CENTRE FOR
CYBER SECURITY

Guidance for cyber security in OT systems on board ships

Ships are increasingly using digital technology to support or manage critical operations on board, including navigation, communications, manoeuvring and cargo handling systems, so-called Operational Technology systems. These systems may be vulnerable to threats such as hacker attacks, viruses, etc. This guide is intended to assist shipping companies in addressing such threats.

The work to address cyber security issues is comparable to other work related to on-board security in which human resources, organizational circumstances and technical solutions are coordinated to limit risks. Illustrative of this are the requirements under the Safety of Life at Sea (SOLAS) convention that dictate well-trained sea crew, clear procedures and approved rescue equipment. Similarly, cyber security requires competencies and insight from staff both on land and at sea, a clear division of responsibilities, and the relevant technical equipment and processes.

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

March 2020

Digital vulnerabilities may be exploited via direct access to the Internet, via suppliers or other external actors with system access, or in connection with crew inadvertently transferring malware to central systems.

Listed below are four recommendations on how to handle four vulnerabilities: Lack of crew knowledge, unclear roles and responsibilities, lack of processes, and insecure technical conditions.

1. **Crews at sea and employees ashore must hold the right competencies**.

   Crews at sea and employees ashore must know why and how to facilitate cyber security in OT systems on board ships. At sea, crew thus need to understand why access across systems may be limited despite the potential inconvenience this may cause. On land, employees must know how to best support the secure operation of the ships.

2. **Clear division of roles and responsibilities is a must.**

   The individual crew members must understand their personal role in upholding cyber security as well as the cyber security responsibilities of other crew members, the captain, and the organization on land.

3. **Procedures to support cyber security efforts on board.**

   Procedures and policies must be in place to handle cyber security both at sea and on land. Supplier contracts, including charter contracts, must prescribe how potential consequences of cyber risks are to be handled. Transparent cyber security efforts facilitate contribution by all crew members.

4. **Technical measures to limit technical vulnerabilities.**

   There are many simple technical measures that can be adopted to promote cyber security. The first one is to create an overview of the networks and components present on each individual ship to prioritize the monitoring of networks.
   Special focus should be on the online connections of the individual ships. Access to the Internet must be monitored and protected. It is recommended that all traffic between the ship's OT and the Internet go through the shipping company via an encrypted and authenticated connection. In this way, the shipping company is able to protect the ship against known threats just as it is able to establish a log of the data traffic.

It is essential to create a bridge between IT and specialized technical areas is necessary when working to protect OT systems against cyber threats. A short checklist with suggestions on how shipping companies may structure such efforts can be found overleaf. The work presupposes an effort both on the part of the crew at sea and on the part of the shipping company that is to back efforts, contributing specialized knowledge and management prioritization.

The checklist is **not** an exhaustive list of recommendations and advice on how to handle the risks potentially posed by the cyber threat to OT systems on board ships. The Centre for Cyber Security has published the guides: *Håndtering af industrikontrolsystemer,* *Informationssikkerhed i leverandørforhold* og *Cyberforsvar der virker.*

Overview of internal systems, networks and external connections

- ○ Create and maintain an overview of all IT and OT system functions, components and networks on board all ships.
- ○ Map external connections from all ships, including their communications technology, and protocols as well as encryption and authentication used.

Formulate a written information security policy

Clarify the division of responsibilities and cooperation between the organization’s units on land and at sea.

Formulate procedures on how to address new threats or vulnerabilities as well as breakdowns or attacks on the different IT and OT systems.

All crew on board the ship and on land must contribute to the controlled preventive and reactive response based on the written down responsibilities and tasks as well as the assigned access and rights of:

- ○ Captain
- ○ Chief engineer
- ○ Mates
- ○ Other officers
- ○ Other crew members
- ○ Accompanying maintenance technicians and external suppliers

Cyber security exercises at sea and on land

Exercises must be held regularly both at sea and on land to train the planned procedures on how to handle warnings of threats and vulnerabilities. Training must include:

- ○ Incident recognition,
- ○ Damage control,
- ○ Emergency operation,
- ○ Re-establishment of system functions and data, including use of local backup

Local conditions determine what is relevant to include in the exercises. Elements may include:

- ○ operation monitoring of propulsion in the absence of digital systems
- ○ handling of unauthorized access to the navigation system
- ○ attacks via suppliers.

The shipping company’s organization on land and its partners such as IT security companies should be involved in the exercises if they are expected to contribute to the operational handling of incidents.

Segment and monitor on-board networks

Divide the on-board network into segments, each with individual security levels and policies.

- ○ Formulate rules for traffic to and from each segment
- ○ Monitor critical segments – activities such as port scans, firmware updates and protocols set off alarms.
- ○ Log access attempts to and from critical segments
- ○ Let the shipping company protect the ship by letting all traffic go via the company’s firewall
- ○ Monitor updates for OT systems.
- ○ Non-updatable OT systems are not to be taken online.

Involve suppliers in the security measures in a controlled manner

- ○ Involve key suppliers in the formulation of emergency response plans and exercises.
- ○ Obligate suppliers to follow rules for remote access, including:
    - Updates of OT systems should be incremental, ensuring continued accessibility of operational systems.
    - Supplier remote access must be logged, time-limited and monitored.