
API
MARINE
POWERED BY
SANGO MARINE
API MARINE SMART
MARINE SOLUTIONS
SENSORS & AUTOMATION SYSTEM · POWER GENERATION · DIGITAL SOLUTIONS

AGENDA

1. E26/E27 In General
2. E26 Regulations
3. Shipyard & Shipowner Responsibilities
4. E26 Security Requirements
5. Class Standard Levels
6. Implementation – Procedures & Steps

1. E26/E27 In General

What is IACS E26 / E27?

What is the involvement from API Marine ?

Is Type Approval necessary for these requirements?

What is the difference between E26 and E27? Who is responsible for what?

What does the shipowner and shipyard need to do to comply?

Which equipment in scope for E26 and E27?

2. E26 Regulations

What types of vessels are covered by the regulations?

- Applies to vessels with a contract after 1 July 2024
- Over 500GT for Passenger ships, cargo ships, offshore platforms – involved in international travels
- Any size of self-propelled platform involved in marine construction (e.g. offshore wind farm)
- Coastal / domestic vessels do not have to meet the requirement

3. Shipyard & Shipowner Responsibilities

IACS E26 (Shipping Company and Shipyard responsibility)

- The rule requires that the ship **detects** the threat to cybersecurity, protects against it and the systems **recover** in the event of a cyber attack - during the design phase to the operational phase.
- E26 considers the ship as a large cyber space configured by different networks.
- E26 requires the ship owner and shipping company to prove that the ship definitely addresses (secures) the cyber attack risk.

IACS E26 (Shipping Company and Shipyard responsibility)

Documentation from design phase to commission phase is the **shipyard's responsibility**

Design → Construction → Commissioning

Documentation under operation (after the delivery of the vessel) is the **shipping company's responsibility**

Preliminary → Annual inspection → Special inspection

What should the Shipyard and the Shipping Company do?

Shipyard

- Documentation of installed equipment, cyber security description etc.
- Implement approved products
- Prepare ”cyber resilience” (resistance) test
- Cyber resilience test must be approved by the class surveyor (physical presence)

Shipowner

- Documentation of ”cyber resilience” program
- Prepare and initiate all annual inspections and a 5-year special inspection

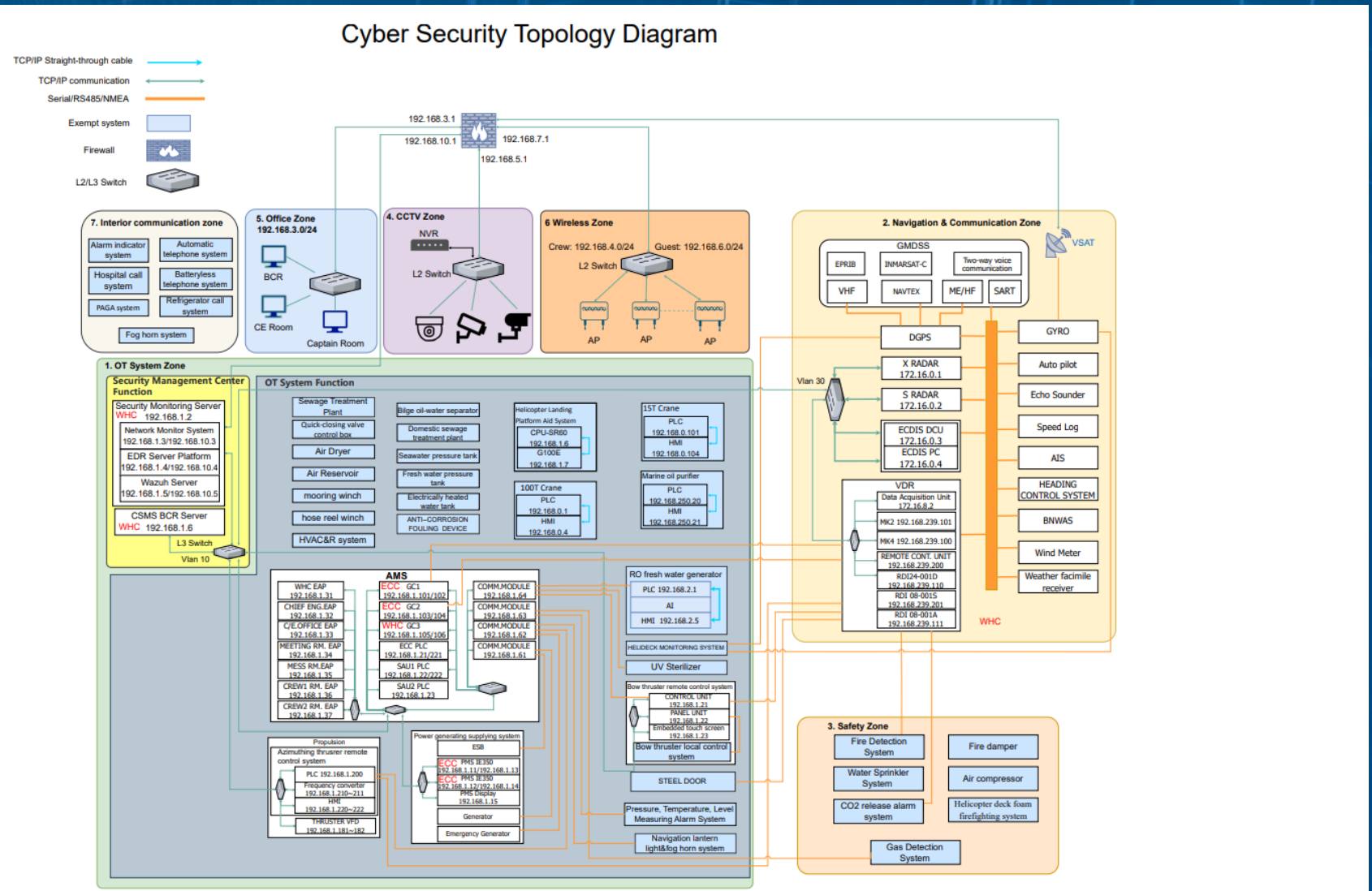
Equipment covered by E26

Equipment that in the event of a cyber attack could cause harm to the safety operation of the crew and the environment:

- Propulsion system
- Steering system
- Anchor
- Generator, power distribution
- Fire and extinguishing systems
- Bilge and ballast system
- Watertight and flooding system
- Light
- Navigation system
  - Radar/sonar/GPS/AIS/VDR/LRIT
  - BNWAS/ECDIS/TCS/THD/HCS
- Communication system
  - Navtex/EGC/VHF/MF-HF/PA/DSC

IP & SERIAL COMMUNICATION – SUBJECT TO E26

Cyber Security Topology Diagram



4. E26 Security Requirements

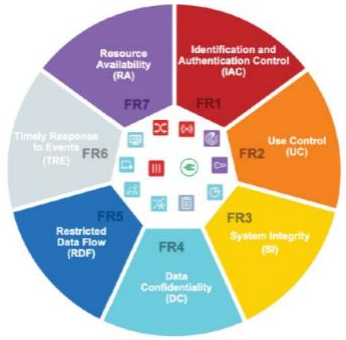
Technical Security Requirements IACS E26

Annual inspection

Identify	Protect	Detect	Response	Recover
Inventory of assets and personnel	**Partition hierarchical active defense**	**Real-time monitoring and alarming**	**Response planning and implementation**	**Recovery planning and implementation**
• 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	• Security defense solution architecture design • Establish security policies and protection methods • Ship-end hardware installation and software configuration	• 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	• Incident and cybersecurity incident response plan • Isolate the network • Fallback measures	• Recovery plan • Backup plan • Restoration and backup technology • Plan implementation

Annual inspection

Technical Security Requirements IACS E26 & E27

	UR E26 Cyber Resilience of Ships	UR E27 Cyber Resilience of On-board Systems and Equipment
Purpose	Integrate ship-wide operational technology(OT) and information technology (IT) equipment into the ship network. (Shipyard's responsibility)	Protect and enhance the integrity of systems and equipment (each CBS supplier's responsibility)
Requirement	17 Detailed Requirement (Based on NIST Framework) 	41 Detailed Requirement (Based on IEC 62443-3-3) 
Application Date	1st Jul, 2024 (This UR is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1st July, 2024). ***UR E26 Revision will be issued in Nov or Dec, 2023.**	
Docs.	1) Inventory list of CBS (Computer-Based Systems) 2) Design & philosophy document 3) Logical map of networks 4) Risk assessment 5) Test Procedure	1) CBS asset inventory 2) Topology diagrams 3) Description of security capabilities 4) Test procedure for security capabilities 5) Secure development lifecycle

Description			Category
4.1	Identify	4.1.1.3.1	Inventory of CBSs and networks onboard Hardware
		4.1.1.3.2	Inventory of CBSs and networks onboard Software
4.2	Protect	4.2.1.3	Security Zones and Network Segmentation
		4.2.2.3	Network protection safeguards
		4.2.3.3	Antivirus, antimalware, antispam and other protections from malicious code
		4.2.4.3.1	Physical access control
		4.2.4.3.2	Physical access control for visitors
		4.2.4.3.3	Physical access control of network access points
		4.2.4.3.4	Removable media controls
		4.2.4.3.5	Management of credentials
		4.2.4.3.6	Least privilege policy
		4.2.5.3	Wireless communication
		4.2.6.3	Remote access control and communication with untrusted networks
		4.2.7	Use of Mobile and Portable Devices
4.3	Detect	4.3.1	Network operation monitoring
		4.3.2	Verification and diagnostic functions of CBS and networks
4.4	Respond	4.4.1	Incident response plan
		4.4.2	Local, independent and/or manual operation
		4.4.3	Network isolation
		4.4.4	Fallback to a minimal risk condition
4.5	Recover	4.5.1	Recovery plan
		4.5.2	Backup and resore capaqbility
		4.5.3	Controlled shutdown, reset, restore and restart

5. Class Standard Levels

API MARINE
POWERED BY SANGO MARINE

Maritime Cyber Security Standards

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	-	-

6. Implementation - Procedures & Steps

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 中国船级社 · 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

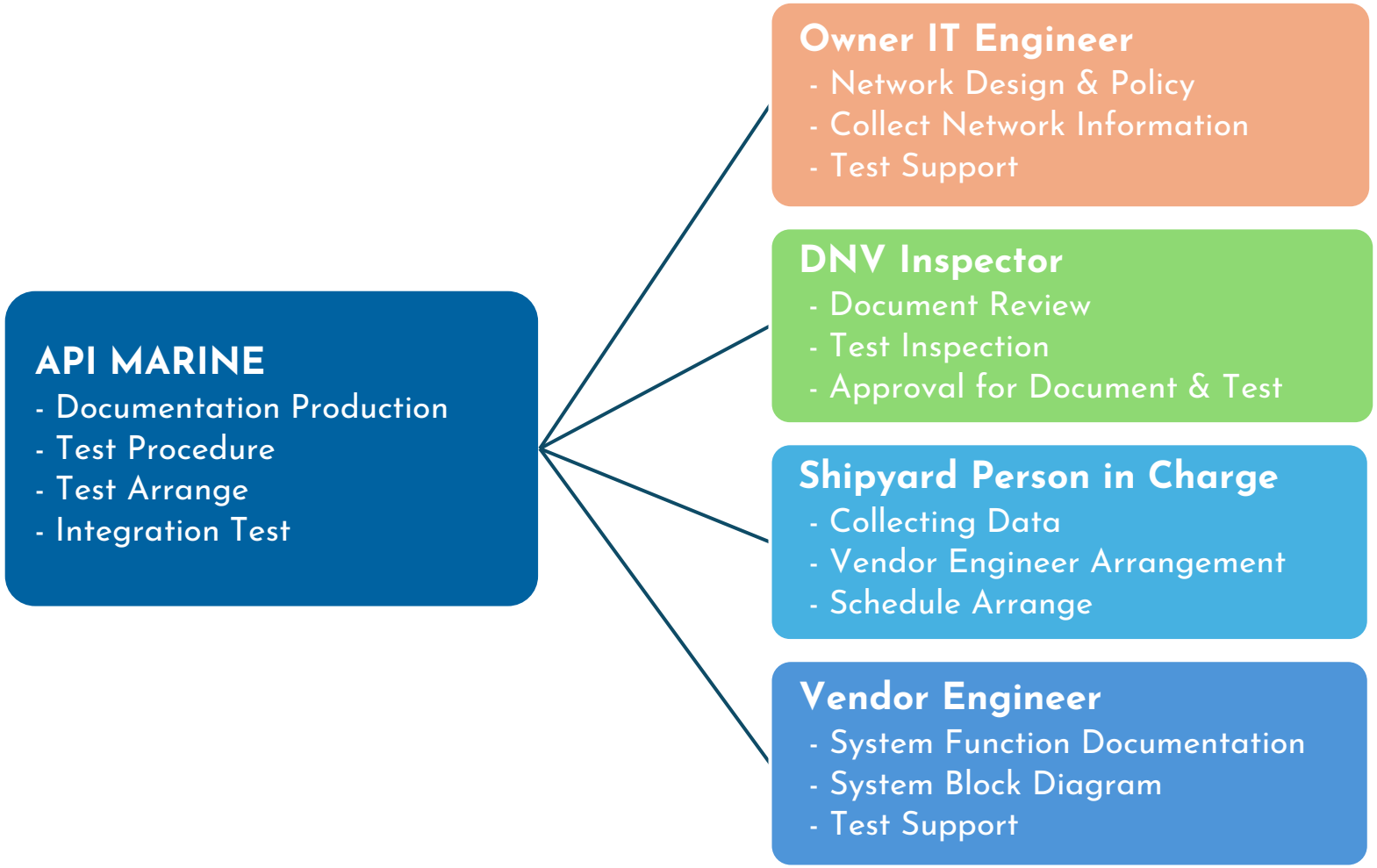
Intrusion prevention system/intrusion detection system, industrial vulnerability mining and detection platform, security situation awareness, network security work platform

O&M Management System

Fortress machine

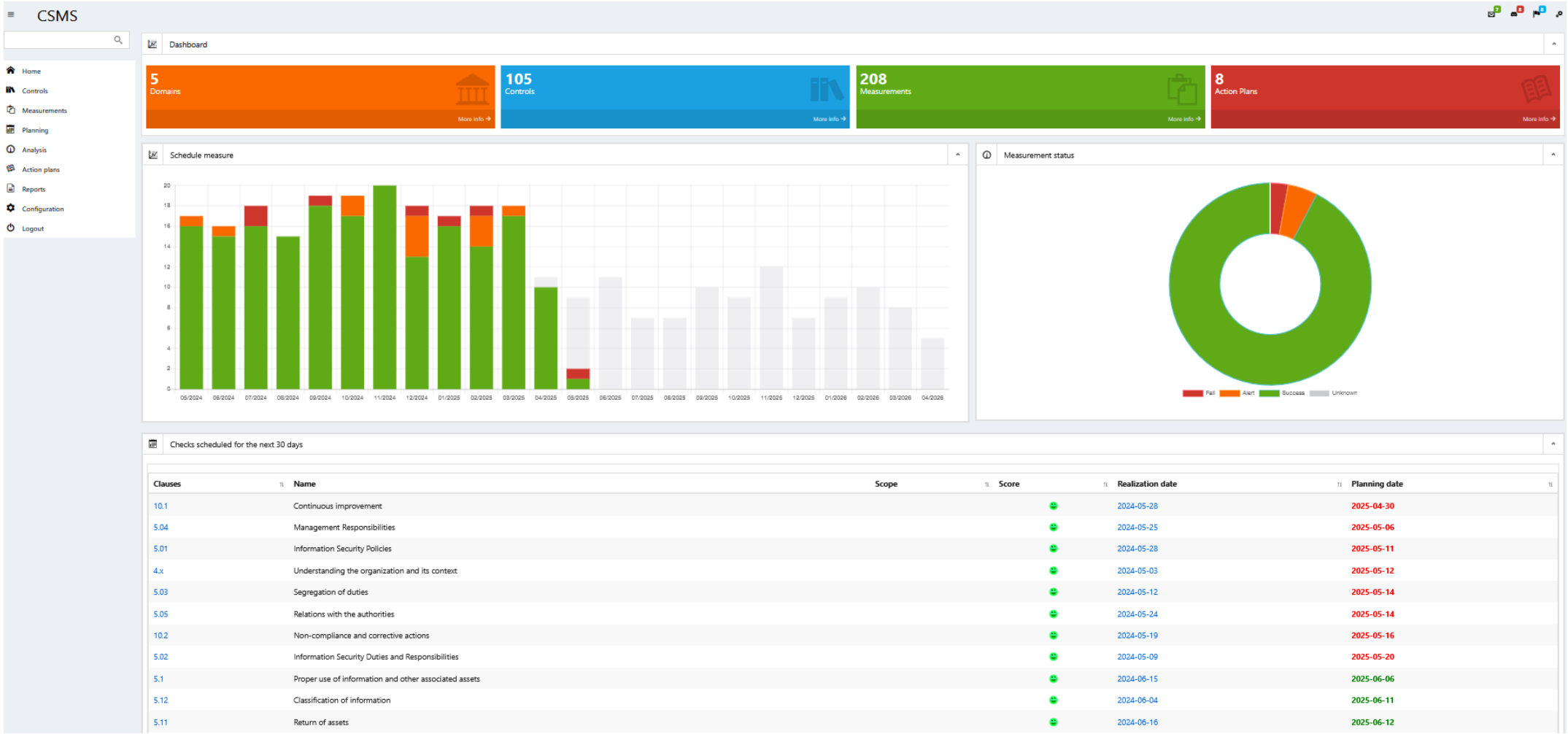
O&M management and auditing systems
- Bastion host

Work scope of each party
(Owner, Class, Shipyard, Integrator, Vendor)



API MARINE
POWERED BY SANGO MARINE

CSMS



Clauses	Name	Scope	Score	Realization date	Planning date
10.1	Continuous improvement			2024-05-28	2025-04-30
5.04	Management Responsibilities			2024-05-25	2025-05-06
5.01	Information Security Policies			2024-05-28	2025-05-11
4.x	Understanding the organization and its context			2024-05-03	2025-05-12
5.03	Segregation of duties			2024-05-12	2025-05-14
5.05	Relations with the authorities			2024-05-24	2025-05-14
10.2	Non-compliance and corrective actions			2024-05-19	2025-05-16
5.02	Information Security Duties and Responsibilities			2024-05-09	2025-05-20
5.1	Proper use of information and other associated assets			2024-06-15	2025-06-06
5.12	Classification of information			2024-06-04	2025-06-11
5.11	Return of assets			2024-06-16	2025-06-12

API MARINE

POWERED BY SANGO MARINE

API MARINE SMART MARINE SOLUTIONS

SENSORS & AUTOMATION SYSTEM · POWER GENERATION · DIGITAL SOLUTIONS

12082025 V1