Cyber threat to ships – real but manageable

KAI HANSEN, AKILUR RAHMAN – If hackers can cause laptop problems and access online bank accounts or credit card information, imagine the havoc they can wreak on a ship's control systems. But is this a real threat or science fiction?

The Information Age has brought enormous benefits. But progress typically brings new problems, and our dependence on computers raises the threat of hacking. This has led to the development of a body of technological processes and practices known as cyber security. Cyber security protects networks, computers, programs and data from attack, damage or unauthorized access.

Vessels have also started to increasingly depend on information technology (IT), taking solutions that offer high functionality at moderate cost out of the office environment. This means we must also take cyber security in the marine sector seriously. EU and US government reports on security in the shipping and transport sectors confirm this view.

Cyber security is much more than a simple technical fix that solves all problems, as it is sometimes portrayed in the media. It is just as much a question of culture and attitude as it is technology. The best encryption algorithms in the world are useless if someone writes the password on a Post-it note and leaves the door open. Security must be in focus during the product design, planning and engineering of a vessel, as well as during the commissioning of the IT equipment and operation of the ship.

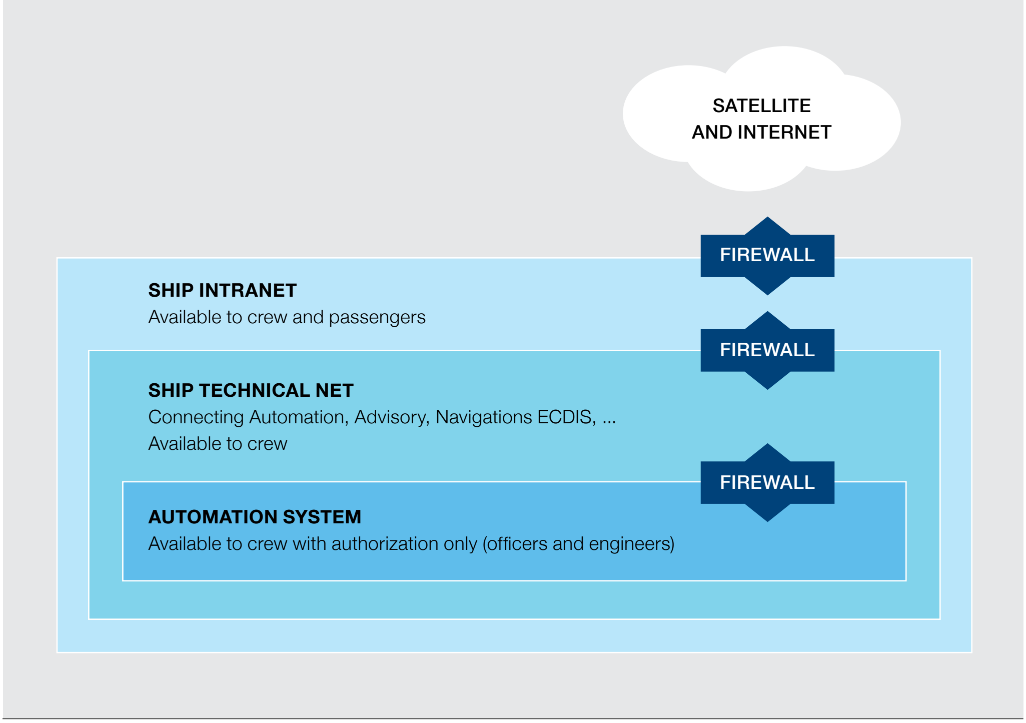
Cyber-threat proof solutions

Even if the yard and the ship owner carry final responsibility, ABB takes security very seriously. We provide products and solutions that have been developed with security in mind and that, used correctly, provide a vessel with good protection against cyber threats. ABB can also evaluate the security level of a fleet to ensure it is cyber-threat proof.

ABB also takes security into account during product development. Internal R&D processes have a checklist of questions on security, ABB has a dedicated robustness test center at its research center in Bangalore and the main systems have been tested at US cyber security laboratories. ABB also has processes in place to handle new security issues that may arise.

One central concern when delivering electrical propulsion systems, electrical generation and protection equipment, and automation and advisory solutions is how all these are connected in a network

1 Defense-in-depth with security zones applied to a vessel


SATELLITE AND INTERNET
FIREWALL
SHIP INTRANET
Available to crew and passengers
FIREWALL
SHIP TECHNICAL NET
Connecting Automation, Advisory, Navigations ECDIS, ...
Available to crew
FIREWALL
AUTOMATION SYSTEM
Available to crew with authorization only (officers and engineers)

architecture and how the network is connected with other systems on the ship and on land. The key word here is defense-in-depth, with security zones in place. Defense-in-depth refers to multiple, independent and redundant layers to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.

Traditionally the different technical solutions have not been connected together in a proper computer network; this has been used to argue that cyber security is not relevant to vessels. This is only partially true. In a disconnected system, there is no risk of a problem occurring during normal operations.

However, typically these systems will occasionally be connected to a maintenance computer, a USB stick or a modem. In these instances, the system is as vulnerable as a connected system. And if a security culture and measures are not in place, malicious code could end up disrupting the system.

A better approach is to accept that security measures always have to be in place and take advantage of the increased functionality a connected system provides – then take the effort to design good network architectures.

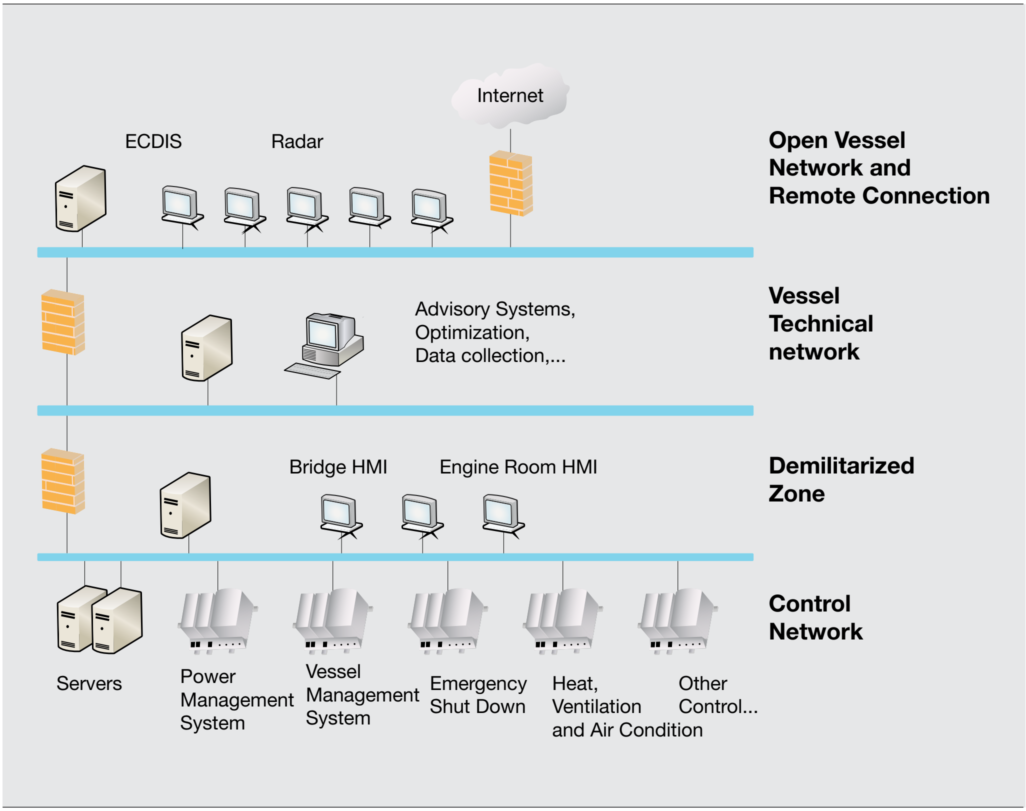
Defining security zones

The security zones illustrated in Figure 1 are a feature of the principle of network architecture. This is also called defense-in-depth because the more critical parts that need better protection there are located deeper into the core of the system – you have to pass a barrier that typically includes a firewall to enter from an outer zone to an inner zone.

A simple threat analysis should be done to define the security zone hierarchy for marine solutions. Critical systems include those that handle propulsion, and power that is part of the marine automation delivery. Typically, all these marine automation systems will be located in one inner security zone as indicated in Figure 1.

Other equally important security zones could include the navigation system network. At the next level up, a zone connects some of the most critical areas, which could also include systems not as critical for running the ship safely. This zone is called the Ship

2 Example of ABB systems with a network security zone structure on a vessel



Technical Net (see Figure 1). It could be connected through a firewall to an open ship network, which is then connected to the world through a satellite link.

Many people access an open ship intranet, such as that of a cruise ship or ferry. On other vessels, off-duty crews use the network for getting news, contacting friends and family, etc. Such generic Internet traffic is valuable and should, of course, be used; however, use should be restricted to the part of the network where malicious code or simple mistakes cannot influence the operation of the vessel. Using the right firewall protection to secure zones can ensure that this does not happen.

Figure 2 is a representation of the conceptual zones, shown in Figure 1, as boxes and links. Here a different type of zone, called a demilitarized zone in security language, has been added. This special type of security zone is suitable for systems that are less critical than those of core automation, but closely linked to the automation system.

Maintaining a secure level

Assuming a vessel is delivered with a state-of-the-art security design, it is equally important that there is a high security level in the operation of the ship. The crew needs to have a basic understanding of the rules and act accordingly.

The vessel owner or operator should at least do the following:

- Have a policy for secure operation and maintenance of the system
- Not connect the secured network to any unknown network or point not in the original design of the plant network
- Not use portable media without virus scanning
- Update security patches and antivirus software as recommended by the vendor of the system
- Keep the ports and services not required for operation closed
- Have a process and system in place for system change management

3 The SD3+C model used for ABB product development

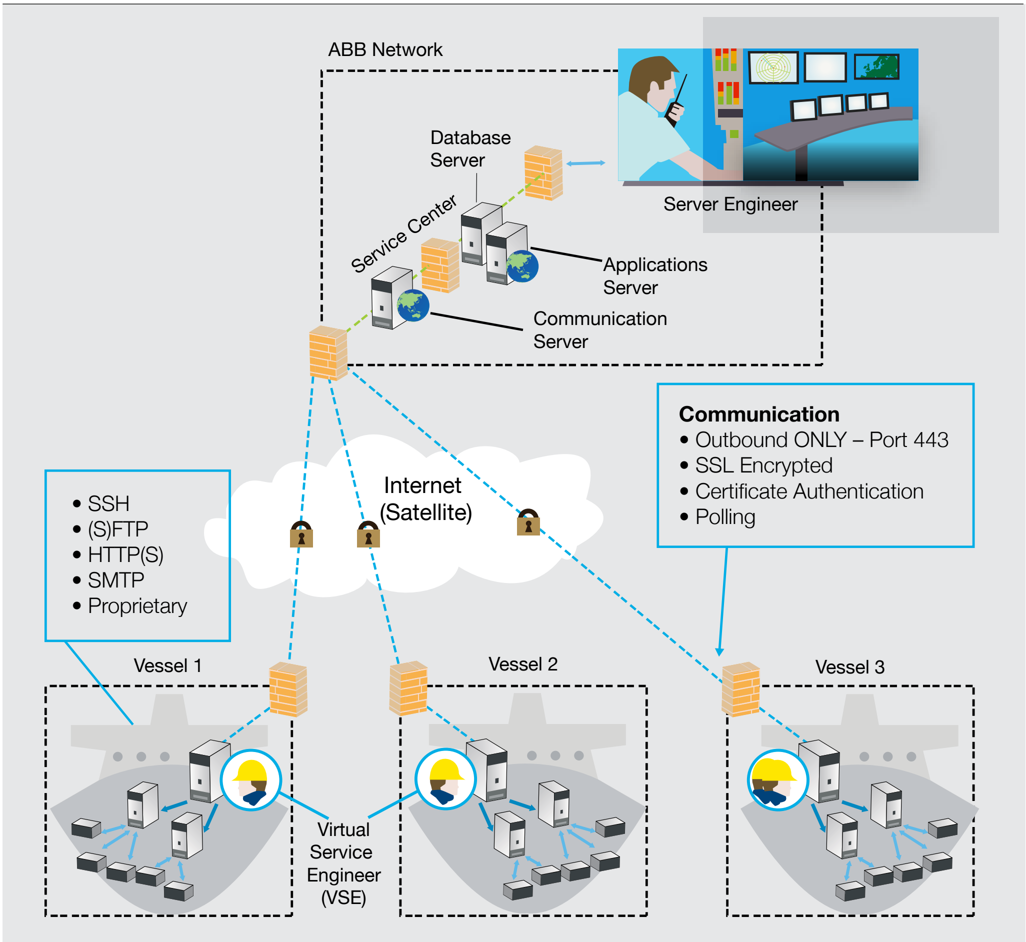
Secure by Design	Security in Product Development Process: Requirements, Design, Implementation, Verification
Secure by Default	Default Installation with Minimal Attack Surface, Defense in Depth, uso of Least Privileges
Secure in Deployment	Product Support for Secure Configuration, Operation and Maintenance, Support for System Updating
Communication	Openly and responsibly communicate with users about detected security flaws: implications and how to mitigate them (corrections and workarounds)

- Back up the system and have a procedure to validate and recover the back-up
- Monitor the system for any suspected security risks, including user rights and activities
- Inform and get support from the system vendor for any security vulnerability and incident in the system

It is not realistic to expect every vessel to have access to IT and cyber security expertise; however, most people today have some level of IT knowledge and security awareness through using their private computers. It is very much about awareness. For example, no crew member will install a computer game in the automation computer if he or she understands that this could increase the risk of a total blackout during a hurricane. Making sure a maintenance computer has an updated virus scanner before connecting it to the control network is a simple step – but it must be remembered and may require a few minutes' delay.

It is not realistic to expect every vessel to have access to IT and cyber security expertise.

Different industries have debated whether cyber security in the technical network is the responsibility of IT or automation experts. With more awareness in the maritime industry, ABB also expects this to become a hot topic. Who is responsible: the chief engineer, the bridge or someone else? There is no simple answer yet; it will be an interesting discussion.



4 Overview of ABB Remote Access Platform (RAP)

Designing robust products

ABB's philosophy regarding security in product design and deployment is called SD3+C. This abbreviation reflects four key concepts:

- Secure by Design
- Secure by Default
- Secure in Deployment
- Communication

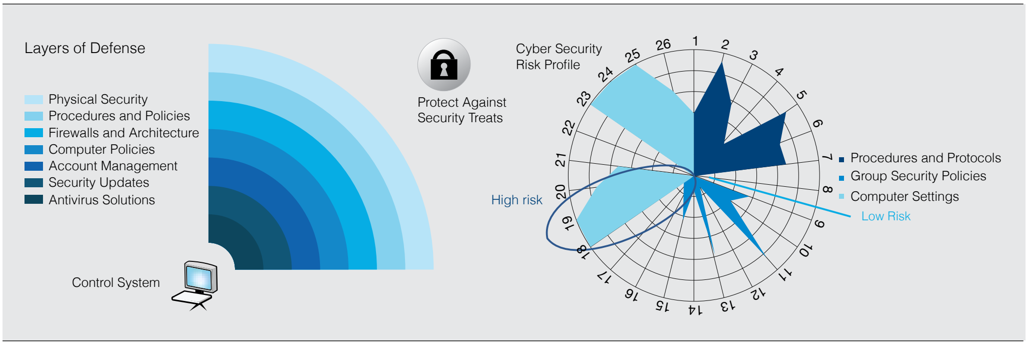
ABB follows the Secure by Design principle when making a new product. This means carrying out the architecture with an understanding of security issues, and coding software in a way that minimizes the risk of bugs being introduced by hostile hackers. Conducting a threat analysis highlights the parts of the product that need special attention.

Secure by Default implies that the product has an acceptable "out of the box" security level. Active engineering work will be necessary to enable features that are not always needed because using all additional functionality in a product increases vulnerability.

Secure in Deployment indicates that the commissioning of equipment was done with security knowhow, that proper documentation was provided, and that functionality supporting operational needs is in place to maintain a high level of security.

Communication is essential to security. Accepting that any system can have flaws is the most important step in a continuous improvement process; this is the only way to ensure a high level of security for ABB solutions.

5 ABB's Security Fingerprint analysis



Offering secure remote access

ABB offers secure access into a remote system. The well-proven solution is called Remote Access Platform (RAP) and is, for example, used in the Remote Diagnostic Service (RDS) that links a number of vessels to the ABB service support center.

A sketch of the RAP is given in Figure 4. The core of this solution consists of an encrypted connection between the ABB Service Center through the open Internet and into the customer's technical network. In the customer network, software called Virtual Service Engineer ensures that only registered clients are allowed to access only predetermined parts of the system. This ensures that only ABB Service engineers have access to a vessel. The advantage is huge; complex problems with drives or switchboards can be solved directly without the need for an engineer to travel to a vessel. This saves both time and money for the customer – without compromising cyber security.

Providing security services

ABB is a global company with long experience in security. ABB Marine and Cranes can access this experience through the wider company's resources worldwide. It can also offer direct service consultancy. The ABB Cyber Security Fingerprint identifies strengths and weaknesses for defending against a cyber attack within a vessel's control systems. It does this by gathering data from system configurations and key personnel and comparing this against best practices using ABB's proprietary analysis tool.

The resulting analysis provides detailed recommendations for reducing cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for control systems.
The ABB Cyber Security Fingerprint reduces security risks by exposing gaps that could endanger employees, assets and uptime. ABB's approach compares customer security policies and settings to industry standards to establish a benchmark and ensure customer control systems have multiple layers of protection.

Based on Security Fingerprint analysis, owner-operators can use ABB services to implement or improve the cyber security of a vessel or fleet. Some services available are:

- security policy for a vessel/fleet
- software patch update
- anti-virus update
- system hardening
- user management and network configuration

Cyber security threats are real and growing. However, with a coordinated approach between owner-operators of marine vessels and vendors like ABB, the risks to business and stakeholders can be minimized. Security needs to be addressed not only as a one-off activity but should also be an ongoing process during the life of vessels, automation products, and systems. A security policy for vessel operation and security solutions and support from vendors will help achieve these security goals.

Kai Hansen
Technology Manager, ABB Vessel Information and Control Center of Excellence, Norway
kai.hansen@no.abb.com

Akilur Rahman
Global head of Cross-BU Strategic Initiatives, ABB India
akilur.rahman@in.abb.com