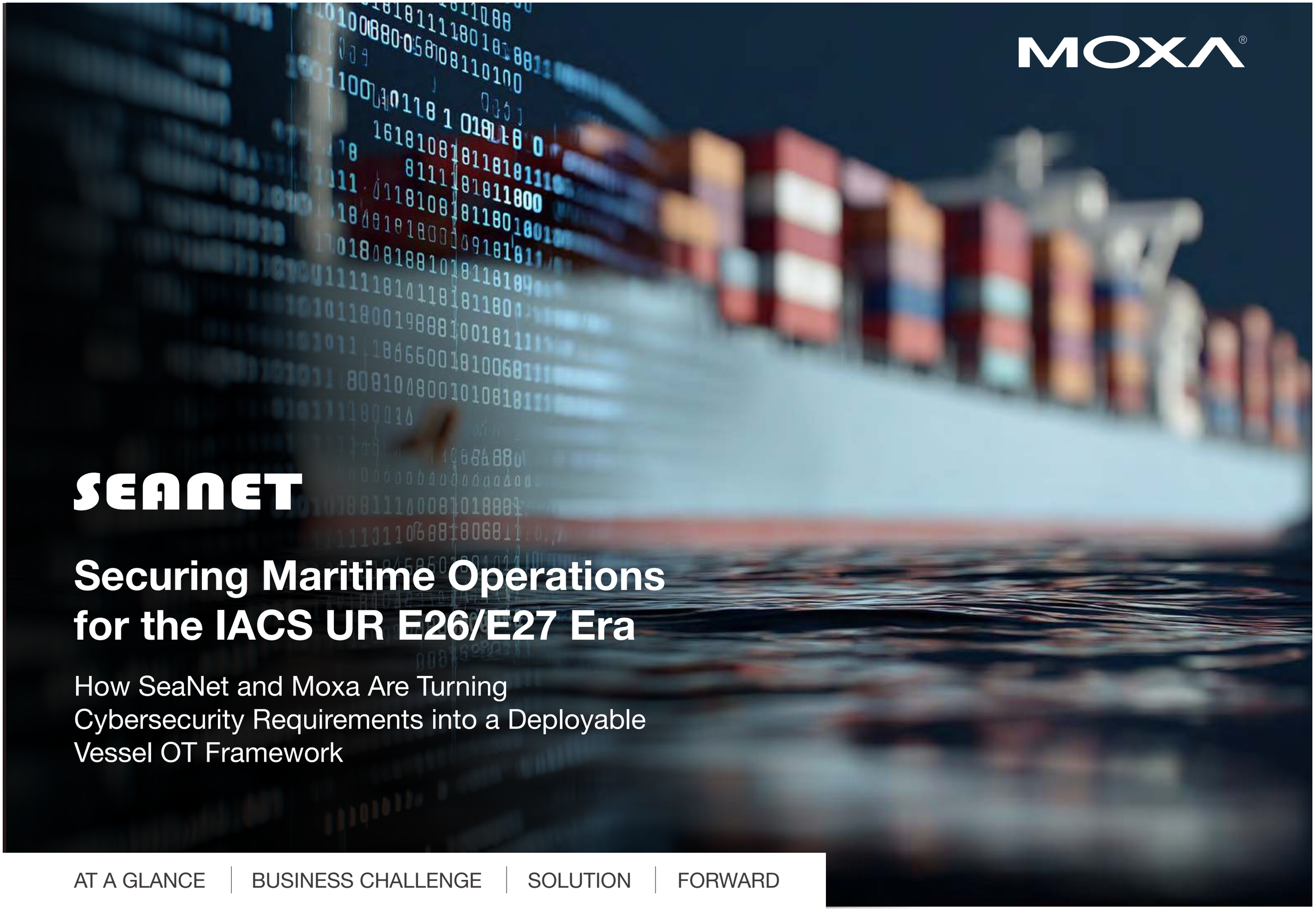


SEANET

Securing Maritime Operations for the IACS UR E26/E27 Era

How SeaNet and Moxa Are Turning Cybersecurity Requirements into a Deployable Vessel OT Framework

AT A GLANCE | BUSINESS CHALLENGE | SOLUTION | FORWARD

AT A GLANCE

Why Maritime Cyber-resilience Must Be Designed In

As digitalization reshapes the maritime industry, modern vessels are becoming highly connected operational platforms where navigation, propulsion, cargo management, safety, and onboard automation depend on continuous communication across operational technology (OT) networks. While this connectivity improves operational efficiency, it also expands the cyberattack surface, making cybersecurity a fundamental requirement for safe and reliable vessel operations rather than simply an IT consideration.

Recognizing this shift, the International Association of Classification Societies (IACS) introduced Unified Requirements E26 (Ship Cyber Resilience) and E27 (Cyber Resilience of On-board Systems and Equipment), which became mandatory for all newly contracted vessels from July 2024. These requirements represent a pivotal milestone for the maritime industry, requiring cybersecurity to be designed into vessel architectures from the outset and verified through classification society approval.

Meeting these new requirements demands far more than just deploying security appliances. Shipbuilders, system integrators, and vessel owners need a comprehensive strategy that combines risk assessment, OT network segmentation, continuous monitoring, and life-cycle security management.

Delivering that strategy requires both deep maritime integration expertise and proven OT networking and cybersecurity technologies—capabilities SeaNet and Moxa bring together to translate evolving cybersecurity requirements into practical vessel architectures.

AT A GLANCE

SeaNet is a Korea-based maritime system integrator with deep roots in ship navigation and communication. Building on its experience in vessel system integration, engineering, commissioning, and onboard services, SeaNet has expanded its capabilities into smart-ship solutions and maritime cybersecurity. Through its **SEATALK**, **SEES**, and **SEACURE** portfolios, SeaNet aims to connect, digitalize, and secure increasingly complex vessel operations while helping shipbuilders, shipowners, and system suppliers address evolving operational and cybersecurity requirements.

Against this backdrop, SeaNet is working with Moxa to translate maritime cybersecurity requirements into an integrated vessel OT design. SeaNet leads the maritime cybersecurity design, system integration, documentation, project coordination, and onboard verification/demonstration, while Moxa contributes industrial networking, OT cybersecurity technology, training, and technical support.

Together, the two companies are building an architecture designed to support IACS UR E26/E27 objectives and future vessel programs. The collaboration combines SeaNet's maritime execution experience with Moxa's industrial networking and OT security expertise, with an emphasis on a reliable and deployable onboard solution.





SEANET

SeaNet Co., Ltd

- **Founded in** ▸ 2008
- **Headquarter** ▸ Busan, Republic of Korea
- **Industry** ▸ Marine
- **Website** ▸ https://en.sea-net.co.kr/

BUSINESS CHALLENGE



Transforming Regulatory Requirements into Operational Cyber-resilience

The introduction of IACS UR E26 and E27 marks one of the most significant changes to maritime vessel design in recent decades. Rather than treating cybersecurity as an isolated technical function, shipbuilders must now integrate cyber-resilience into every phase of vessel design, construction, commissioning, and operation.

Navigating Diverse Classification Society Requirements

Although IACS provides a unified cybersecurity framework, classification societies may apply their own certification methodologies, documentation requirements, and technical interpretations. Preparing for approval therefore requires more than regulatory knowledge; it demands practical expertise in cybersecurity architecture, compliance planning, and system integration.

Securing Mission-critical OT Networks Without Compromising Operations

Unlike conventional IT environments, shipboard OT networks support mission-critical functions where reliability and continuous availability are essential. Cybersecurity controls must strengthen protection without increasing operational complexity, disrupting deterministic communications, or consuming valuable onboard space.

Achieving Actionable OT Visibility

Modern vessels integrate numerous OT subsystems across navigation, machinery control, propulsion, safety, and auxiliary operations. Without centralized visibility, crews face significant challenges in identifying abnormal traffic, detecting cyberthreats, and maintaining situational awareness. Real-time network visibility has therefore become a cornerstone of both operational resilience and regulatory compliance.

Complementary Expertise Built on a Long-term Partnership

SeaNet brings deep maritime domain knowledge, cybersecurity architecture expertise, system integration capabilities, and experience working with shipbuilders and classification societies. Moxa complements these strengths with industrial networking, OT cybersecurity technologies, network visibility, and technical expertise developed for mission-critical operational environments.

This partnership is also grounded in long-term collaboration. Through continued technical exchanges, joint project discussions, and close engagement between both teams, SeaNet has developed confidence not only in Moxa's products, but also in the people and technical support behind them.





From Requirements to a Deployable Onboard Architecture

This combination allows SeaNet to focus on designing and integrating the overall maritime cybersecurity solution while leveraging Moxa's industrial networking and security technologies to make the architecture reliable and deployable onboard.

SeaNet integrates Moxa's products into a complete solution and leads customer projects. Moxa supports SeaNet with technology, products, training, and project expertise as both companies work together to address target applications and expand maritime cybersecurity opportunities.

SOLUTION

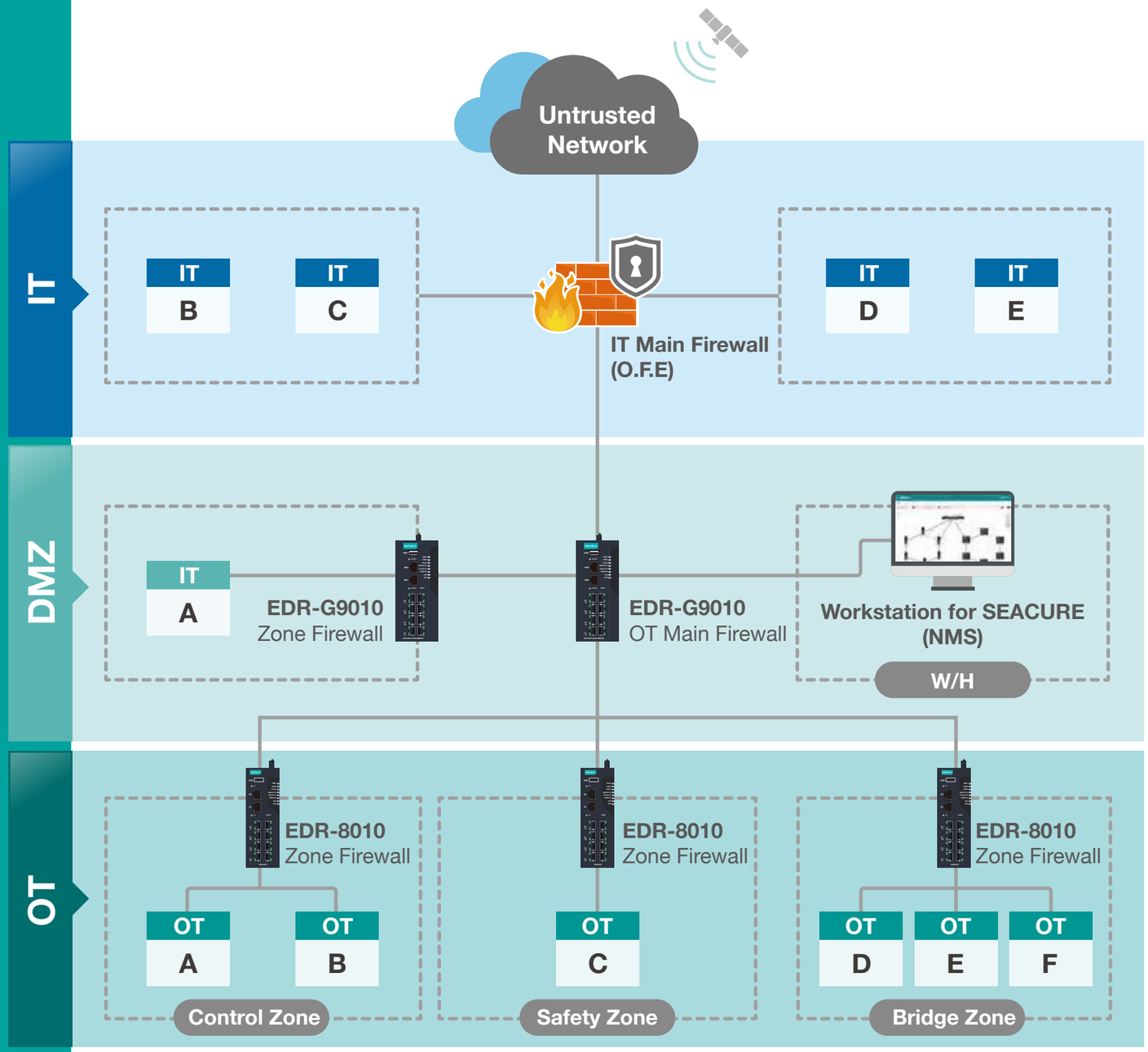
Designing a Cybersecurity Architecture Built for Maritime OT

Based on a comprehensive cybersecurity risk assessment, SeaNet's defense-in-depth cybersecurity architecture follows IEC 62443 zone-and-conduit principles to support IACS UR E26/E27 objectives. Moxa helps implement this design with industrial networking and security solutions, together with technical expertise in secure OT communications, network segmentation, and centralized network visibility.

Rather than protecting individual devices separately, this solution secures the vessel as an integrated operational system by identifying critical assets, segmenting OT networks according to operational function and risk level, and enforcing security policies between each security zone.

Establishing a Secure OT Perimeter

The Moxa EDR-G9010 Series industrial secure routers serve as the primary security gateways between the vessel's IT and OT networks. Acting as the first line of defense, they centrally enforce security policies while using integrated firewall, intrusion prevention (IPS), and intrusion detection (IDS) capabilities to inspect network traffic, identify abnormal behavior, and block potential cyberthreats before they reach mission-critical systems.



Looking ahead, SeaNet emphasizes the value of combining maritime application expertise with dependable OT technology and long-term technical collaboration.



> ***As IACS UR E26/E27 requirements become increasingly important, practical OT visibility and centralized monitoring are becoming essential elements of maritime cybersecurity. By combining SeaNet's maritime expertise with Moxa's industrial networking and OT security capabilities, we are building a practical architecture designed to support the evolving needs of shipbuilders and vessel operators.***
>
> **Mr. Ok Dong-Won**
> Cybersecurity Team Lead, SeaNet

Protecting Critical Operational Zones

Within the OT network, Moxa EDR-8010 Series industrial secure routers provide dedicated protection for critical operational zones, including navigation, control, and safety systems. Through network segmentation and allowlist-based protocol enforcement, each zone remains securely isolated, preventing cyberincidents from propagating laterally while ensuring uninterrupted communication for authorized industrial traffic.

Delivering Real-time OT Visibility

Complementing the secure networking infrastructure, SeaNet's SEACURE platform—built on Moxa's MXview One industrial network management platform—provides centralized visibility across the vessel's OT environment. Operators can monitor network topology, equipment health, traffic conditions, and cybersecurity events through a unified management interface, enabling faster anomaly detection, simplified troubleshooting, and more proactive cybersecurity management throughout the vessel's operational life cycle.

These capabilities establish a resilient cybersecurity foundation designed to support regulatory objectives and increasingly connected maritime operations.

Building a Foundation for Future Vessel Programs

By combining SeaNet's maritime cybersecurity and system integration expertise with Moxa's industrial networking and OT security technologies, this collaboration is translating IACS UR E26/E27 objectives into a deployable framework for vessel OT environments. The architecture is intended to provide a repeatable reference for future shipbuilding projects as the industry adapts to new cybersecurity requirements. Its defense-in-depth design brings together network segmentation, centralized policy enforcement, and OT visibility. This foundation is designed to help crews identify abnormal conditions more quickly and support cybersecurity management throughout the vessel life cycle.

The work reflects a shared long-term commitment: SeaNet will continue applying its maritime domain and integration expertise, while Moxa will continue contributing through industrial networking, OT cybersecurity technology, training, and project support to help shipbuilders and vessel operators build more connected and cyber-resilient operations.

© 2026 Moxa Inc. All rights reserved.
The Moxa logo is a registered trademark of Moxa Inc. All other logos appearing in this document are the intellectual property of the respective company, product, organization associated with the logo.

LEARN MORE →

MOXA®