Cyber Security by Design

The **Cyber Security by Design** consultancy service, created by Aeromarine and S2 Grupo in 2020, has been adapted to comply with the new **IACS E26 and E27** regulations.
It is a shipyard turnkey service that allows the outsourcing of all cybersecurity tasks necessary for the mandatory cybersecurity certification of new ship buildings.

The service focuses on obtaining the necessary information from manufacturers, analyzing it, checking compliance, correcting deficiencies, overseeing the implementation of systems and their integrations and conducting technical tests to ensure that the vessel complies with the notation.

All this prior to the final certification tests of the vessel done by the Certification Society.

IACS E26 & E27 Regulations

The new regulation is mandatory for new buildings of ships of 500GT and upwards engaged in international voyages, since the 1st of July 2024, depending on their type:

Mandatory for	Non- mandatory Guidance to
✓ Passenger ships	× Ships of war and troopships
✓ Cargo ships	× Vessels not propelled by mechanical means
✓ High Speed Craft	× Wooden Ships
✓ Mobile offshore drilling units	× Passengers' yachts (< 12 passengers)
✓ Self-propelled mobile offshore	× Pleasure yachts
	× Fishing vessels

Turnkey Solution

Cyber Security by Design introduce cybersecurity in all phases of the building of a new ship or offshore platform, from the request for tenders to suppliers to the delivery of the vessel. It is a process in which all IT and operation systems (OT) are analyzed. It involves all construction stakeholders: manufacturers and suppliers, integrators, shipyard, shipowner and certifier.

01 Specification

Definition of the main axes and start-up of the project:

- classification society
- cyber security notation
- list of manufacturers
- consultancy with manufacturers to receive the right documentation
- additional shipowner Criteria

02 Systems

Systems Documentation analysis to:

- verify the systems to include in the project
- check compliance with IACS requirements
- consultancy with manufacturers to remedy identified deficiencies
- Define counter-measures

03 Integration

Systems Integration analysis to:

- Classify systems by security level
- Ensure the security of internal / external communications
- Design / configure networks and security devices
- check compliance with IACS requirements

04 Tests

- System & integration tests to verify that the implementation is in line with the configuration reflected in the documentation
- Industrial cyber security technical tests
- Assistance in the certification tests carried out by the classification society

Aeromarine will provide the shipyard with the necessary information for the certification of the vessel, based on the mandatory documents to be submitted by each manufacturer, both for their systems and for the interrelation with the others.

This documentation will allow the shipowner to prepare the CSMS (Cyber Security Management System) that will be required by the classifier in the first annual review of the certification.

Benefits of the Service

Cost Control

Fixed price per project including all cyber security tasks up to certification. The shipyard acts as a coordinator between parties.

Expert Team

knowledge and experience in IT/OT equipment, compliance, cyber security and technical identification and intrusion tests.

Proven Method

with the right workforce at each stage, and tested In other projects, ensuring the certification with any Classification Society

Software

Documentation of the Project will be delivered on an internally developed software, which facilitates its management.

About Us

+ 20 YEARS INSTALING OT SYSTEMS ON SHIPS

- Integrated bridges
- Navigation equipment
- Internal / external communications
- Fleet management software
- Creation of equipment, spares and maintenance databases

+ 200 IT/OT CYBER CONTRACTS

- Energy / Petrochemical
- Engineering
- Manufacturing / Infrastructure
- Transportation / Logistics
- Banking / Insurance
- Healthcare
- Government Agencies

PROPRIETARY MONITORING SOFTWARE

- **GLORIA** monitoring system that, with its **ARGOS, TRITON, CARMEN, EMAS** and **HERA** modules, makes it possible to monitor the security status of a facility, detect attacks and apply preventive remediation

SOCs: SECURITY MONITORING CENTERS

SOC with more than 300 experts dedicated to monitoring customer facilities. Main locations:

- Madrid
- Valencia
- Bogotá
- Méjico

Other Advance Services

Cyber Security Audit

On-site study of the shipyard's facilities to make then cyber-resilient.

Monitoring System

monitor installations to, resolve incidents and prevent attacks

Treat Hunting

proactive search for latent threats to prevent incidents

Ransomware Resilience

Simulation to validate procedures, tools and skills.

Digital Company Surveillance

Monitoring of company information in open networks

Malware scanning and protection

Research, collection and classification of IoC indicators of threats.

Digital Trace

search for available economic, social, ideological info of a company or person

Forensic Analysis

Origin of infection, infected assets, activities carried out....

Threat Modelling

Service that creates customized malware for defense and attack teams Training.

Need More Information?

aeromarine

Cybersecurity.aeromarine.es

✉ comercialsoft@aeromarine.es

☎ 913 456 828