FORTINET | ASi AQUASYNC INNOVATION
YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

AQUASYNC INNOVATION(SINGAPORE) PTE. LTD.

Address: 8 Temasek Boulevard #11-01.Suntec city Tower 3, Singapore 038988

E-mail: sales@aquasync.sg **Website:** www.aquasync-marine.com

ASi

SHIP CYBERSECURITY SOLUTION

Made available for
UR E27 (Rev.1) Cyber resilience of on-board systems and equipment
UR E26 (Rev.1) Cyber resilience of ships

DNV ABS Lloyd's Register CCS KR KOREAN REGISTER RINA ClassNK

Content.

SHIP CYBERSECURITY SOLUTION

AQUASYNC INNOVATION
YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

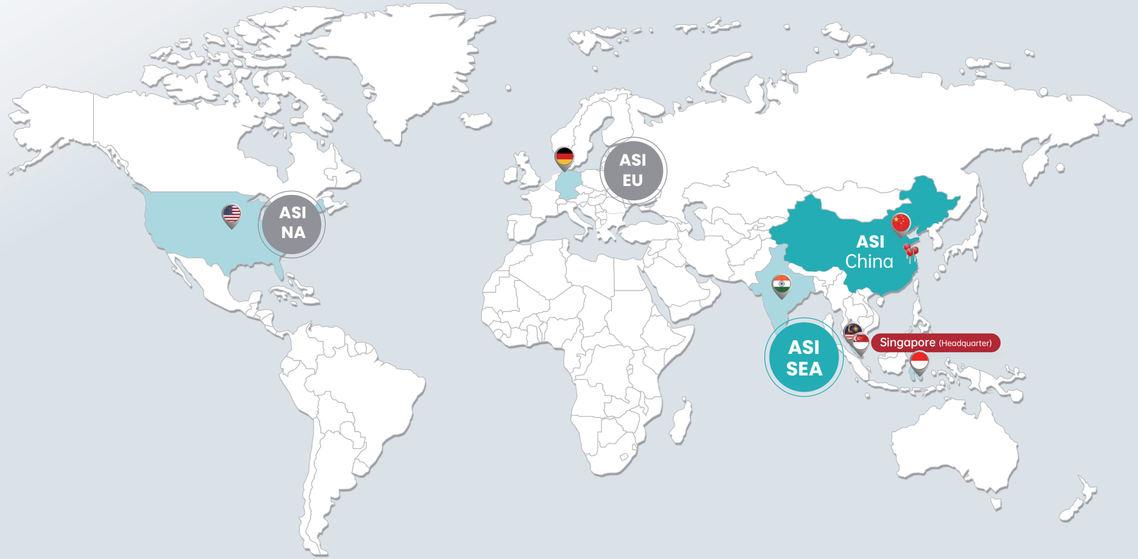
1.1 Company Profile

AquaSync Innovation (hereinafter referred to as ASI) provides a full package of solutions for comprehensive automation, intelligence, integrated ship-shore information and ship cyber security etc. in marine and offshore industries through cutting-edge technology, empowers the global maritime industry. Our advanced solutions ensure safe, reliable, efficient performance and promote the rapid sustainable development of the maritime industry's digitalization process.

ASI has obtained the **DNV-issued ISO 9001** Quality Management System, **ISO/IEC 27001** Information Security Management System, **ISO/IEC 20000-1** Information Technology Service Management System certificates, and the **ISO/IEC 17025** Marine Cybersecurity Laboratory Test Capability Recognition.

- Integrated Gauging Monitoring-Alarm and Controlling System
- Informatization Integrated Solution
- Intelligent ship system
- Ship-Shore Fleet Management System
- **Ship Cybersecurity Solutions**
- Sensor Transmitters, Valves, Flow Meters and Other Underlying Hardware

Global Presence & Headquarters Map



ASI China
- Hangzhou, Zhejiang
- Wuxi, Jiangsu Province
- Shanghai

ASI SEA
- Singapore
- India
- Indonesia
- Malaysia

ASI EU
- Germany, Hamburg

ASI NA
- America

PART TWO

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

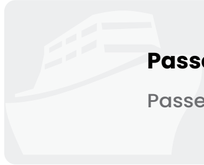
Interpretation of Ship Cybersecurity Standards

IACS UR E26&E27

	IACS UR E26 (Ship Cyber Resilience)	IACS UR E27 (On-Board Systems Cyber Resilience)
Scope	Whole-Ship Cyber Resilience (Ship Level)	Individual CBS Certification (System & Equipment Level)
Core Objective	Secure and Dependable Maritime Transport	CBS & Equipments
Key Requirements	① Identify ② Protect ③ Detect ④ Respond ⑤ Recover	① Identification and Authentication ② Access Control ③ System Integrity ④ Data Confidentiality ⑤ Restricted Data Flow ⑥ Timely Response to Events ⑦ Resource Availability
Certifications	- ISO/IEC 17025(DNV&CNAS) - ISO/IEC 27001 :2022 - Personnel： CISSP - ISO/IEC 20000-1:2018	- IEC 62443-4-1 & 4-2 & 2-4 - ISO/IEC 27001 :2022 - IACS UR E10 - ISO/IEC 20000-1:2018
Testing Requirements	Whole-Ship Cyber Resilience Testing	Individual Equipment Functionality & Security Testing
Deliverables	- Approved supplier documentation - Zones and conduit diagram - Cyber security design description - Vessel asset inventory - Risk assessment for the exclusion of CBSs - Description of compensating countermeasures - Ship cyber resilience test procedure - Ship cyber security and resilience program	- CBS Asset Inventory - Topology Diagrams - Description of Security Capabilities - Test Procedure for Security Capabilities - Security Configuration Guidelines - Secure Development Lifecycle - Plans for Maintenance and Verification - Information Supporting Incident Response and Recovery Plans - Management of Change Plan - Test Reports

" Effective Period: Ships Contracted for Construction on or After 1 July 2024."

Applicable Ship Types



Passenger Ships

All Tonnages

Passenger ships engaged in international voyages (Including high-speed passenger ships).

Mobile Offshore Drilling Units

500 GT+

Mobile offshore drilling units with a gross tonnage of 500 GT or more.

Cargo & High-Speed Vessels

500 GT+

Cargo ships of 500 GT or more engaged in international voyages & High-speed vessels of 500 GT or more engaged in international voyages.

Self-Propelled Construction Units

Specialized Units

Self-propelled offshore construction units (such as those for wind turbine installation and maintenance, crane units, drilling tenders, accommodation units, etc.)

Main Classification Society Registration Symbols

China Classification Society（CCS）

The Additional Notation for Ship Cybersecurity.	The Ship Cyber Resilience Level.	
	Ship-Level	CBS-Level
M	Compliant With Cyber Risk Management.	-
P	SL0 (Corresponding to IACS UR E26).	SL0 (Corresponding to IACS UR E27).
S	SL1	SL1
	SL2	SL2
	SL3	SL3
	SL4	SL4

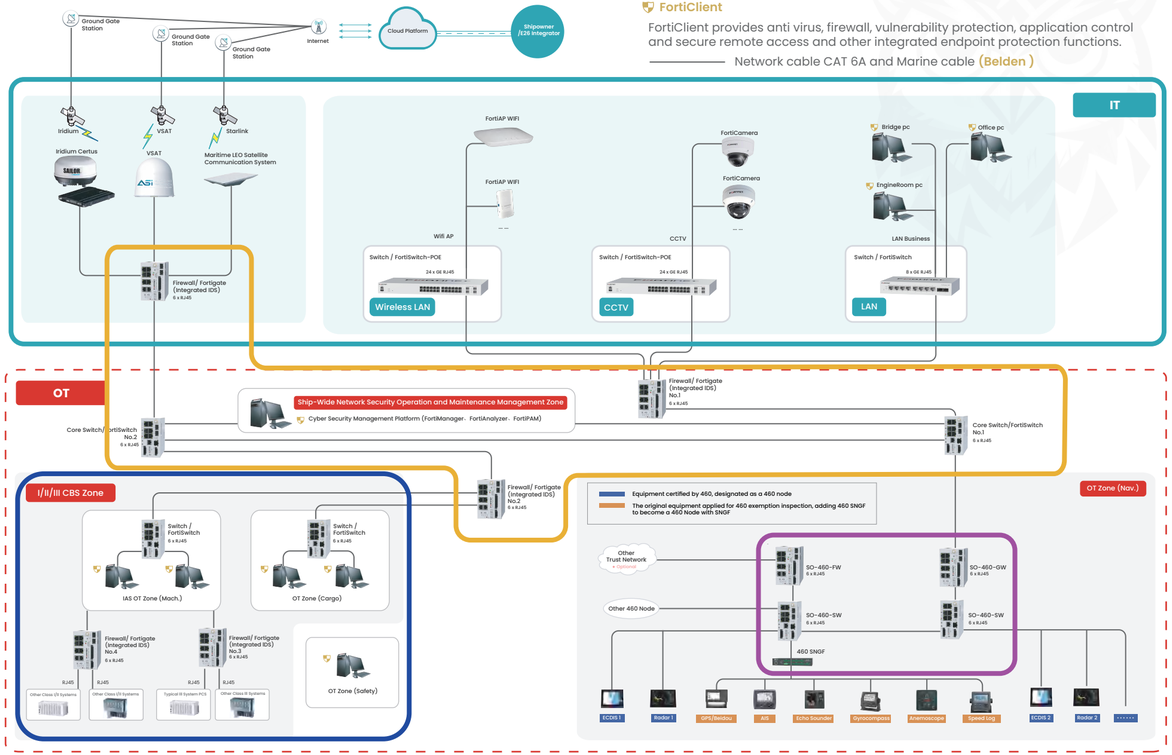
Det Norske Veritas（DNV）

Class Notation (Default Suc)	Security Profile	Class Notation (Additional Systems)
Cyber Secure	SP0	(+)
Cyber Secure (Essential) (Corresponding to IACS UR E26 & E27).	SP1	
	SP2	
Cyber Secure (Advanced)	SP3	
	SP4	

PART THREE

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

Ship Cybersecurity (IT+OT) Solution

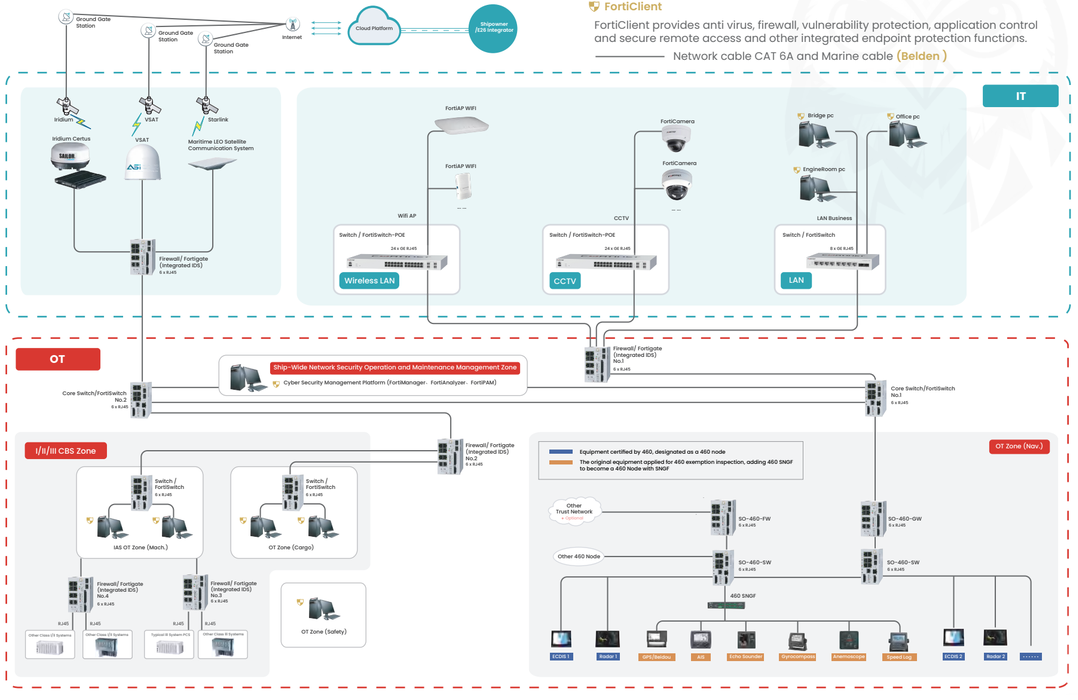


FortiClient

FortiClient provides anti virus, firewall, vulnerability protection, application control and secure remote access and other integrated endpoint protection functions.

Network cable CAT 6A and Marine cable (Belden)

Ship Cybersecurity (IT+OT) Solution



IT Cabinet

01 Switch (Fortinet)
02 VSAT Antenna Adapter (ASI)
03 LEO Satellite Power Supply Unit (Starlink)
04 VSAT billing gateway (ASI)
05 Video Compression Module (ASI)
06 PDU (ASI)
07 NVR (ASI)
08 UPS (Eaton)
09 Switch-POE (Fortinet)
10 Waterproof PoE Extender (ASI)
11 Firewall (Fortinet)
12 Switch Power Supply Unit (Weidmüller)
13 Terminal (Weidmüller)
14 Micro Circuit Breaker (Schneider)

Network cable CAT 6A and Marine cable (Belden)
Cabinet (Rittal)

Cybersecurity Cabinet

01 UPS (Eaton)
02 PDU (ASI)
03 460 SNGF (ASI)
04 Cybersecurity Management Platform (Fortinet)
05 KVM Control Platform (ASI)
06 SO-460-GW (Fortinet)
07 SO-460-SW (Fortinet)
08 SO-460-FWD (Fortinet)
09 Firewall (Integrated IDS) (Fortinet)
10 Core Switch (Fortinet)
11 Switch (Fortinet)
12 Micro Circuit Breaker (Schneider)
13 Switch Power Supply Unit (Weidmüller)
14 Terminal (Weidmüller)

Network cable CAT 6A and Marine cable (Belden)
Cabinet (Rittal)

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

3

PART THREE

Core Objectives

Enhancing Ship Cyber Resilience

E26 Systems integrator treating ships as integrated cyber entities to ensure the secure integration of IT (Information Technology) and OT (Operational Technology) equipment and system throughout their lifecycle. This comprehensive approach safeguards against cyber threats while minimizing risks to personnel, the environment, and vessel safety.

Design	Construction	Commissioning	Operation
Security-first architecture planning	Secure implementation practices	Validation and testing protocols	Continuous monitoring and updates

Establishing a Unified Regulatory Framework

E26 Systems integrator providing mandatory cybersecurity baseline requirements for the global maritime industry, promoting accountability among stakeholders in both technical and managerial aspects.

Shipowners	Shipyards	CBS maker
Ensuring vessels comply with **E26 certification standards** and maintaining cybersecurity throughout vessel operations.	Incorporating comprehensive cybersecurity solutions into vessel designs from the ground up.	Delivering equipment and systems that meet **IEC 62443 standards** or **E27 specifications.**

According to the requirements of the "Guidelines for Ship Cybersecurity," the cybersecurity design for ship products must cover the five key elements of ship network risk management: **Identification, Protection, Detection, Response,** and **Recovery**. Additionally, the design should be systematically structured based on the product's cybersecurity classification.

Device Overview

Statistical time:June 1, 2025

Device Name	Function Product Introduction	Corresponding Specification Requirements										
		E26	E27	CCS	DNV	ABS	BV	RINA	KR	RS	LR	NK
Class Notation (E26)		Rev.1	Rev.1	2024 CyberSecurity (P[SL0])	2024 Cyber Secure (Essential)	2024 CR	2024 Cyber Resilient	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience
FortiClient	A ship terminal protection software integrating white list protection, virus detection, patch management, security baseline inspection, access control and peripheral control.	4.2.3 4.2.7	SR1.2 SR2.3 SR2.4 SR3.2 SR3.3 SR7.7	4.3.14.1 4.3.14.2 4.3.18.1 4.3.18.2 4.3.18.3	5.3.3 5.3.5	13.3.3 13.3.7	3.2.6.2.2 3.2.6.3.1 3.2.6.4 3.2.6.5 3.2.6.5.3.-d 3.2.6.8.1	4.3.4 4.3.8	2.402.3 2.402.7	2.2.2.3 2.2.2.7	2.16.5.c 2.16.5.h	5.4.3(3) 5.4.3(7)
Marine Network Firewall	It integrates traditional packet filtering, VPN, application and identity recognition, anti-virus, intrusion prevention, behavior management, application layer content security protection and other comprehensive security defense functions.	4.2.1 4.2.2 4.2.4 4.4.3	SR1.2 SR2.3 SR2.4 SR3.2 SR3.3 SR7.7	4.3.6.1 4.3.10.1 4.3.6.2 4.3.13.2 4.3.7.2 4.3.14.3 4.3.8.1 4.3.15.2 4.3.8.2 4.3.15.3	3.2.1 5.4.8 3.2.2 5.4.9 4.6.3 4.6.4 5.3.4	13.3.1 13.3.2	3.2.6.2.1 3.2.6.3.3 3.2.6.5.1 3.2.8.4	4 3 2 4 3 3 4.3.7	2.402.1 2.402.2 2.404.3 2.402.4 2.402.6	2.2.2.1 2.2.2.2 2.2.2.5 2.2.4.3	2.1.6.5.b	5.4.3(1) 5.4.3(4) 5.4.3(6) 5.4.5(3)
Marine Network Core Switch	Core switch designed for marine vessels, enabling high-speed, stable data transmission and ensuring secure, reliable communication in harsh maritime environments.	4.2.1 4.2.5 4.4.2	SR 2.11	4.3.5.4 4.3.17.1 4.3.5.5 4.3.17.3 4.3.7.1 4.3.18.4 4.3.7.3 4.3.21.7								
Cybersecurity Management Platform	Used for unified management of ship network security Device, including auditing logs, analyzing event behavior, and configuring device parameters uniformly.	4.1.1 4.2.6 4.3.1	SR1.1	4.3.2.1 4.3.15.4 4.3.2.2 4.3.15.5 4.3.5.1 4.3.16.1 4.3.13.1 4.3.23.1 4.3.13.3	5.4.9 5.4.12	13.1.1 13.7.3 13.3.6	3.2.5.2 3.2.6.5.3.f 3.2.6.7.3 5.2.4.1.3.23 5.4.7.1.1 6.2.7.3	422 4.3.7	2.401.1 2.402.6 2.403.1	2.2.1.1 2.2.2.6 2.2.3.1	2.16.4 2.16.5.f 2.16.5.g 2.16.5.h 2.16.6	5.4.4(2)

From 《E26 Cyber Resilience of Ships》 Rev.1

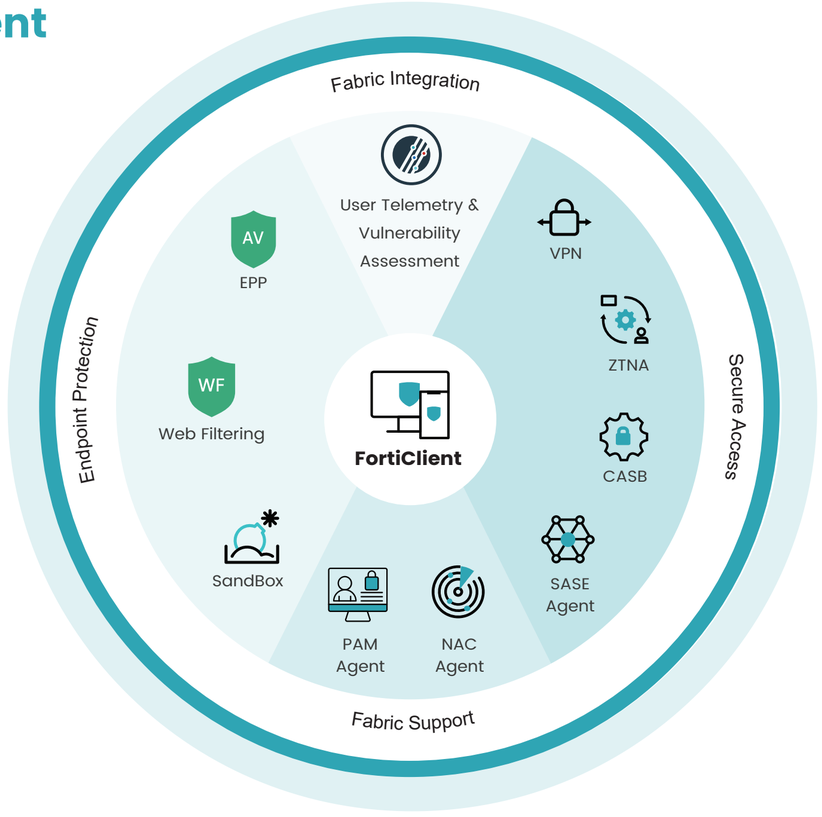
Document (E26)	Systems integrator			Shipowner			
	Design	Construction	Commissioning	Operation	1st AS	AS	SS
Approved Supplier Documentation [5]	Submit	Maintain	Maintain	Maintain			
Zones and Conduit Diagram [5.1.1]	Submit	Maintain	Maintain	Maintain			
Cybersecurity Design Description [5.1.2]	Submit	Maintain	Maintain	Maintain			
Vessel Asset Inventory [5.1.3]	Submit	Maintain	Maintain	Maintain			
Risk Assessment for the Exclusion of CBS [5.1.4] NOTE 1	Submit	Maintain	Maintain	Maintain			
Description of Compensating Countermeasures [5.1.5] NOTE 1	Submit	Maintain	Maintain	Maintain	Submit	Submit	Demonstrate
Ship Cyber Resilience Test Procedure [5.2.1]		Submit	Demonstrate	Maintain			
Ship Cybersecurity and Resilience Program [5.3.1] - Management of Change (Moc) [4.1.1.4.4] - Management of Software Updates [4.1.1.4.4] - Management of Firewalls [4.2.1.4.4] - Management of Malware Protection [4.2.3.4.4] - Management of Access Control [4.2.4.4.4] - Management of Confidential Information [4.2.4.4.41 - Management of Remote Access [4.2.6.4.4] - Management of Mobile and Portable Devices [4.2.7.4.4] - Detection of Security Anomalies [4.3.1.4.4] - Verification of Security Functions [4.3.2.4.4] - Incident Response Plans [4.4.1.4.4] - Recovery Plans [4.5.1.4.4]				Maintain	Submit	Demonstrate	

Fortinet meets the E26 functional requirements

Ship cybersecurity and resilience program [5.3.1]	FortiAnalyzer	FortiPAM	FortiManager	EMS	CyberR Platform
Management of change (MoC) [4.1.1.4.4]			✓		✓
Management of software updates [4.1.1.4.4]			✓		
Management of firewalls [4.2.1.4.4]	✓		✓		
Management of malware protection [4.2.3.4.4]				✓	
Management of access control [4.2.4.4.4]		✓	✓		
Management of confidential information [4.2.4.4.4]		✓			
Management of remote access [4.2.6.4.4]	✓	✓		✓	
Management of mobile and portable devices [4.2.7.4.4]				✓	
Detection of security anomalies [4.3.1.4.4]	✓				
Verification of security functions [4.3.2.4.4]					✓
Incident response plans [4.4.1.4.4]					✓
Recovery plans [4.5.1.4.4]					✓

Cybersecurity Management Platform Composed of FortiAnalyzer, FortiPAM, FortiManager, EMS, CyberR Platform.

FortiClient



Product Benefits

Security Integration
Deeply embedded in the security framework, automatically collects threat intelligence for early threat detection and automated response

Zero-Trust Access
Unified control of local/remote application access with continuous endpoint verification and dynamic permission adjustment

Unified Agent
Single lightweight agent supporting multiple security services, reducing endpoint load and management overhead

Network Control
Filters malicious websites and cloud application content, prevents phishing and botnet attacks

Vulnerability Management
Automatically scans endpoint vulnerabilities and integrates with security policies for automated remediation or isolation

Extended Advantages

Automated Patch Management

Centrally manages endpoint patches, supports offline devices, and ensures systems remain up-to-date with the latest security fixes.

Advanced Threat Protection

Integrates cloud sandboxing and global threat intelligence to analyze files in real time, blocking unknown malware and exploit attempts.

Ransomware Protection

Uses behavior-based detection to identify ransomware activity and allows one-click restoration of tampered files.

Flexible Licensing Models

Offers both device-based and user-based licensing to suit different enterprise procurement preferences.

Smart VPN Experience

Supports split tunneling to reduce latency, and includes auto-connect, multi-factor authentication, and other features that balance user experience and security.

Seamless Zero-Trust Transition

Combines VPN and zero-trust capabilities within the same agent, reducing the risk and complexity of migrating to a zero-trust architecture.

Extended Advantages

FortiGate Integration

Unified endpoint visibility
Real-time endpoint and user identity monitoring directly on the firewall console.

Dynamic access control
Automatically adjusts firewall policies based on endpoint security posture groups.

Automated threat response
Detects and isolates suspicious or compromised endpoints to stop lateral movement.

Application-based split tunneling
Routes VPN traffic by application type to optimize bandwidth and user experience.

Granular content filtering
Blocks web pages by keywords and controls access to specific YouTube channels.

FortiSASE Integration

Endpoint-to-cloud integration
FortiClient license included with SASE subscription for seamless coverage.

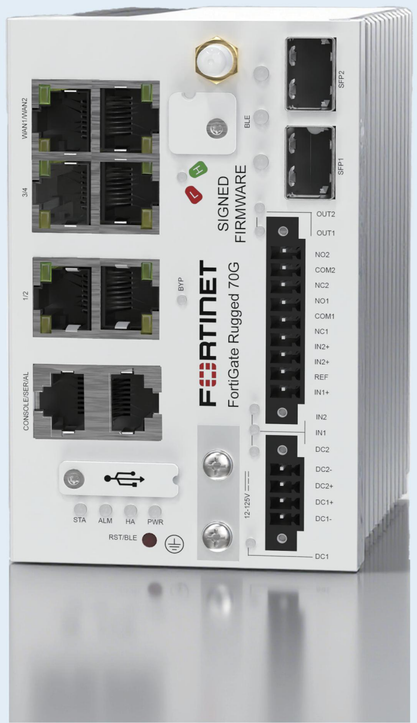
Centralized endpoint management
Unified enrollment, policy deployment, and status monitoring via the SASE platform.

Global encrypted tunnels
Automatically establishes encrypted connections to the nearest SASE PoP worldwide.

Risk-based access control
Endpoint vulnerability assessments feed real-time ZTNA application access policies.

Enhanced endpoint protection
Integrates local anti-malware and behavioral detection within the SASE architecture.

Marine Network Firewall



FGR-70G

Industrial Network Security: Protecting SCADA, DCS, and other OT environments.

Critical Infrastructure: Power, Oil & Gas, Transportation, Water Utilities.

Harsh Environment Deployment: Factory floors, substations, rail lines, outdoor cabinets.

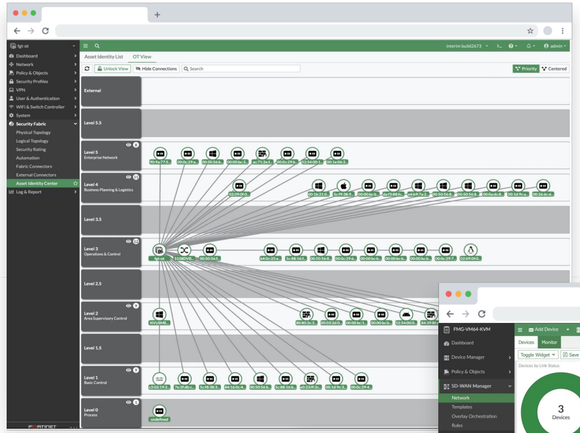
Network Segmentation: Implementing security isolation between IT/OT networks or within OT networks.

Secure SD-WAN: Providing secure, optimized WAN connectivity for remote and branch offices.

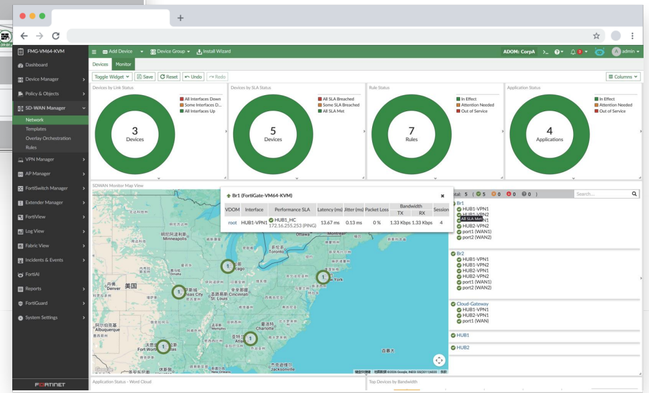
The **SO-460-FWD** is a network forwarding device specifically designed for maritime network environments. It securely transmits data between the 460-Network and other trusted networks (such as other 460-Networks or onboard control networks).
Compliant with the IEC 61162-460 standard, it ensures secure cross-network communication by providing data flow isolation and filtering capabilities.

The **SO-460-GW** is a high-performance maritime cybersecurity ateway specifically engineered for shipboard network environments, fully compliant with the IEC 61162-460 standard.
Functioning as a secure bridge between 460-Network and untrusted networks (such as the Internet), it delivers robust security protection and access control capabilities to safeguard vessel networks against external threats.

Software



OT focused dashboard for assets and analytics



Visibility and control for OT applications and protocols

Core Functional Features

01 Rugged Industrial Design

Fanless, IP40 rating, DIN-rail mountable, operational in extreme temperatures from -40°C to 75°C.

02 High-Performance NGFW

FIntegrates Next-Generation Firewall (NGFW), Intrusion Prevention System (IPS), and Advanced Threat Protection (ATP) capabilities.

03 Purpose-Built Security Processor

Equipped with Fortinet's proprietary FortiSP5 Security Processing Unit (SPU) for hardware-accelerated security performance.

04 Comprehensive Security Services

Supports AI-powered FortiGuard security subscriptions, including IPS, Anti-Malware, Web Filtering, Sandboxing, and more.

05 Integrated Secure SD-WAN

Supports application-based intelligent link steering, load balancing, and WAN optimization.

06 OT/Industrial Security

Provides Deep Packet Inspection (DPI), visibility, and control for 80+ OT industrial protocols, featuring an OT asset dashboard.

07 Universal ZTNA

Supports both agent-based (via FortiClient) and agentless (via proxy portal) Zero Trust Network Access for granular application access control.

08 Centralized Management

Enables unified policy management and automated operations via FortiManager, with log analysis and reporting via FortiAnalyzer.

09 Network Segmentation

Supports security zone and policy-based network segmentation and microsegmentation to prevent lateral threat movement.

10 High Availability

Supports Active-Active, Active-Passive, and clustering modes for business continuity.

11 Hardware Security Module

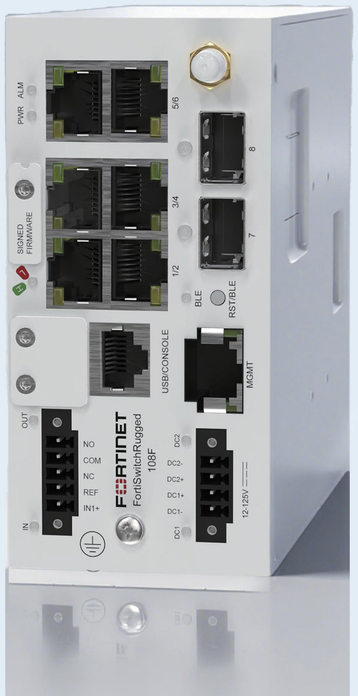
Features a Trusted Platform Module (TPM) for secure key storage and management.

Product Specifications

Model	FGR-70G
IPS	2.5 Gbps
NGFW	1.5 Gbps
ATP	1.3 Gbps
Interfaces	• 6 GE RJ45 ports • 2 SFP slots • 1 bypass pair • MicroSD card slot • Digital I/O module • Variant with dual 5G modems and GPS • Dual SIM (active/active) • Redundant 12V-125V DC inputs
IP Rating	IP40
Power Supply	12V to 125V DC redundant dual inputs, 2 pins per terminal block, negative or positive ground, DC cables not included
Operating Temperature	(-40°C to 75°C)
Humidity	5% to 95% non-condensing

Model	FGR-70G
Electric Power Industry	IEC 61850-3 and IEEE 1613 Certified
EMC	EN 55032:2015 + A1:2020, Class A, EN 55035:2017 + A11:2020 ETSI EN 301 489-1 V2.2.3 (2019-11), ETSI EN 301 489-17 V3.2.4 (2020-09)
Health and Safety	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB USGv6/IPv6
RF	EN 300 328 V2.2.2 (2019-07) EN 18031-1:2024 EN IEC 62311:2020 EN 50665:2017 FCC Part 15 Subpart C 15.247 FCC 47 CFR Part 2.1091 ISED RSS-247 Issue 3 RSS-102 Issue 6
RoHS	EN IEC 63000:2018 EN 50581:2012
Rolling Stock Industry	EN 50155:2021 EN 50121-1:2017 EN 50121-3-2:2016 + A1:2019 EN 50121-4:2016 + A1:2019 EMC, Environmental, Shock and Vibration Certified

Marine Network Core Switch



FSR-108F

Built for harsh environments, FortiSwitch Rugged delivers enterprise performance with enhanced durability and OT compliance. It seamlessly integrates with FortiGate via FortiLink for centralized security management.

Key Features:

- Rugged Design: IP30/IP40 rated, fanless, operates in extreme temperatures
- OT Ready: Supports IEEE 1588v2, HSR/PRP, and meets IEC 61850-3 standards
- High Performance: Gigabit+ speeds on all ports with auto-negotiation
- Power Delivery: PoE/PoE++ for cameras, sensors, and wireless APs
- Easy Management: Zero-touch deployment and unified security policy with FortiGate

Ideal for industrial networks requiring reliable, secure connectivity in challenging conditions.

The **SO-460-SW** is a network switch specifically designed for maritime network environments, compliant with the IEC 61162-460 standard, to deliver high-security and high-reliability network connectivity. As a core infrastructure component of the 460-Network, it connects multiple 460-Nodes and other network devices, ensuring efficient and secure data transmission across the network.

Product characteristics

Durable

MTBF > 25 years, IP30/IP40 protection for harsh environments

Zero-Touch Deployment

Auto-discovery and simplified setup for rapid network

Industrial-Ready

IEEE 1588v2 timing, HSR/PRP zero-loss redundancy, compliant with IEC 61850-3

Layer 2/3 Options

Models available for different networking needs

Fanless Design

Fully passive cooling with no moving parts

Advanced PoE Support

PoE across all models, PoE++ on select models for cameras/sensors/APs

High Performanc

Gigabit+ speeds on all ports with auto-negotiation for backward compatibility

Basic NAC Included*

Secure IoT device onboarding via FortiGuard IoT service (OT

Flexible Mounting

DIN-rail and rack-mount options

Redundant Power Inputs

Eliminates downtime from single power source failure

Product Specifications

Model	FSR-108F
Total Network Interfaces	6x 1G/100M/10M RJ45 2x 1G/100M SFP
Packet Buffers	1.5 MB
DRAM	1 GB DDR4
FLASH	32 MB SPI + 1 GB NAND
Ingress Protection	IP40
ACL	32 MB SPI + 1 GB NAND
Power Input	Redundant input terminals
Input Voltage Range	+/-12V to +/-57V DC
Operating Temperature Range	Operating temperature: -40°C to 75°C -40°C to 65°C (sealed enclosure - 0m/s air flow) -40°C to 70°C (vented enclosure - 0.2m/s air flow) -40°C to 75°C (fan or blower equipped enclosure - 1m/s air flow)
Humidity	5% to 90% RH non-condensing

Model	FSR-108F
EMI	FCC, CE, RCM, VCCI, BSMI (Class A), ICES, UKCA
EMS	CE, UKCA
RoHS and WEEE	Compliant
FCC	FCC Part 15, Subpart B, Class A
CE	Electro Magnetic Compatibility (EMC) Directive: 2014/30/EU EN 55032:2015:2020, Class A, CISPR 32 EN 55035:2017/A11:2020 ESD: IEC61000-4-2 Radiated RF (RS): IEC61000-4-3 EFT: IEC61000-4-4 Surge: IEC61000-4-5 Conducted RF (CS): IEC61000-4-6 Power Frequency Magnetic Field: IEC61000-4-8 Emission standard for industrial environments: EN 61000-6-4 IEC 61850-3 Ed 2.0: 2013
ISED	ICES-003:2020 Issue 7, Class A
RCM	AS/NZS CISPR 32, Class A

Cyber Security Management Platform

FortiManager

FortiManager centrally manages and automates security policies across Fortinet devices. 01

FortiAnalyzer

FortiAnalyzer centralizes logs and provides unified threat analytics with AI. 02

FortiPAM

FortiPAM secures privileged access with zero-trust, automation, and full session control. 03

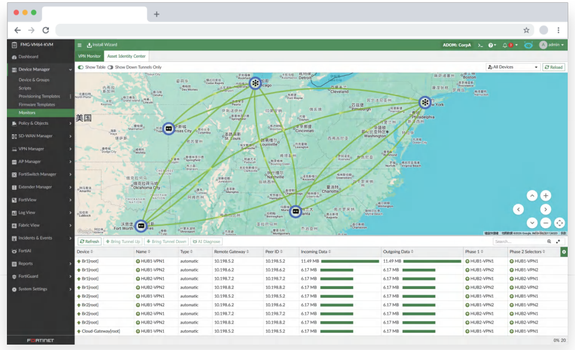
FortiClient EMS

Unified endpoint management with automated security and access controls. 04

CyberR Platform

Unified visibility, asset control, secure logs, and remote cybersecurity maintenance. 05

FortiManager



Highlights

- Transform network operation and speed up troubleshooting with add-on FortiAI subscription
- Centrally manage network and security policies
- Centralize distribution of security content, signatures, and firmware images
- Simplify configuration, deployment, and maintenance
- Reduce complexity and costs
- Automate workflows and configurations
- Separate customer data and manage domains
- Automate backups with streamlined software and security updates

Key Features

Unified Management – Control all Fortinet devices & updates from one console.

Offline Updates – Distribute security content to isolated networks.

Simple SD-WAN – Easily deploy and manage large SD-WAN networks.

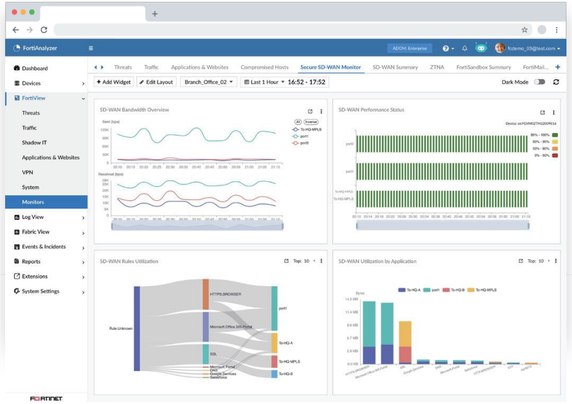
Automation Tools – Reduce work with APIs, scripts, and templates.

Auto-Configuration – Automate setup for firewalls, switches, and Wi-Fi.

Multi-tenant Control – Separate customer data and manage multiple domains securely.

Flexible Scaling – Grow capacity with cluster support for large deployments.

FortiAnalyzer



Highlights

• Centralized log collection. Unified visibility across network and security assets
• Real-time system and network monitoring
• Prebuilt reports and dashboards
• Built-in SIEM and SOAR
• Advanced threat detection
• Regularly updated SOC Automation Content packs
• Generative AI assistant
• Built-in threat intelligence. Enriches events with real-time context from FortiGuard
• Scalable data lake and XDR-ready. Unified data lake connects events across endpoints, network and cloud
• Designed to complement and work alongside any SIEM or logging solution customers use

Key Features

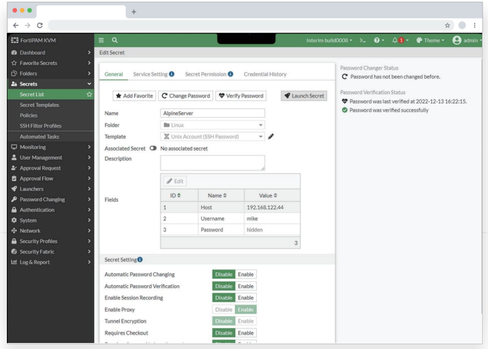
Unified Data Lake – Collects logs from all sources for full visibility and faster threat detection.

Smart Analytics – Connects events to find hidden attacks with automated response.

Live Threat Intel – Uses FortiGuard feeds for proactive defense.

Automation & Reporting – Handles alerts automatically and provides compliance dashboards.

FortiPAM



Highlights

• Encrypted Credentials: AES256 encryption & obfuscation protect stored and in-use secrets.
• Certificate Vault: Secure storage for certificates/keys with full audit logging.
• ZTNA Access Control: Continuous endpoint validation ensures only trusted users/devices connect.
• Session Monitoring: Records and can terminate privileged sessions with video playback.
• Automated Service Accounts: Auto-discovers, imports, and rotates service credentials.
• MFA & SSO: Supports SAML, RADIUS, LDAP, and AD for secure login.
• Audit Trail: Centralized, tamper-proof logs for compliance.
• Fortinet Integration: Works with FortiClient EMS, FortiToken, FortiAuthenticator, and FortiSandbox.

Key Features

Enterprise PAM Platform – High-availability credential & session management with API integrations.

Secure Sessions & Credentials – AES256 encryption, credential obfuscation, SSH/Windows filtering.

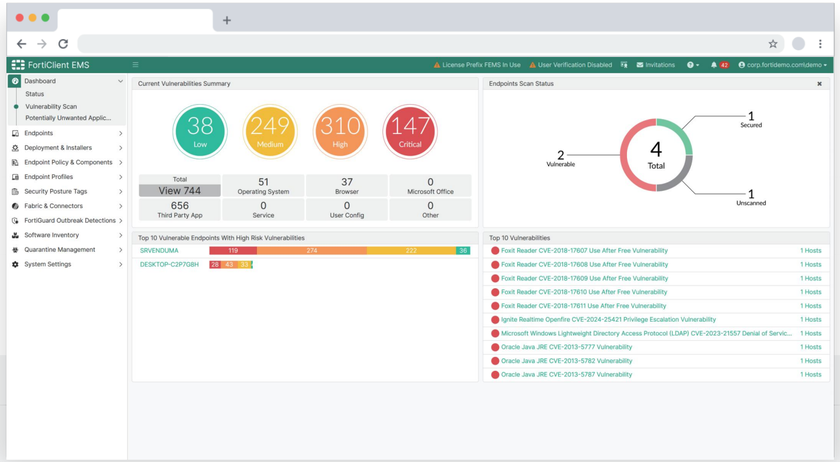
Zero-Trust Access – Real-time endpoint validation via FortiClient EMS.

Session Monitoring & DLP – Full recording, antivirus/DLP to block data leaks.

Automated Credential Management – Auto-discovery, rotation & secure certificate storage.

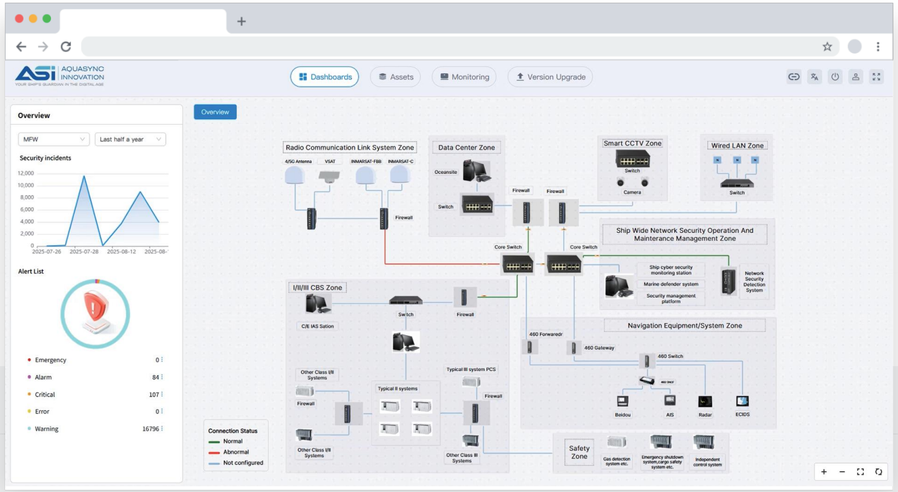
Integrated Authentication – SAML/RADIUS/LDAP/AD + Fortinet ecosystem (EMS/Token/Authenticator/Sandbox).

FortiClient EMS



- Simple and user-friendly UI
- Remote FortiClient deployment
- ZTNA orchestration
- Real-time dashboard
- Software inventory management
- Active Directory (AD) and Microsoft Entra ID integration
- Central quarantine management
- Automatic group assignment
- Dynamic access control
- Automatic email alerts
- Supports custom groups
- Remote actions
- On-premise and cloud-based options
- Zero trust tagging rules

CyberR Platform



- Visualizes the connectivity and real-time status of all onboard cybersecurity devices, providing clear insights into security alerts, perimeter protection, and network monitoring.
- Supports seamless import/export of vessel asset inventories with customizable editing options to meet diverse operational needs.
- Enables detailed log auditing and traceability, with strict control and recording of secure access activities.
- Empowers users to perform remote operations on cybersecurity devices, with full session recording and playback for accountability and review.

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

3

PART THREE

IACS UR E27

The Progress of the ASI's "Integrated Measurement, Monitoring, Alarm, and Control System" E27 Type Approval Certificate.

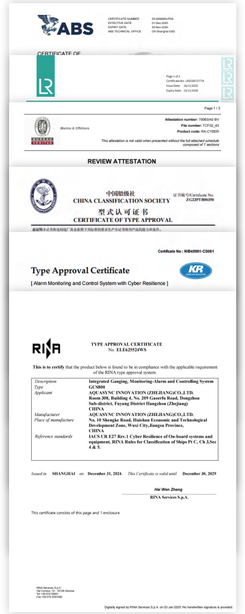
System Function

- Monitoring and Alarm (Including Engineer Alarm)
- Control System for Valve/Motor/Fan/ Cargo/Other AUX. Machineries and Level Guaging
- Pressure, Temperature and Liquid Level Measurement

Integrated Gauging, Monitoring-Alarm and Controlling System

Type Approval Certificate

- Certified
- Under Review



Integrated Gauging, Monitoring-Alarm and Controlling System

ABS Certificate of Product Design Assessment GCS800 （Endorsements: CyberSecurity)

ABS

CERTIFICATE NUMBER 25-0456005-PDA
EFFECTIVE DATE 01-Dec-2025
EXPIRY DATE 30-Nov-2030
ABS TECHNICAL OFFICE CN Shanghai ESD

CERTIFICATE OF

Product Design Assessment

This is to certify that a representative of this Bureau did, at the request of

AQUASYNC INNOVATION (ZHEJIANG) CO., LTD

located at

ROOM F402, SUPCON SCIENCE AND TECHNOLOGY PARK, NO. 309 LIUHE ROAD, BINJIANG DISTRICT,, , HANGZHOU, China, 311401

assess design plans and data for the below listed product. This assessment is a representation by the Bureau as to the degree of compliance the design exhibits with applicable sections of the Rules. This assessment does not waive unit certification or classification procedures required by ABS Rules for products to be installed on ABS classed vessels or facilities. This certificate, by itself, does not reflect that the product is Type Approved. The scope and limitations of this assessment are detailed on the pages attached to this certificate.

Product: Integrated Alarm and Monitoring System
Model: GCS800
Endorsements: CyberSecurity
Tier: 2 - PDA Issued

This Product Design Assessment (PDA) Certificate remains valid until 30-Nov-2030 or until the Rules and/or Standards used in the assessment are revised or until there is a design modification warranting design reassessment (whichever occurs first).

Acceptance of product is limited to the "Intended Service" details prescribed in the certificate and as per applicable Rules and Standards.

This Certificate is valid for installation of the listed product on ABS units which exist or are under contract for construction on or previous to the effective date of the ABS Rules and standards applied at the time of PDA issuance. Use of the Product for non-ABS units is subject to agreement between the manufacturer and intended client.

American Bureau Of Shipping
Yu Gang, Engineering Consultant

NOTE: This certificate evidences compliance with one or more of the Rules, Guides, standards or other criteria of ABS or a statutory, industrial or manufacturer's standards. It is issued solely for the use of ABS, its committees, its clients or other authorized entities. Any significant changes to the aforementioned product without approval from ABS will result in this certificate becoming null and void. This certificate is governed by ABS Rules 1-1-A3/5.9 Terms and Conditions of the Request for Product Type Approval and Agreement (2018).

Certificate of Product Design Assessment Rev.3 Page 1 of 1

Sensitivity: Internal & Restricted

Integrated Gauging, Monitoring-Alarm and Controlling System

LR Type Approval Certificate GCS800

Page 1 of 2
Certificate No: LR23187277TA
Issue Date: 26/11/2025
Expiry Date: 25/11/2030

Type Approval Certificate

This is to certify that the undernoted product(s) has/have been tested with satisfactory results in accordance with the relevant requirements of the Lloyd's Register Type Approval System.

Manufacturer	**AquaSync Innovation (Zhejiang) Co., Ltd.**
Address	Room 326, 3rd Floor, Building 1, No. 307 Liuhe Road, Puyan Sub-district, Binjiang District, Hangzhou City, Zhejiang Province, 310053, China
Place of Production	AquaSync Innovation (Zhejiang) Co., Ltd.
	No. 10 Shengke Road, Economical&Technological Development Zone, Huishan District, Wuxi City, 214177, China
Place of Production	AquaSync Innovation (Zhejiang) Co., Ltd.
	Room 1808, Ping'an Fortune Center, Binhu District, Wuxi City, Jiangsu Province, 214125, China
Type	Integrated Alarm, Monitoring and Control System
Description	Integrated Gauging, Monitoring Alarm and Controlling System. -Monitoring and Alarm (including Engineer Alarm); -Control System for Valve/Motor/Fan/Cargo/Other aux. machinery and Level Gauging; -Pressure, Temperature and Liquid Level Measurement.
Trade Name	GCS800
Application	Marine and offshore use in environmental categories ENV2for Monitoring and Alarm Unit, E as described in Lloyd' Register Test Specification No. 1- July 2024.
Specified Standard	Manufacturer's Specification

Ewan Ning

Ning Kwan
Electrical & Control Technical Manager - Southeast Hub & Great China to Lloyd's Register Classification Society (China) Co.,

Room 02-05, 46F, Raffles City Shanghai Office Tower, No.268 N Zang Middle Road, Huangpu District, Shanghai, 200053, China

Issue 2.0

Integrated Gauging, Monitoring-Alarm and Controlling System

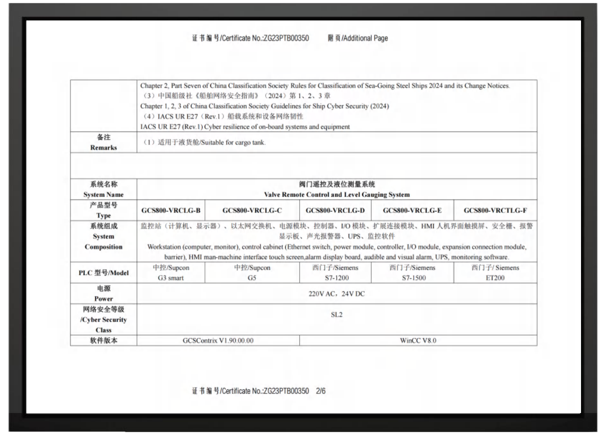
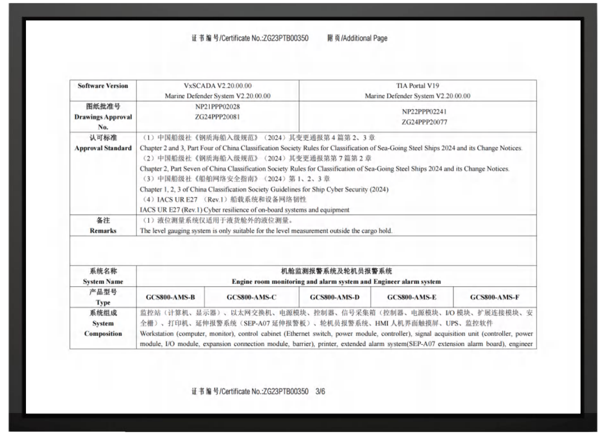
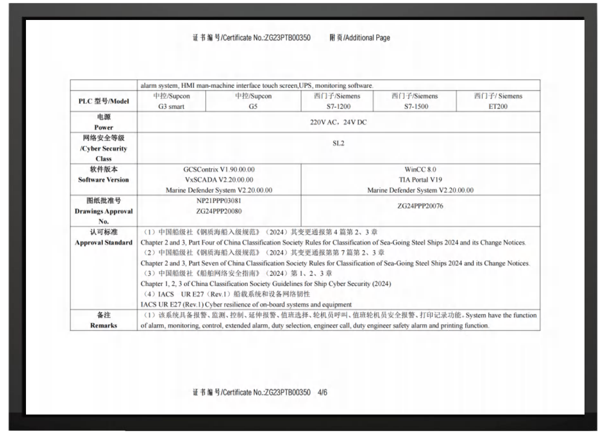
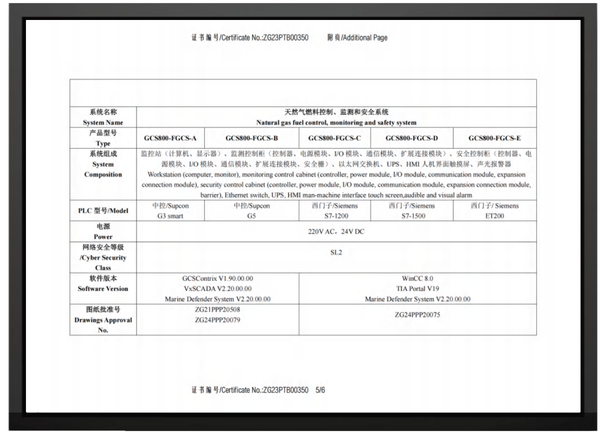
CCS Certificate of Type Approval (Meet Cybersecurity Level SL2)

Integrated Gauging, Monitoring-Alarm and Controlling System includes AMS, VRCS & LGS and CMS, wwhich has obtained the world's first type approval certificate with cybersecurity （cybersecurity SL2 level）issued by CCS and supports real-time communication between ship and shore.


中国船级社
CHINA CLASSIFICATION SOCIETY
型式认可证书
CERTIFICATE OF TYPE APPROVAL

Certificate Annex

- Pressure, Temperature and Liquid Level Measurement Alarm System
- Valve Remote Control and Level Gauging System
- Engine Room Monitoring and Alarm System and Engineer Alarm System
- Natural Gas Fuel Control, Monitoring and Safety System
- Energy Management System


Integrated Gauging, Monitoring-Alarm and Controlling System

KR Certificate of Type Approval (Meet UR E27 Cybersecurity)

Certificate No : NIB48981-CS001

Type Approval Certificate

[Alarm Monitoring and Control System with Cyber Resilience]

Initial Approval	6 January 2025
Applicant	AquaSync Innovation (Zhejiang) Co., Ltd.
	Rm308, Building 4, No.209 Gaoerfu Road, Dongzhou Subdistrict, Fuyang District, Hangzhou City, Zhejiang Province, China
Product Description	Type : GCS800
	- Application : Trusted network only
	* Manufacturing Place - No.10 Shengke Road, Economic and Technological Development Zone, Huishan District, Wuxi City, Jiangsu Province, China - Room 402, F Annex Building, Supcon Park, No. 309, Liuhe Road, Binjiang District, Hangzhou City, Zhejiang Province, P.R. China
	" See Appendix 1 "
Approval Condition	" See Appendix 1 "

THIS IS TO CERTIFY that the above-mentioned product has been approved in accordance with the relevant requirement of this Society's Rules and / or of the recognized standards as follows.

Ch. 3 of the Guidance for Cyber Resilience of Ships and Systems
IACS UR E27 Rev.1 Cyber Resilience of On-board Systems and Equipment

This Certificate is valid until 5 January 2030

Issued at Shanghai, China on 6 January 2025

This certificate is signed electronically in accordance with IMO FAL.5/Circ.39/Rev.2. Validation and authentication of the certificate can be confirmed from "http://e-cert.krs.co.kr" by using the tracking No(ME25003173353) and certificate No.(NIB48981-CS001).

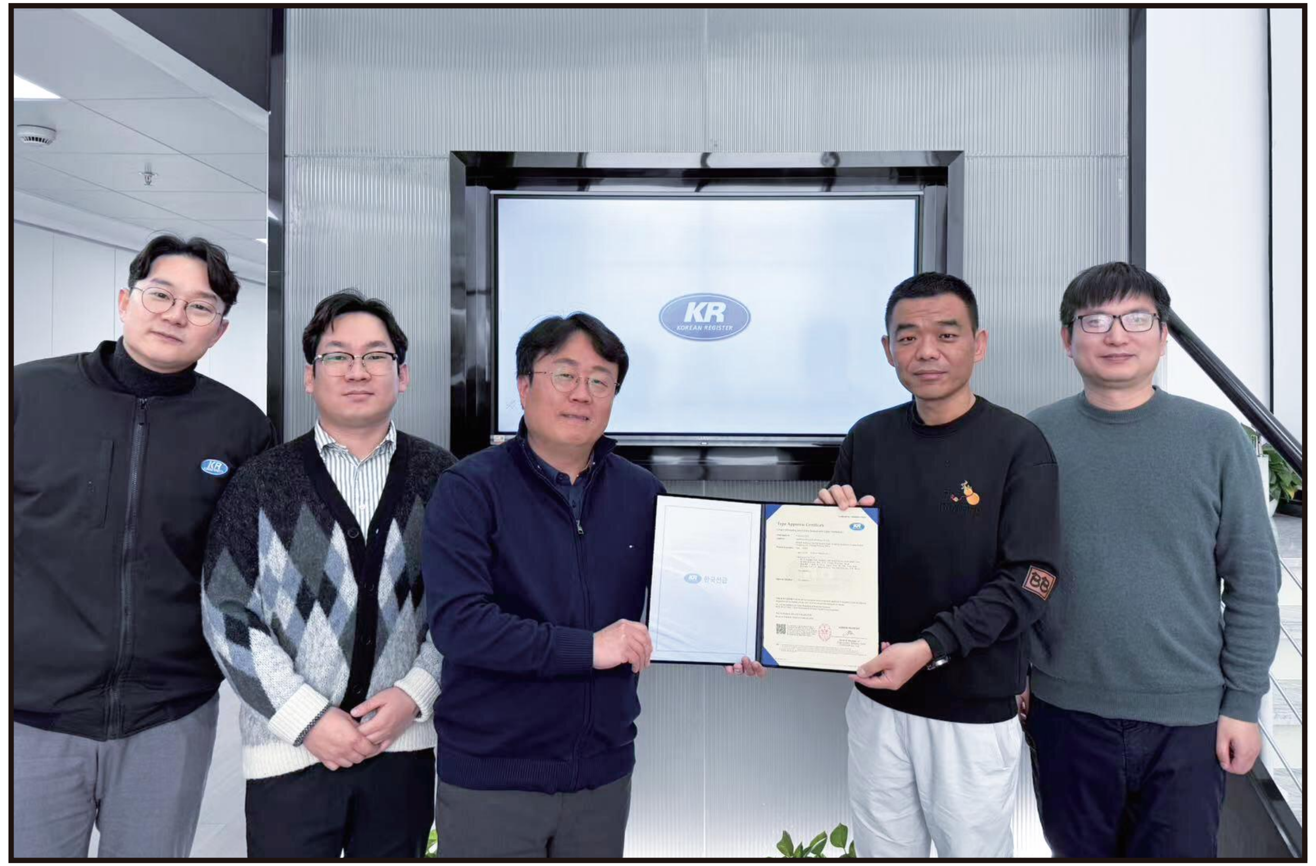
KOREAN REGISTER

General Manager of Ship System Solution Team CHINA KR Co., Ltd.

Note : 1. This certificate will be valid subject to complying with the approval conditions described on the certificate and/or on the Rules of this Society.
2. This certificate will be invalid from the expiry date aforementioned unless the extension or renewal has been granted to the applicant or the manufacturer.
3. Any significant modifications or changes in design or construction to the above product without approval from this Society will render this certificate invalid.
4. Should the specified rules, regulations or standards be amended during the validity of this certificate, the product is to be re-approved by this Society in accordance with the requirements as amended.

AC-2A (2021.01) 1/5

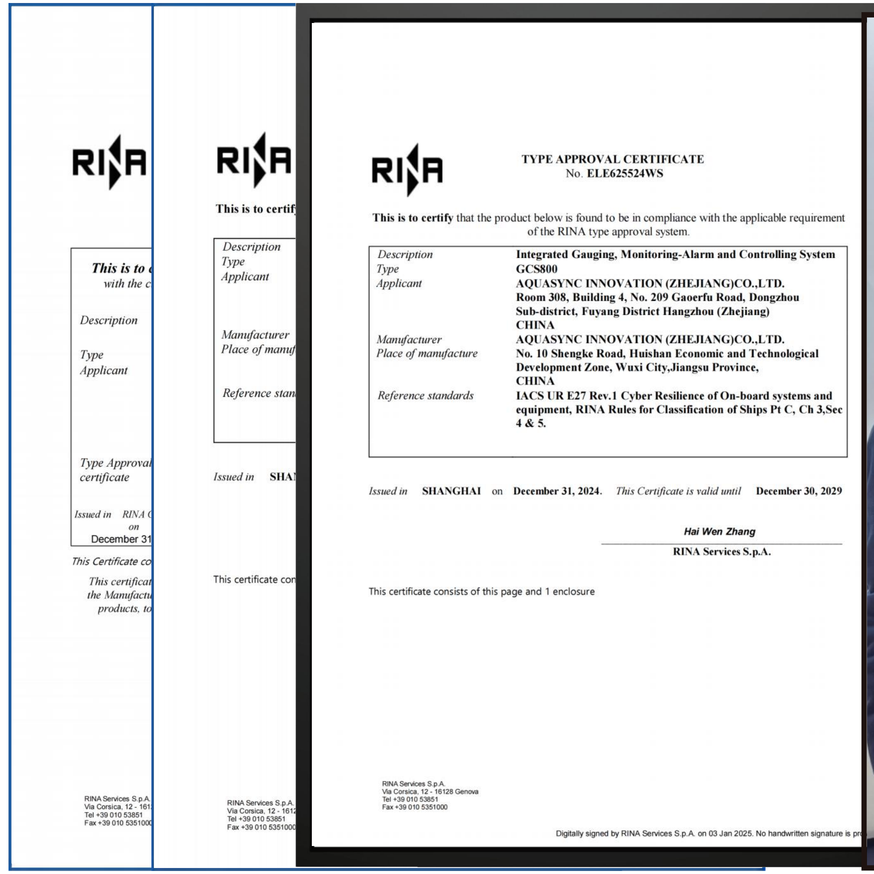
KOREAN REGISTER



RINA Certificate of Type Approval

RINA Certificate of Type Approval (Meet UR Rules for the Classification of Ship)

RINA Certificate of Type Approval (Meet UR IACS UR E27 Rev.1 Cyber Resilience of On-board systems and equipment)



TYPE APPROVAL CERTIFICATE
No. ELE625524WS

This is to certify that the product below is found to be in compliance with the applicable requirement of the RINA type approval system.

Description	**Integrated Gauging, Monitoring-Alarm and Controlling System**
Type	**GCS800**
Applicant	**AQUASYNC INNOVATION (ZHEJIANG)CO.,LTD. Room 308, Building 4, No. 209 Gaoerfu Road, Dongzhou Sub-district, Fuyang District Hangzhou (Zhejiang) CHINA**
Manufacturer	**AQUASYNC INNOVATION (ZHEJIANG)CO.,LTD.**
Place of manufacture	**No. 10 Shengke Road, Huishan Economic and Technological Development Zone, Wuxi City,Jiangsu Province, CHINA**
Reference standards	**IACS UR E27 Rev.1 Cyber Resilience of On-board systems and equipment, RINA Rules for Classification of Ships Pt C, Ch 3,Sec 4 & 5.**

Issued in **SHANGHAI** on **December 31, 2024.** *This Certificate is valid until* **December 30, 2029**

Hai Wen Zhang

RINA Services S.p.A.

This certificate consists of this page and 1 enclosure

Interpretation of CBS Cybersecurity Requirements

The "Guidelines on Ship Cybersecurity" 2024, Chapter 2 and Chapter 3, respectively, elaborate on CBS Cybersecurity requirements, levels, and the requirements for CBS inspection/evaluation. The Cybersecurity requirements for CBS are developed from the following 7 aspects:

Identification and Authentication

Identify and authenticate all users (personnel, software processes, and devices) before granting access to the system.

Usage Control

Assign permissions to identified and authenticated users (personnel, software processes, or devices) to perform authorized operations requested by the system, and monitor the use of permissions.

System Integrity

Ensure the integrity of the system to prevent unauthorized operations.

Data Confidentiality

Ensure the confidentiality of data in communication channels and storage areas to prevent unauthorized disclosure.

Restricted Data Flow

Segment the system into zones and conduits to limit unnecessary data flow.

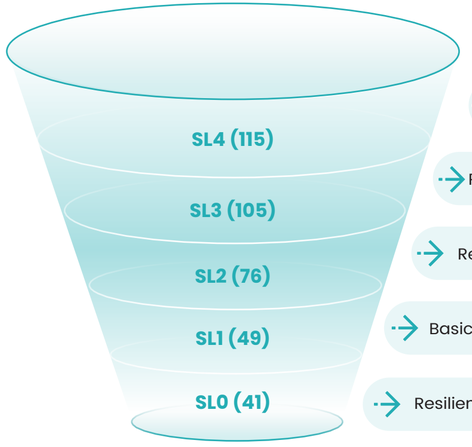
Incident Response

Respond to actions that violate Cybersecurity requirements, notify relevant personnel, report necessary evidence, and take measures upon discovering incidents.

Resource Availability

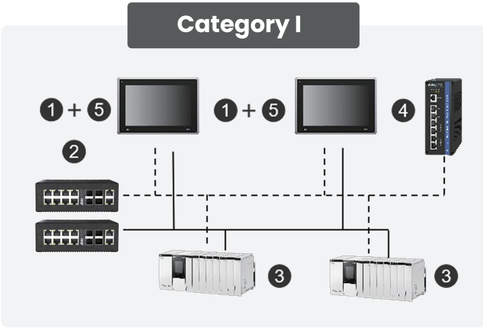
Ensure the availability of the system to prevent critical services from being impacted or denied.

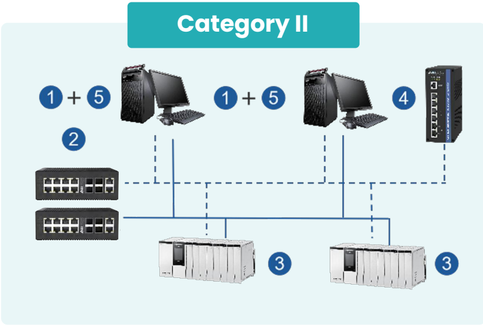
CBS Cybersecurity Classification Levels



- Resilience Against Organized and Targeted Cyber Incidents
- Resilience Against Cyber Incidents Initiated with Abundant Resources
- Resilience Against Sporadic Cyber Incidents
- Basic Cyber Defense Capabilities
- Resilience Against Cyber Incidents Initiated with Limited Resources

Cybersecurity Levels (Corresponding to the Number of Requirements in the Standards)	Cybersecurity Capabilities





System Categories	Domestic Series Models of CBS	International Series Models of CBS
CBS Core Functional Components	① Monitoring Station (Touchscreen + SCADA + Configuration Software) 	① Monitoring Station (WINDOWS+SCADA + Configuration Software) 
	② Switch ③ PLC & I/O Modules	
Additional Cybersecurity Equipment	④ Marine Network Firewall ⑤ Marine Defender System (software)	

CBS Components - Specification Comparison Table (SL0)

In the CBS system, the components work together complementarily to meet the requirements of Security Level 0 (SL0). Each component provides protection against various threats to the CBS system, with the detailed network security clauses that each component meets as follows:

Core Functional Modules of CBS			Additional Network Security Equipment	
①	②	③	④	⑤
Monitoring Station	Switch	PLC & I/O Modules	Marine Network Firewall	Marine Defender System
35 Clauses	2 Clauses	11 Clauses	9 Clauses	7 Clauses

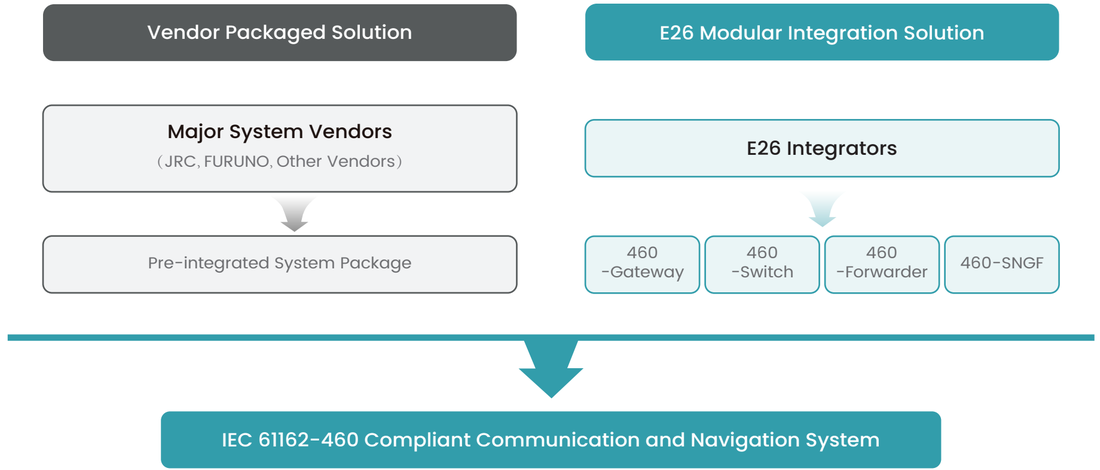
"As indicated in the table above, to achieve Network Security Level SL0, the system must include both a ship network firewall and ship endpoint security software. "

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

3

PART THREE

460 Practical Implementation - Communication and Navigation System: IEC 61162-460



Device Overview

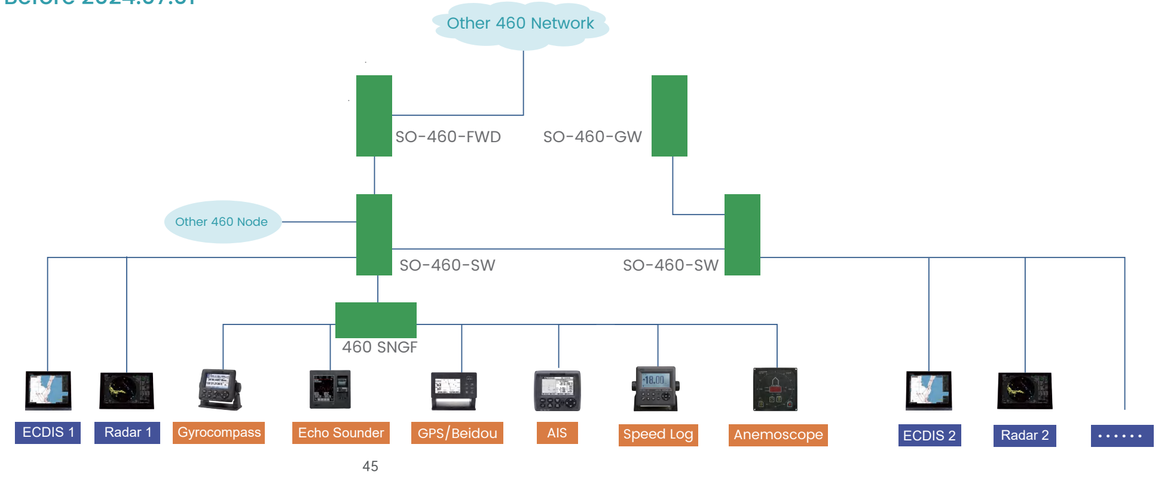
Statistical time:June 1, 2025

Device Name	Function Product Introduction	Corresponding Specification Requirements										
		E26	E27	CCS	DNV	ABS	BV	RINA	KR	RS	LR	NK
Class Notation (E26)		Rev.1	Rev.1	2024 CyberSecurity (P[SL0])	2024 Cyber Secure (Essential)	2024 CR	2024 Cyber Resilient	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience	2024 Cyber Resilience
460-Gateway	Connected to 460-networks and to Uncontrolled	1.3.2	1.3	1.1.1.5	Pt4.CH9. Sec.13:5. 1.1 Pt4.CH9. Sec 14:5	Pt4,ch9, Sec14 5	NR659, Ch3, Sec2:1.3 1 NR659, Ch5, Sec2:1 3 1	PtC, Ch 3, Sec 4:1.4.2	CH1. Sec1:106 CH3. Sec1:102	Part XXI 1.1.5	Pt6. CH1. Sec.2:2.16	Chapter 1 4
460-Switch	Interconnect Nodes on A 460-network											
460-Forwarder	Exchange Data Streams Between A 460-network and other Controlled Networks											
460-SNGF	Convert GPS, AIS and other devices that transmit via serial port into network port for transmission											

460 Practical Implementation - Communication and Navigation System: IEC 61162-460

- Equipment certified by 460, designated as a 460 node
- The original equipment applied for 460 exemption inspection, adding 450 SNGF to become a 450 Node with SNGF
- Other 460 Network, Untrusted Network

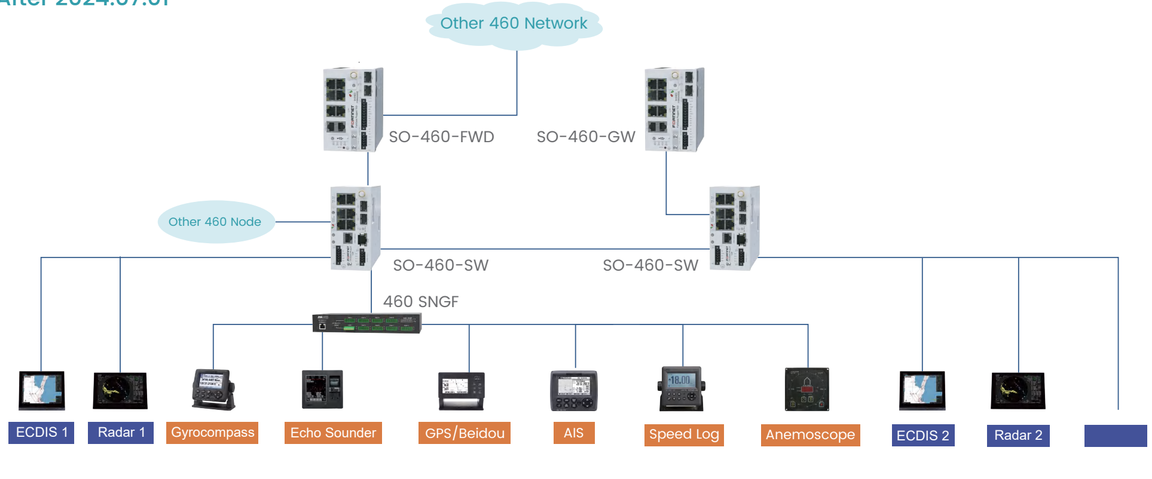
Before 2024.07.01



45

- Equipment certified by 460, designated as a 460 node
- The original equipment applied for 460 exemption inspection, adding 450 SNGF to become a 450 Node with SNGF

After 2024.07.01



Distribution of functions around 460-Network

IEC61162-460

Function	SO-460-SW	SO-460-FWD	SO-460-GW
Network Access Control (6.2.4.2)	✓	✓	✓
Syslog Implemented (Source) (8.1)	✓	✓	✓
Data Output Bandwidth Defined (5.16.2.2.1)	✓	✓	✓
Network Traffic Management (5)	✓	✓	✓
Security -No Wireless (6.2.1)	✓	✓	✓
Security -Excessive Traffic Protection (6.2.2.1, 5.3.3)		✓	
Security -Dos Attack Icmp Igmp Protection (6.2.2.2)	✓	✓	✓
Security -Access Control (Password) (6.2.4.1)	✓	✓	✓
Redundancy (7.1, 7.2)	As Installed ✓	As Installed ✓	✓
Network Monitoring	✓ (For at Least One Node or Switch, 8.2.1)		✓(List Of Connections)

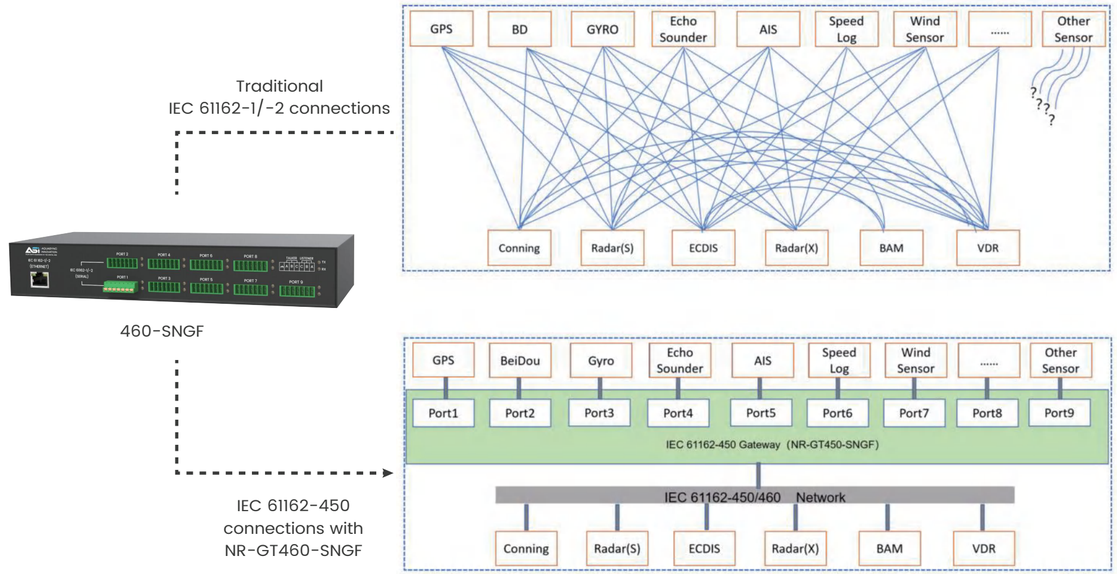
Function	SO-460-SW	SO-460-FWD	SO-460-GW
If Applicable -Reds Security (6.2.3)	✓	✓	✓
Configuration of Network Flows (5.2.1, 5.3.2)	✓	✓	
Allocation of Bandwidth (5.2.1, 5.3.2)	✓	✓	
In/out Traffic in Register Allowed, Deny Other Traffic (6.2.4.2)	✓		
If Applicable -Vlan Config Per Interface (5.2.1)	✓		
Igmp Multicast Snooping (5.2.1)	✓		
Syslog(Sink)	✓ (For at Least One Node Or Switch, 8.2.1)		
Caution/Warning Source(6.3.4, 6.3.5, 8.2.7.1)	✓		✓
Firewall (6.3.2)		✓	✓

460 SNGF

Technical Data

- 9x isolated full-duplex RS-422/485 serial ports (9 talkers + 9 listeners), compliant with IEC 61162-1/-2 standards
- 1x 10/100M Ethernet port
- LED indicators for data transmission and reception on each serial port
- Compliant with IEC 61162-450 standard
- Configurable SFIDs for each serial port
- Configurable transmission groups and sentence filtering on each serial listener
- Configurable sentence forwarding rules on each serial transmitter
- Ethernet-based configuration. All settings can be configured over Ethernet, including the IP address
- (Optional) additional SFIDs to calculate and output fused data based on multiple sensors
- (Optional) industrial fieldbus (e.g. Modbus) support
- 24V DC and 110/220V AC dual power supply
- Operating temperature range: -15~+55°C

Easier Connections with460-SNGF

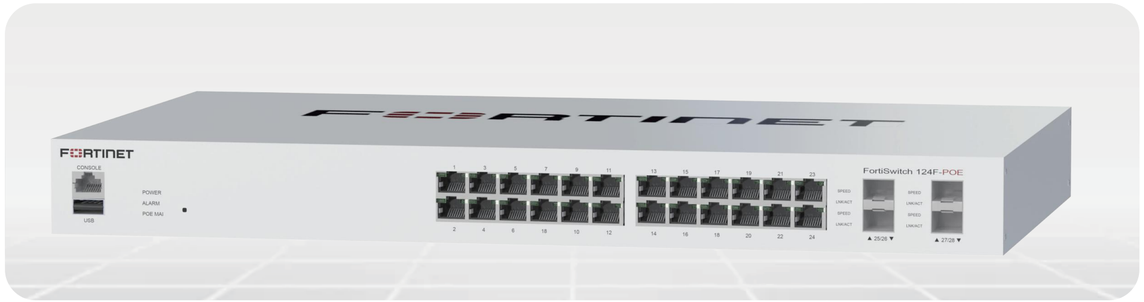


YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

3

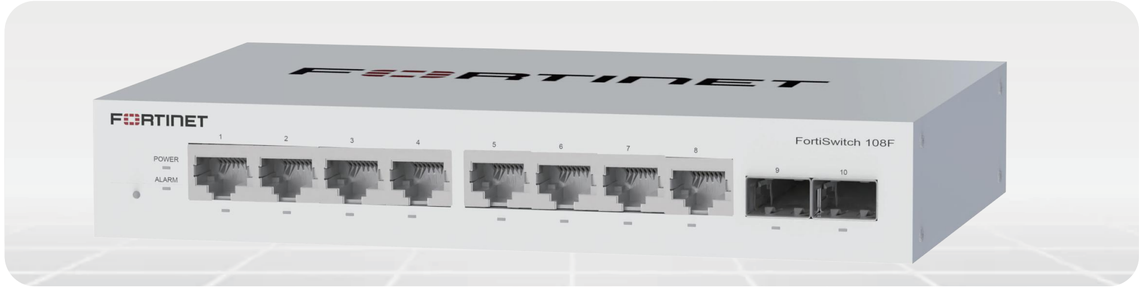
PART THREE

FortiSwitch-124F-POE



- CONSOLE (RJ45): Management console port, default IP: 192.168.1.99, USB (2.0): Reserved for future use
- POWER: Power input port
- ALARM: Alarm interface port
- PoE Ports 1 to 12 (RJ45) GE network connections
- Ports 1 to 24 (RJ45) GE network connections
- Ports 25 to 28 (SFP+) 10Gbps SFP connections
- FortiLink Ports 21 to 28 (RJ45 & SFP+) FortiLink interface connections

FortiSwitch-108F



- Industrial-grade rugged design with IP40 rating, operating from -40°C to 75°C, fanless cooling.
- Dual power options: 12V DC adapter or PoE (802.3af/at) via Port 8 for flexible deployment.
- 8 Gigabit Ethernet ports + 2 SFP ports with dual-speed indicators.
- Integrates with FortiGate via FortiLink for centralized policy management.
- Port and system LEDs enable quick status diagnostics.
- Supports industrial protocols like IEEE 1588v2 and complies with IEC 61850-3 certification.
- Zero-touch deployment and centralized management through FortiGate.

FortiCamera

FortiCamera FD50

Fixed dome camera providing a clear image with a 4x optical zoom for indoor or outdoor environments. With a built-in microphone and strong low-light sensitivity through true shutter WDR make this camera work in almost any light situation.

FortiCamera FD51

Fixed dome camera with a fixed wide-angle lens designed for indoor or outdoor environments. The built in Digital IO integrates with motion sensors, alarms, and strong low-light sensitivity through true shutter WDR.

Technical parameters	FortiCamera FD50	FortiCamera FD51
Type	Fixed dome	Fixed dome
Installation	Indoor / outdoor	Indoor / outdoor
Sensor Resolution	5 MP	5 MP
Zoom	4x Optical	-
View Angle	H: 30°~90°, V: 23°~65°, D: 38°~115°	H: 111°, V: 59°, D: 133°
Audio	Built-in mic, line out	Line in/out
IR Illumination	30m	30m
Rating	IP66 / IK10	IP66 / IK10

FortiAP

FAP-231K

These enterprise class Wi-Fi 7 indoor APs provide three radios and two spatial streams. These access points support the 6 GHz band and have one 5 Gigabit Ethernet port. The APs can provide 24/7 background scanning across all bands while still providing access on 2.4 GHz, 5 GHz, and 6 GHz bands. The integrated BLE/ ZigBee radio can be used for beacons and location applications.

Technical parameters

Type	Indoor AP
Number of Antennas	6. x2 Dual band Wi-Fi + x2 6GHz band Wi-Fi + x1 BLE/ZigBee antenna + x1 GPS antenna
Interfaces	x1 100M/1000M/2.5G/5.0G Multigigabit Ethernet (RJ45) x1 RS-232 RJ45 Serial Port
Power over Ethernet (PoE)	x1 802.3at PoE default
Maximum Tx Power (Conducted)	2.4GHz band: 26 dBm/400 mW (2 chains combined)* 5.0GHz band: 23 dBm/200 mW (2 chains combined)* 6.0GHz band: 22 dBm/158 mW (2 chains combined@320MHz BW)*
IEEE Standards	802.11a, 802.11b, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3bt, 802.3az
Wireless Monitoring Capabilities	Rogue Scan radio modes,WIPS / WIDS radio modes, Packet Sniffer Mode, Spectrum Analyzer
Power Supply	802.3bt PoE: GPI-145 or 802.3at PoE: GPI-130 or 12V, 2.5A, 30 Watt DC power supply SP-FAP200-PA-XX

FortiAP 23JF

This enterprise class Wi-Fi 6 wall plate AP provides three radios with internal antennas and two spacial streams, as well as features such as OFDMA and is PSE-capable. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications. Additional features include PoE out for downstream devices and RJ45 passthrough. This access point can be installed in minutes, right over the existing wall plate , or with the optional desk mount, makes a perfect remote / work from home AP.

Technical parameters

Type	Indoor walljack/desktop AP
Number of Antennas	3 dual band internal Wi-Fi + 1 single band 2.4 GHz BLE/ZigBee
Interfaces	4x 10/100/1000 Base-T RJ45 Ports (1x 802.3at PoE(PD), 1x 802.3af PoE (PSE), 2x Non-PoE Ports) 3 RJ-45 Ports (1xPass-through in, 1x Pass-through out, 1x RS-232 Serial Port)
Maximum Tx Power (Conducted)	Radio 1: 2.4 GHz: 25 dBm / 158 mW (2 chains combined)* Radio 2: 5 GHz: 21 dBm / 158 mW (2 chains combined)* Radio 3: N/A
IEEE Standards	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i,802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
Wireless Monitoring Capabilities	Rogue Scan radio modes,WIPS / WIDS radio modes, Packet Sniffer Mode, Spectrum Analyzer
Power Supply	802.3at PoE: GPI-130, Optional DC power adaptor SP-FAP23J-PA-10

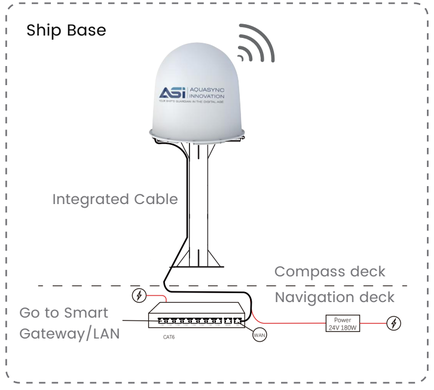
VSAT Satellite Communication System

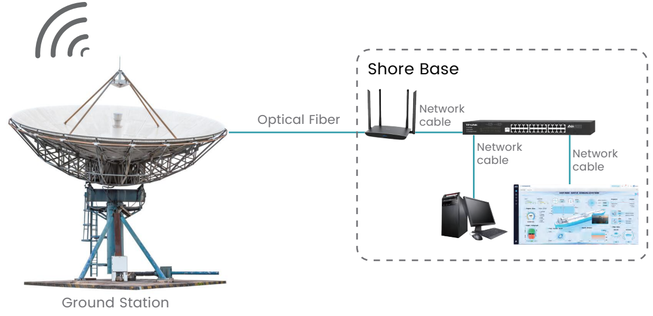
System Introduction

The VSAT system is composed of a hub station and many remote VSATs scattered in each user's location. It can access the Internet without any ground lines, and is not limited by terrain, distance and ground communication conditions.

Technical parameters

Antenna Type	Three-Axis (Polarized) Ship Mounted Dynamic Communication
Antenna Diameter	100cm
BUC	8W
Environment Rating	IP56





Maritime LEO Satellite Communication System

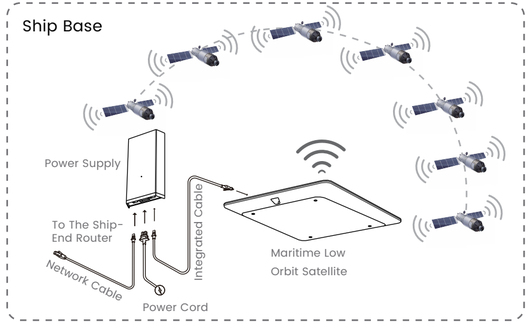
System Introduction

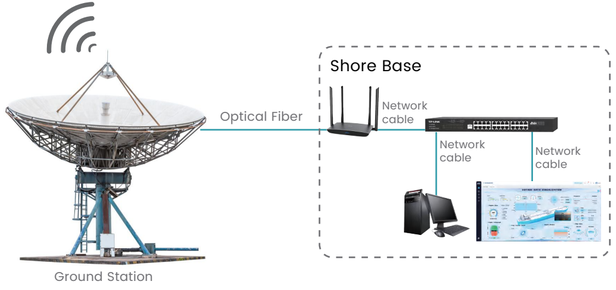
The maritime LEO satellite system can provide high bandwidth, low latency broadband and communication services for global consumers and commercial users.

Technical parameters

Field of View	140°
Dimensions	57.5x51.1cm
Support Up and Down Speeds	8-25Mbps Up and 40-220Mbps Down
Environment Rating	IP56

Please note that due to the relatively new technology of maritime LEO satellite services, there is no network service within 15 nautical miles offshore in countries where their use is not allowed. Generally, there is network service beyond 15 nautical miles offshore, and the distance may vary among different countries. The actual effect shall prevail.





PART FOUR

4

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

ASI's Ship Cybersecurity Service Qualifications

Golden Triangle Alliance for a Comprehensive E26/27 Solution

ASI AQUASYNC INNOVATION YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE × FORTINET × DNV

SOLUTION DESIGN

ASI × DNV

- ◇ Ship Asset Inventory
- ◇ Ship Network Topology Diagram
- ◇ Ship Cybersecurity Design Description
- ◇ Risk Assessment for the Exclusion of CBSs (If applicable)
- ◇ Description of Compensating Countermeasures (If applicable)
- ◇ Ship Cybersecurity Testing Procedure
- ◇ Template File for Ship Cybersecurity and Resilience

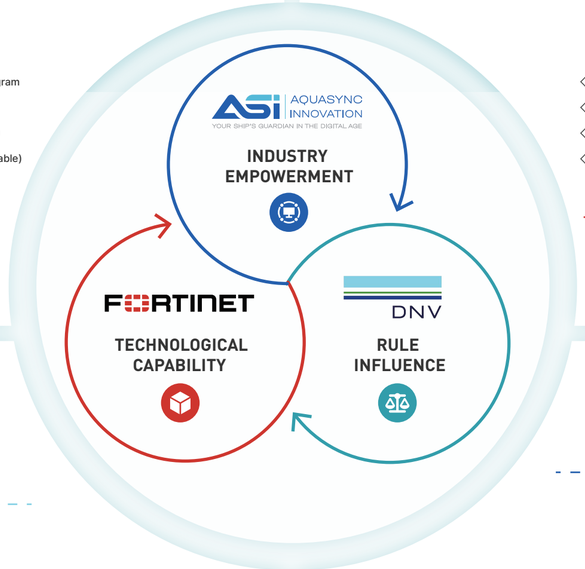
- ◆ ISO/IEC 27001 : 2022
- ◆ Certified Personnel: CISSP

PROVISION OF HARDWARE

ASI × FORTINET

- ◇ Marine Network Core Switch
- ◇ 460-Gateway
- ◇ Marine Network Firewall
- ◇ 460-Switch
- ◇ Marine Defender System
- ◇ 460-Forwarder
- ◇ Cybersecurity Management Platform
- ◇ 460-SNGF

- ◆ IEC 62443-4-1
- ◆ IEC 62443-4-2
- ◆ IEC 61162-460



CYBERSECURITY TEST SERVICE

ASI × DNV

- ◇ Providing Cybersecurity Capability Testing Based on Approved Test Procedures

- ◆ ISO/IEC 17025:2017(DNV&CNAS)
- ◆ Tester : CISSP

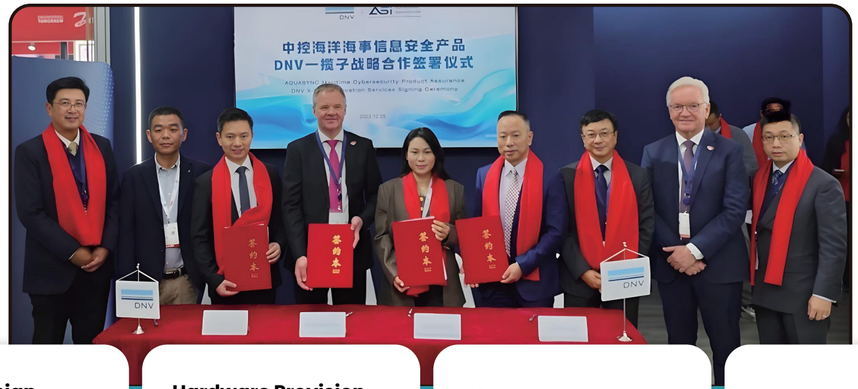
OPERATIONAL MAINTENANCE SERVICES

ASI × FORTINET × DNV

- ◇ Cybersecurity Operational Maintenance Services

- ◆ ISO/IEC 20000:2018
- ◆ IEC 62443-2-4
- ◆ ISO/IEC 17025:2017(DNV&CNAS)
- ◆ Certified Personnel: CISSP

JOINT TENDER AGREEMENT



Solution Design

Providing Comprehensive Cybersecurity Solution Design for Vessels in Compliance with E26 Requirements

Hardware Provision

Providing Cybersecurity Devices Compliant with IEC 62443-4-1 and IEC 62443-4-2 Requirements

Cybersecurity Test Service

Providing Cybersecurity Capability Testing Based on Test Procedure

Operational Maintenance Services

Cybersecurity Operations and Annual Assessment

DNV × ASI AQUASYNC INNOVATION

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

联合体协议书 Consortium Agreement

船舶网络安全E26&E27咨询测试项目投标

Bidding for the E26&E27 Consulting and Testing Project on Ship Cybersecurity

联合体单位一与联合体单位二自愿组成联合体，共同参与船舶网络安全 IACS UR E26&E27咨询、测试（以下简称“本项目”）的投标工作。

Consortium Member One and Consortium Member Two voluntarily form a consortium to jointly participate in the bidding work of IACS UR E26&E27 consultation and testing for Ship Cybersecurity (hereinafter referred to as "this project").

联合体名称：ASI - 挪华威(DNV) 船舶网络安全E26&E27咨询及测试联合体。

Consortium Name: ASI - DNV Ship Cybersecurity E26&E27 Consulting and Testing Consortium.

联合体牵头方为：

The leading party of the consortium is:

中控海洋装备（新加坡）有限公司

AquaSync Innovation (Singapore) Pte. Ltd

本协议适用于接受联合体投标的船舶及海工项目，此协议对工作期限及工作范围做出如下规定：

This agreement is applicable to ship and offshore engineering projects that accept joint bids. This agreement stipulates the working period and scope as follows:

1、合作期限及退出

Term of cooperation and withdrawal

（1）本协议自签定之日起一年内有效；

This agreement shall be valid for one year from the date of signing.

（2）到期后由双方共同决定是否续签联合体协议；

After expiration, both parties shall jointly decide whether to renew the consortium agreement.

（3）在协议期内，单一方可提出退出该协议，经双方共同确定后本协议可解除；

During the term of the agreement, either party may propose to withdraw from the agreement. This agreement may be terminated upon mutual confirmation by both parties.

（4）在协议期内，任何一方如违反本协议及附件中所规定内容，经另一方书面要求限期整改后仍不符合约定的，本协议可立即解除。

During the term of this agreement, if either party violates the contents stipulated in this agreement and its annexes and still fails to comply with the agreement after being requested in writing by the other party to rectify within a specified period, this agreement may be immediately terminated.

2、**联合体单位一（ASI）**负责的主要工作内容：

The main tasks of Consortium Member One (ASI) are as follows:

（1）客户市场推广；

Customer marketing promotion

（2）提供测试工程师及测试设备并执行测试工作。

Provide test engineers and test equipment and carry out test work.

3、**联合体单位二（挪华威DNV）**负责的主要工作内容：

The main tasks of the member two of the consortium (DNV) are as follows:

（1）提供技术咨询，提供技术方案和测试大纲；

Provide technical consultation, technical solutions and test Outlines;

（2）对测试工程师进行培训；

Train test engineers;

（3）对现场测试进行见证，并核准测试报告。

Witness the on-site tests and approve the test reports.

4、双方在公正和独立的情况下共同承担工作内容：

Both parties shall jointly undertake the work content in a fair and independent manner:

（1）以联合体形式对外市场推广和承接订单；

Promote the external market and undertake orders in the form of a consortium;

（2）对技术方案、测试大纲、测试报告共同确认。

Jointly confirm the technical solution, test outline and test report.

5、项目投标确认

Project bid confirmation

（1）项目投标时需确认联合体投标意愿，共同确认后本协议生效。

When bidding for the project, the willingness of the consortium to bid must be confirmed. This agreement shall come into effect after joint confirmation.

（2）双方就具体项目需签署附页B中的《投标项目确认书》。

Both parties are required to sign the "Confirmation of Bidding Project" on Appendix B for the specific project.

此协议附加条款见附页A

The additional terms of this agreement can be found on Appendix A

联合体单位一：

Consortium Member One

中控海洋装备(新加坡)有限公司

AquaSync Innovation(Singapore) Pte.Ltd

PAYA LEBAR ROAD #07-54 PAYA LEBAR SQUARE SINGAPORE (409051)

沈丽丽 Shen Li Li

管理代表 On Behalf

本协议自双方签字盖章之日起生效

This agreement shall come into effect as of the date when both parties sign and affix their seals

终止条件：双方书面协商签终止。

Termination condition: Both parties mutually agree in writing to terminate

联合体单位二：

Consortium Member One

上海挪华威认证有限公司

DNV Business Assurance China Co.Ltd.

中国上海市长宁区娄山路580号B幢6楼

Site A, House 6, 580 Loushan Road, Changning, Shanghai, China

康文煜 Kang Wen Yu

管理代表 On Behalf

签约地点及日期：

Place and Date

上海,2025年8月5日

5 August 2025, Shanghai

Corresponding Qualifications for Ship Cybersecurity E26

On April 02, 2024, DNV, a professional risk management service agency, has issued certificates of **ISO 9001:2015** quality management system, **ISO/IEC 27001:2022** Information security management system and **ISO/IEC 20000:2018** Information technology service management system to AguaSync Innovation.

GB/T 19001-2016/ISO 9001:2015

Quality Management System

ISO/IEC 27001:2022

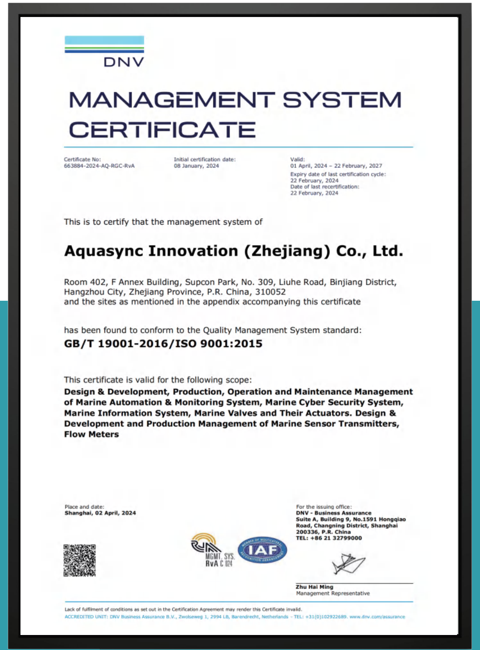
Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements

ISO/IEC 20000-1:2018

Information Technology-service Management
Part 1: Service Management System Requirements

IEC 62443 4-1 & 2-4

Security for Industrial Automation and Control Systems



DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate No: 663884-2024-AQ-RGC-RvA
Initial certification date: 08 January, 2024
Valid: 01 April, 2024 – 22 February, 2027
Expiry date of last certification cycle: 22 February, 2024
Date of last recertification: 22 February, 2024

This is to certify that the management system of

Aquasync Innovation (Zhejiang) Co., Ltd.

Room 402, F Annex Building, Supcon Park, No. 309, Liuhe Road, Binjiang District, Hangzhou City, Zhejiang Province, P.R. China, 310052
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Quality Management System standard:
GB/T 19001-2016/ISO 9001:2015

This certificate is valid for the following scope:
Design & Development, Production, Operation and Maintenance Management of Marine Automation & Monitoring System, Marine Cyber Security System, Marine Information System, Marine Valves and Their Actuators. Design & Development and Production Management of Marine Sensor Transmitters, Flow Meters

Place and date:
Shanghai, 02 April, 2024

For the issuing office:
DNV - Business Assurance
Suite A, Building 9, No.1591 Hongqiao Road, Changning District, Shanghai 200336, P.R. China
TEL: +86 21 32799000

Zhu Hai Ming
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV Business Assurance B.V., Zwolseweg 1, 2994 LB, Barendrecht, Netherlands - TEL: +31(0)102922689. www.dnv.com/assurance

DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate no.: 686326-2024-AIS-RGC-UKAS
Initial certification date: 15 May 2024
Valid: 14 November 2024 – 14 May 2027

This is to certify that the management system of
AQUASYNC INNOVATION (SINGAPORE) PTE. LTD.
Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, China
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Information Security Management System standard:
ISO/IEC 27001:2022

This certificate is valid for the following scope:
Information Security Management System Covers Design& Development, Production, Operation and Maintenance Management of Marine Automation & Monitoring System, Marine Cyber Security System, Marine Information System. The Related Facilities, Infrastructure and Personnel for above Services. This is in Accordance with the Statement of Applicability, Version V1.1

Place and date:
Shanghai, 15 November 2024

For the issuing office:
DNV - Business Assurance
Building 9, No. 1591 Hongqiao Road, Changning District, Shanghai, China 200336

Zhu Hai Ming
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV Business Assurance UK Limited, 5th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom - TEL:+44(0) 203 816 4000. www.dnv.co.uk

DNV

MANAGEMENT SYSTEM CERTIFICATE

Certificate no.: 686325-2024-AQ-RGC-UKAS
Initial certification date: 15 May 2024
Valid: 14 November 2024 – 14 May 2027

This is to certify that the management system of
AQUASYNC INNOVATION (SINGAPORE) PTE. LTD.
Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, China
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the IT Service Management System Standard:
ISO/IEC 20000-1:2018

This certificate is valid for the following scope:
The IT Service Management System Covers the Provide of Maintenance Services in Marine Automation & Monitoring System, Marine Cyber Security System, Marine Information System to External Contracted Customers from Corp Office Site in Accordance with the Service Catalog

Place and date:
Shanghai, 15 November 2024

For the issuing office:
DNV - Business Assurance
Building 9, No. 1591 Hongqiao Road, Changning District, Shanghai, China 200336

Zhu Hai Ming
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV Business Assurance UK Limited, 5th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom - TEL: +44(0) 203 816 4000. www.dnv.co.uk

DNV

CERTIFICATE

Certificate No.: IPA-CS-10488181-2024DC01
Initial certification date: 2024-12-08
Valid Until: 2029-12-07

Certificate Holder: AQUASYNC INNOVATION (SINGAPORE) PTE.LTD.

Location: (1): 60, PAYA LEBAR ROAD, #07-54 (409051), PAYA LEBAR SINGAPORE
(2): Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, CHINA

Scope of Certificate: **IEC 62443-4-1:2018** (Edition 1.0)
Security for industrial automation and control systems,
Part 4-1: Secure product development lifecycle requirements.
IEC 62443-2-4:2015 +A1:2017 (Edition 1.1)
Part 2-4: Security program requirements for IACS service providers

Validity: This certificate is valid until **2029-12-07**.

The certificate holder has successfully demonstrated a Security Development Lifecycle Management Process that complies with the requirements of IEC 62443-4-1 and a Security Program Management Process as defined in Part 2-4, including adherence to the maturity levels specified within IEC 62443-2-4, achieving **Maturity Level 3 (Defined)**.

This certificate of conformity is based on an assessment conducted by DNV, the results of which are documented in Report No. *Rep-IPA-CS-10488181-2024DC01*, dated *2024-11-10*. This certificate is valid only for processes and practices that are identical to those evaluated during the assessment.

This certification does not apply to or certify any specific security-related products.

Place and date:
Shanghai, China
2024-12-08

Vincent Zhao Ph.D
Head of Transportation & Cybersecurity Assurance

Li Xiang
Product Assurance & Inspection Service Director of Greater China

DNV BUSINESS ASSURANCE CHINA Co. LTD, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: 86 (0) 21 3279 9000 Fax: 86 (0) 21 6278 8090

Laboratory Certificate

Laboratory Capabilities

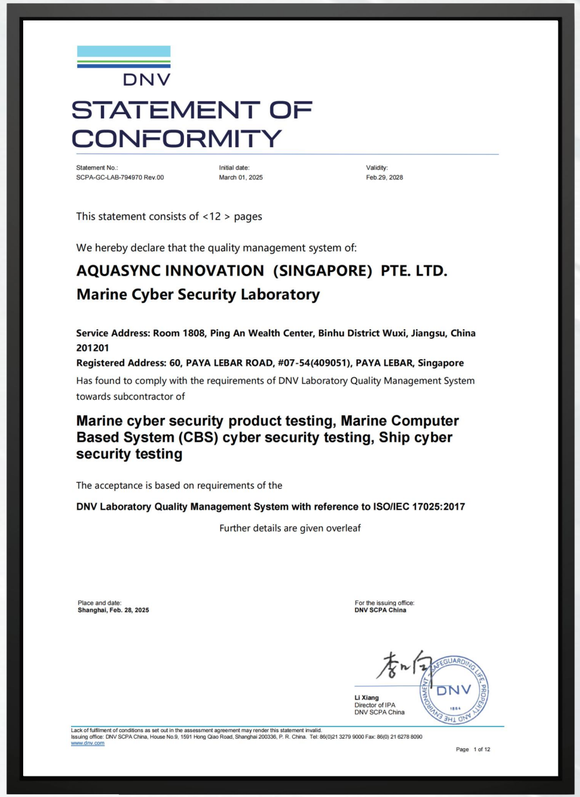
DNV ISO/IEC 17025 Certification

- **Baseline Verification**
- **Vulnerability Scanning**
- **Penetration Testing**
- **E27 & E26 Compliance Testing**

DNV

ISO/IEC 17025:2017

Marine Cybersecurity Product Testing, Marine Computer Based System(CBS) Cybersecurity Testing, Ship Cybersecurity Testing



DNV

STATEMENT OF CONFORMITY

Statement No.: SCPA-GC-LAB-794970 Rev.00

Initial date: March 01, 2025

Validity: Feb 29, 2028

This statement consists of <12 > pages

We hereby declare that the quality management system of:

AQUASYNC INNOVATION (SINGAPORE) PTE. LTD.
Marine Cyber Security Laboratory

Service Address: Room 1808, Ping An Wealth Center, Binhu District Wuxi, Jiangsu, China 201201
Registered Address: 60, PAYA LEBAR ROAD, #07-54(409051), PAYA LEBAR, Singapore

Has found to comply with the requirements of DNV Laboratory Quality Management System towards subcontractor of

Marine cyber security product testing, Marine Computer Based System (CBS) cyber security testing, Ship cyber security testing

The acceptance is based on requirements of the

DNV Laboratory Quality Management System with reference to ISO/IEC 17025:2017

Further details are given overleaf

Place and date: **Shanghai, Feb. 28, 2025**

For the issuing office: **DNV SCPA China**

Li Xiang
Director of IPA
DNV SCPA China

Lack of fulfilment of conditions as set out in the assessment agreement may render this statement invalid.
Issuing office: DNV SCPA China, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: (86)(21 3279 9000 Fax: (86)(0 21 6278 8090
www.dnv.com

Page 1 of 12

IEC 62443 4-2

Marine Defender System

DNV

CERTIFICATE

Certificate No.:	Initial certification date:	Valid Until:
IPA-CS-10488181-2025JA01	2025-01-10	2030-01-09

Certificate Holder: AQUASYNC INNOVATION (SINGAPORE) PTE.LTD.

Location: (1) 60, PAYA LEBAR ROAD, #07-54 (409051), PAYA LEBAR SINGAPORE
(2) Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, CHINA

Codes and Standards: **IEC 62443-4-2:2019**

Certificate Coverage (including Version): Product: Marine Defender System
Model: SO-MDS01
Version: V2.20.00.00

Security Level Achieved: **Security Level 2**

Requirements Assessed Total Requirements: FR 1 - Identification and Authentication Control (AC): 13/14
FR 2 - Use Control (UC): 11/13
FR 3 - System Integrity (DI): 12/14
FR 4 - Data Confidentiality (DC): 3/5
FR 5 - Restricted Data Flow (RDF): 3/5
FR 6 - Timely Response to Events (TRE): 2/2
FR 7 - Resource Availability (RA): 8/8

Validity: This certificate is valid until **2030-01-09**.

This certificate of conformity is based on an assessment conducted by DNV, the results of which are documented in Report No. *Rep-IPA-CS-10488181-2025JA01*, dated *2025-01-06*. The process capability for this product has been previously assessed for compliance with the IEC 62443-4-1 standard, as detailed in Report Reference No. *Rep-IPA-CS-10488181-2024DE01*.

This certification applies only to the products specified within the coverage statement, including names, models, and version.

Place and date: Shanghai, China 2025-01-10

Vincent Zhao Ph.D
Head of Transportation & Cybersecurity Assurance

Li Xiang
Product Assurance & Inspection Service Director of Greater China

DNV BUSINESS ASSURANCE CHINA Co. LTD, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: 86 (0) 21 3279 9000 Fax: 86 (0) 21 6278 8090

Marine Network Firewall

DNV

CERTIFICATE

Certificate No.:	Initial certification date:	Valid Until:
IPA-CS-10488181-2024DC02	2024-12-12	2029-12-11

Certificate Holder: AQUASYNC INNOVATION (SINGAPORE) PTE.LTD.

Location: (1) 60, PAYA LEBAR ROAD, #07-54 (409051), PAYA LEBAR SINGAPORE
(2) Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, CHINA

Codes and Standards: **IEC 62443-4-2:2019**

Certificate Coverage (including Version): Product: Marine Network Firewall
Model: SO-MFW-100M
Version: SO-MFW V4.0

Security Level Achieved: **Security Level 2**

Requirements Assessed Total Requirements: FR 1 - Identification and Authentication Control (AC): 12/14
FR 2 - Use Control (UC): 9/13
FR 3 - System Integrity (DI): 12/14
FR 4 - Data Confidentiality (DC): 3/5
FR 5 - Restricted Data Flow (RDF): 3/5
FR 6 - Timely Response to Events (TRE): 2/2
FR 7 - Resource Availability (RA): 8/8

Validity: This certificate is valid until **2029-12-11**.

This certificate of Conformity is based on an assessment conducted by DNV, the results of which are documented in Report No. *Rep-IPA-CS-10488181-2024DC02*, dated *2024-12-08*. The process capability for this product has been previously assessed for compliance with the IEC 62443-4-1 standard, as detailed in Report Reference No. *Rep-IPA-CS-10488181-2024DC01*.

This certification applies only to the products specified within the coverage statement, including names, models, and version.

Place and date: Shanghai, China 2024-12-12

Vincent Zhao Ph.D
Head of Transportation & Cybersecurity Assurance

Li Xiang
Product Assurance & Inspection Service Director of Greater China

DNV BUSINESS ASSURANCE CHINA Co. LTD, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: 86 (0) 21 3279 9000 Fax: 86 (0) 21 6278 8090

Network Security Detection System

DNV

CERTIFICATE

Certificate No.:	Initial certification date:	Valid Until:
IPA-CS-10488181-2025MR01	2025-02-28	2030-02-27

Certificate Holder: AQUASYNC INNOVATION (SINGAPORE) PTE.LTD.

Location: (1) 60, PAYA LEBAR ROAD, #07-54 (409051), PAYA LEBAR SINGAPORE
(2) Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, CHINA

Codes and Standards: **IEC 62443-4-2:2019**

Certificate Coverage (including Version): Product: Network Security Detection System
Model: SO-NSDS01
Version: V4.0

Security Level Achieved: **Security Level 2**

Requirements Assessed Total Requirements: FR 1 - Identification and Authentication Control (AC): 13/16
FR 2 - Use Control (UC): 9/23
FR 3 - System Integrity (SI): 17/35
FR 4 - Data Confidentiality (DC): 3/3
FR 5 - Restricted Data Flow (RDF): 4/4
FR 6 - Timely Response to Events (TRE): 2/2
FR 7 - Resource Availability (RA): 8/9

Validity: This certificate is valid until **2030-02-27**.

This certificate of conformity is based on an assessment conducted by DNV, the results of which are documented in Report No. *Rep-IPA-CS-10488181-2025MR01*, dated *2025-02-26*. The process capability for this product has been previously assessed for compliance with the IEC 62443-4-1 standard, as detailed in Report Reference No. *Rep-IPA-CS-10488181-2024DE01*.

This certification applies only to the products specified within the coverage statement, including names, models, and version.

Place and date: Shanghai, China 2025-02-28

Vincent Zhao Ph.D
Technical Director of Transportation & Cybersecurity Assurance

Li Xiang
Product Assurance & Inspection Service Director of Greater China

DNV BUSINESS ASSURANCE CHINA Co. LTD, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: 86 (0) 21 3279 9000 Fax: 86 (0) 21 6278 8090

Cybersecurity Management Platform

DNV

CERTIFICATE

Certificate No.:	Initial certification date:	Valid Until:
IPA-CS-10488181-2025MA02	2025-03-03	2030-03-02

Certificate Holder: AQUASYNC INNOVATION (SINGAPORE) PTE.LTD.

Location: (1) 60, PAYA LEBAR ROAD, #07-54 (409051), PAYA LEBAR SINGAPORE
(2) Room1808, Pingan Fortune Center, Binhu District, Wuxi, Jiangsu, CHINA

Codes and Standards: **IEC 62443-4-2:2019**

Certificate Coverage (including Version): Product: Network Security Management Platform
Model: SO-NSMP01
Version: V3.0

Security Level Achieved: **Security Level 2**

Requirements Assessed Total Requirements: FR 1 - Identification and Authentication Control (AC): 13/16
FR 2 - Use Control (UC): 9/23
FR 3 - System Integrity (SI): 17/35
FR 4 - Data Confidentiality (DC): 3/3
FR 5 - Restricted Data Flow (RDF): 4/4
FR 6 - Timely Response to Events (TRE): 2/2
FR 7 - Resource Availability (RA): 8/9

Validity: This certificate is valid until **2030-03-02**.

This certificate of conformity is based on an assessment conducted by DNV, the results of which are documented in Report No. *Rep-IPA-CS-10488181-2025MA02*, dated *2025-02-28*. The process capability for this product has been previously assessed for compliance with the IEC 62443-4-1 standard, as detailed in Report Reference No. *Rep-IPA-CS-10488181-2024DE01*.

This certification applies only to the products specified within the coverage statement, including names, models, and version.

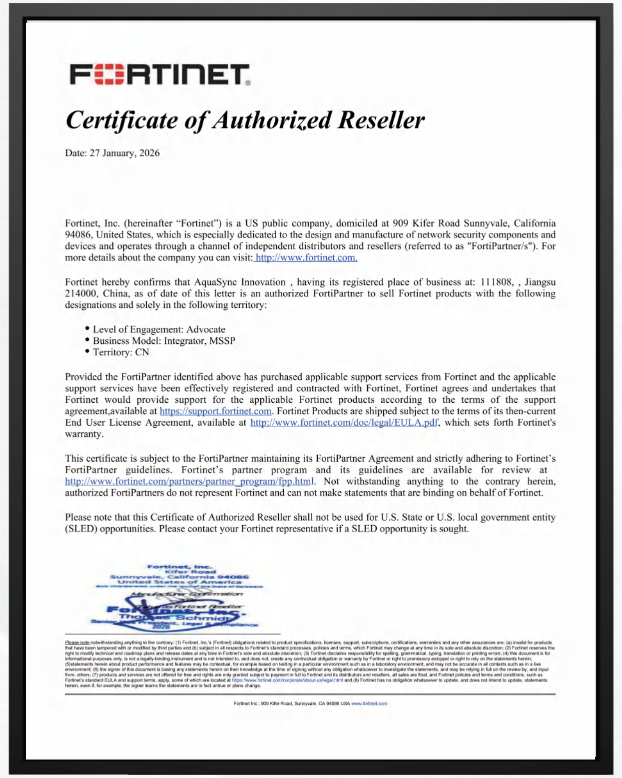
Place and date: Shanghai, China 2025-03-03

Vincent Zhao Ph.D
Technical Director of Transportation & Cybersecurity Assurance

Li Xiang
Product Assurance & Inspection Service Director of Greater China

DNV BUSINESS ASSURANCE CHINA Co. LTD, House No.9, 1591 Hong Qiao Road, Shanghai 200336, P. R. China. Tel: 86 (0) 21 3279 9000 Fax: 86 (0) 21 6278 8090

ASI Forms Strategic Alliance with Fortinet



FORTINET

Certificate of Authorized Reseller

Date: 27 January, 2026

Fortinet, Inc. (hereinafter "Fortinet") is a US public company, domiciled at 909 Kifer Road Sunnyvale, California 94086, United States, which is especially dedicated to the design and manufacture of network security components and devices and operates through a channel of independent distributors and resellers (referred to as "FortiPartner/s"). For more details about the company you can visit: http://www.fortinet.com.

Fortinet hereby confirms that AquaSync Innovation , having its registered place of business at: 111808, , Jiangsu 214000, China, as of date of this letter is an authorized FortiPartner to sell Fortinet products with the following designations and solely in the following territory:

- Level of Engagement: Advocate
- Business Model: Integrator, MSSP
- Territory: CN

Provided the FortiPartner identified above has purchased applicable support services from Fortinet and the applicable support services have been effectively registered and contracted with Fortinet, Fortinet agrees and undertakes that Fortinet would provide support for the applicable Fortinet products according to the terms of the support agreement,available at https://support.fortinet.com. Fortinet Products are shipped subject to the terms of its then-current End User License Agreement, available at http://www.fortinet.com/doc/legal/EULA.pdf, which sets forth Fortinet's warranty.

This certificate is subject to the FortiPartner maintaining its FortiPartner Agreement and strictly adhering to Fortinet's FortiPartner guidelines. Fortinet's partner program and its guidelines are available for review at http://www.fortinet.com/partners/partner_program/fpp.html. Not withstanding anything to the contrary herein, authorized FortiPartners do not represent Fortinet and can not make statements that are binding on behalf of Fortinet.

Please note that this Certificate of Authorized Reseller shall not be used for U.S. State or U.S. local government entity (SLED) opportunities. Please contact your Fortinet representative if a SLED opportunity is sought.

Fortinet, Inc.
Kifer Road
Sunnyvale, California 94086
United States of America

Thomas Schmidt
Senior Vice President, Legal & Compliance

The maritime cybersecurity company ASI has signed a strategic cooperation agreement with Fortinet. Together, they will target global shipowners and shipyards, promoting cybersecurity cooperation and market promotion.

CCS Certification

中国船级社
CHINA CLASSIFICATION SOCIETY

证书编号/Certificate No.
ZG23PTB00184

型 式 认 可 证 书
CERTIFICATE OF TYPE APPROVAL

兹证明本证书所述制造厂具备按照下列标准的要求生产本证书所列产品的能力和条件。
This is to certify that the manufacturer stated in the certificate meets the requirements of the standards listed below and is available with the ability and conditions to produce the products described in the certificate.

制造厂/Manufacturer

中控海洋装备（浙江）有限公司
Supcon Ocean Technology (Zhejiang) Co., Ltd

地址/Address

中国浙江省杭州市富阳区东洲街道高尔夫路 209 号第 4 幢 308 室，邮编：311401
Room 308, Building 4, No.209 Gaoerfu Road, Dongzhou Subdistrict, Fuyang District, Hangzhou City, Zhejiang Province, postal code:311401

产品名称/Product

船舶网络防火墙
Marine Network Firewall
船舶网络安全设备
Marine Network Security Device

附加标志/Notations

无/Nil.

认可标准/Approval Standard

1. 中国船级社《钢质海船入级规范》（2023）及其变更通报第7篇第2章
Chapter 2, Part Seven, China Classification Society Rules for Classification of Sea-going Steel Ships 2023 and its Change Notices
2. 中国船级社《船舶网络防火墙检验指南》（2023）
China Classification Society Guidelines for Inspection of Ship Network Firewall
3. IACS UR E27《船载系统和设备的网络韧性》
IACS UR E27 Cyber Resilience of On-board Systems and Equipment

用于/Intended for

船舶/Ships

产品明细/Product Description

船舶网络安全设备/Marine Network Security Device (M0001)

名称/Name	属性（值）/Value	单位/Unit
产品名称/Product Name	船舶网络防火墙 Marine Network Firewall	

证书有效期至/This Certificate is valid until 2027年09月18日/ Sep. 18,2027

发证机构 中国船级社浙江分社 签发日期 2023年09月19日
Issued by CCS Zhejiang Branch Date Sep. 19,2023

本证书根据中国船级社规范和相关规定签发。所有证书页为一个整体，必须同时使用。纸质证书每页均须由本社盖章方为有效，电子证书含数字签名方为有效，本证书复印件无效。任何单位和个人均不应摘录或节选本证书的部分内容。有关方对所持证书的真实性有疑问时，可以向我社检验机构咨询。
This Certificate is issued pursuant to the Rules of the Society and related regulation. All pages of the certificate are taken as a whole and are used simultaneously. No paper certificate page is valid without bearing the stamp of the Society, no electronic certificates is valid without the digital signature, and no copied form of the certificate is regarded as valid. Any part of the certificate is not to be extracted or abridged by any unit or individual in any form. Related parties who are doubted about the authenticity of the certificate may inquire of the Society or its offices.

Form No: T01. 联系方式/Contact Us，见本社官方网站/See official web site of the Society（http://www.ccs.org.cn） UTN:P023-99158695

第1页共3页/Page 1 of 3

The Marine Network Firewall we provide has obtained the first CCS Domestic Type Approval Certificate for Cybersecurity equipment.

China National Accreditation Service for Conformity Assessment
Inspection body accreditation certificate —— DNV, SUPCON (ASI)

China National Accreditation Service for Conformity Assessmer

LABORATORY ACCREDITATION CERTIFICATE

(Registration No. CNAS L15265)

Automatic Instrument & Control System Laboratory Center, Zhejiang SUPCON Technology Co., Ltd.

(Legal Entity: Zhejiang SUPCON Technology Co., Ltd.)

4/F., Zone C, & 1/F., Zone A, SUPCON Park, No.309, Liuhe Road, Binjiang District, Hangzhou, Zhejiang, China

is accredited in accordance with ISO/IEC 17025: 2017 General Requirements for the Competence of Testing and Calibration Laboratories(CNAS-CL01 Accreditation Criteria for the Competence of Testing and Calibration Laboratories) for the competence to undertake the service described in the schedule attached to this certificate.

The scope of accreditation is detailed in the attached schedule bearing the same registration number as above. The schedule forms an integral part of this certificate.

Effective Date：2022-10-21

Expiry Date：2027-08-11

Signed on behalf of China National Accreditation Service for Conformity Assessment

China National Accreditation Service for Conformity Assessment (CNAS) is authorized by Certification and Accreditation Administration of the People's Republic of China (CNCA) to operate the national accreditation schemes for conformity assessment. CNAS is a signatory of the International Laboratory Accreditation Cooperation Mutual Recognition Arrangement (ILAC MRA) and the Asia Pacific Accreditation Cooperation Mutual Recognition Arrangement (APAC MRA).
The validity of the certificate can be checked on CNAS website at http://www.cnas.org.cn/english/findanaccreditedbody/index.shtml.

China National Accreditation Service for Conformity Assessment

INSPECTION BODY ACCREDITATION CERTIFICATE

(Registration No. CNAS IB0481)

DNV Business Assurance (China) Co., Ltd.

(Legal Entity: DNV Business Assurance (China) Co., Ltd.)

Block A, Building 9, No.1591, Hongqiao Road, Changning District, Shanghai, China

is accredited in accordance with ISO/IEC 17020: 2012 General Criteria for the Operation of Various Types of Bodies Performing Inspection(CNAS-CI01 Accreditation Criteria for the competence of Inspection Bodies) as Type A inspection body for the competence to undertake inspection services as described in the schedule attached to this certificate.

The scope of accreditation is detailed in the attached schedule bearing the same registration number as above. The schedule forms an integral part of this certificate.

Effective Date：2025-02-28

Expiry Date：2031-02-27

Signed on behalf of China National Accreditation Service for Conformity Assessment

China National Accreditation Service for Conformity Assessment (CNAS) is authorized by Certification and Accreditation Administration of the People's Republic of China (CNCA) to operate the national accreditation schemes for conformity assessment. CNAS is a signatory of the International Laboratory Accreditation Cooperation Mutual Recognition Arrangement (ILAC MRA) and the Asia Pacific Accreditation Cooperation Mutual Recognition Arrangement (APAC MRA).
The validity of the certificate can be checked on CNAS website at http://www.cnas.org.cn/english/findanaccreditedbody/index.shtml.

Our Service Capabilities - Personnel Qualifications

YOUR SHIP'S GUARDIAN IN THE DIGITAL AGE

Performance Report

PART FIVE

Statistics on Ships Supported for Cybersecurity Certification – E26

	NO.	Ship Type	LR	ABS	BV	NK	CCS	RINA	DNV	TOTAL
2024	1	Container	10				10			20
	2	Oil ChemicalTanker	24							24
		TOTAL	**34**	**0**	**0**	**0**	**10**	**0**	**0**	**44**

	NO.	Ship Type	LR	ABS	BV	NK	CCS	RINA	DNV	TOTAL
2025	1	Container	6	3	10		13		16	48
	2	Oil ChemicalTanker	10	36	6		13	4	8	77
	3	Platform supply Vessel		3			4			7
	4	CableLaying Vessel	1							1
	5	AHT		6	2					8
	6	Deck Carrier					1			1
	7	Bulk carrier					7			7
	8	refrigeratedtransportvessel					6			6
	9	Offshore Operation Vessel		4			1			5
		TOTAL	**17**	**52**	**18**	**0**	**45**	**4**	**24**	**160**

	NO.	Ship Type	LR	ABS	BV	NK	CCS	RINA	DNV	TOTAL
2026/3/30	1	Container	4	8	8		11		28	59
	2	Oil ChemicalTanker					2		4	6
	3	Platform supply Vessel			2					2
	4	CableLaying Vessel								0
	5	AHT								0
	6	Deck Carrier								0
	7	Bulk carrier			1	3			2	6
	8	refrigeratedtransportvessel								0
	9	Offshore Operation Vessel		6	2					8
		TOTAL	**4**	**14**	**13**	**3**	**13**	**0**	**34**	**81**

As of March 30, 2026: **285**

“Assisting SWS with Obtaining China's First CCS Ship Cybersecurity Principle Recognition (SL2 AIP) Certificate for 300,000-ton Ammonia Dual-Fuel VLCC”

On June 26, 2024, the 300,000-ton ammonia dual-fuel VLCC independently developed by SHANGHAI WAIGAOQIAO SHIPBUILDING CO.,LTD (SWS) received the Approval in Principle (AIP) certificate for ship cybersecurity from the CCS. This certification satisfies the IACS unified requirements for ship cyber resilience (UR E26) and meets the classification symbol requirements of CCS cybersecurity (P[SL2]). According to the CCS "Guidelines for Ship Cybersecurity," cybersecurity ratings range from SL0 to SL4, with five levels in total. Compared to the entry-level SL0, this project achieved SL2, which was determined by comprehensively balancing the ship's cybersecurity and implementation feasibility. This certification significantly enhances the ship's ability to defend against cyber-attacks and meets the high-security network demands driven by the digital, intelligent, and green transformation trends in the shipping industry.

“Assisting COSCO with Achieving CCS Cybersecurity Level SL0 AIP Recognition”

On June 18, 2024, CHINA CLASSIFICATION SOCIETY (CCS) AWARDED COSCO SHIPPING HEAVY INDUSTRY CO., LTD. (referred to as COSCO) the first-ever cybersecurity principle recognition certificate for their 64,000 DWT bulk carrier. This certification marks the first time CCS has issued a principle recognition certificate for ship cybersecurity on an actual vessel. The recognition meets the requirements of both IACS UR E26 and CCS "Guidelines for Ship Cybersecurity," providing a reasonable and feasible solution for this type of bulk carrier to comply with IACS UR E26 standards.

Testing Services for A Total of 20 Vessels Were Actually Delivered

16 Vessels

HULL NOS.: NTS 0311544/ 0311545 115K DWT DOUBLE HULL OIL TANKER

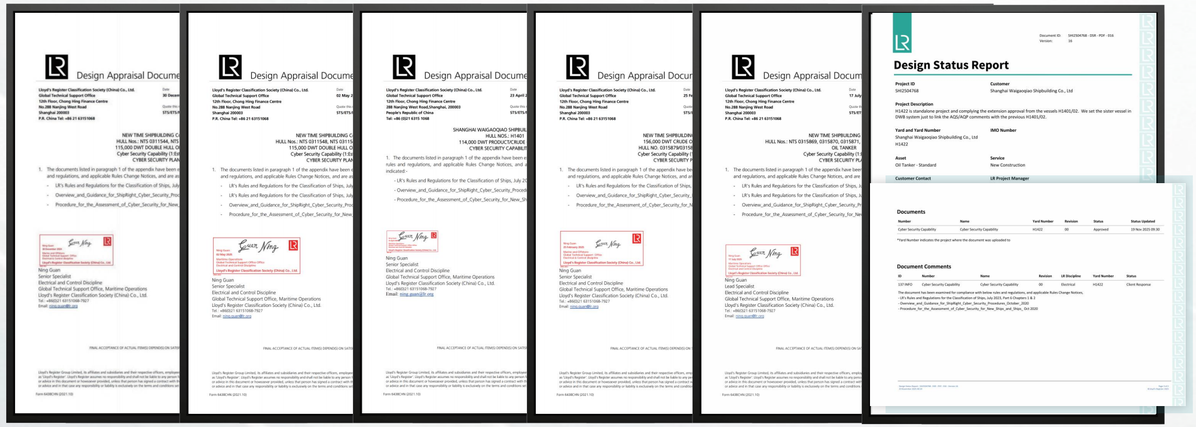
HULL NOS.: NTS 0311548/0311549/0311556 115K DWT DOUBLE HULL OIL TANKER

HULL NOS.: H1401 114K DWT PRODUCT/CRUDE OIL TANKER

HULL NOS.: 0315879/0315880/0315881 156K DWT CRUDE OIL TANKER

HULL Nos.: NTS 0315869/0315870/0315871/0315872/0315873/0315874 OIL TANKER

HULL Nos.: H1422 114000DWT Cybersecurity Services



8 Vessels

HullNo.:0330001/0330002 299500DWT CRUDE OIL TANKER

HullNo.:H1594/H1595 114K DWT POT-ABS Cybersecurity Technology Supply and Services

Hull No.: 0315843/0315844/0315847/0315848 Cyber Security Capability

1 Vessels

Hul No.:0307373 PETROKARAVO