO PAGA SYSTEM

Navigating Cyber Threats in Maritime Operations

Cyber-Approved Critical Communication Solution Reliable. Cyber-resilient. Future-ready.

www.zenitel.com

Digitalization at Sea — Great Opportunities, New Cyber Challenges

The technologies driving operational efficiency, improving crew routines, and enhancing safety and well-being onboard are becoming increasingly complex.

The adoption of IoT, OT, advanced data analytics, AI, and machine learning unlocks new possibilities across the maritime industry. At the same time, the cyber threat landscape is evolving — and maritime stakeholders are firmly in the sights of cybercriminals.

According to a DNV survey:

- **31%** of maritime professionals experienced one or more cyberattacks in the 12 months leading up to October 2024
- **37%** believe cyber threats will only continue to grow in scale and complexity

EXIGO PAGA System — Cyber Approved

- Fully Compliant with DNV rules – Pt.6 Ch.5 Sec.21 Cyber Security Profile level 1 (SP1)
- Compliant with IACS Unified Requirement E27 for cybersecurity in onboard systems

For all stakeholders, this calls for a system-level approach to cybersecurity — one that ensures protection against both current and future threats.

DNV Cyber Security Type Approval — Clear Benefits for Maritime Stakeholders

- Full compliance with IACS UR E27 requirements
- Easy and fast integration into projects that require cybersecurity-certified systems
- Simplified planning and documentation processes
- Assurance of a high level of protection against advanced, modern cyber threats

At Zenitel, we have a deep understanding of the needs of maritime customers — and we continuously evolve our practices to meet them.

That's why cybersecurity is embedded at the core of our critical communication systems.

Our goal is to deliver reliable, high-performance solutions where protection against cyber threats never compromises availability, integration capabilities, or ease of use.

www.zenitel.com

Deep-Level Protection

Effectively countering today's advanced cyber threats requires all stakeholders in the maritime industry to join forces in ensuring reliable and consistent protection of onboard digital systems.

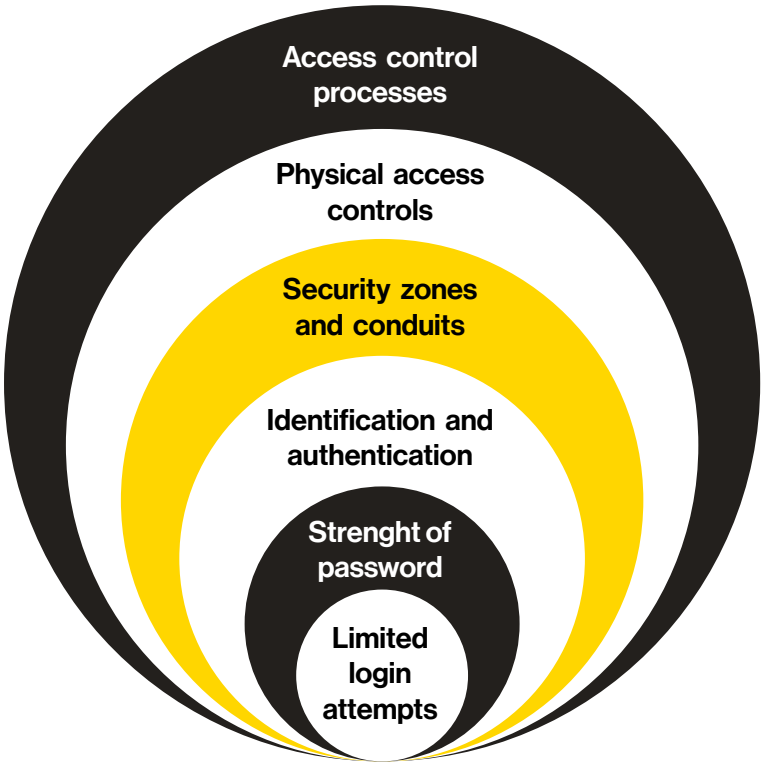
That's why the IACS Unified Requirements on Cyber Security apply not only to suppliers (as outlined in UR E27), but also to yards, designers, and owners (under UR E26), setting standards for all safety-related systems including communication systems.

As a supplier, we ensure that the EXIGO PAGA System complies with the following requirements:

- Security capabilities based on IEC 62443-3-3
- System hardening
- Configuration of security features
- Secure development lifecycle processes

A multi-layered approach to protecting onboard communication systems from cybercriminals includes:

- Access control policies
- Physical access controls
- Network segmentation
- Identification and authentication
- Password strength
- Limited login attempts



What Effective Cybersecurity Means in Practice

As cybercriminal tools continue to evolve and become more sophisticated, building a reliable “shield” against threats becomes an ongoing process-one focused on protecting every layer that could potentially be targeted by a cyberattack.

A multi-layered cybersecurity approach that ensures cyber resilience includes:

Ship Owners

Developing and implementing effective physical and procedural barriers to protect vessel systems

Shipyards

Ensuring network security and safeguarding connections between zones and systems with remote access

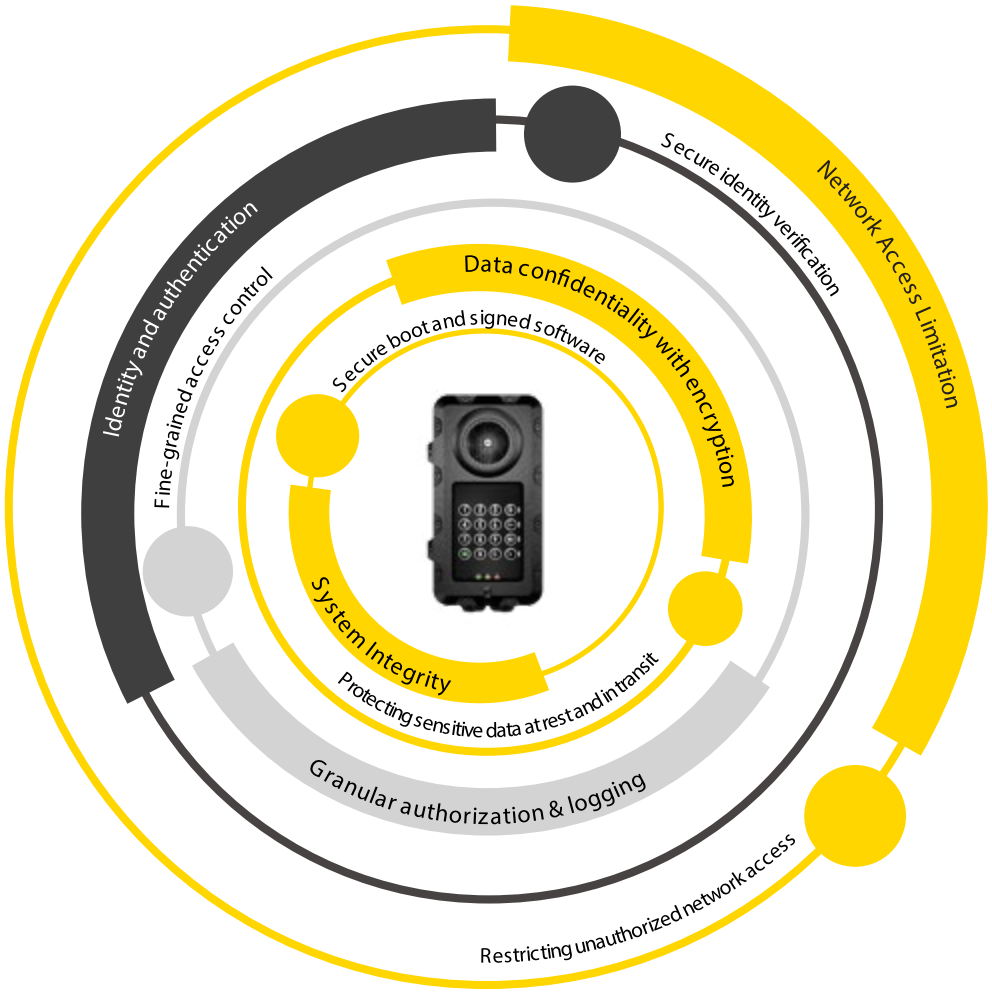
Suppliers

Designing products with built-in system security, including encryption, removable device control, user access and authentication, event logging, backup, and recovery

Zenitel's Approach:
Focused on Cyber Resilience and Multi-Layered Defense

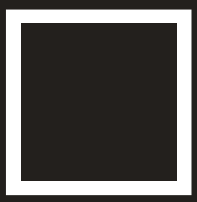
Cybersecurity on board is no longer optional. As of July 1st, 2024, IACS UR E27 sets mandatory cybersecurity requirements for onboard systems. The goal is clear: to ensure that vendors secure and reinforce the integrity of onboard systems with a strong focus on cyber resilience.

In this new regulatory environment, DNV's Cyber Security Type Approval becomes a critical assurance of digital system reliability at sea. It confirms that the equipment meets specific cybersecurity standards, helps reduce the risk of cyberattacks, and simplifies the certification process for vessels.



zenitel

Explore EXIGO PAGA system's cyber security resilience



- System "Remote Control" via VPN
- Training
- 24/7 Service
- Service agreements
- Type-approved systems
- Innovative technology
- Monitoring of system solution with follow-up on sailing ships
- Spare parts policy
- Extended warranty terms
- Crew training program

WHY ZENITEL?

You need systems that work. Every time. We provide reliable and resilient integrated communication solutions. We understand that the safety and efficiency of your most valuable resource – your employees – is key to your success.

We're specialists in the maritime and energy segments: we know the ocean industry, and we speak your language. Our innovative solutions for critical and intelligent communication deliver reliable performance in all conditions. We also understand your need to safeguard your assets, whether it is an ocean-going vessel or an energy plant. That's why we offer integrated communication solutions that enable seamless information sharing, so you can make better decisions more quickly.

Our systems and solutions provide high availability, scalability, reliability, maintainability and cyber defensibility. Our flexible and innovative solutions for intelligent communication, data, safety and entertainment systems deliver reliable performance in all conditions.

A100K12124 20.09.2021

www.zenitel.com | maritime@zenitel.com