No. 160
(Nov 2018)

Vessel System Design

Contents

1 Introduction

1.1 General

Shipboard systems have evolved from the simple and readily recognizable, mechanical, piping, electrical and pneumatic interconnection of individual components to digitally interconnected systems. The ease with which systems can now be digitally interconnected and the difficulty of comprehending the extent, nature and behavior of the digitally interconnected systems has resulted in a gap in understanding between the way that a vessel works and the capabilities of those involved in managing, maintaining and operating the systems and the vessel.

This gap in understanding makes decisions by those managing and operating the vessel when it behaves or performs outside of its normal characteristics difficult and can cloud assessments of risk.

The nature of Cyber Systems is that they do not lend themselves to fault identification, quick assessments and simple fixes post installation. Any features and precautions that need to be available after commissioning need to be considered during the design and development stages and installed as part of the complete system.

Advantages of using Cyber Systems include scope for innovation and flexibility in original design but disadvantages include less insight into working systems and less ability to make modifications without introducing flaws. The inherent reduced insight can also be a challenge to class surveys as a system overview or identification of the parts that deliver the vessel's performance and safety is not readily apparent when digital systems are involved.

These disadvantages need to be compensated by the development and design of Cyber Systems having means to:

- deliver any required system updates or modifications to the same quality as the original and

- record system updates and demonstrate their continued performance and safety to the Class Surveyor throughout the life of the vessel.

1.2 Objective

This recommendation is intended to drive an overarching or holistic view of design objectives where designers are given the maximum freedom to innovate while still delivering vessels whose safety is not diminished through the introduction of computer-based systems.
This is mostly achieved through encouraging a comprehensive approach to 'systems design' where the following are taken into account:

Human factors

The vessel's crew should have the means to identify system malfunctions and the means to take appropriate remedial action in a timeframe that is meaningful in terms of preventing accidents.

The vessel's operators need to be provided with sufficient system information in order to be reassured that the systems are operating normally and that any backup systems can be monitored or periodically tested and demonstrated.

System Architecture

The basis of the SOLAS approach is a 'single failure concept' and the availability of appropriately trained crew to take the appropriate action in the case of failure. The same approach is considered with regard to cyber systems however,

- greater rigor is necessary to establish the extent of the impact of any single failure
- a potential failure mode includes accidental or deliberate infection of the system
- as systems get more complex unintentional interdependencies can be introduced and traditional review and inspection of individual components or systems may not deliver the safety and reliability that has been achieved in the past. Similarly, modifications made without a full understanding of the system could inadvertently introduce interdependencies which may mean that the independence is degraded, and the single failure principle has been undermined unless an overview of the complete vessel design is maintained when changes are made
- the ship's crew should be capable of operating any backup systems designed to deal with the single failure criteria and may have some competence in computer operation and , but it is unlikely that crew members will be able to deal with every type of cyber system failure without either external support or the provision of a secondary system or equipment to take remedial action within his/her competence. The crew competence and the provision of the necessary support should be considered together in for safe operation following a cyber event.

1.3 Scope

The other Recommendations in this series cover specific and generally known aspects addressing risks resulting from the installation of Cyber Systems on onboard, however it is recognized that the specific and predetermined precautions may not always be sufficient. This Recommendation, in encouraging an overarching or holistic approach, applies to those stakeholders- such as designers, integrators and shipyards - who have responsibility for delivering a vessel designed and built to be operated safely following a cyber event.

Once the vessel is in service its safe operation following a cyber event will depend on the systems installed but also upon the other stakeholders in the industry playing their part to support its continued safe operation.

This recommendation is relevant to on-board cyber systems, which are susceptible to cyber events and which, if affected, could lead to dangerous situations for the safety of human life, vessel or cargo, or threat to the environment, or compromise the confidentiality, integrity and/or availability of critical information.

The extent and level of application may also be affected by additional factors related to the ship as a whole, like type of service and navigation, overall level of digitalization onboard, extension and interconnection of different networks, etc.

This recommendation may be applied to new ships as well as to ships in service as appropriate.

1.4 Exclusion

Items subject to statutory regulations, such as navigation systems required by SOLAS Chapter V, Radio-communication systems required by SOLAS Chapter IV, and vessel loading instrument/stability computer cannot be considered as subject to the provisions contained in this recommendation (see also UR E22).

Nonetheless, when the aforementioned systems are integrated with or connected to systems under the scope of Class, measures should be provided in order to prevent or reduce as much as possible the propagation of possible effects of adverse cyber events to and from such systems.

1.5 References

The following list provides references to international or industrial standards that may be considered as technical background for this recommendation.

[1] IMO MSC-FAL.1/Corc.3, *“Guidelines on Maritime Cyber Risk Management”*, July 2017

[2] ISO/IEC 27001:2013, *“Information technology – Security techniques – Information security management systems – Requirements”*, 2013

[3] NIST *“Framework for Improving Critical Infrastructure Cybersecurity”*, version 1.1, 2017

[4] *“The Guidelines on Cyber Security Onboard Ships”*, version 2.0, BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI, 2017

[5] *“The CIS Critical Security Controls for Effective Cyber Defense”*, version 6.0, Center of Internet Security, October 2015

[6] ISO/IEC 27033-1:2015, *“Information technology, Security techniques – Network security – Part 1: Overview and concepts”*, 2015

[7] IACS UR E22 *“On Board Use and Application of Computer Based Systems”*, June 2016

2 General matters

2.1 Vessels' Cyber Systems and Types

Mainly the onboard Vessels' Cyber Systems are related to:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Ballast water control systems;
- Communication systems;
- Safety systems; and
- Integrated alarm and control systems.

The design of systems and communications between systems and sub-systems should be such that if one of the systems/sub-systems is affected by a cyber event this is not to affect other systems and is to allow continuation of safe operation.

Cyber System should provide automatic control with ability of the crew for manual control in case of cyber event.

2.2 Vessel's System categories

System may be generally assigned with 3 categories (refer to UR E22).

Category I- systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. These systems usually perform only monitoring function for informational/administrative tasks.

Formally the Category I systems are not subject for classification matters, however if they are improperly connected to Category II and III systems the cyber event in Category I systems may affect Category II and III systems.

Category II systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. These systems usually perform alarm and monitoring functions and some control functions which are necessary to maintain the ship in its normal operational and habitable conditions.

Category III systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. These systems usually perform control functions for maintaining the vessel's propulsion and steering and vessel safety functions.

(See Appendix II – Typical System Categories II and III)

3 Philosophy

The basic design philosophy of the cyber system should be documented during the conceptual phase in the Design Philosophy Document (DPD). The DPD should be prepared by designers, integrator and shipyard and maintained by the shipowner after delivery. It can be referred for any subsequent changes to confirm that the intent of the original design philosophy is maintained or not compromised, due to new changes. The changes may also arise due to modifications carried to address field problems and/or technology changes. The DPD can support a holistic approach to modifications and assist in preventing inadvertent errors due to poor comprehension of interdependencies.

Information to be documented in DPD:

- Physical areas covered by the integrated system (engine room, bridge, accommodation etc.);
- Systems integrated (propulsion, steering, power, safety, navigation etc.)

The criteria for system design should be based on following:

- Reliability
- Maintainability
- Extensibility
- Interoperability

A preliminary identification of the consequences associated with failure of systems/sub systems which could lead to a hazardous event should be documented in the DPD. The analysis should confirm safe operation/continued operation with single point failure.

Physical and logical cyber security measures should be implemented to prevent cyber events in the systems/sub systems. These risks and the measures to mitigate the same should be identified and documented in the DPD.

Information to be documented:

- External interfaces connected to the system;
- Protection philosophy;
- Threat analysis and Mitigation methods;
- Response plan/contingency plan for critical systems/sub-systems.

4 Cyber systems’ architecture overview

4.1 Cyber systems’ devices

Onboard Vessels’ cyber systems with critical functions (mainly Category III, but sometimes Category II e.g. when false alarm may affect Category III systems) cover the processes in vessels’ system related to essential services (see IACS UI SC134).

Cyber systems are based on devices that are directly used to control, protect and monitor ship systems and may include one or more, but not limited to, the following components:

- Distributed control systems (DCSs) and associated devices;
- Supervisory Control And Data Acquisition (SCADA) systems and associated devices;
- Programmable logic controllers (PLCs) and associated devices;

- Routers, switches;
- Human Machine Interface (HMI) stations;
- Other shipboard computers and programmable devices.

The actual components of systems may vary with each installation according on the systems being controlled and /or monitored.

4.2 Cyber systems’ fault tolerance

For systems of Category III and II connections within the sub-systems and their networks should be resilient to faults with self-correcting propertiesthat guarantee to provide data to be transmitted without failures.

Local controls and indicators should be a part of the fault tolerance architecture.

The requirements for architecture should be based on risk assessment.

Components without complete traceability should not be used in critical systems to reduce the attack surface and limit the damage and spread of exploits when they do occur.

This may reduce attacks on critical processing and data by separating them from non-critical data and processing.

The goal should be also to decouple capabilities in order to prevent ripple effects that can contaminate large portions of the systems as the result of a single cyber event.

5 Equipment standards for vessel’s cyber systems

5.1 Cyber systems devices

The network devices for Category III and II systems should be suitable for marine application and should be tested as specified in IACS UR E22 and E10.

5.2 Connections, networks, cables:

All network cables for categories III, II, I should be flame retardant and should be designed, manufactured and tested as per relevant National/International Standards. Cables should be fire resistant type where required by rules.

5.3 Wireless equipment

Wireless equipment should be designed and tested as per requirements specified in IACS UR E22 for Category II systems.

6 Data requirements

Data categorization, data classification, data format and data content should be as per Recommendation number 5.

7 Vessel's cyber systems access control, monitoring and alarm

7.1 Communication networks

To ensure reliability and quality of the network, suitable network monitoring and alarm systems should be deployed. The network-monitoring device should be installed at suitable location.

The crew should be able to identify the locations of errors from the network-monitoring device.

7.2 Access control

Access control is the method of controlling who or what resources can access premises of systems and what type of access is permitted.

There are three key aspects associated with access control:

- account administration;
- authentication;
- authorization.

All these aspects should work together to establish a sound and secure access control strategy.

The access control system should provide the capability to protect the integrity of sessions.

The access control system should reject any usage of invalid session IDs.

7.3 Monitoring

Following functions as minimum should be monitored:

- Link up of each port on the network device;
- Link down of each port on the network device;
- Power on or hardware reset;
- Loop guard (only if the network device has a loop detection function);
- Fan (only if the network device has a fan and a fan-stop detection function);running status
- Abnormal temperature (only if the network device has an abnormal-temperature detection function;
- Network loss/delay tomography.

7.4 Alarm function

The network-monitoring device should have a function to detect abnormal state changes and notify the user of them:

- When a link is disconnected or the power is turned off for a network device or network terminal;
- When a link is connected, or the power is turned on for a network device or network terminal which was not in the original configuration;
- Network congestion thresholds.

7.5 Wireless Communication

- The access control system should provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

- The access control system should provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted cyber security industry practices.

- The communication control system should provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.

7.6 Installation requirements

The cyber systems' devices should be installed in protective cases unless the ingress protection of the device meets the Class requirements. The protective cases should allow access for maintenance.

The devices should be located in well ventilated areas and should be installed at a sufficient distance from vibration sources so that it is not adversely impacted by external vibration. Equipment should be installed sufficiently distant from noise sources so that it is not adversely impacted by external noise.

7.7 Cabling

The minimum bending radius specified for the cable should not be exceeded especially for optical cables where it may lead to signal loss.

The requirements of segregation from Electromagnetic Interference Sources (EMI) sources should be met (e.g. IEC-60050 or other equivalent standards).

It is recommended to group and separate key systems into zones with common cyber security levels in order to manage appropriate risks and to achieve a desired target of cyber security level for each zone.

7.8 Demilitarized zone (DMZ)

For high risk control systems or remote access systems, a DMZ should be used in conjunction with a Control zone to offer additional risk reduction opportunities between the low-cyber security level zone and the high-cyber security level control zone. A DMZ eliminates or reduces all direct communication between the control zone and the other non-essential zones. Use of DMZ minimizes the number of people directly accessing critical control zone devices. Segmenting networks is consistent with risk management in accordance with IEC 62443 for industrial controls.

8 Testing

8.1 General

Vessel's cyber system testing should be carried out to verify the intended operations successful performance.

The testing should be carried out after complete installation of network cables and all devices.

The simulation tests should demonstrate how the commands from the cyber system may be executed.

8.2 Scope of testing

The scope of verification & testing of the cyber system should at least include the following:

- All cabling and network devices;
- All functionality relating to network communication by nodes connected to the network system;
- All external and internal communications;
- Monitoring and alarm systems;
- Backup procedures and results;
- Verify effective response and recovery in a failure event of critical computer based system (contingency plan);
- Local control ability in case of cyber event.

Appendix I - Definitions

Automatic control:
Control of machinery without human intervention as per predefined logic.

Back-up procedure:
Procedure used to restore local operation after a cyber event.

Computer Based System:
The system based on computer technology which may be comprised of hardware, software and the associated interfaces for input and output.

Contingency Plan:
The plan which provides essential information and established procedures to ensure effective response and recovery in a failure event of critical computer based system. (

Cyber event
Cyber event is an occurrence, which actually or potentially results in adverse consequences to an on-board system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Cyber System
Computer based system, combination of interacting programmable devices and/or cyber sub-systems organized to achieve one or more specified purposes. Cyber System may be a combination of Cyber Sub-Systems, connected via network. Cyber System may be connected directly or via public means of communications (e.g. Internet) to ashore based Cyber Systems, other vessels' Cyber System and/or other facilities.

Cyber Sub-system:
Identifiable part of a system, which may perform a specific function or set of functions.

Cyber safety:
The condition of being protected against vulnerabilities resulting from inadequate operation, integration, maintenance and design of cyber related systems, and from intentional and unintentional cyber threats.

Cybersecurity:
The preservation of confidentiality, integrity and availability of information due to malicious attacks which can be both intentional and unintentional cyber threats.

Demilitarized zone (DMZ):
Common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones

Failure mode effect analysis:
The analysis which identifies if the system is able to continue to conduct mission-critical processing in a manner that preserves the confidentiality, integrity, and availability of the data in case of cyber event.

Human Machine Interface (HMI):
The operators interface to the concerned process / machinery.

Local control:
Control from a location in the immediate vicinity of the concerned machinery.

Local indicators:
Indicators located in the immediate vicinity of the concerned machinery.

Manual Control:
Command given manually by the operator. Manual control may be through operation of mechanical, hydraulic, electrical, computer-based systems or a combination of some/all.

Network:
A network is defined as a group of two or more computer systems linked together. There are many types of computer networks.

Programmable device/ Programmable logic controller (PLC):
Physical component where software is installed.

Simulation tests:
Control system testing where the equipment under control is partly or fully replaced with simulation tools, or where parts of the communication network and lines are replaced with simulation tools.

Software:
Programs and operating instructions used in shipboard equipment, including firmware.

Sub-system:
Identifiable part of a system, which may perform a specific function or set of functions.

System:
Combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes.

System Categories:
(I, II, III) Those systems, failure of which:

I. will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

II. could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

III. could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Vessel:
Ship or offshore unit where the system is to be installed.

Network devices
Various components /equipment forming part of network. Example Computers, PLC, Switches, routers etc.

Appendix II – Typical System Categories II and III

The following systems typically belong to Category II, the exact category being dependent on the risk assessment for all operational scenarios:

- Liquid cargo transfer control system;
- Bilge level detection and associated control of pumps;
- Fuel oil treatment system;
- Ballast transfer valve remote control system;
- Stabilization and ride control systems;
- Alarm and monitoring systems for propulsion systems.

The following systems typically belong to Category III, the exact category being dependent on the risk assessment for all operational scenarios:

- Propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship (devices used only during maneuvering are not in the scope of this requirement such as bow tunnel thrusters);
- Steering system control system;
- Electric power system (including power management system);
- Ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in operation of life saving appliances equipment;
- Dynamic positioning system of equipment classes 2 and 3 according to IMO MSC/Circ.645;
- Drilling systems.

In some cases a Category I or II system may be escalated to higher category when:

- System with lower category has direct impact on the higher category system (e.g. fire alarm system may disrupt main engine fuel supply system);
- Due to the specific integration of higher and lower category systems the higher category may be assigned to the lower category system to avoid cyber event disrupting higher category system via lower category system;
- In other cases when the risk assessment requests extra measures to prevent cyber event.

End of Document