API MARINE

POWERED BY
SANGO MARINE

API MARINE TRIDENT CYBER SECURITY SYSTEM

SENSORS & AUTOMATION SYSTEM · POWER GENERATION · DIGITAL SOLUTIONS

API
MARINE
POWERED BY
SANGO MARINE

WWW.API-MARINE.COM

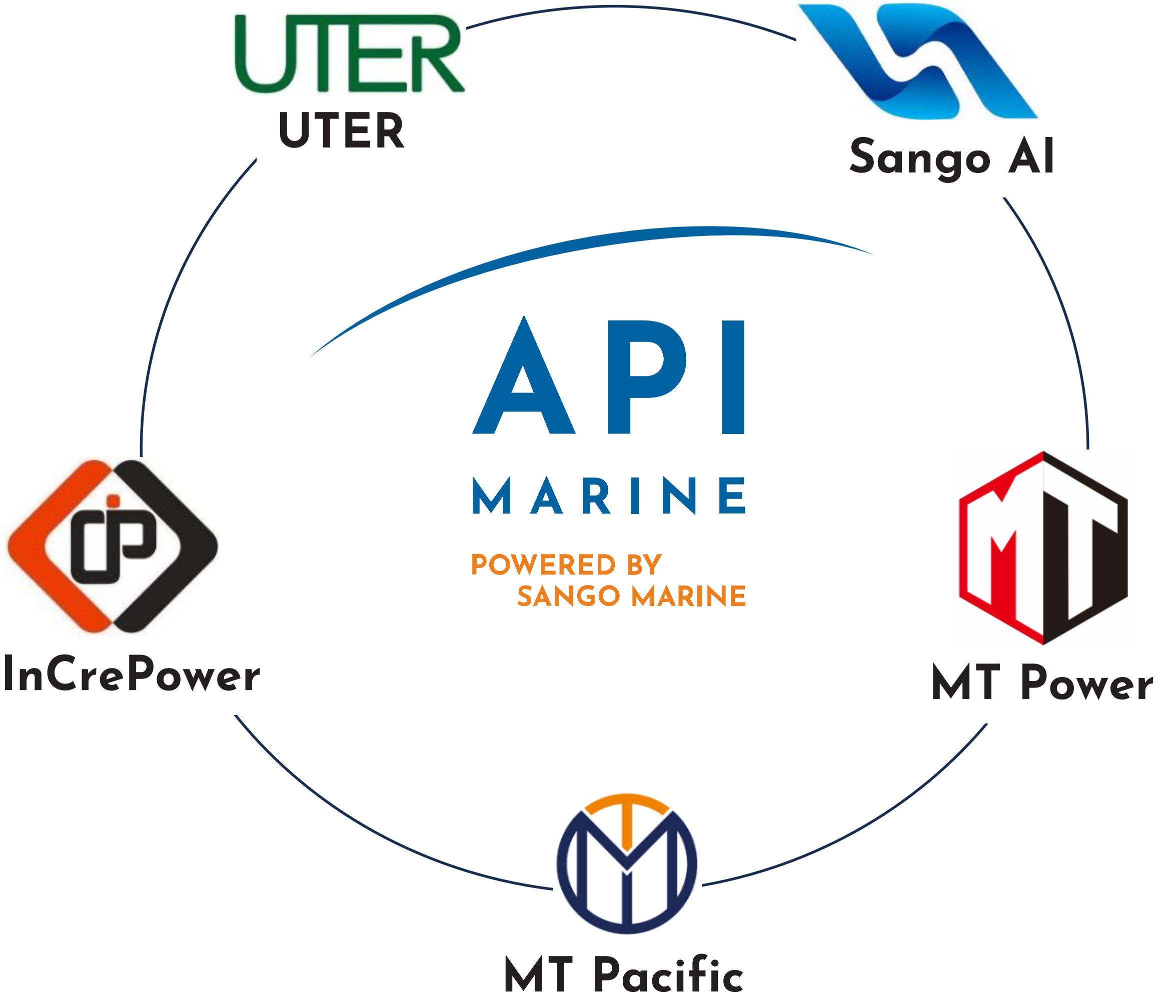
API MARINE
Trident Cyber Security System

AGENDA

1. Company Information
2. Rules & Regulations
3. Scope of Service & Supply
4. Reference Projects

1. Company Information

API MARINE / MT POWER
Group Companies



UTER

Sango AI

API
MARINE
POWERED BY
SANGO MARINE

InCrePower

MT Power

MT Pacific

API
MARINE
POWERED BY
SANGO MARINE

API MARINE / MT POWER
Group Locations

Europe Region
API Marine Aps
Troensevej 12, Aalborg Oest, Denmark

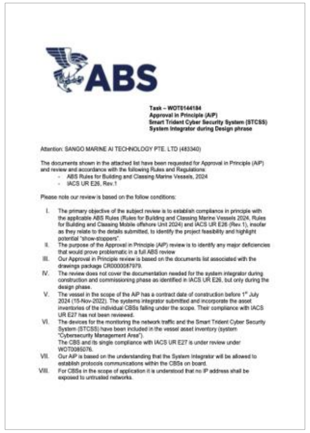
Asia Region
Sango Marine AI Pte Ltd
50 Ubi Crescent #01-10Ubi Techpark,
Singapore 408568

Greater China Region
Fujian Sango Marine AI Co., Ltd
Xiamen, Wuhan , Zhuhai,
P.R. China

Middle East Region
Sango Marine AI LLC
3204 12 EKAA3204 , Al Khobar, Saudi Arabia

24/7 global integrated one-stop service

Class Society Certifications



ABS

Task – WOT0144184
Approval in Principle (AiP)
Smart Trident Cyber Security System (STCSS)
System Integrator during Design phrase

Attention: SANGO MARINE AI TECHNOLOGY PTE. LTD (483340)

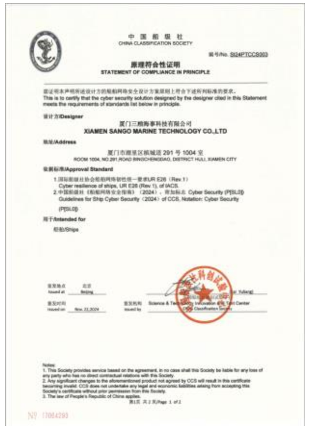
The documents shown in the attached list have been requested for Approval in Principle (AiP) and review and accordance with the following Rules and Regulations:

- ABS Rules for Building and Classing Marine Vessels, 2024
- IACS UR E26, Rev.1

Please note our review is based on the follow conditions:

I. The primary objective of the subject review is to establish compliance in principle with the applicable ABS Rules (Rules for Building and Classing Marine Vessels 2024, Rules for Building and Classing Mobile offshore Unit 2024) and IACS UR E26 (Rev.1), insofar as they relate to the details submitted, to identify the project feasibility and highlight potential "show-stoppers".
II. The purpose of the Approval in Principle (AiP) review is to identify any major deficiencies that would prove problematic in a full ABS review
III. Our Approval in Principle review is based on the documents list associated with the drawings package CR0000087979.
IV. The review does not cover the documentation needed for the system integrator during construction and commissioning phase as identified in IACS UR E26, but only during the design phase.
V. The vessel in the scope of the AiP has a contract date of construction before 1st July 2024 (15-Nov-2022). The systems integrator submitted and incorporate the asset inventories of the individual CBSs falling under the scope. Their compliance with IACS UR E27 has not been reviewed.
VI. The devices for the monitoring the network traffic and the Smart Trident Cyber Security System (STCSS) have been included in the vessel asset inventory (system "Cybersecurity Management Area").
The CBS and its single compliance with IACS UR E27 is under review under WOT0085076.
VII. Our AiP is based on the understanding that the System Integrator will be allowed to establish protocols communications within the CBSs on board.
VIII. For CBSs in the scope of application it is understood that no IP address shall be exposed to untrusted networks.

ABS Cyber Security
(UR E26 & Cyber Resilience)



中 国 船 级 社
CHINA CLASSIFICATION SOCIETY

编号/No. SI24PTCCS003

原理符合性证明
STATEMENT OF COMPLIANCE IN PRINCIPLE

This is to certify that the cyber security solution designed by the designer cited in this Statement meets the requirements of standards list below in principle.

设计方/Designer
厦门三顺海事科技有限公司
XIAMEN SANGO MARINE TECHNOLOGY CO.,LTD

地址/Address
厦门市湖里区槟城道 291 号 1004 室
ROOM 1004, NO.291,ROAD BINGCHENGDAO, DISTRICT HULI, XIAMEN CITY

依据标准/Approval Standard
1. Cyber resilience of ships, UR E26 (Rev.1), of IACS.
2. Guidelines for Ship Cyber Security（2024）of CCS, Notation: Cyber Security (P[SL0])

用于/Intended for
船舶/Ships

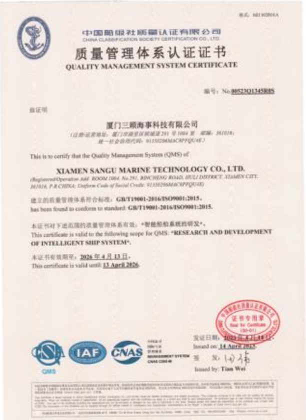
签发地点 Issued at: 北京 Beijing
签发时间 Issued on: Nov. 22,2024
签发机构 Issued by: Science & Technology Innovation and Test Center, China Classification Society

Notes:
1. This Society provides service based on the agreement, in no case shall this Society be liable for any loss of any party who has no direct contractual relations with this Society.
2. Any significant changes to the aforementioned product not agreed by CCS will result in this certificate becoming invalid. CCS does not undertake any legal and economic liabilities arising from accepting this Society's certificate without prior permission from this Society.
3. The law of People's Republic of China applies.

第1页 共2页/Page 1 of 2

№ 1064293

CCS Cyber Security
(P SL[0])



中国船级社质量认证有限公司
CHINA CLASSIFICATION SOCIETY CERTIFICATION CO., LTD

质量管理体系认证证书
QUALITY MANAGEMENT SYSTEM CERTIFICATE

编号：No.00523Q1345R0S

兹证明
厦门三顺海事科技有限公司

This is to certify that the Quality Management System (QMS) of

XIAMEN SANGU MARINE TECHNOLOGY CO., LTD.

(Registered/Operation Add: ROOM 1004, No.291, BINCHENG ROAD, HULI DISTRICT, XIAMEN CITY, 361016, P.R.CHINA; Uniform Code of Social Credit: 91350206MA8CBPFQU4E)

建立的质量管理体系符合标准：GB/T19001-2016/ISO9001:2015。
has been found to conform to standard: GB/T19001-2016/ISO9001:2015.

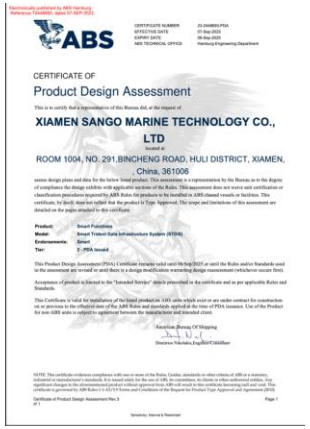
本证书对下述范围的质量管理体系有效："智能船舶系统的研发"。
This certificate is valid to the following scope for QMS: "RESEARCH AND DEVELOPMENT OF INTELLIGENT SHIP SYSTEM".

本证书有效期至：2026年4月13日。
This certificate is valid until 13 April 2026.

发证日期：2023年4月14日
Issued on: 14 April 2023
签发：
Issued by: Tian Wei

证书专用章
Seal for Certificate

ISO-9001



Electronically published by ABS Hamburg.
Reference T2448693, dated 07-SEP-2023.

ABS

CERTIFICATE NUMBER 23-2448693-PDA
EFFECTIVE DATE 07-Sep-2023
EXPIRY DATE 06-Sep-2025
ABS TECHNICAL OFFICE Hamburg Engineering Department

CERTIFICATE OF
Product Design Assessment

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

XIAMEN SANGO MARINE TECHNOLOGY CO., LTD

located at

ROOM 1004, NO. 291,BINCHENG ROAD, HULI DISTRICT, XIAMEN, , China, 361006

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 in 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:	Smart Functions
Model:	Smart Trident Data Infrastructure System (STDIS)
Endorsements:	Smart
Tier:	2 - PDA Issued

This Product Design Assessment (PDA) Certificate remains valid until 06/Sep/2025 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.

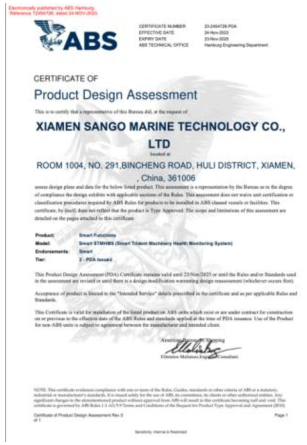
This Certificate is valid for installation of the listed product on ABS units which exist or are under contract for construction on or previous to the effective date of the ABS Rules and standards applied at the time of PDA issuance. Use of the Product for non-ABS units is subject to agreement between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

American Bureau Of Shipping
Dimitrios Nikolakis, Engineer/Consultant

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

Sensitivity: Internal & Restricted

ABS
SMART(INF)



Electronically published by ABS Hamburg.
Reference T2454728, dated 24-NOV-2023.

ABS

CERTIFICATE NUMBER 23-2454728-PDA
EFFECTIVE DATE 24-Nov-2023
EXPIRY DATE 23-Nov-2025
ABS TECHNICAL OFFICE Hamburg Engineering Department

CERTIFICATE OF
Product Design Assessment

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

XIAMEN SANGO MARINE TECHNOLOGY CO., LTD

located at

ROOM 1004, NO. 291,BINCHENG ROAD, HULI DISTRICT, XIAMEN, , China, 361006

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 in 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:	Smart Functions
Model:	Smart STMHMS (Smart Trident Machinery Health Monitoring System)
Endorsements:	Smart
Tier:	2 - PDA Issued

This Product Design Assessment (PDA) Certificate remains valid until 23/Nov/2025 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.

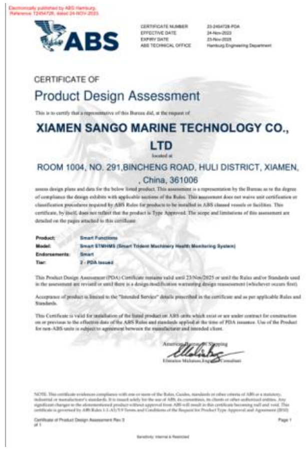
This Certificate is valid for installation of the listed product on ABS units which exist or are under contract for construction on or previous to the effective date of the ABS Rules and standards applied at the time of PDA issuance. Use of the Product for non-ABS units is subject to agreement between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

American Bureau Of Shipping
Eleftherios Mahairas, Engineer/Consultant

Certificate of Product Design Assessment Rev 3 of 1
Page 1

Sensitivity: Internal & Restricted

ABS SMART
(MHM Tier 2)



Electronically published by ABS Hamburg.
Reference T2454728, dated 24-NOV-2023.

ABS

CERTIFICATE NUMBER 23-2454728-PDA
EFFECTIVE DATE 24-Nov-2023
EXPIRY DATE 23-Nov-2025
ABS TECHNICAL OFFICE Hamburg Engineering Department

CERTIFICATE OF
Product Design Assessment

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

XIAMEN SANGO MARINE TECHNOLOGY CO., LTD

located at

ROOM 1004, NO. 291,BINCHENG ROAD, HULI DISTRICT, XIAMEN, , China, 361006

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 in 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:	Smart Functions
Model:	Smart STMHMS (Smart Trident Machinery Health Monitoring System)
Endorsements:	Smart
Tier:	2 - PDA Issued

This Product Design Assessment (PDA) Certificate remains valid until 23/Nov/2025 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
Eleftherios Mahairas, Engineer/Consultant

Certificate of Product Design Assessment Rev 3 of 1
Page 1

Sensitivity: Internal & Restricted

ABS SMART
(SHM Tier 2)

The sole entity worldwide with ABS INF, MHM, and SHM PDA Certifications.

ABS Cyber Security certification

CCS Cyber Security certification

2) Rules and Regulations

Evolution of Maritime Cyber Security

2017

IMO

Resolution MSC.428(98): The safety management system should incorporate cyber risk management. Management companies are encouraged to establish a shipboard cyber risk management system and integrate it into the vessel's safety management system.

2021/01/01

IMO

Resolution MSC.428(98): Officially in effect, marking the beginning of heightened cybersecurity awareness in the shipping industry.

2022/04

IACS

The cybersecurity requirements UR E26 and UR E27 have been approved.

It is mandatory for ships contracted for construction after January 1, 2024, to comply with these requirements within IACS member countries.

2023/11

IACS

Updated UR E26 and UR E27 requirements, with the mandatory enforcement starting on July 1, 2024, signaling the maritime industry's transition into the full implementation phase of cybersecurity.

2024/07/01

Full implementation of UR E26 & UR E27 key milestones.

Maritime Cyber Security System

3 Pillars

Technical means

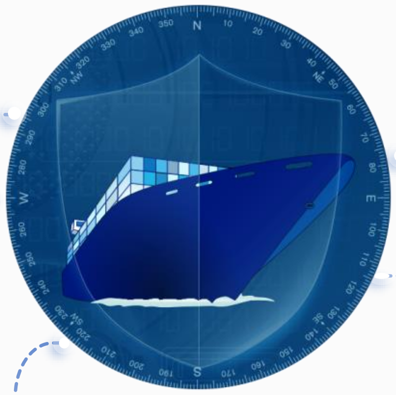
- System design, safety equipment configuration
- Defensive perimeter protection design
- Monitoring & Surveillance Technology

Organization (Person)

- Training and awareness, emergency drills
- Professional skills and qualifications, authorizations and certifications

Procedure

- Management system
- Governance framework, systems and procedures
- Supplier follow-up audits



2 Systems

Product service system

- Defensive products
- Supply and service
- Design/Shipyard/Integrator

Management system

- Ship-end safety management system
- Onshore management system
- Shipowners/Integrators

API
MARINE
POWERED BY
SANGO MARINE

Maritime Cyber Security Standards

WWW.API-MARINE.COM

Class	DNV	BV	CCS	ABS	LR
Security Class	**Cyber secure** Entry-level Establish a cyber security management system to meet IMOMSC.428(98) resolution	**CYBER MANAGED** Applicable to newbuild/operating vessels Establish a cyber security management system	Cyber Security (M, P[SL0]/S[SLx]) **SL0** minimum	**CS-System** Applicable to equipment vendors CS-PDA	**Established Level 1** (IEC62443 SL1) Establishment level, suitable for those who do not have mature interconnection and ship-to-shore interconnection
	Cyber secure (ESSENTIAL) Basic level Verify CBS safety features Ensure SP1 (IEC62443 SL1)	**CYBER SECURE** Only applicable to newbuilding Establish the safety design of the ship and the security of the ship-to-shore communication network	**SL1** Incidental	**CS-Ready** Applicable to newbuilding	**Enhanced Level 2** (IEC62443 SL2) Enhanced, suitable for high-level interoperability or certain threats
	Cyber secure (ADVANCED) Senior Ensure SP3 (IEC62443 SL3)	**CYBER RESILIENT** For newbuilding only Establish the minimum required security resilience against cyberattacks	**SL2** small amount	**CS-1/CS-2** Applicable to operating vessels CS-1 < CS-2	**Accomplished Level 3** (IEC62443 SL3) Completed, suitable for managing complex threats and taking on more advanced risks
	Cyber secure+ Additional, flexible, not part of the basic and advanced. Other systems	-	**SL3** abundant	-	**Optimized Level 4** (IEC62443 SL4) Optimized, suitable for mature security policies and high assurance capabilities
	-	-	**SL4** Organized	-	-

Class Society Certifications

Class Notation Cyber Secure

DNV

SECTION 21 CYBER SECURITY

Cyber secure Entry-level for all merchant vessels/FIS vessels	• For **standard merchant vessel**, security is ensured through policies & procedures, segmentation of networks/zones, secure remote access, etc. • Alligned with compliance towards **IMO Resolution 428(98)** • Intended for existing and newbuildings in of **standard merchant vessel segments**
Cyber secure (ESSENTIAL) Existing vessels with SOLAS essential system coverage	• **Essential** covers the above plus system security capabilities at **Security Profile 1** • Aligned with compliance towards **IACS UR E26&27** • **~ 40 system requirements** from up to IEC62443-3-3 SL-1 • Primarily intended **for existing high end vessels** and **complex newbuilds**
Cyber secure (ADVANCED) Complex newbuildings with higher securty requirements	• **Advanced** covers above plus system security capabilities at **Security Profile 3** • **~ 80 system requirements** from up to IEC62443-3-3 SL-1 • Primarily intended for **advanced ship segments and newbuilds** where cyber security is key focus area; typically require tailored solutions and higher investment
Cyber secure (+) Additional systems and security profiles	• **(+)** provides flexibility. Additional systems and/or other security profiles

API
MARINE
POWERED BY
SANGO MARINE

Class Notation Cyber Security

CCS
CHINA CLASSIFICATION SOCIETY
中国船级社

M, P **(SL0)**	• Defenses that meet minimum security requirements (UR E26). • Meets cyber risk management requirements • There are 68 CCS requirements to be met
SL1	• Defenses against sporadic cyber incidents • Covers the requirements of SL0 • There are 90 CCS requirements to be met
SL2	• Defenses against cyber incidents that utilize a small number of resources • Covers the requirements of SL1 • There are 96 CCS requirements to be met
SL3	• Defenses against cyber incidents that leverage abundant resources • Covers the requirements of SL2 • There are 112 CCS requirements to be met
SL4	• Defenses against organized, purposeful cyber incidents • Covers the requirements of SL3 • There are 119 CCS requirements to be met

API
MARINE
POWERED BY
SANGO MARINE

Class Notation Cyber Security

WWW.API-MARINE.COM

ABS

CS-READY

CS-READY indicates that vessels being outfitted with cyber-enabled systems are constructed and documented in accordance with the ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries in order to support more rapid completion of CS-1 requirements following delivery to the owner.

CS-SYSTEM

CS-SYSTEM indicates that the Original Equipment Manufacturer (OEM) has developed, embedded, and described cybersecurity capabilities in the critical system submitted for notation and communicated unresolved potential cybersecurity vulnerabilities to the shipbuilder and owner.

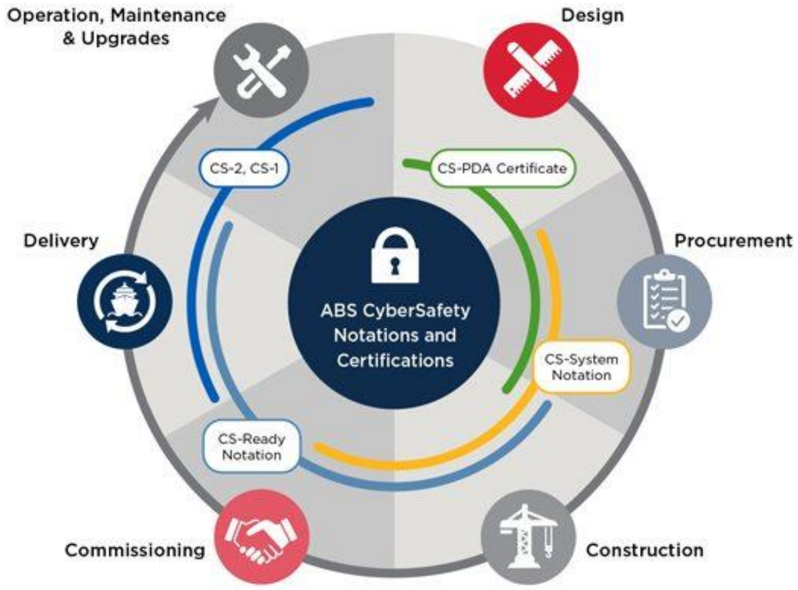
CS-1

CS-1 indicates that cybersecurity risks have been identified onboard, and the necessary steps have been taken to implement the requirements within cybersecurity activities that address those risks.

CS-2

CS-2 indicates the extension of CS-1 cybersecurity activities with additional policies and procedures concerning cybersecurity system management and technical evolution – typically, this is needed for large fleets of vessels.

Cybersecurity for Every Stage of an Asset's Lifecycle

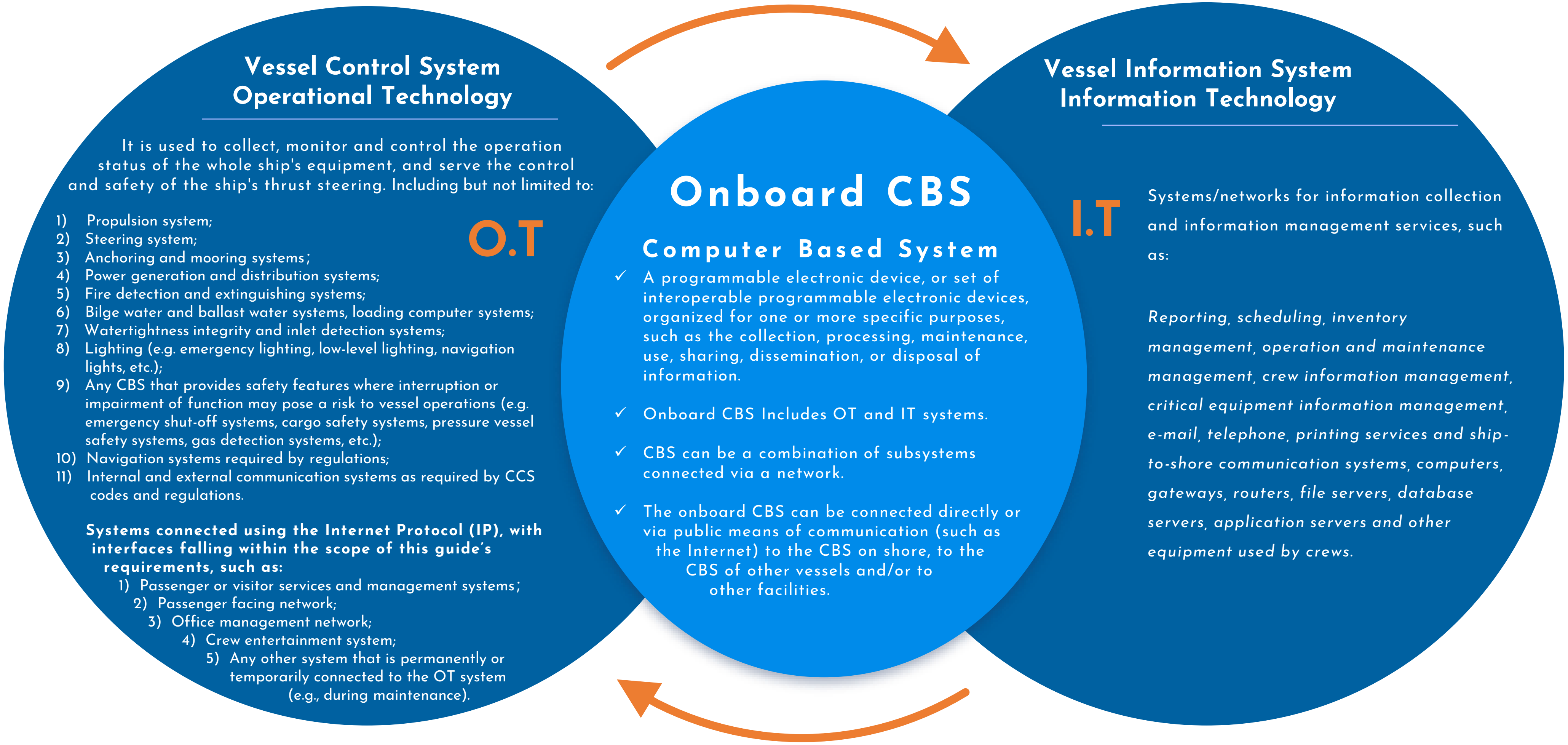


Note: For CS-PDA certification, refer to the ABS *Guide for ABS CyberSafety® for Equipment Manufacturers – ABS CyberSafety® Volume 7.*

API MARINE
POWERED BY SANGO MARINE

Onboard CBS (Computer-Based-System)

WWW.API-MARINE.COM



Vessel Control System
Operational Technology

O.T

It is used to collect, monitor and control the operation status of the whole ship's equipment, and serve the control and safety of the ship's thrust steering. Including but not limited to:

1) Propulsion system;
2) Steering system;
3) Anchoring and mooring systems;
4) Power generation and distribution systems;
5) Fire detection and extinguishing systems;
6) Bilge water and ballast water systems, loading computer systems;
7) Watertightness integrity and inlet detection systems;
8) Lighting (e.g. emergency lighting, low-level lighting, navigation lights, etc.);
9) Any CBS that provides safety features where interruption or impairment of function may pose a risk to vessel operations (e.g. emergency shut-off systems, cargo safety systems, pressure vessel safety systems, gas detection systems, etc.);
10) Navigation systems required by regulations;
11) Internal and external communication systems as required by CCS codes and regulations.

Systems connected using the Internet Protocol (IP), with interfaces falling within the scope of this guide's requirements, such as:

1) Passenger or visitor services and management systems;
2) Passenger facing network;
3) Office management network;
4) Crew entertainment system;
5) Any other system that is permanently or temporarily connected to the OT system (e.g., during maintenance).

Onboard CBS

Computer Based System

✓ A programmable electronic device, or set of interoperable programmable electronic devices, organized for one or more specific purposes, such as the collection, processing, maintenance, use, sharing, dissemination, or disposal of information.

✓ Onboard CBS Includes OT and IT systems.

✓ CBS can be a combination of subsystems connected via a network.

✓ The onboard CBS can be connected directly or via public means of communication (such as the Internet) to the CBS on shore, to the CBS of other vessels and/or to other facilities.

Vessel Information System
Information Technology

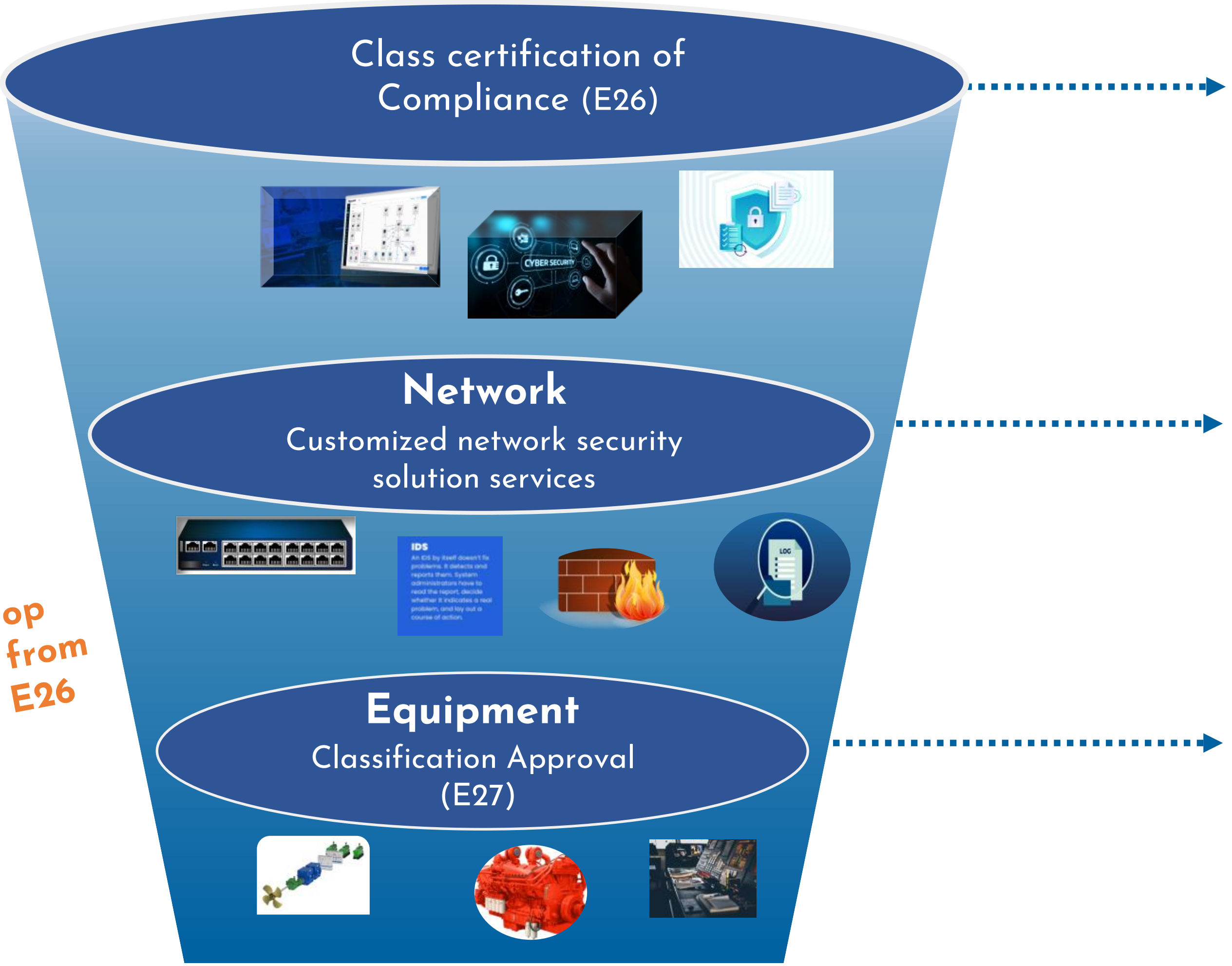
I.T

Systems/networks for information collection and information management services, such as:

Reporting, scheduling, inventory management, operation and maintenance management, crew information management, critical equipment information management, e-mail, telephone, printing services and ship-to-shore communication systems, computers, gateways, routers, file servers, database servers, application servers and other equipment used by crews.

3. Scope of Service & Supply

Business Scope



Class certification of Compliance (E26)

Network
Customized network security solution services

Equipment
Classification Approval (E27)

One-stop solution from E27 to E26

Manage maritime cybersecurity

- Network management and maintenance
- Security management and maintenance
- Cloud management and maintenance
- Remote management and maintenance

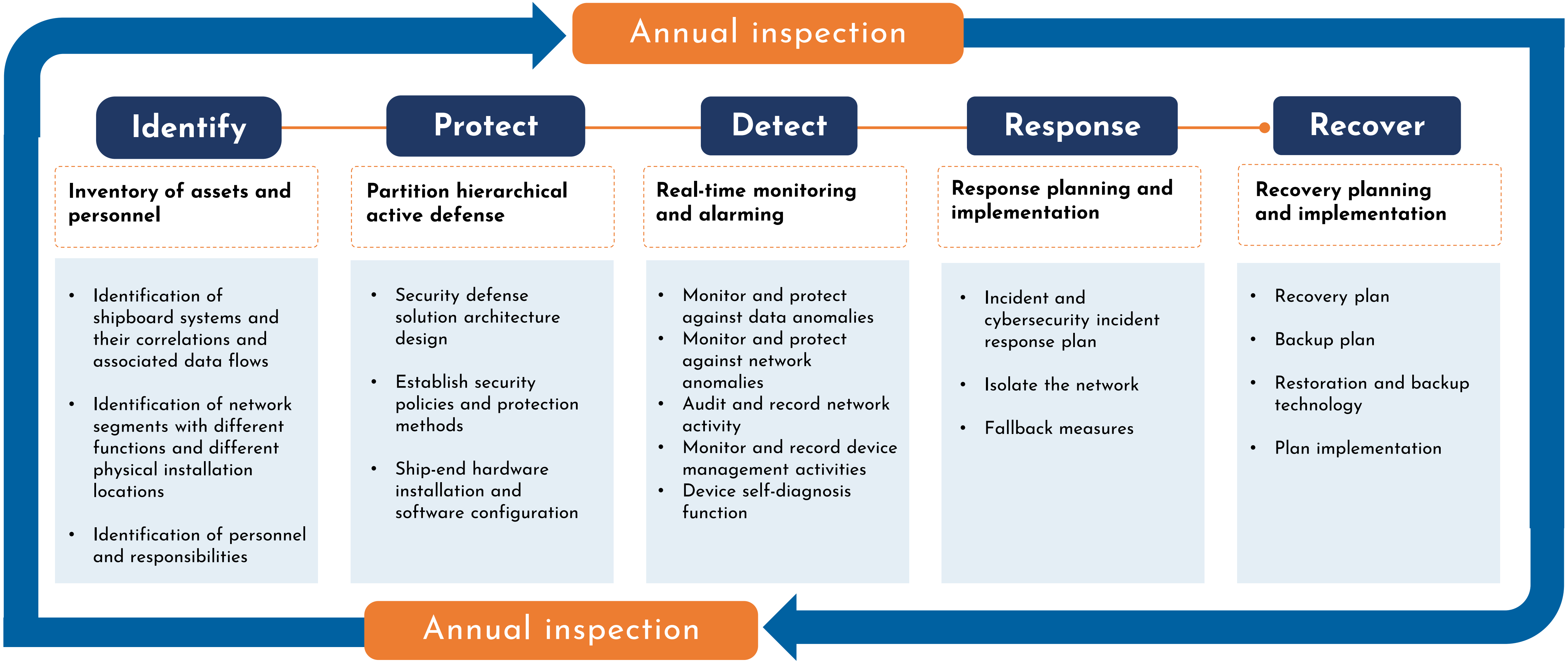
Protect maritime cybersecurity

- Meet UR E26 requirements
- Network partitioning and demarcation of security boundaries
- Establish a security zone and associated links
- Threat protection policies for different security zones

Choose secure IT/OT equipment

- Meet UR E27 requirements
- Identify the security boundaries of device interconnection.
- Determine the level of security
- Determine different levels of security defense strategies

Lifecycle Solutions



Annual inspection

Identify

Inventory of assets and personnel

- Identification of shipboard systems and their correlations and associated data flows
- Identification of network segments with different functions and different physical installation locations
- Identification of personnel and responsibilities

Protect

Partition hierarchical active defense

- Security defense solution architecture design
- Establish security policies and protection methods
- Ship-end hardware installation and software configuration

Detect

Real-time monitoring and alarming

- Monitor and protect against data anomalies
- Monitor and protect against network anomalies
- Audit and record network activity
- Monitor and record device management activities
- Device self-diagnosis function

Response

Response planning and implementation

- Incident and cybersecurity incident response plan
- Isolate the network
- Fallback measures

Recover

Recovery planning and implementation

- Recovery plan
- Backup plan
- Restoration and backup technology
- Plan implementation

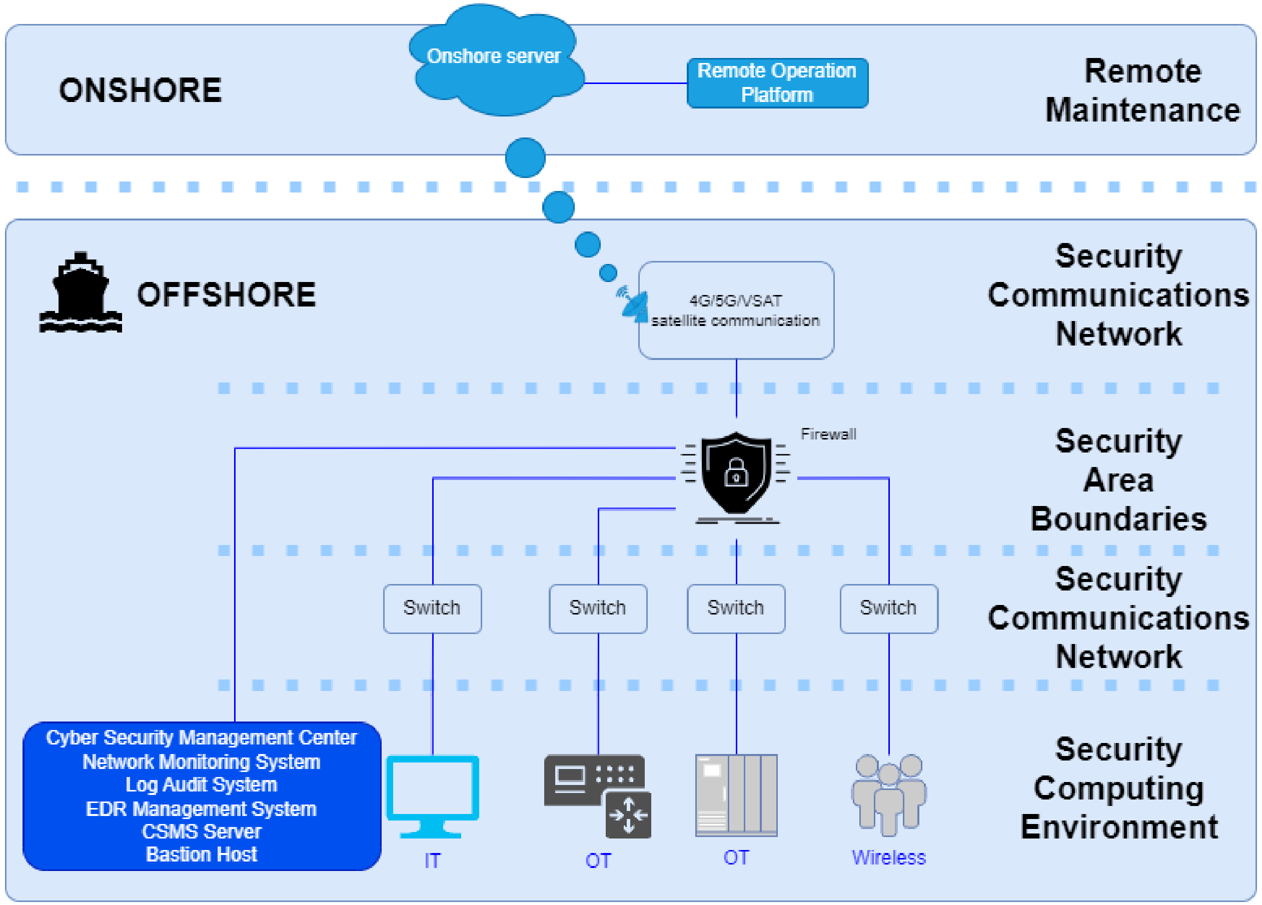
Annual inspection

One-Stop Solution for Cyber Security

Onshore cybersecurity architecture customization service

Class Certification Standards
E26
/
E27

Offshore cybersecurity architecture customization service


ONSHORE
Onshore server
Remote Operation Platform
Remote Maintenance
OFFSHORE
4G/5G/VSAT satellite communication
Security Communications Network
Firewall
Security Area Boundaries
Switch
Switch
Switch
Switch
Security Communications Network
Cyber Security Management Center
Network Monitoring System
Log Audit System
EDR Management System
CSMS Server
Bastion Host
IT
OT
OT
Wireless
Security Computing Environment

Service Process and Steps

Role \ Process	Initial Research	Programme Design	Submission for Approval / Implementation Preparation	Implementation and Delivery	Post-Maintenance
Integrator	1) Provide cybersecurity consulting to shipowners/shipyards. 2) Provide a draft asset equipment list (including device connection methods) that meets E26 requirements. 3) Discuss and develop a specific implementation plan for the project with the shipowner/shipyard, and provide the initial version of the security architecture design and TA.	1) Based on the formal E26 asset equipment list provided by the shipowner/shipyard, prepare the complete "asset list" required for the E26 application. 2) Prepare all materials required for E26 in accordance with classification society requirements. 3) Identify the list of vendors that are exempted/non-exempted.	1) Submit the review documents and complete the approval process as per classification society requirements. 2) Provide the shipyard with system installation/wiring diagrams. 3) Prepare hardware equipment procurement and basic setup. 4) Develop test outlines and conduct internal testing.	1) Responsible for on-site installation, commissioning, configuration, testing, and rectification, as well as cybersecurity technical reinforcement. 2) Responsible for completing the classification society inspection, successfully conducting the evaluation, and obtaining the cybersecurity compliance symbol. 3) Responsible for providing cybersecurity operation and maintenance training to relevant personnel.	1) Assist the shipowner in organizing and preparing all materials for the E26 annual inspection. 2) Assist the shipowner in completing the E26 annual inspection. 3) Provide system technical support, after-sales warranty, system upgrades, and other services.
Shipowner	Provide existing cybersecurity policy documents and personnel information for the integrator's reference.	Cooperate with the shipyard/integrator to collect the required materials when necessary.		Cooperate with the integrator to provide cybersecurity operation and maintenance training to relevant personnel.	Shipowner submits all materials for the E26 annual inspection application.
Shipyard	1) Provide a draft of the asset equipment list required for E26 (including device model, connection methods, system versions, and other relevant information). 2) Coordinate with equipment vendors to provide the necessary content in the asset list.	Cooperate with the shipyard/integrator to collect the required materials.	Complete pre-implementation preparations such as hardware installation and fixation of cybersecurity devices, power cable routing, and communication cable routing, based on the system installation/wiring diagrams provided by the integrator.	Responsible for coordinating/cooperating with the integrator to complete the on-site installation and implementation.	
Equipment Supplier		Provide the required documentation (including but not limited to backup and recovery plans, emergency response plans, etc.) in accordance with the classification society's E26 requirements.			

Scope of Supply - Hardware

Marine Network Firewall & Switch & Cabinet

1200(H)*600(W)*1100mm(D)

88mm(H)*440(W)*520(D)

44.5mm(H)*300(W)*440(D)

KR KOREAN REGISTER Lloyd's Register ABS CCS DNV ClassNK

适用于 IACS UR E27 (Rev.1) 船载系统和设备的网络安全性
适用于 IACS UR E26 (Rev.1) 船舶网络安全性
Made available for IACS UR E27 (Rev.1) Cyber resilience of on-board systems and equipment
Made available for IACS UR E26 (Rev.1) Cyber resilience of ships

Cybersecurity Risk Management System - CRMS

Network Management Server

748.79mm(W)×482mm(D)×42.8mm(H)

Security Audit System

Network Monitor System

Cyber Security Management system (CSMS)

Endpoint Detection and Response - EDR

Maritime Cybersecurity Resilience Advanced CRMS

IPS/IDS, Situational Awareness

Intrusion prevention system/intrusion detection system, industrial vulnerability mining and detection platform, security situation awareness, network security work platform

O&M Management System

Fortress machine

O&M management and auditing systems
- Bastion host

4. Reference Projects

API MARINE
POWERED BY SANGO MARINE

Reference Project

Shipowner	Jana Marine (Saudi Arabia)
Shipyard	Guangzhou Salvage Bureau of the Ministry of Transport
Delivery	1 vessel
Classification Society	ABS

97.8M DE Hybrid DSV

Scope of supply:

- **SMART System:** INF, MHM, SHM Tier 2
- **Digitalization**
- **Cyber Security, CS-2**
- **Crew Behavior Monitoring**
- **Alarm Monitoring System**

Reference Project

Shipowner	Jana Marine (Saudi Arabia)
Shipyard	WMMP-HHMC
Delivery	3 vessels
Classification Society	ABS

350Ft Jack up Barge (Type B, C)

Scope of supply:

- **SMART System:** INF, MHM, SHM Tier 2
- **Digitalization**
- **Cyber Security,   CS-2**
- **Alarm Monitoring System**

Reference Project

Shipowner	Jana Marine (Saudi Arabia)
Shipyard	WMMP-HHMC
Delivery	4 vessels
Classification Society	ABS

350Ft Jack up Barge (Type D)

Scope of supply:

- **SMART System:** INF, MHM, SHM Tier 2
- **Digitalization**
- **Cyber Security, CS-2**
- **Alarm Monitoring System**

SANGO AI
SANGO AI

Reference Project

Shipowner	Jana Marine (Saudi Arabia)
Shipyard	WMMP-HHMC
Delivery	4 vessels
Classification Society	ABS

80M DE Maintenance Accommodation Vessel

Scope of supply:

- **Digitalization**
- **Cyber Security, CS-1**
- **Alarm Monitoring System**

API
MARINE
POWERED BY
SANGO MARINE

API MARINE TRIDENT CYBER SECURITY SYSTEM

SENSORS & AUTOMATION SYSTEM · POWER GENERATION · DIGITAL SOLUTIONS