DYNAMIC POSITIONING CONFERENCE
October 11-12, 2016

CYBERSECURITY SESSION

Who Said That DP Does Not Rhyme With Cybersecurity?

By Olivier Cadet & Arne Rinnan
Kongsberg Maritime

Abstract

The maritime industry is being transformed by the integration of the digital world with machinery, turning traditional assets into interconnected devices generating data. A lot of critical equipment on board vessels are "connected", including advanced control systems which most likely were not meant to be connected to the internet in the first place. There are a few documented cases (and most likely a lot of undocumented cases) of cyber-attacks over the past 5 years. So how do you protect these expensive and often strategic assets against malware and cyber threats, while maintaining their integrity and reliability? Taking the DP system as a case study, this paper first explores different types of cyber threats: from a position reference system being spoofed to a USB memory stick infecting a DP computer, we will review practical cases of cyber threats to the DP system, and review countermeasures and best practices when it comes to cybersecurity.

This paper is intended to be used as an introduction to cybersecurity and DP and aims at increasing awareness among the DP community of the importance of cybersecurity.

Contents

1. Introduction 2
2. Impact of digitalization on the maritime industry 3
3. DP (system of systems) and cyber threats 5
3.1. Main functions of a DP system 5
3.2. Built-in resilience of the DP system 6
3.3. Life-cycle of a DP system 8
3.4. Types of cyber threats for DP and their impact 9
4. Countermeasures 10
4.1. End-to-end approach to cybersecurity 10
4.2. Example 1: GNSS (Position Reference System) 12
5. Conclusion and a glimpse into the future 15
References 16
Appendix A – End-to-End Approach to Cybersecurity 17

List of Figures

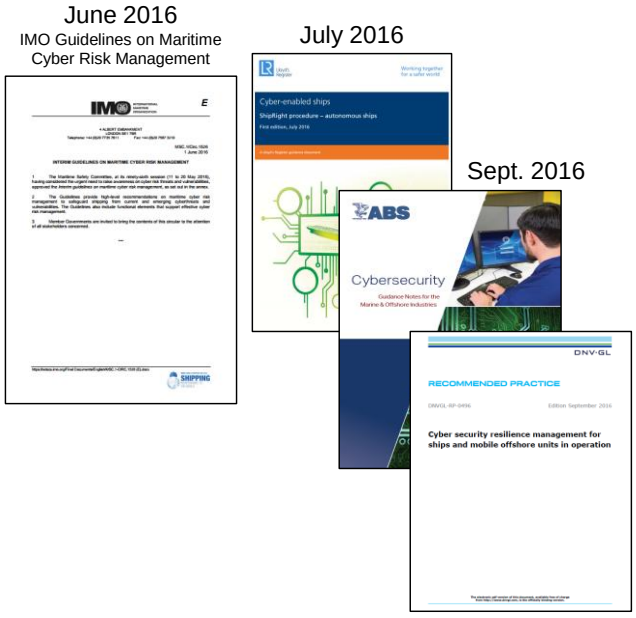
Figure 1 - Digitalization draws new industry boundaries 3
Figure 2 - Maritime VSATs in service 4
Figure 3 - New dynamic and real time links between land and sea in real time 4
Figure 4 - Simplified view of DP controls functions 5
Figure 5 - DP System as a "system of systems" 6
Figure 6 - Typical signal pre-processing included in a DP system 7
Figure 7 - DP lifecycle (high level) and associated cyber threats 8
Figure 8 - End-to-end approach to cybersecurity for DP 10
Figure 9 - One of these antennas could be a transmitter... 13
Figure 10 - GNSS jammer available on the Internet 14

1. Introduction

The traditional image of a vessel being an isolated asset with the ocean acting as a physical barrier is not applicable in today's connected world. This poses an interesting challenge in terms of cyber security.

Cyber threats are real in the maritime industry. As reported in the editorial issue of Drilling Contractor in September 2015[1], DP systems can be a target for cyber-attacks. A first case was officially reported by the USCG in summer 2015 where malware was mistakenly downloaded onto a Mobile Offshore Drilling Unit and impacted the DP system. It is likely that more cases go either un-noticed or un-reported.

The recent release over this summer of cyber risk management guidelines by IMO followed by cybersecurity guidelines and recommended practice by classification societies is also an indication that the maritime industry is increasing its level of awareness on cybersecurity. An overall low level of awareness coupled with a low level of knowledge sharing and training was in fact pointed out by a 2011 report by the European Network and Information Security Agency (ENISA) on the *Analysis of cyber security aspects in the maritime sector*. That analysis report stressed the importance of "stimulating dialogue and information exchange between key stakeholders", "raise awareness about the criticality of this subject" and "develop strategies and good practices defining security requirements for Information and Communication Technology in the maritime sector".



This paper is aimed at contributing to increase the awareness among the DP community and provide some elements of consideration to have more secure DP operations.

[1] ***Industry recognizing need for better cyber defences as hackers become more sophisticated and drilling equipment becomes more interconnected,*** by Linda Hsieh, Managing Editor, Drilling Contractor (Sept/Oct 2015). http://www.drillingcontractor.org/drilling-cybersecurity-36727

2. Impact of digitalization on the maritime industry

Digitalization is redefining industry boundaries in the maritime segments as identified in Figure 1. If you consider the DP system as a "product", over the years this product has had more intelligence built in and has become more connected to other systems. Links with Power Management for instance, or the addition of functions specific to marine operations have made the DP system "smarter". The next step in its evolution has been to make the DP system "connected", with the ability to remotely connect to Operator Stations and Controllers from shore for example. This connectivity enables more timely and effective support. The next phase that we anticipate is to consider this "smart" and "connected" DP system as an integral part of the vessel operation, directly connected to other critical systems on the vessel. For instance, on a drilling unit, we are seeing more and more links between the drilling operations and DP. Ultimately, the "smart", "connected" and "integrated" DP system will become a vital part of a bigger operation that the vessel gets involved with, including planning, reporting, maintaining and optimizing operations.

With this "smart", "connected" and "integrated" DP system, cybersecurity becomes essential, not only to protect the DP system itself, but in a broader perspective the entire operation of the vessel.

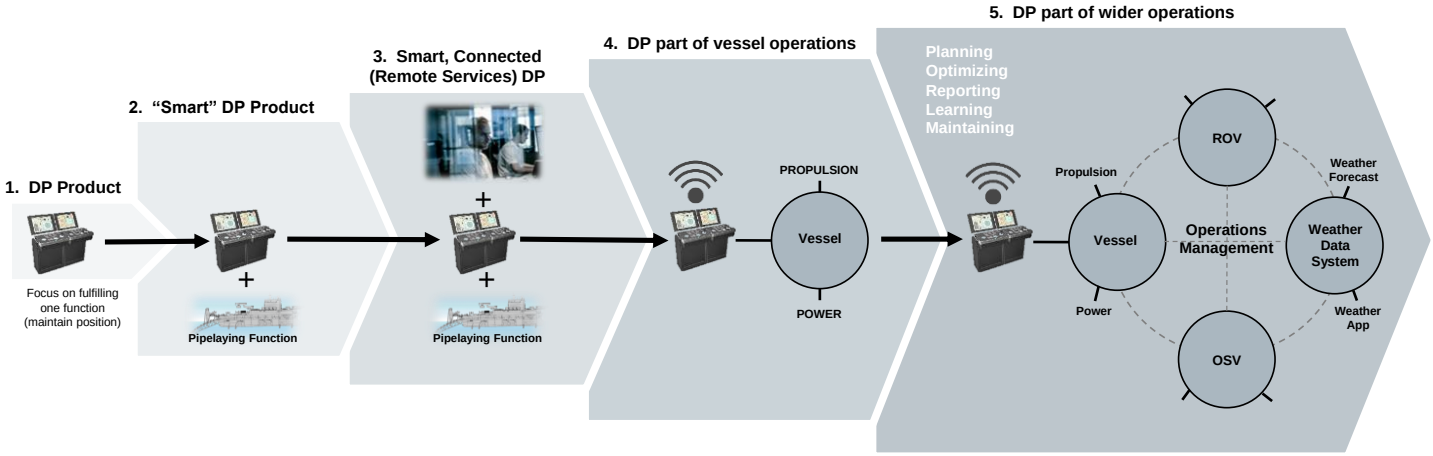


Figure 1 - Digitalization draws new industry boundaries (adapted from HBR article from Michael E. Porter and James E. Heppelmann "How Smart, Connected Products Are Transforming Competition", Nov. 2014)

The improvement of communication channels between offshore vessels and onshore support centers also introduces additional communication paths for cyber threats. In addition, digitalization introduces dynamic connections between land and sea in real time as illustrated in Figure 3. This is what Mr. *Oliver Fitton*, Dr. *Daniel Prince*, Dr. *Basil Germond* and Dr. *Mark Lacy* refer to as "*the extension of the Littoral*" in their paper on the Future of Maritime Cybersecurity (see References).

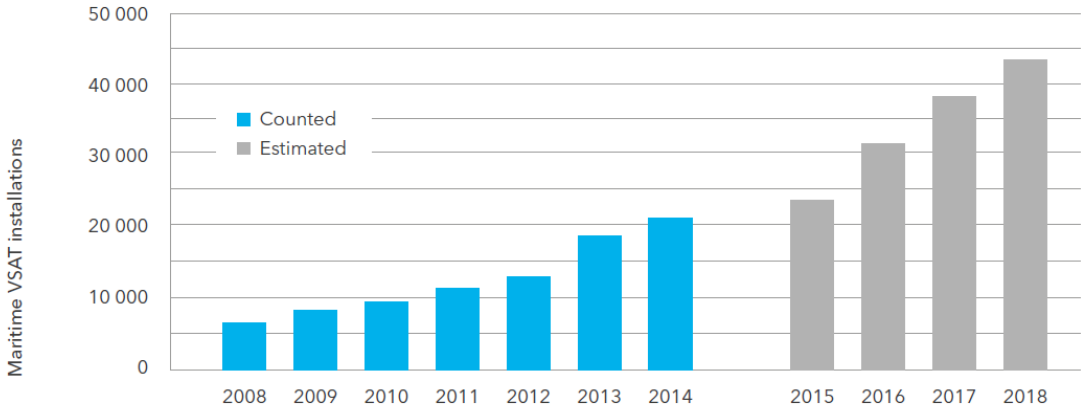


Figure 2 - Maritime VSATs in service (source: Ship Connectivity position paper by DNV GL with data from COMSYS)

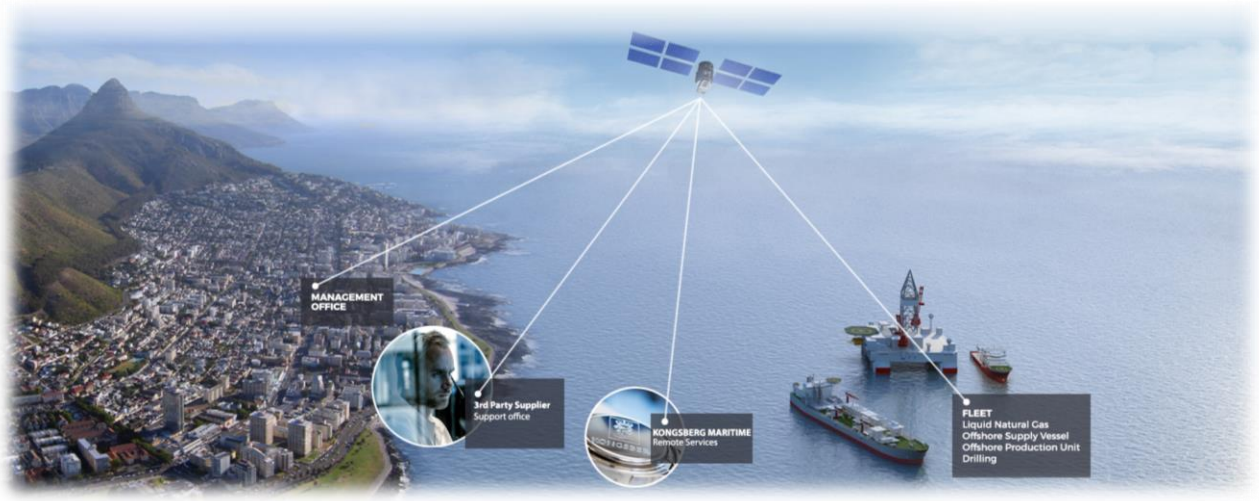


Figure 3 - New dynamic and real time links between land and sea in real time

3. DP (system of systems) and cyber threats

3.1. Main functions of a DP system

As indicated in figure 4, the main functions performed by a DP system consist of:

- Estimating the vessel position and heading
- Determining the position and heading errors between setpoints and estimates
- Determining the corrective action to be applied
- Calculating the command to the thrusters

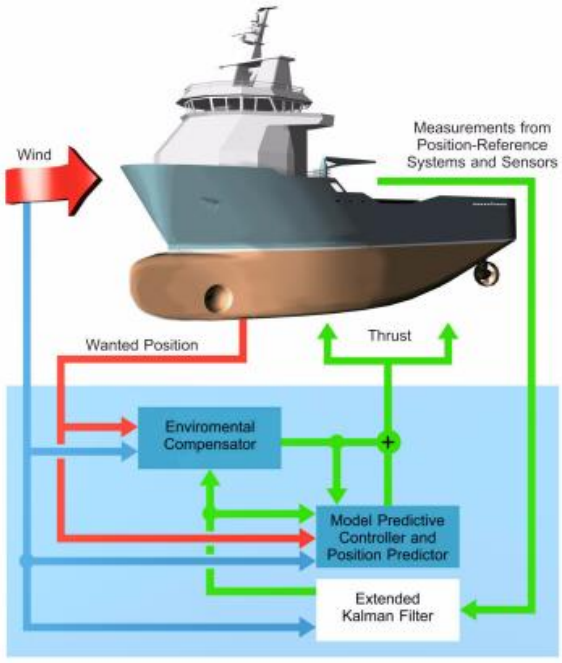


Figure 4 - Simplified view of DP controls functions

In addition to the control portion of the DP system, other important functions shall be included in order for the DP system to be usable. These functions include:

- Data Distribution (Networking)
- Human Machine Interface
- Alarms and reporting functions
- Data logging functions
- Other systems interface functions
- DP consequence analysis
- DP Process Management (error checking, calibration, maintenance, etc…)

As a result, the DP system is a highly interconnected system, with Position Reference Systems, Sensors, Power Management and other external systems. This is illustrated on Figure 5 as a "**system of systems**".

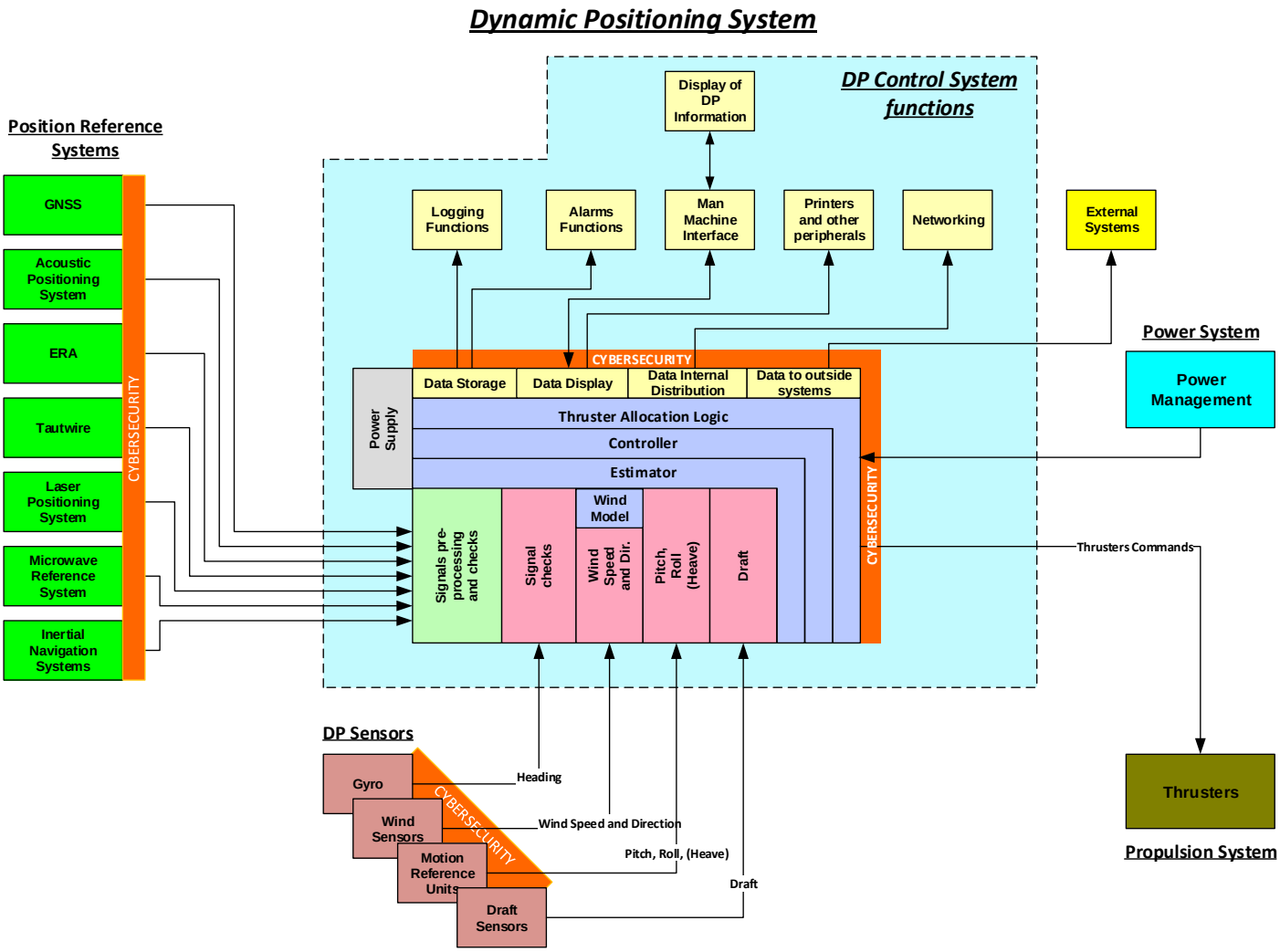


Figure 5 - DP System as a "system of systems"

3.2. Built-in resilience of the DP system

By design, the DP system has a level of built-in internal resilience, including resilience to the impact of cyber threats. Indeed, as identified by the Marine Technology Society[2], there are 7 key attributes of robust systems used for Dynamic Positioning operations that need to be considered from a design perspective. These attributes apply to all systems and sub-systems that make DP operations possible, from the power plant to the thrusters, and including the DP control system itself and the position reference systems and sensors:

- **Independence** – the main systems (thrusters, generators, etc…) should be as independent as possible.
- **Segregation** – the systems intended to provide redundancy should have as few common points connecting them as possible.

[2] DP Vessel Design Philosophy Guidelines, by the Marine Technology Society, Part 2

- **Autonomy** – each individual system or piece of machinery should be capable of making itself ready for DP operations independently of any centralized control system.
- **Fault tolerance**
- **Fault resistance**
- **Fault ride-through capability**
- **Differentiation**

As a result, by design, the DP system has a certain level of resilience against cyber threats. For instance a false position fix from a spoofed GNSS signal should be handled by the tests validating the Position Reference System measurement as identified in Figure 6. It is important to note that this pre-processing only offers a limited level of resilience. In any case, the consistency between several reference systems should also be checked, and the right cyber security measures should be implemented as identified in section 4.

In addition, system redundancy also contributes to increased resilience of the DP system against cyber threats. The level of redundancy built in also constitutes an internal defence mechanism to minimize the impact of a cyber attack. Redundancy does not reduce the risk of a cyber attack, but it reduces its potential impact.

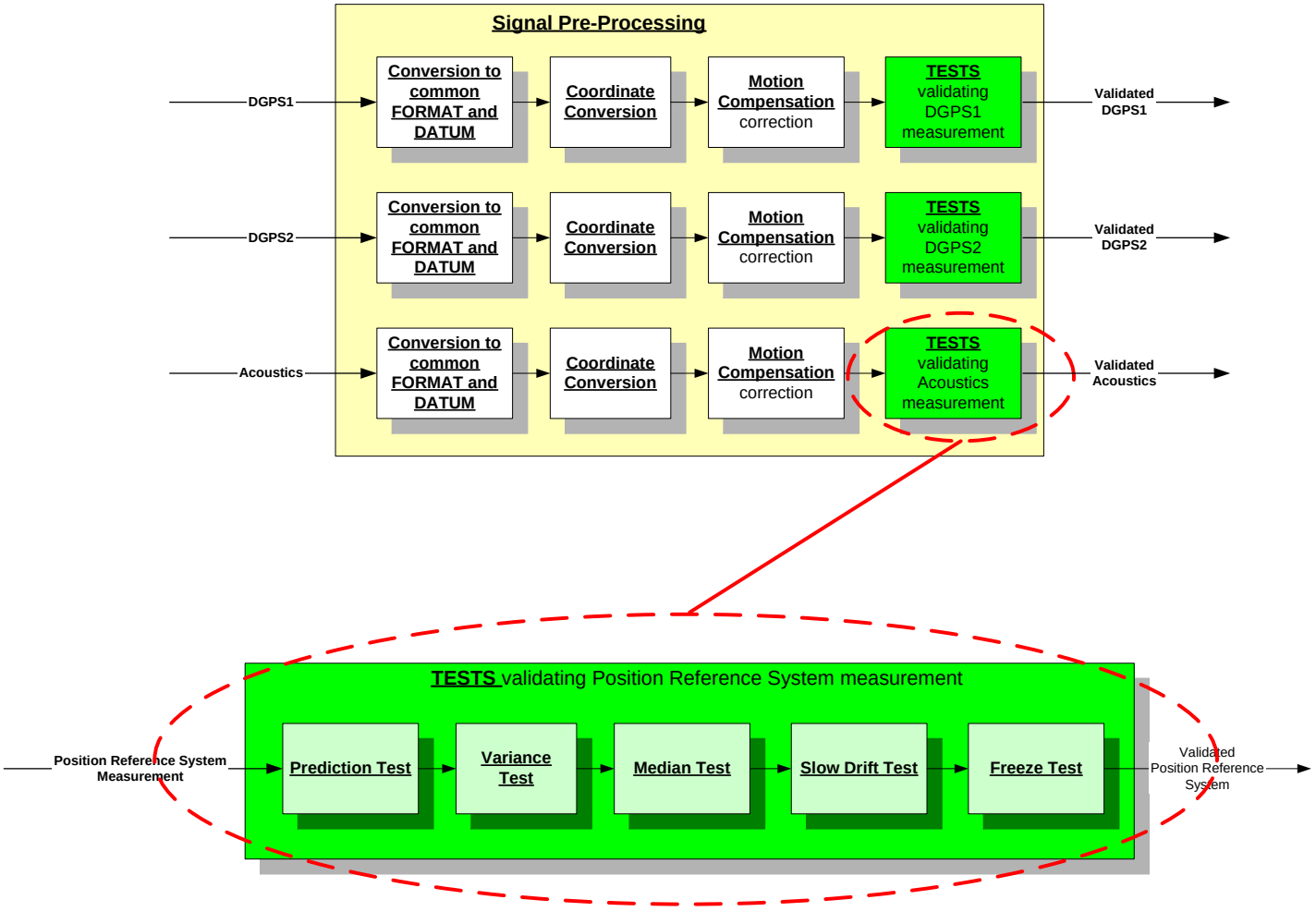


Figure 6 - Typical signal pre-processing included in a DP system

3.3. Life-cycle of a DP system

When looking at cyber security for DP, we need to consider the complete lifecycle of the system. Indeed different phases of the life-cycle introduce different risk levels for cybersecurity as identified in Figure 7.

- **Development/Production** – this is typically the phase when the DP "system" is assembled and software configured. The DP system typically stays under the full control of the vendor at that stage, with the responsibility to enforce the proper cyber security measures, including access control, antivirus, etc. Because the DP system is not in operations yet, the impact is fairly low at that stage. Having said that, it is possible at that stage to have a Trojan or sleeping software function that will wake up at a later point in time and cause problems. It is therefore critical that proper cyber security guidelines are followed throughout this stage, including thorough testing.
- **Commissioning** – from experience, this is the phase with the highest level of risk when it comes to cyber security. The impact can be quite substantial as well during that critical phase of a project. Because of the high access rate to computers with removable media (for example USB memory sticks) and difficulty to restrict access during commissioning, the likelihood of a cyber incident increases. Security measures might have been partially implemented as well at that stage, exposing vulnerabilities. It is critical to have the right level of monitoring and testing on a regular basis at that stage.
- **Operations** – this phase also includes maintenance of the system as well as upgrades and refit. A comprehensive cyber security strategy needs to be implemented at that stage of the life cycle of the product, with a complete end-to-end approach as identified in section 4.1. This is especially critical if remote support is enabled. Other aspects that are critical include awareness, training and regular assessments of cyber threats.

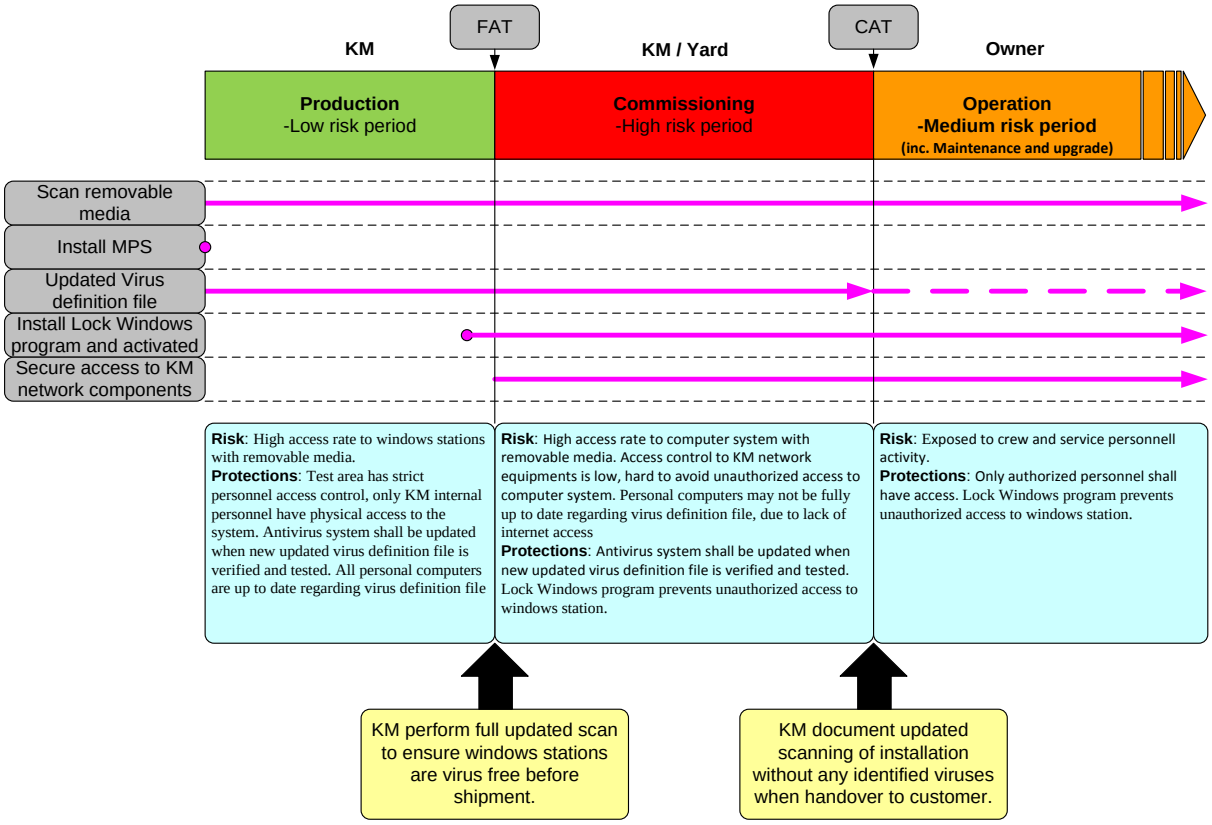


Figure 7 - DP lifecycle (high level) and associated cyber threats

3.4. Types of cyber threats for DP and their impact

Cybersecurity is defined as "*protection from theft or damage to the hardware, software and to the information generated, as well as from disruption or misdirection of the services they provide*"[3].

The types of attacks that could affect a DP system include (but are not limited to):

- **Denial of Service** – refers to attacks that make a specific component (part of the DP system) or a network resource unavailable to its intended users. This component could be an Operator Station, a controller or a position reference system for example.
- **Direct access attacks** – refers to attacks where the hacker has direct access to a computer (Operator Station for instance, or DP Controller) and is able to make changes or download data.
- **Spoofing** – refers to falsification of data, such as a wrong position fix from a Position Reference System into DP for example.
- **Backdoors** – a backdoor is a method of bypassing normal authentication, leading for example to un-authorized remote access to DP Operator Stations for example.

The image of a cybercriminal hacking into a DP system remotely and taking over control through a direct access attack is a possibility. But without going to that extreme, we see that we can often be our own worst enemy. Poor software design for instance could cause Denial of Service. This is not uncommon to observe during a DP software development phase. Denial of Service on a network component could be as problematic as on an individual component part of the DP system. Network storms of different kinds could lead to Denial of Service as well. This has been observed a dozen of times over the last 10 years and has led to changes in the way software is quality checked and tested and in the way controllers are load tested for example.

[3] https://en.wikipedia.org/wiki/Computer_security

4. Countermeasures

4.1. End-to-end approach to cybersecurity

It is critical to implement a complete end-to-end strategy to cybersecurity around DP. And to consider the complete life-cycle of the DP system, from planning to development to installation & commissioning, to operations and support, to refit and finally to obsolescence.

This end-to-end approach is not only on the network, not only on physical IT systems part of the DP system, but all the way from physical protection to software implementation, including in the way our control systems are designed today, taking security into account. This is a significant change from the way control systems were designed in the past. It is also important to note that the traditional and simple IT approach of running an anti-virus and disinfecting the system by removing malware detected will not work on a mission-critical industrial control system such as DP (for example, just removing an infected file could cause the control system to crash).

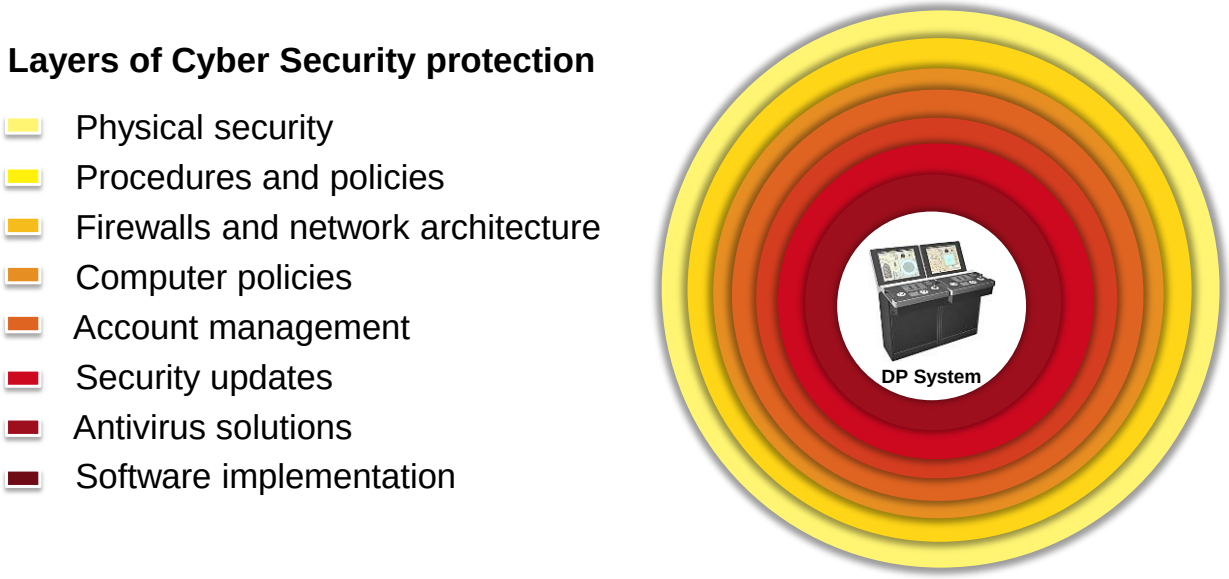


Figure 8 - End-to-end approach to cybersecurity for DP

Physical Security – The primary source of malware on a vessel remains the use of removable media such as USB Memory Sticks. A widely reported case in 2010 involved a new build offshore drilling vessel that was infected with malware during construction. Multiple computers were affected, including the BOP control system. The rig was shut down for 19 days[4].

Physical security also deals with physical protection of critical hardware, including blocking of un-used physical ports or USB locks. In case Remote Access is enabled, it is important to ensure full control (through security access for example) of the location used to conduct remote support or remote operations.

[4] http://www.drillingcontractor.org/drilling-cybersecurity-36727

Procedures and policies – We will use Remote Support as an example of the importance of having the right procedures and policies in place. To ensure safe and secure remote connection to the DP system for example, the following good practice can be used:

- All remote operations are initiated from the **vessel operator**
- **Remote Safe Job Analysis** has to be conducted before remote operation
- Remote operations can only be performed by **trained personnel**
- All remote operations **journaled** in remote software
- Critical operations done **onsite**, not remote

Firewalls and network architecture – As outlined in the Guidelines on Cyber Security onboard Ships by BIMCO (see References), a secure network has many different aspects, from topology to hardware and software technologies, authentication and authorization system to name a few. It is critical to ensure that networks that are critical to the ship's operations are controlled. That includes for instance the "process network" that links the DP system with the Automation, Navigation and other critical bridge or vessel management systems. Separate zones onboard the vessel need to be defined in order to segregate the control system network (secure zone). Malware protection should be implemented and should scan traffic going in and out of the different zones.

Computer policies – Computer policies refer to the type of hardware and software used in DP systems in general. It is critical to have full control of the software running on each computer for example (with certificates) and to disable anything that is not used. A clear policy with regards to automatic update has to be enforced as well. Hardening and lockdown of image for servers can be performed.

Antivirus solutions and software implementation – As opposed to non-critical computers that can be re-started on demand to implement anti-virus patches, the DP control system cannot be taken offline on demand without careful planning. Any new software update needs to be carefully tested before being implemented, and that includes cyber security testing. Hardware In the Loop (HIL) testing throughout the life of a DP system is one way of ensuring a more robust implementation onboard.

4.2. Example 1: GNSS (Position Reference System)

4.2.1. Reference systems and cyber threats

Taking care of cyber security is about building barriers at several levels. There is no single solution to a good protection strategy. Even if the DP provides some cyber security protection means, it is important to implement a protection strategy on individual reference system level. The main categories of vulnerability for reference systems are:

- Denial of Service
  - Signal interference
  - Signal jamming
  - System intervention
- Spoofing
  - Fake signals
  - System intervention

All reference systems based on observations of a signal propagating through air or water can experience signal interference. Even if this interference is un-intentional, the effect on the reference system can be Denial of Service. Hostile and intentional interference is described as jamming. It is in principle possible to jam all kinds of electromagnetic or hydro acoustic signals (however, some of them are quite difficult to jam efficiently). Denial of Service can also be done by intervention into the system. All known reference systems are built on at least a minimum of software or firmware, and it is in principle possible to intervene with this software or firmware. This is even possible for Inertial Navigation Systems, not relying on propagation of electromagnetic or hydro acoustic signals.

Signal spoofing usually is much more difficult and takes more resources that Denial of Service. On the other side, the effect can be much more severe. Fake signal can fool the reference system to report false positions to the DP and consequently cause a drive-off. It should be noted that spoofing also could be achieved by manipulating the software or firmware in the reference system.

The bottom line is that there is no reference system with guaranteed protection against cyber threats. Independence and segregation are still good principles in a protection strategy.

4.2.2. Cyber threats to GNSS

The first real GNSS, GPS, was designed to give military users protection from cyber threats already from the beginning. Authorized users were given access to an encrypted signal and the basic infrastructure were under US governmental control.

Un-authorised users do still not have access to the encrypted signals, but have over the years developed several protection barriers:

- RAIM (Receiver Autonomous Integrity Monitoring) is used to detect and remove measurement outliers
- Data from several global constellation (GPS, GLONASS, Beidou and Galileo) is adding diversity and segregation
- Data from several frequencies is also adding diversity since every of the four constellations supports at least two different frequencies also for un-authorised users

- GNSS data can be integrated with inertial data to reduce the risk of Denial of Service and spoofing
- An advanced reference system will usually process several positions and use statistical tests to identify and remove erroneous data sets

4.2.3. GNSS interference

The GNSS signals is usually very weak and susceptible to interference and interference is usually un-intentional. Some common sources of interference are:

- Radars or communication equipment
- Faulty GNSS antennas transmitting because the built-in LNA (Low Noise Amplifier) is oscillation and making interference with other GNSS antennas in the vicinity

A good antenna is important to protect against interference. When using multiple GNSS installations, it is a good idea to separate the antennas with at least 30m if possible. Algorithms monitoring the signal levels can also give an indication of interference problems.

Figure 9 - One of these antennas could be a transmitter...

4.2.4. GNSS jamming

Jamming of GNSS can be done by transmitting a more or less complex signal to block the reception of the satellite signal by the user antenna. Since GNSS was implemented as the basis of road tolling systems, GNSS jammers have become easily available for anyone. A rather advanced jammer can be bought on the Internet for just a few dollars, even if use of jammers is strictly prohibited and potentially very dangerous.

Dependent on the resources available it is possible to jam GNSS signals over quite large distances (e.g. from an aircraft or an UAV).

Figure 10 - GNSS jammer available on the Internet

4.2.5. GNSS spoofing

GNSS spoofing is done by transmitting fake GNSS signals to fool the reference system to calculate a faulty position. Spoofing requires high skills and large resources to be a significant threat to a DP operation. The spoofer needs to be located closely to the GNSS antenna to be effective.
Several protections can be implemented to prevent spoofing even for a un-authorised GNSS user, like:

- RAIM algorithms to check inconsistencies between GNSS observations
- Integration with inertial navigation systems to check inconsistencies between GNSS and inertial observations
- Using dual antennas can be effective and make spoofing much more difficult
- Authentication methods can be implemented to verify the validity of GNSS data
- Using CRPA (Controlled Radiated Pattern Antennas) will reduce the risk of both jamming and spoofing

4.2.6. Conclusion

The most frequently reported anomaly to GNSS based reference systems is caused by un-intended interference. The authors of the paper know no examples of spoofing, so far and the risk should neither be exaggerated nor ignored. It is in any case important to include reference systems in a consistent DP cyber security strategy.

5. Conclusion and a glimpse into the future

As a connected and smart "system of systems", the DP system constitutes a critical component to be taken into account in the development of a cybersecurity strategy for marine operations. The complete life-cycle of the DP system has to be considered, from design to end of life, taking special attention to the commissioning and operations phases of the system. As presented in this paper, a complete end-to-end approach maximizes protection against cyber threats.

In the field of cyber security, technology is only one component of the solution. As identified in BIMCO's *Guidelines on Cyber Security onboard Ships*, cyber security awareness includes identifying threats and vulnerabilities, assessing risk exposure, developing protection and detection measures, establishing contingency plans and responding to incidents. The level of training of operators needs to be augmented with cyber-attacks scenarios, including detection of cyber incidents and response to these incidents. A more transparent and efficient reporting of cyber incidents in the DP community needs to be established as well, in order to share lessons learned and better protect our industry as a whole against cyber threats.

In an article of the Harvard Business Review (Nov. 2014 issue), MIT Media Lab's Alex Pentland argued that "With Big Data Comes Big Responsibility". This title applies to cyber security as well: as the maritime industry accelerates its Big Data revolution with more connected objects and more connected vessels, the responsibility to ensure cyber security is greater. All actors need to work together and collaborate more efficiently to improve the security of all this information generated.

References

Technical standards (non exhaustive list)

- **ISA/IEC 62433** – series of standards on the cyber security of industrial automation and control system
- **IEC 62351** – Information security for power system control operations
- **IEC 61162-450** and **460** – Digital interfaces for navigational equipment within a ship
- **IEEE 1686** – standard for intelligent electronic devices cyber security capabilities
- **ISO/IEC 27001:2013** – Information technology, security techniques, information security management systems, requirements

Guidelines (non exhaustive list)

- **Lloyd's Register guidance on cyber-enabled ships**
- **ABS cybersecurity guidance notes for the marine & offshore industries**
- **DNV GL Recommended Practice (RP-0496) Cybersecurity resilience management for ships and mobile offshore drilling units in operation**
- **US Coast Guard Cyber Strategy**, June 2015
- **Framework for Improving Critical Infrastructure Cybersecurity**, NIST, version 1.0, 2014
- **The Guidelines on Cybersecurity onboard Ships**, BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO, version 1.1, February 2016.

Other references

- **Ship Connectivity,** Position Paper by DNV GL, April 2015
- **The Future of Maritime Cyber Security**, by Mr. Oliver Fitton, Dr. Daniel Prince, Dr. Basil Germond and Dr. Mark Lacy, Lancaster University.
- **Analysis of cybersecurity aspects in the maritime sector**, European Network and Information Security Agency (ENISA), November 2011
- **The Internet of Everything**, Harvard Business Review, November 2014
- **The Industrial Cybersecurity Problem**, ISA White Paper by Eric Byres, PE

Appendix A – End-to-End Approach to Cybersecurity

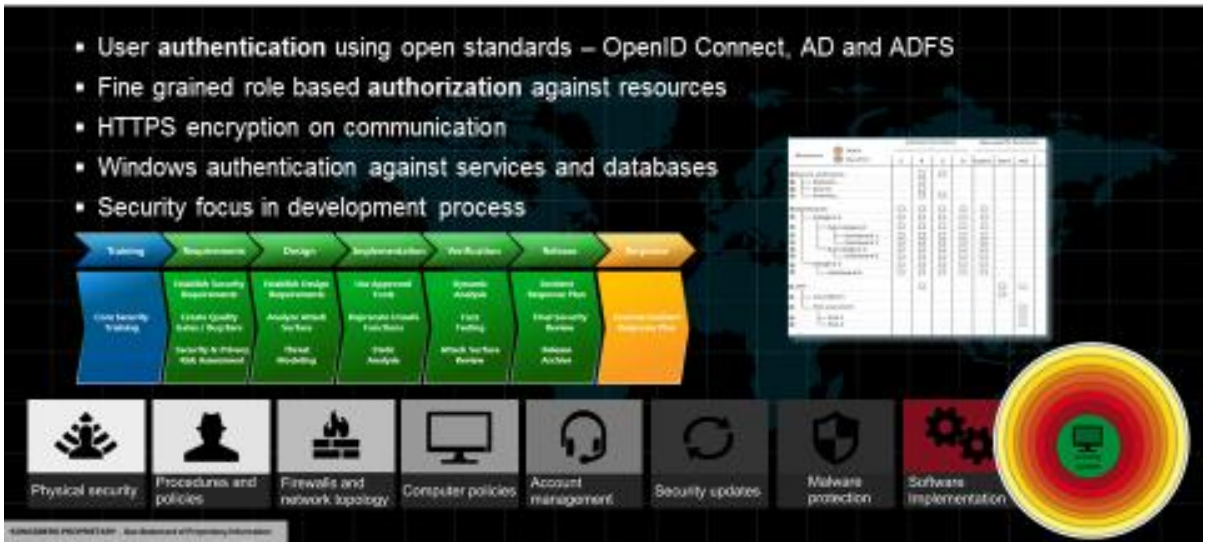
Cyber Security – Procedures and policies

Cyber Security – Firewalls and network

Cyber Security – Computer policies

Cyber Security – Account management

Cyber Security – Security updates

Cyber Security – Malware protection

Cyber Security – Software implementation