API MARINE
POWERED BY SANGO MARINE

API Marine
Trident Cyber Security System

Technical Agreement:

Version A

To:		**From:**	
Quantity:		**Signature:**	
REV:	A	**Date:**	
Project		**Validity:**	3 months

Catalog

1. Preamble

As the global shipping industry increasingly relies on digital technology and network systems, ship cybersecurity has become a key factor in ensuring shipping safety and operational continuity. Modern ships not only face traditional marine environmental challenges, but also must deal with complex network threats such as malware, cyber-attacks and data leaks. These threats not only affect the safety of the ship itself, but also have an impact on economic losses to ship operations.

This ship cybersecurity solution complies with the requirements of classification societies, IMO, etc., and can ensure that ships maintain safe, reliable, and efficient operations in the face of various potential threats. The solution builds a multi-level defense system through advanced security technology, strict monitoring mechanisms and efficient emergency response processes, including:

1. Defense in Depth
    - Network security: The zone is isolated by firewalls, and the EDR server and client are deployed to ensure the security of the ship's network communication and data transmission when threatened by network attacks.
    - Network monitoring: Implement strict network monitoring mechanisms, deploy network monitoring systems, and log audit systems, track ship network activities in real time, and promptly detect and respond to abnormal behaviors and potential network attacks.
    - Emergency response: By establishing a sound cybersecurity management system and deploying a CSMS system, we can take prompt measures when a cybersecurity incident occurs to reduce the impact on shipping operations.
2. Regulatory Compliance:
    - Ensure that all vessels and personnel comply with the latest

requirements of international, national and industry regulations and guidelines, and maintain compliance and effectiveness of cybersecurity management.

This ship cybersecurity solution provides all-round security protection for existing ships, ensuring that ships can remain safe, reliable and efficient when facing complex network threats.

2. Reference Specifications

All vessels and personnel must comply with the latest requirements related to international, national and industry regulations and guidelines. In the event of any conflict between classification society rules and/or regulatory documents and the minimum vessel specifications and manning requirements outlined in the contract and /or SA documents, the higher specifications shall prevail.

3. Solution Architecture

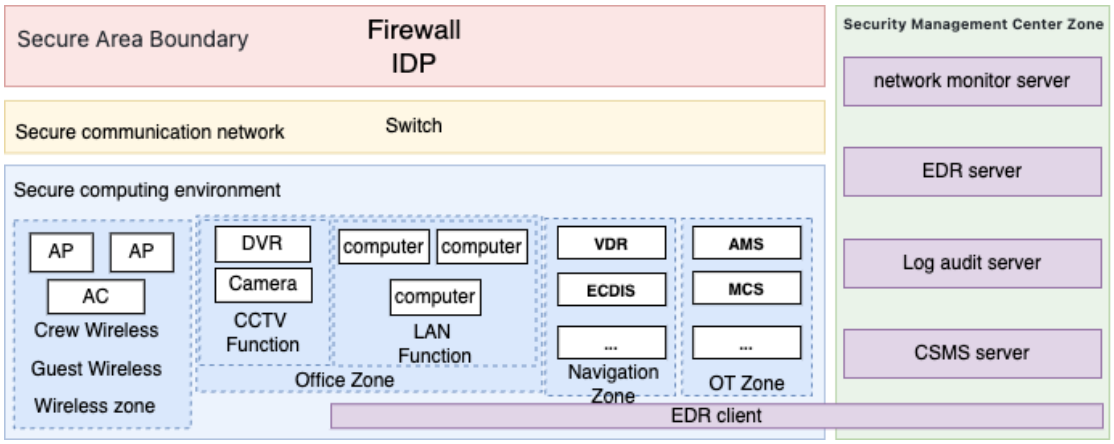
This solution architecture consists of a network security architecture and a network topology diagram.

Network security architecture describes and defines the functions and software and hardware components of network security.

The network topology diagram describes and defines the network area division and device connections.

3.1 Network security architecture

The network security architecture design of this solution includes a security management center, a secure communication network, a secure area boundary, and a secure computing environment. The specific architecture design is shown in the figure below:



As shown in the figure above, only TCP/IP connected devices are listed in the figure. The light blue area in the architecture diagram is the secure computing environment, including all devices in the shipborne wireless network area, devices in the office area, CBS in the OT Zone area: AMS and MCS, ECDIS and VDR in the communication and navigation area. Among them, the CBS in the LAN subarea of office area, OT area, and communication and navigation area need to install EDR client to achieve terminal security and anti-tampering requirements.

The yellow area is the secure communication network, and all monitored system and network monitoring data must be transmitted through the switch.

The red area is the boundary of the security zone, which is isolated and blocked by deploying a firewall.

Light green area is the security management center, which includes a rack-mounted network monitoring server and a CSMS workstation. The network monitoring server is installed with the network monitoring system, log audit system, and EDR management system, and the CSMS workstation is installed with CSMS. All systems need to install the EDR client to achieve terminal security and anti-tampering requirements.

Functions of the security management center include the following aspects:

1. Monitoring and response: Monitor network traffic and system activities in real time to quickly identify and respond to potential security threats and attacks.
2. Risk assessment: Regularly assess network and system security risks, identify vulnerabilities, and make corresponding improvement recommendations.
3. Incident Management: Handling security incidents and incidents, conducting investigations and analyses to determine root cause and impact.
4. Security Strategy Development: Develop and update cybersecurity policies, standards, and procedures to ensure security compliance of the vessel.
5. Training and awareness raising: Provide cybersecurity training for crew members to improve overall safety awareness and reduce human errors.
6. Technical support and implementation: Deploy and maintain security technology tools such as firewalls, EDR, network monitoring systems, log audit systems, and CSMS systems.
7. Compliance management: Ensure that the ship complies with relevant laws, regulations, and industry standards, and conduct regular compliance inspections.

The network security management center can effectively protect the ship's information assets and reduce security risks.

The main functions of the security zone boundary include the following aspects:

1. Access Control: Define crew members, users and devices that can access specific network areas, thereby limiting unauthorized access and protecting sensitive data and resources.
2. Traffic monitoring: Monitor and analyze network traffic passing through the network security zone boundaries to identify abnormal activities or potential security threats and take timely measures.

3. **Layers of defense:** Create multiple layers of security to prevent attackers from moving laterally between different areas, thereby reducing overall risk.
4. **Isolation and segmentation:** Divide the entire ship network into multiple areas, limit direct communication between different areas, and improve security.
5. **Security policy implementation:** Implement different security policies and technologies at the boundaries of network security zones, such as isolating network egress zones with firewalls to enhance network security.
6. **Data leakage prevention:** Reduce the risk of data leakage by monitoring and controlling the flow of data in and out of the boundary.

Cybersecurity zone boundaries can effectively protect the ship's network and data security and reduce the impact of security threats.

The main functions of a secure computing environment include the following:

1. **Data protection:** Provide a secure computing platform to ensure the confidentiality, integrity, and availability of CBS data during storage and transmission.
2. **Isolation and segmentation:** Through network segmentation and isolation, direct communication between different systems and applications is limited, the attack surface is reduced, and critical assets are protected.
3. **Malware protection:** By installing anti-virus and anti-malware tools, the terminals are able to detect and block the spread of malware, protecting CBS equipment and the ship's network security.
4. **Access Control:** Implement strict authentication and authorization mechanisms to limit access to systems and data, ensuring that only authorized users can access sensitive information.
5. **Security Auditing:** Record and analyze user activities and system events for security audits and post-mortems to help identify security vulnerabilities.
6. **Continuous updates and maintenance:** Regularly update systems and

applications, patch security vulnerabilities, and ensure the security and stability of the computing environment.

7. **Backup and recovery:** CBS should provide data backup and recovery solutions to prevent data loss and business interruption and ensure business continuity.

Network security computing protection can effectively enhance the ship's information security protection capabilities, reduce security risks, and protect key business operations.

The main functions of the secure communication network include the following aspects:

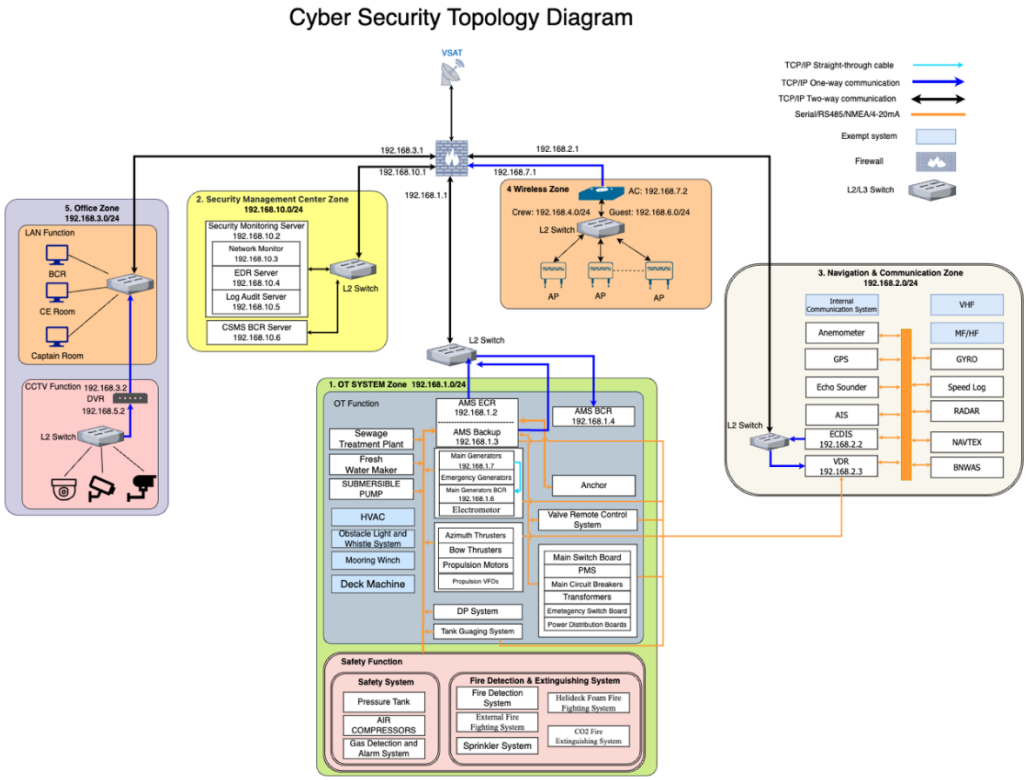
1. **Data protection:** Encrypted transmission ensures the confidentiality and integrity of data during transmission, preventing unauthorized access and data tampering.
2. **Authentication:** Verify the identities of both parties in communication through encryption and authentication mechanisms to prevent impersonation and fraud.
3. **Privacy protection:** Through encrypted transmission and access isolation, user information and sensitive data are protected from being leaked and infringed.
4. **Anti-denial of service:** Prevent denial of service attacks through traffic filtering and ensure the availability of communication networks.
5. **Integrity verification:** Use hash function technology to ensure the integrity of data during transmission and detect whether it has been tampered with.
6. **Security protocol:** Use secure communication protocols (such as TLS/SSL) to encrypt data transmission and improve the security of network communications.
7. **Monitoring and response:** Monitor network traffic in real time, detect potential threats, and respond quickly to security incidents.

Network secure communication can effectively protect the information security of ships and ensure a safe and reliable communication environment.

3.2 Ship network topology

The construction of ship network security, we ensure compliance with the requirements and technical standards of the ship society. According to the different equipment types, CBS types, protection priorities and security strategies in the ship of this project, the overall security areas are divided into the following areas. The specific division results are as follows:

Note: Since the equipment list is not provided by shipyard, the following topology is for reference only.



According to the requirements of IACS UR E22, and taking into account the communication efficiency between systems, the ship system divides the OT CBS

into one area according to the form of expression, such as: propulsion-related systems and power generation-related systems are divided into the same area, in order to facilitate the implementation of a unified security strategy. Each area needs to be isolated with a firewall or ACL.

A ship network security management center shall be built on board, and trained network security management specialists shall be arranged to centrally monitor the network of the entire ship. The network center shall operate under the ship network security system.

A network security monitoring system needs to be installed on board the ship, and the system needs to provide monitoring access portals in the wheelhouse, captain's office, and chief engineer's office so that relevant personnel can keep abreast of network activities at any time.

4. Description of the network security architecture of this project

According to the network security architecture shown in 3.1, the following network security architecture is described according to the specific equipment of this ship.

4.1 Secure computing environment description

The secure computing environment includes various CBSs, office PCs and wireless access devices in various areas on the ship.

OT system area: All CBS in this area: AMS, MCS should install EDR client, and equipment suppliers should make regular backup plans to ensure terminal security and data tamper-proofing.

Wireless area: All CBS and office PCs in this area should install EDR client, and equipment suppliers should make regular backup plans to ensure terminal security and data tamper-proofing.

Office area: The office area includes CCTV sub-area and office LAN sub-area. EDR client should be installed on all CBS and access PCS in the office LAN sub-area, and equipment suppliers should make regular backup plans to ensure terminal security and data tamper-proof. All CBS in the CCTV sub-area should change the default password, update firmware regularly, disable unnecessary functions, and equipment suppliers should make regular backup plans.

Communication and navigation area: All CBS, ECDIS and VDR in this area should be installed with EDR client, and the equipment supplier should make regular backup plans to ensure terminal security and data tamper-proof.

Security management center area: All CBS in this area: EDR server, network monitor system, log audit system, CSMS server should be installed with EDR client, and equipment suppliers should make regular backup plans to ensure terminal security and data tamper-proofing.

4.2 Secure Network Communications Instructions

Network egress and internal network transmission require the use of secure transmission protocols for data transmission.

When data needs to be transmitted across regions, it must pass through a firewall or switch to be transmitted to the target area.

When data needs to be transmitted to the ship's external network, it needs to be encrypted using a secure transmission protocol and authenticated. At the same time, the firewall should specify the transmission target and prohibit CBS from transmitting data to any place when transmitting to the outside.

4.3 Safe Area Boundary Description

The border is protected by a firewall. Access control should be performed on the firewall to the internal CBS in this area. Only the minimum permissions required for users to complete their work should be granted according to their roles, and the user 's access to sensitive data and systems should be restricted. At the same time, the effectiveness of the security policy and configuration of the border firewall should be regularly checked and evaluated.

4.4 Security Management Center

4.4.1 Firewall

Firewalls are mainly used to provide border protection in different security areas of the ship network:

1 Access Control

Policy-based access: The firewall can set up access control lists (ACLs) based on IP addresses, port numbers, and protocol types to ensure that only authorized users and devices can access the protected CBS.

2 Traffic filtering

Deep Packet Inspection (DPI): The firewall not only inspects the header information of the data packets accessing the CBS, but also deeply analyzes their contents to identify malware and attack patterns.

Application layer filtering: Traffic can be filtered based on application layer protocols to prevent abuse or attacks of specific applications.

3 Security policy enforcement

Real-time update: The firewall can receive the latest security threat information in real time and automatically update security policies to respond to emerging network threats.

4 Logging and Monitoring

Event Logging: All access attempts, successful and failed logins, and abnormal traffic are recorded in detail.

Real-time monitoring dashboard: Provides a real-time monitoring interface to display network traffic and potential security threats, allowing security administrators to respond quickly.

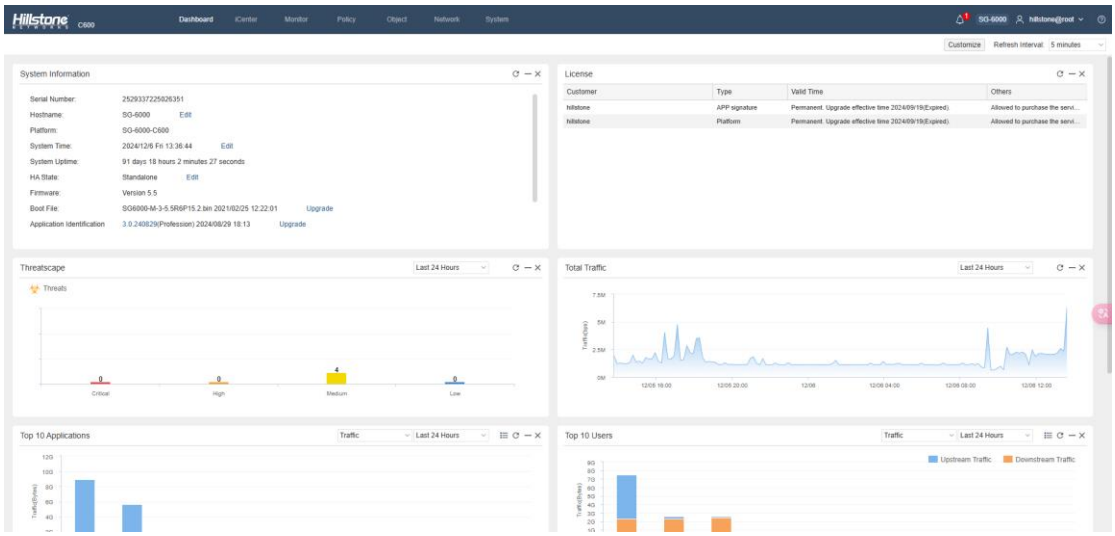
5 Network Isolation

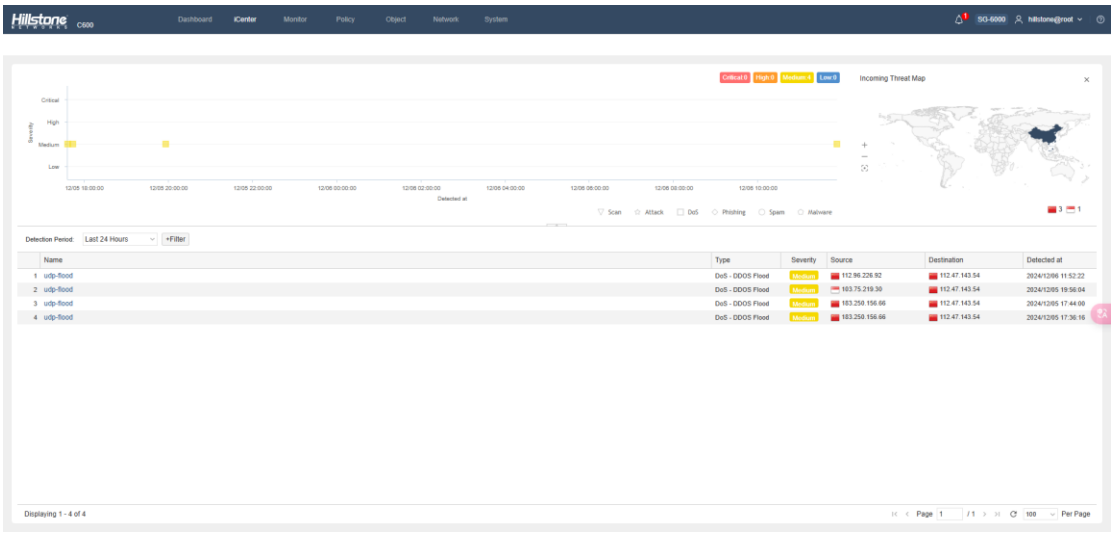
Regional isolation: Physically or logically isolate different functional areas (such as control systems and office networks) to prevent cross-domain propagation of security incidents and protect the ship's CBS from being affected by other network activities.

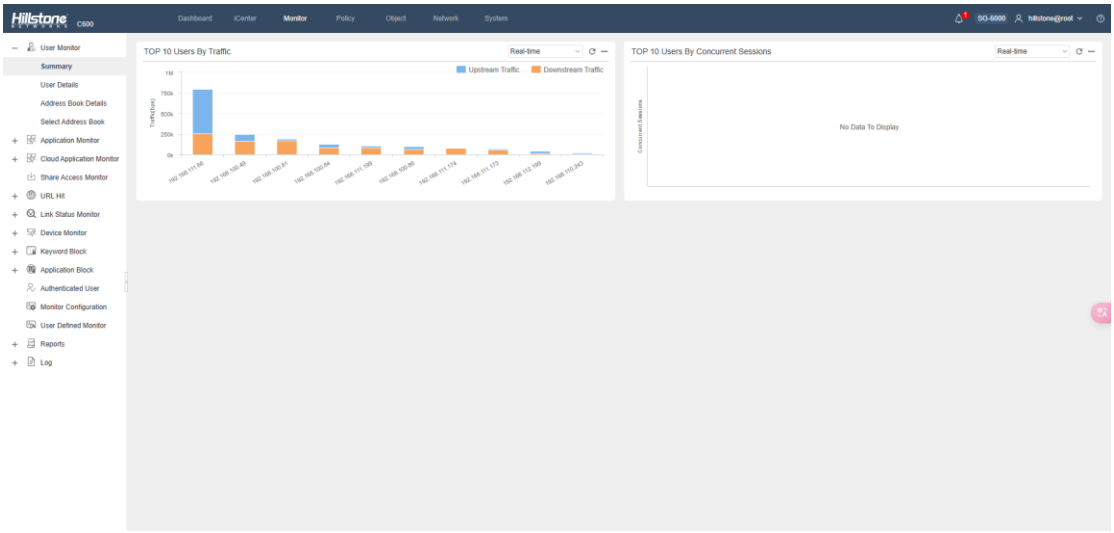
6 VPN Support

Secure Remote Access: The firewall can support Virtual Private Network (VPN) functionality, providing crew with secure remote access to perform work ashore or monitor ship systems.

Encrypted communication: Encryption technology is used to protect the content of remote communications and prevent data from being stolen or tampered with.







4.4.2 Network monitoring system

Through the network monitoring system deployed in the security management center area, the ship network security can be monitored in real time:

1. Real-time monitoring

Provides real-time status of the network environment, including traffic patterns, user activities, and security events, enabling timely detection of abnormal activities and potential threats, thereby improving network security response capabilities.

2. Event Alert

When a corresponding event is detected (such as network disconnection), the network monitoring system will trigger an alarm mechanism and send an email alert to relevant personnel to improve response capabilities.

3. Decision support

Provide accurate intelligence and analysis results to provide decision-making basis for ships and help formulate effective safety strategies and emergency response plans.

4. Incident Response

After a security incident occurs, situational awareness can provide detailed event analysis to help ships quickly resume normal operations and prevent similar incidents from happening again.

4.4.3 Log audit system

The log audit platform will collect all CBS logs on the ship, including terminal security logs. The main functions of log audit are as follows:

1. Event Log

   Comprehensive log: Records all ship CBS (including CBS of the security management center) activities, user behaviors and security events, providing basic data for subsequent analysis.

   Compliance assurance: Meet regulatory and standard requirements and ensure data retention and audit compliance.

2. Forensic Analysis

   Event Reproduction: Reconstruct the event process through log backtracking to help analyze the attack path and method.

   Evidence preservation: Provide strong evidence support for security incident investigations and legal proceedings.

3. Trend Analysis

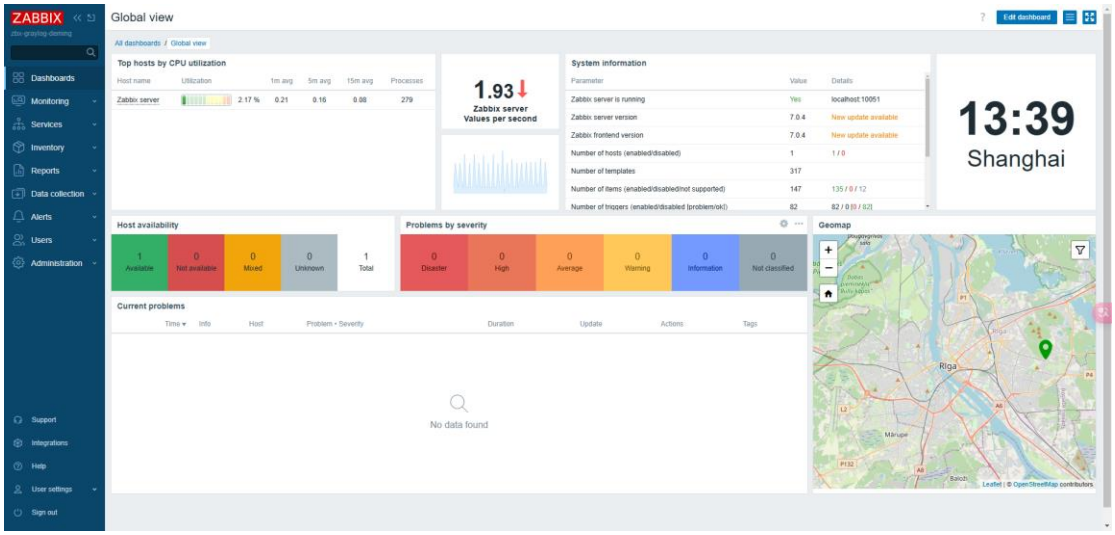
   Historical data analysis: By analyzing historical logs, we can identify patterns and trends of network attacks and provide reference for defense strategies.

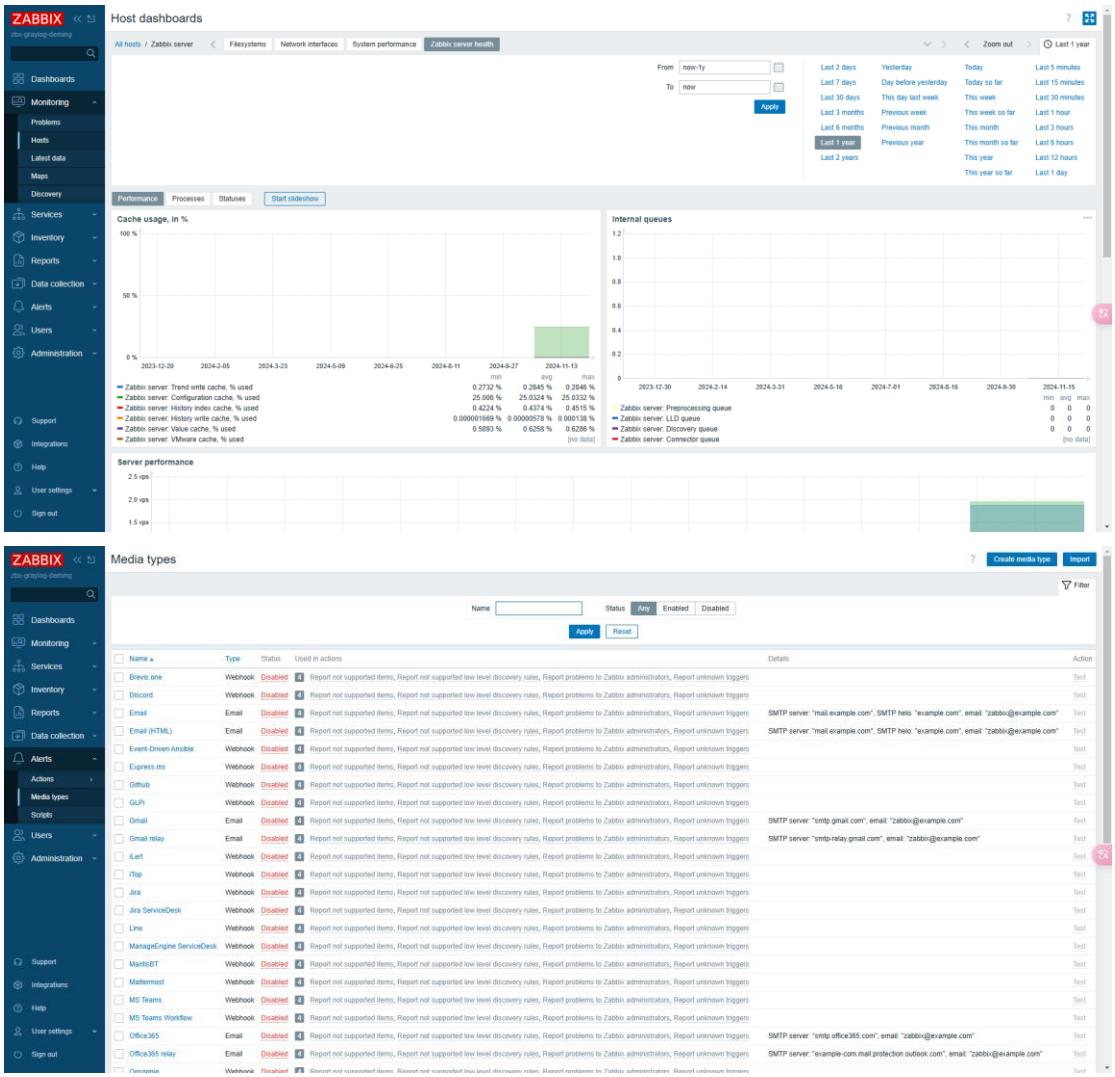
   Performance monitoring: Monitor system performance and identify potential performance bottlenecks and anomalies.

4. Security policy optimization

   Feedback mechanism: Based on the log audit results, network security strategies are continuously optimized and adjusted to enhance protection capabilities.

   User behavior analysis: Cooperate with situational awareness to analyze user activities, identify internal threats and abnormal behaviors, and improve overall security.





4.4.4 EDR System

The EDR system is divided into EDR client and EDR server. EDR client (Endpoint Detection and Response) is focused on monitoring, detecting, and responding to security threats on ship CBS equipment. It has the functions of malware protection, authorization of mobile media on the CBS system and blocking access to illegal mobile media. EDR server is the management software that uniformly manages all terminals and distributes security policies.

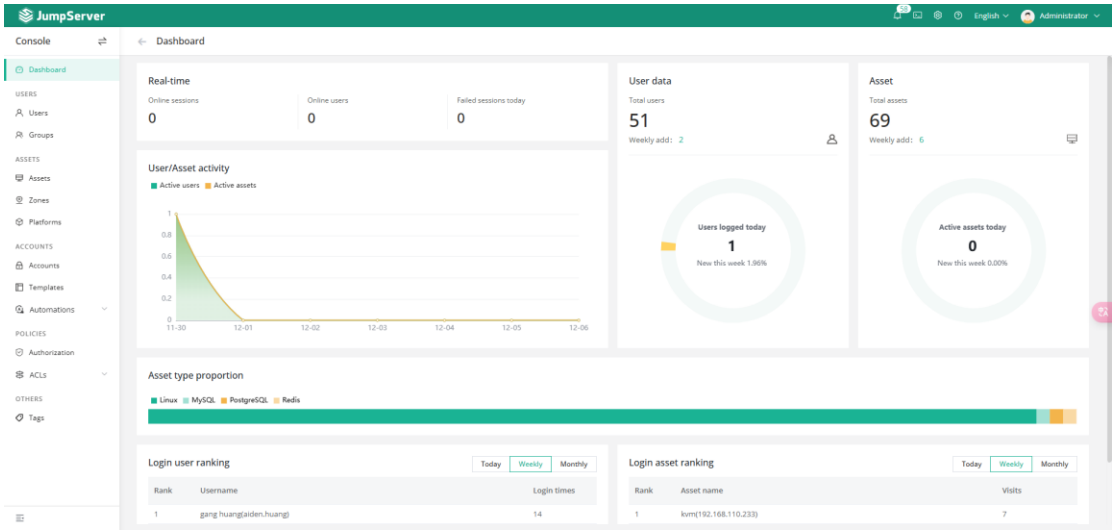
1. **Real-time monitoring and alerts:** EDR tools monitor endpoint devices (including CBS, access PCs) in real time, capture various activities, quickly identify potential threats, such as abnormal logins or suspicious process launches , and generate alerts based on set rules.

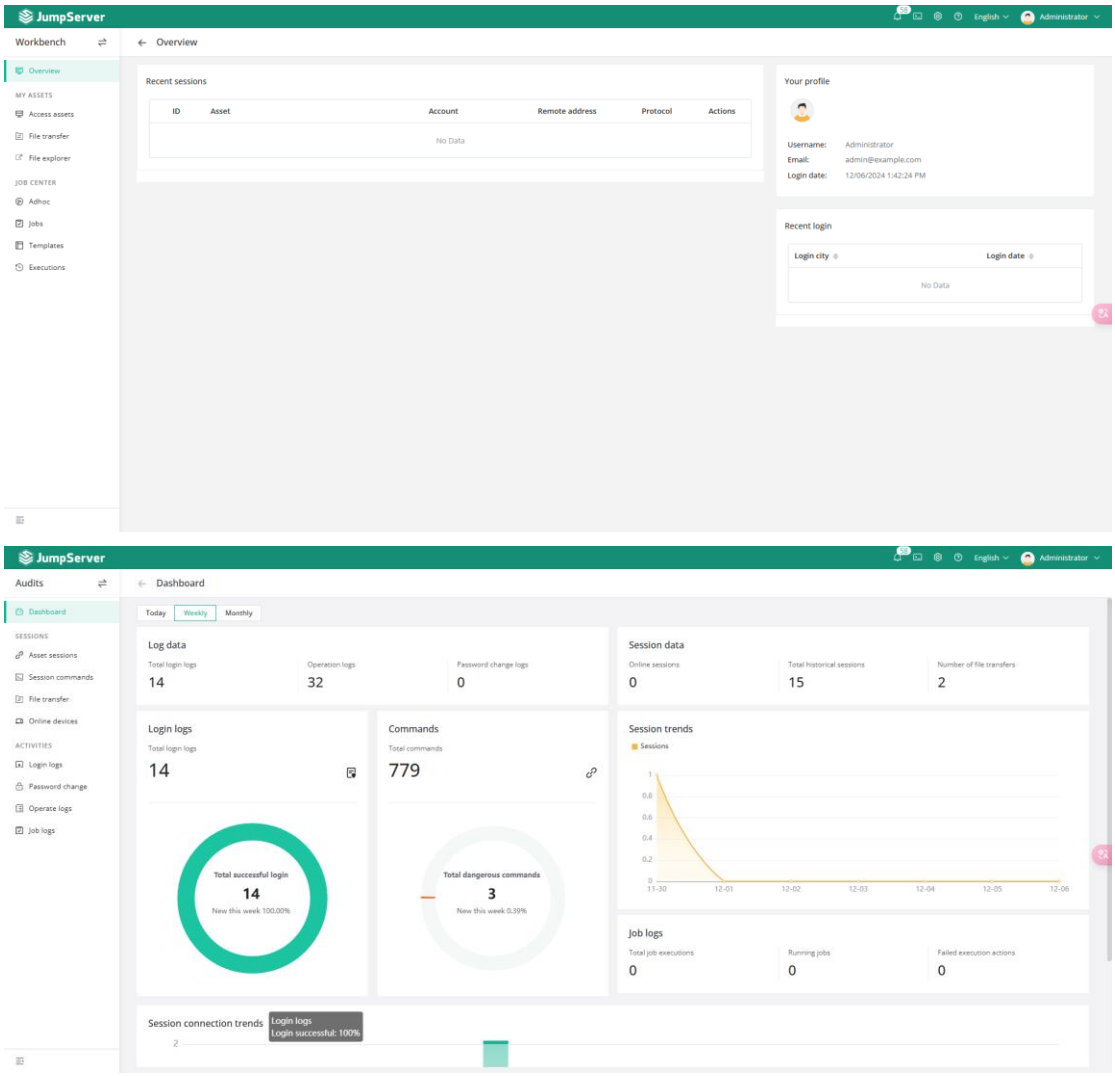
2. **Incident response and investigation:** When suspicious activity is detected, EDR can not only issue alerts but also automatically take actions, such as isolating infected CBS devices.
3. **Data collection and evidence collection:** The EDR system collects detailed activity logs on the ship's CBS, including file modifications, process startups, and network connections, and uploads all logs to the log audit system for log analysis.

4.4.5 Bastion host (on demand)

The bastion host is used in the ship network. It needs to be deployed when the ship CBS needs remote access and maintenance, and plays a protection role:

1. **Security access control:** The bastion host requires users to be authenticated before accessing sensitive resources in the internal network, ensuring that only authorized users can enter.
2. **Monitoring and Auditing:** Record all operations and activities in logs to provide follow-up auditing and monitoring.
3. **Isolate internal and external networks:** Deployed in the DMZ area of the ship's network security management center to isolate the external network from the internal network and reduce the risk of external attacks on the internal system.
4. **Enforce security policies:** Implement strong passwords and two-factor authentication security measures to ensure compliance with security standards.
5. **Normal behavior alarm:** For abnormal behaviors during operation and maintenance, such as unauthorized access and execution of commands that should not be executed, alarms are sent in a timely manner to remind management personnel to screen and handle abnormal behaviors and respond to destructive behaviors as early as possible.
6. **Centralized management:** Centralized access management of multiple internal devices, simplified permission allocation and user management, and improved security and management efficiency.





4.4.6 Cyber Security Management System

The CSMS system ensures the effectiveness and efficiency of the ship's cybersecurity measures. Its main functions include the evaluation of cybersecurity performance and the review of the effectiveness of the cybersecurity management system. CSMS can also help ships continuously optimize security management processes and has document and record management functions. It is a powerful and intuitive cybersecurity management tool that ensures that ships comply with relevant safety regulations and ensure smooth operations.

The CSMS regularly monitors and evaluates safety measures to achieve the following goals:

1. Assess the effectiveness of existing controls.
2. Verify that security requirements are met.
3. Continuously improve cybersecurity.
4. Provide accurate data for decision making.
5. Prove the necessity to improve the cybersecurity management systems.

4.4.6.1 System Features

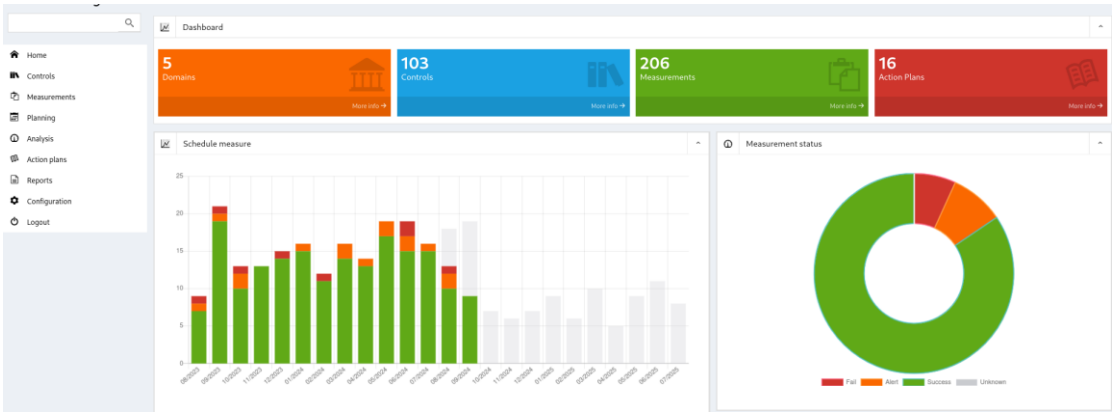
The CSMS provides a variety of capabilities, including security measures management, control planning, control process creation, evidence recording, monitoring of action plans, as well as dashboards and CSMS management reports to help ships monitor the maintenance of cybersecurity measures.

CSMS is compatible with the UR E26 standard and follows the specific requirements of the standard in terms of planning, implementation, verification and continuous improvement of cybersecurity management systems. It also helps ships prepare for classification society certification audits, provides detailed reports on security controls, and evaluates their effectiveness.

4.4.6.1.1 Front page

This system provides an overview of the CSMS and the checks to be performed. It consists of the following sections:

- Number of security domains
- Number of selected controls
- Number of enforcement measures
- Number of action plans



4.4.6.1.2 Monitor

Process monitoring: Real-time monitoring of the ship's cybersecurity processes to ensure they operate in accordance with predetermined standards and to identify abnormalities in a timely manner.

Standard Setting: Helping ships define and maintain safety control standards to ensure consistency of products and services.

Control chart generation: Automatically generate control charts, analyze data variation, and the ship should make timely adjustments and improvements.

Alerts and notifications: When abnormal process is detected, alerts are sent in a timely manner to quickly respond and handle problems.

Performance evaluation: Evaluate the effectiveness of controls to ensure continual improvement and optimization.

4.4.6.1.3 Analyze

Data Collection: Systematically collect and record quality-related data for subsequent analysis.

Indicator Setting: Helping ships define key performance indicators (KPIs) to measure the achievement of business and quality goals.

Data Analysis: Provides a variety of analytical tools to help identify trends, issues, and opportunities for improvement.

Report generation: Automatically generate detailed measurement reports for easy sharing and communication of quality status.

Visualization: Display data through charts and graphs to help users intuitively understand quality performance.

4.4.6.1.4 Cooperation

Task allocation: Ship cybersecurity managers effectively allocate specific tasks and responsibilities to team members to ensure smooth workflow.

Permission management: Set different levels of access permissions to ensure that the right people have access to relevant information and tools.

Progress tracking: Monitor task progress in real time to ensure that each task is completed on time.

Collaboration support: Promote collaboration and communication among team members and improve overall work efficiency.

Performance evaluation: Evaluate team and individual performance based on completion to provide a basis for subsequent improvements.

4.4.6.1.5 Planning

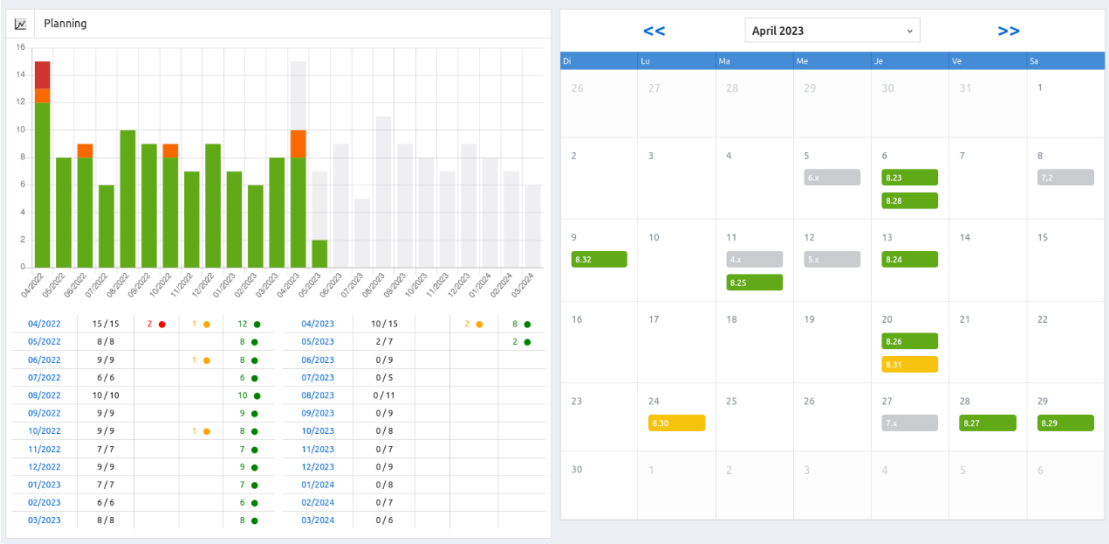
Strategy formulation: Help ships formulate long-term and short-term goals and clarify development directions.

Resource allocation: Allocate resources rationally to support the smooth implementation of the plan.

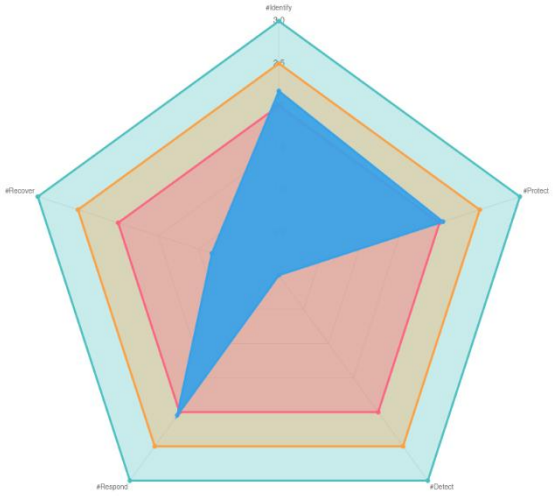
Task decomposition: Break down big goals into small, manageable tasks and achieve them step by step.

Risk Management: Identify potential risks and develop response strategies to ensure the robustness of the plan.

Scheduling: Develop a detailed timetable to ensure that all tasks are carried out on time.



Cybersecurity Concepts	Note
#Identify	20 - 2 - 1
#Protect	67 - 9 - 6
#Detect	0 - 0 - 0
#Respond	9 - 1 - 1
#Recover	1 - 1 - 1



4.4.6.1.6 Dashboard

Data visualization: Display key performance indicators (KPIs) in the form of charts and graphs to make data more intuitive and easier to understand.

Real-time monitoring: Real-time tracking of business and quality indicators helps ship cybersecurity managers quickly understand the current situation.

Decision Support: Provides powerful support to help make timely decisions by aggregating and analyzing data.

Problem Identification: Quickly identify unusual trends or problems so that timely action can be taken.

Report Generation: Automatically generate shareable reports to facilitate information communication between teams and management.

4.4.6.1.7 Action Plan

Develop action strategies: Help the team identify improvement goals and specific measures to solve problems or achieve goals.

Responsibility allocation: clearly define the person in charge of each task to ensure that all work is carried out in an orderly manner.

Progress tracking: Monitor the implementation progress of the action plan to ensure it is completed on time.

Evaluate effectiveness: Assess the effectiveness of actions after implementation, analyzing results and room for improvement.

Collaboration platform: Promote communication and collaboration among team members and jointly promote the implementation of plans.

5. Description of the network topology diagram of this project

The network topology diagram shows how each device is connected in the entire ship network. Direct interconnection between areas through switches within the area is prohibited.

OT system area: All CBS in this area: AMS and MCS and other network devices in this area are connected to the switches in this area and connected to the L2 switch. Main Generators and Main Generators BCR are networked separately and are not connected to other networks.

Wireless area: All CBS and other network devices in this area are connected to the switch in this area and connected to the firewall.

Office area: The office area includes CCTV sub-area and office LAN sub-area. All CBS and other network devices in the CCTV sub-area are connected to switches in the area and connected to switches in the office LAN area. All CBS and other network devices in the office LAN sub-area are connected to switches in the area and connected to the firewall.

Communication area: All CBS in this area: ECDIS, VDR and other network equipment in this area are connected to the switch in this area and connected to the firewall.

Security Management Center Area: All CBS in this area: Network monitoring servers and CSMS workstations need to be connected to the switch of the aera they belong and to the firewall.

6. Cybersecurity Products and Services

No.	Product Name	Function Introduction	Quantity
1	Ship Cyber Security Symbol Forensics Service	Help shipowners complete the deployment and implementation of the entire solution, complete all submission documents and other materials required by the classification society with the support of the shipyard and shipowner, and complete CBS exemption application and risk assessment documents	1
2	Vulnerability scanning and penetration testing services	Provide on-site commissioning of the ship's cybersecurity system, testing services for the ship's cybersecurity system, and test outlines	1
3	Management system construction services	Based on the results of risk assessment and compliance analysis, and in accordance with the requirements of the ship industry, a safety management framework is formulated	1

		to clarify management policies, strategies, and corresponding regulations, operating procedures, business processes and record forms, and to establish a ship network security management system.	
4	Firewall	Boundary protection, spam filtering, division of security areas, provision of regional boundary access control, strict control of access to each security area, clear access source, access object and access type, ensure the normal conduct of legal access, and eliminate illegal and unauthorized access; at the same time, effectively prevent, discover, and handle abnormal network access.	1
5	Network monitoring system	Realize network monitoring and analysis of network devices, security devices, databases, middleware and other CBS.	1
6	Bastion Host	The operation and maintenance bastion host are a hardware security-specific device that can achieve effective security control in terms of administrator authentication, access control and security auditing. It can control access rights for management tasks based on users, target devices, operation protocols, system accounts, and time conditions. It can also conduct complete audit records of management behaviors of Telnet, SSH, RDP, PCAnywhere, X-Windows, FTP, SFTP, Http, and Https login operations.	On Demand
7	Log audit system	Monitor system activities in real time, record user behavior and system events, and ensure detailed records of all operations. Detect and analyze abnormal activities, potential security threats or intrusions to help identify and respond to security incidents.	1

8	EDR	Check and kill viruses, worms, and malicious codes	Server 1 client on demand
9	CSMS	It mainly helps ships with quality management and continuous improvement during the implementation of cybersecurity, centrally manages documents and records during the implementation of ship cybersecurity and ensures that compliance requirements for ship cybersecurity are met.	1
10	Wireless Controller	Build a secure, efficient and easy-to-manage wireless network	1
11	Wireless Access Point	Wireless network access equipment	On Demand
12	POE Switch	Wireless network AP networking and power supply	On Demand
13	Fiber Optic Module	Used to connect wireless and POE switches to other switches.	On Demand
14	Cabinet	42U server cabinet: Because there is server equipment, you need to use a server cabinet, not a network cabinet. If there is still space in the computer room, there is no need to add additional	On Demand

15	UPS	In the case of power failure, the UPS can support the running time of all devices and switches in the security management center for more than half an hour.	1
16	8-port industrial switch	Used for CBS and safe area networking where the total number of network devices is less than 8	On Demand
17	16-port industrial switch	Used for CBS and safe area networking with less than 16 network devices	On Demand
18	24-port industrial switch	Used for CBS and safe area networking where the total number of network devices is less than 24	On Demand

7. Hardware Specifications

Product name	Firewall
Product indicator items	Product indicator item
Hardware Features	8 10/100/1000M adaptive Ethernet ports 2 1G SFP ports
	1 RJ45 MGMT port (using GE0/0/0) and one RJ45 Console port
	Single Power Supply
	1 USB 2.0 port

Product Name	Network monitoring server
Product indicators	Parameter
Memory	At least 64 GB
Hard disk space	8 TB or more of hard disk space
CPU	Intel Xeon 32 -core CPU or equivalent
Network Card	1000Mbps full-duplex network card

Product Name	CSMS workstation
Product indicators	Parameter
Memory	At least 16G
Hard disk space	Hard disk space greater than or equal to 2TB
CPU	Intel Xeon 8-core CPU or equivalent
Network Card	1000Mbps full-duplex network card

Product name	switch
Product indicator items	Parameters
Service Interface	24 10/100/1000M adaptive electrical ports
Power Supply	AC power supply
Rated input voltage	AC (AC) input: • Rated voltage range: 100V~240V • Frequency: 50/60Hz

Product Name	UPS Uninterruptible Power Supply
Product indicators	Parameter
Rated input voltage	Rated capacity: 2KVA Input voltage range: 115-295V Input power factor: >0.98 Output voltage range: 220V Output power: 50HZ

Product name	POE Switch (on demand)
Product indicator items	Parameters
Service Interface	24 10/100/1000M adaptive electrical ports, 4 1G SFP+ optical ports, maximum PoE output 370W.
Power Supply	Fixed single AC power supply
Rated input voltage	AC (AC) input: • Rated voltage range: 100V~240V • Frequency: 50/60Hz

Product name	Optical Module (on demand)
Model number	MINI-GBIC-SX-MM850

Product name	Wireless AP（on demand）
Product indicator items	Parameters
Service Interface	1 10/100/1000Base-T adaptive Ethernet electrical port, support IEEE 802.3af Ethernet standard PoE power; 1 2.5G SFP port,

	compatible with 1G SFP port
Management port	Console port for 1 RJ45
Rated input voltage	Rated DC input voltage current: 48V/0.6A PoE Ethernet power supply (meet 802.3af Ethernet power supply standard)

Product name	Wireless controller
Product indicator items	Parameters
Service Interface	8 10/100/1000BASE-T interfaces 2 1GE SFP/RJ45 photoelectric multiplexing interfaces ● RJ45 ports support 10/100/1000BASE-T ● The port numbered "9/MGMT" can also be used as an MGMT port Note: The photoelectric multiplexing interface is an interface type that consists of two Ethernet ports (one optical port and one electrical port) on the panel of the device. The electrical port and optical port cannot work at the same time on the device, and when one interface is activated, the other interface is automatically disabled. You can select one interface type based on the actual networking. Two 10GE SFP+ ports
Management port	1 RJ45 Console port 2 USB 3.0 (compatible with 2.0) ports
Rated input voltage	100V AC~240V AC，50Hz~60Hz

Product name	8-port industrial switch（on demand）
Product indicator items	Parameters

Service Interface	8 10/100M adaptive electrical ports

Rated input voltage	• Connection
	  o 2 removable 4-contact terminal block(s)
	• Input Current
	  o 0.47 A @ 24 VDC
	• Input Voltage
	  o 12/24/48/-48 VDC
	  Redundant dual inputs
	• Operating Voltage
	  o 9.6 to 60 VDC

Product name	16-port industrial switch（on demand）
Product indicator items	Parameters
Service Interface	14 10/10M adaptive electrical ports, 2 1G SFP+ optical ports.

Rated input voltage	• Connection
	  o 2 removable 4-contact terminal block(s)
	• Input Current
	  o 0.47 A @ 24 VDC
	• Input Voltage
	  o 12/24/48/-48 VDC
	  Redundant dual inputs
	• Operating Voltage
	  o 9.6 to 60 VDC

Product name	24-port industrial switch（on demand）
Product indicator items	Parameters

Service Interface	24 10/100M adaptive electrical ports, 4 1G SFP+ optical ports.

Rated input voltage	• Connection
	  o 2 removable 4-contact terminal block(s)
	• Input Current
	  o 0.47 A @ 24 VDC
	• Input Voltage
	  o 12/24/48/-48 VDC
	  Redundant dual inputs
	• Operating Voltage
	  o 9.6 to 60 VDC