ABB recognizes the importance of cyber security in the marine industry and is working closely with shipowners, yards and classification societies to enhance cyber resilience of ships. As vessels become more electric, digital and connected than ever before, it is of vital importance that we equip and empower seafarers with reliable solutions that are cyber secure.

### Foundation

**ASSESSMENT**

**Cyber Security Assessment**

Cyber security assessment identifies your most vulnerable control system assets and give an overall system cyber security status update. Based on system in scope, it uses non-invasive data gathering techniques and provides operators with a color-coded report highlighting areas for improvement. It provides an instant overview of your system current ability to deal with a cyber-attack.

In order to accelerate understanding, decision making and problem solving, the results are presented in an intuitive easy-to-understand “stop-light” report. System KPIs, represented by three colors red, yellow and green indicate high, medium or low risk.

**Cyber Security Risk Assessment**

Cyber security risk assessment is a consulting service based on IEC62443 standard that takes a holistic approach to cyber security. The result is a cyber security action plan that highlights the risks identified, prioritizes those risks, and provides actionable remediation steps. Operators can employ this plan to prevent the disruption of operations by even the most determined attackers.

**Cyber Security Gap Assessment**

Cyber security gap assessment is a consulting service that provides customers with a detailed gap description against DNV GL cyber secure class notation with suggested mitigation. The service covering only automation, propulsion, remote control system (RCS) and switchboard scope.
SECURITY CONTROLS
Once the risk identified through security assessment, risk assessment and gap assessment, customer should be ready for next step which is applying security controls to mitigate gaps/risk.

Secure remote access
The Remote Access Platform (RAP) is default remote access solution from ABB, the solution provides a secure remote access and secure file transfer. ABB’s Remote Access Platform allows highly secure, real-time central monitoring and control of devices located at customer sites. It also provides audit and security features, including audit logs to track user and application access.

Security Update Service
The ABB security server is updated with the latest patches validated and approved by ABB for control system use, that covers Microsoft Windows patches (monthly update), McAfee virus definition files (daily update) and Symantec virus definition files (daily update). The downstream server at the customer site synchronizes with the ABB security server via ABB’s Remote Access Platform and distribute the updates internally to all system nodes.

Backup and Restore
ABB experts work alongside customer team to outline and put into effect a detailed backup strategy and recovery plan. ABB installs and manages the backup system platform, relieving you of the burden of testing and maintaining this all-important aspect of your operational readiness.

USB security Kiosk
The goal of the USB security kiosk is the protection of customer Operational Technology (OT) systems against USB borne malware and attacks. To achieve this goal, USB security kiosk Scans and validates removable USB device, allows you to choose to delete the infected files and enforces security policies for removable USB device usage.

Advanced Access management
Advanced Access management based on AAA security designed to enable network administrator to dynamically configure the type of authorization and authentication needed by creating a method list for specific services and interfaces. AAA security means increased flexibility and control over access configuration and scalability, access to standardized authentication methods such as RADIUS.
Application white listing
ABB provides white listing solution based on McAfee Application control which prevents zero-day and APT attacks by blocking execution of unauthorized applications. Using McAfee Application control inventory feature, ABB can easily find and manage application-related files. It groups binaries (.exe, .dll, drivers, and scripts) across the system by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications.

Log aggregation
There is value having all the (event) logs from devices in the production system in one place for easy access, searching, data mining, and consistency. The log aggregation function is a database where multiple streams of logs are normalized and stored. The user can access the logs through the user interface and configure queries, notification rules, generate reports, export data, or configure the database to forward, all or some, of the data to an external system like a SIEM.

Event Monitoring
Security Information and Event Management (SIEM) system helps security administrator accurately detect and prioritize threats across the entire system, and it provides intelligent insights that enable administrator to respond quickly to reduce the impact of incidents. By consolidating log events and network flow data from devices, endpoints and applications distributed throughout OT network, SIEM system correlates all this different information and aggregates related events into single alerts to accelerates incident analysis and remediation.

Cyber Security Asset Inventory
ABB cyber security asset inventory automatically identifies cyber assets and captures updated inventory information on ports, services and software connected to the control networks. The solution enables users to make better operational, compliance and risk decisions related to cyber security controls, asset lifecycle and asset management.

TRAINING
H830 - Cyber Security Basic level
- Learner will be able to identify risks, threats and vulnerabilities of a vessel.
- Basic knowledge about technology mitigations for cyber security
- How a human resource can be used as a vector for a cyber-attack

H831 - Cyber Security Advanced level
- Learner will get to know how to Perform risk assessment and how to analyze risk mitigation
- Advanced knowledge about cyber security controls and how it can be utilized to mitigate the risk
Service

MAINTENANCE
A service contract is to be signed with customer to maintain security controls deployed onboard the vessel.

Security Health Check
Most simple cyber security service contract, where ABB expert log into the system through secure remote access to health check system security and provide customer with status report with recommended actions.

Security Update
ABB cyber security expert visit customer site periodically, recommended every three/six months based on system in scope criticality. During the visit ABB cyber security expert shall execute security health check using ABB advanced security health check tools, install latest security updates and create new system backups.

Cyber Security Care
This cyber security care kit focuses on fulfilling international cyber security standards and regulations
• IMO.428 (98)
• DNV GL Cyber Secure Class notation
• IEC 62443

ABB Cyber security expert visit customer site periodically, recommended every three/six months based on system in scope criticality to maintain all security controls deployed onboard to fulfill the requirements. Cyber security care have three levels
• Essential: Maintain security controls deployed to fulfill IMO.428 (98) cyber security regulations
• Intermediate: Maintain security controls deployed to fulfill DNV GL cyber secure class notation Essential requirements (based on IEC 62443-3-3 SL1)
• Advanced: Maintain security controls deployed to fulfill DNV GL cyber secure class notation Advanced requirements (based on IEC 62443-3-3 SL3)

CONSULTING
A one-time job based on customer request

Strategy and Policy
ABB works with the customer to develop and document the customers’ cyber security strategy and policy.

Hardening
Makes sure that the defined settings of the computers in the system remain as defined by the DCS vendor and adjusted for the customers’ needs.

Disaster Recovery
ABB cyber security expert work with the customer to resume production as quickly as possible after a cyber disaster.

Remediation
Any work relating to implementing or addressing a cyber security weakness.

Security Controls re-commissioning
ABB re-commission the system to comply with a specific cyber regulation or best practice. This often includes adding various security controls and applying ABBs Reference Architecture.

Operations

This is the last step in the maturity model of the customer (and ABB). In this service, we offer the customer to take over the whole cyber operations or selected pieces of it. ABBs experts (through a partner(s)) provides the customers with ongoing cyber security monitoring, threat intelligence, incident response, and much more as part of a multi-year contract.

Collaborative operations are services delivered by teams working together to deliver services to many customers around the world.