PLC hacking on sea vessels

D. Billard

University of Applied Sciences in Geneva – HES-SO, Switzerland
David.Billard@hesge.ch

Abstract. This paper presents a case of alleged PLC (Programmable Logic controller) hacking aboard a commercial ship, and the forensic investigation of PLC components. It presents the lessons drawn from this case and the particular difficulty of investigating PLC and SCADA systems onboard. Whereas hacking is often seen as taking control of a ship, or part of a ship, it is also related to the alteration of the sensors, the PLCs, the data logger or the SCADA systems. This alteration can be done from a hacking group but in the investigated case, it is more likely an action triggered either by the ship owner, or the ship manufacturer himself. This paper also advocates for an addition of a section concerning cybersecurity in the SOLAS - Safety Of Life At Sea - convention or one of other IMO (International Maritime Organization) conventions.

1. Introduction

The maritime environment has dramatically changed over the last decades. In particular, the Global Maritime Distress and Safety System (GMDSS) has been included in the Safety of Life at Sea Convention [1] (SOLAS) and uses advanced technologies ranging from Digital Selective Calling (DSC) or Cospas-Sarsat satellite-based system. It is worthwhile to note that even recreational vessels are more and more adopters of these new technologies.

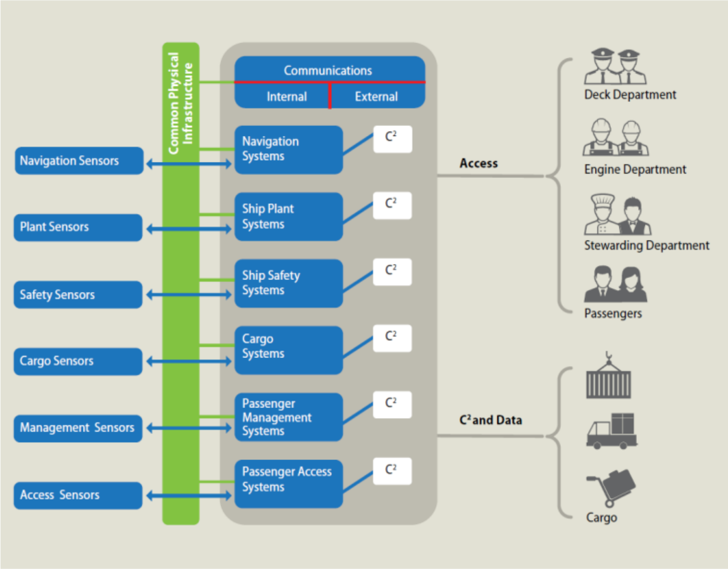
But a most notable evolution of ships is their information system, that regulates almost every aspect of life at sea, or in port. It is very common to have PLC (Programmable Logic controller) systems for automation control and/or navigation, SCADA (Supervisory Control And Data Acquisition) systems for supervision and classical computers for management (passenger or cargo management for instance). As all other automated systems, information systems aboard ships do not evade the cybersecurity risk which is now included in every risk assessment of any company.

The information system in a vessel is often sub-divided [2] in information technology (IT), operational technology (OT) and communications systems (CS). IT is mainly responsible for providing high level information and leverage for the management of the ship and her businesses (passengers, cargo, crew, etc.). IT is very similar in vessels and in traditional companies, excepted that it can be more often disconnected from a data network while at sea, and far from the suppliers. IT uses data from different sources (passenger records for instance) and also from OT. OT is connected to the physical world by the way of sensors and has the capacity to interact with it in many ways. In vessels, one think quite immediately to the navigation system that takes input from GPS location, wind speed and direction, water flows, but also fuel tank capacity, engines power and so on. IT and OT communicate through networks (specialized as Profibus or more versatile as Ethernet) or through the manual plugging of removable media.

The reader can find a brief descriptive summary of IT, OT and CS systems in **Figure 1**, taken from [2]. Although it was originally intended to show an overview of ship assets that can be affected by cyber security, it can help the reader for a better understanding. PLC systems are on the left side of the figure, but one can notice that PLCs are not just only sensors, since they can interact with their environment (closing valves, switching circuits, etc.).

Many researches [3] [4] [5] [6] [7] [8] [9] have studied information systems aboard ships from the angle of cybersecurity, but most of them apply on-land cybersecurity practice to ships whereas vessels have some distinguished features, as we will see further in this work. None of these researches has a section dealing with digital forensics at the notable exception of [10] concerning the investigation of the Costa Concordia shipwreck. Digital forensics is however a cornerstone of a cybersecurity policy since it captures evidences in the view of trial in front of a court of law, or at least to find responsibilities.

Figure 1. Ship assets affected by cyber security



The major difference that separates IT/OT of a ship than from a company is of course that a ship can take the sea and be completely autonomous for its operations. Once a ship is at sea, she can be considered as an autonomous complex system with limited networking capacities. When a ship is in port, then the ISPS Code [11] applies for the ship herself and port operations.

This paper presents lessons learned while investigating an alleged PLC hacking aboard of a ship and is structured as follows: section 2 describes the case that was the starting point of the investigation, section 3 presents the investigation and some of its difficulties, section 4 draws some lessons learned and ways to mitigate risk associated when investigating IT and OT aboard ships and section 5 provides some recommendations at a broader level.

2. The case

In 2007, several ships of the same category have been delivered by manufacturer X to company Y. Company X is a renowned ship builder and manufactures mainly work vessels like dredgers, split barges, drill barges or self-elevating platforms. Company Y has a large fleet of ships and operates worldwide.

The manufactured ships rely heavily on automation for operation, for instance cranes or propellers, and several operator cabins may be in service, accessing the same equipment. The OT infrastructure is therefore quite complex.

When a ship is deployed to its working zone, the drilling, dredging, cranes and other equipment are powered up. For the OT infrastructure, it means that at this time, the PLC programs are activated as well as the operator consoles. This activation requires a booting process through different removable media.

Each ship has two PLCs, one in the bridge, and the other in the engine room. The two PLCs can be accessed indifferently via a socket in the bridge panel, or the engine room panel since the two PLCs are serviced by the same network. Each PLC controls different equipment, but the operating consoles can manage indifferently equipment linked to one or another PLC. Before activation, the PLC programs are stored in two MMC cards of 256MB. During the activation, the programs are transferred to the PLCs themselves. The access to the PLC programs is password-protected and only company X knows the password.

Each ship has two operating consoles, one in the bridge and the other at the top of a movable crane. The programs for managing these consoles are stored in two SD card of 1GB. There is no password protection for the consoles and the consoles have identical software (and screens).

During operation, all the data (measures, movements, actions) are stored in a data logger. This data logger is a Windows PC, equipped with a MSSQL database. The PC is password protected. It can be accessed from outside via a dedicated access point configured with a SIM card providing data transport. This access point needs to be powered on manually by a crew member.

During their two first years of exploitation, the ships encountered different malfunctions with some equipment. For instance, company Y claimed that the operation time for some hardware was below the expected ratio or that hydraulic leakages occurred or that the navigation was hazardous during operation.

The company Y then complained that the ships were delivered with faulty functionalities and entered in litigation with company X in 2009. Although the litigation focused mainly on faulty equipment, in 2016 the event of a PLC software malicious modification was first mentioned. First, it was brought to the attention of the court by company Y accusing company X of using its direct link (via the access point) to the system (PLC and datalogger) to make unwanted modifications and thus altering the normal behavior of equipment. Then the same accusation was made by company X who claimed that company Y changed some original equipment and modified the PLC software in order to service the new equipment. Company X claimed that this modification of software led to an alteration of the normal processing of data and hence to unexpected behavior of the ships. Also, company X accused company Y of intellectual property infringement by stealing the knowhow stored inside the PLC programs.

The two companies agreed to appoint experts in order to investigate the PLCs' programs and the data loggers. The purpose of the investigation was to determine if the PLC software has been tampered with, and if the data logger has registered abnormal behavior. The court, an arbitration tribunal, ordered the investigation.

Due to multiple unexpected and surprising developments in this case, of all the three concerned ships, only one was still available for investigation. All the data loggers and PLCs aboard the other ships have been decommissioned and destroyed.

The analyze of the data logger was possible without going directly onboard of the ship, since the data logger of this ship, a simple PC running Windows, has been sent for repair in Europe and the disk drive has been copied and made available to the experts. The investigation of this disk was done using traditional forensics procedures.

Concerning the investigation of the PLCs, it proves to be more complex and is the subject of the next section of this paper. On the first place, the investigation was to take place aboard the ship since it was currently servicing the equipment of the ship. Secondly, since the ship was in operation, the investigation should not disturb her work beyond an agreed period of time. And of course, the ship should resume her operation after the investigation.

3. Investigation of the PLCs

This investigation was decomposed into three parts: (1) testing the equipment with the current PLC, (2) extracting the programs from the PLCs and (3) comparing the extracted program with the official program shipped with the vessel.

The two first parts were to be realized aboard the ship, whereas the last part was realized in the expert lab. Of course, company X and company Y were present aboard the ship and scrutinized every action of the expert. During the visit aboard the ship, the expert also examined the SIM-card access point but could not determine the dates when it was used since no log was kept.

3.1. Testing the equipment

This step was important. It was vital to reveal if the equipment is operating properly with the PLC currently being used on the ship. As a matter of fact, the ship owner could have reinstalled the original PLC programs just for the time of the investigation, and then reverted back to modified PLC programs after the expert departure. By testing the equipment with the current PLC programs, and then extracting the PLC software from the PLC itself, the expert has the guarantee that the extracted PLC program was in use and the equipment was performing accordingly.

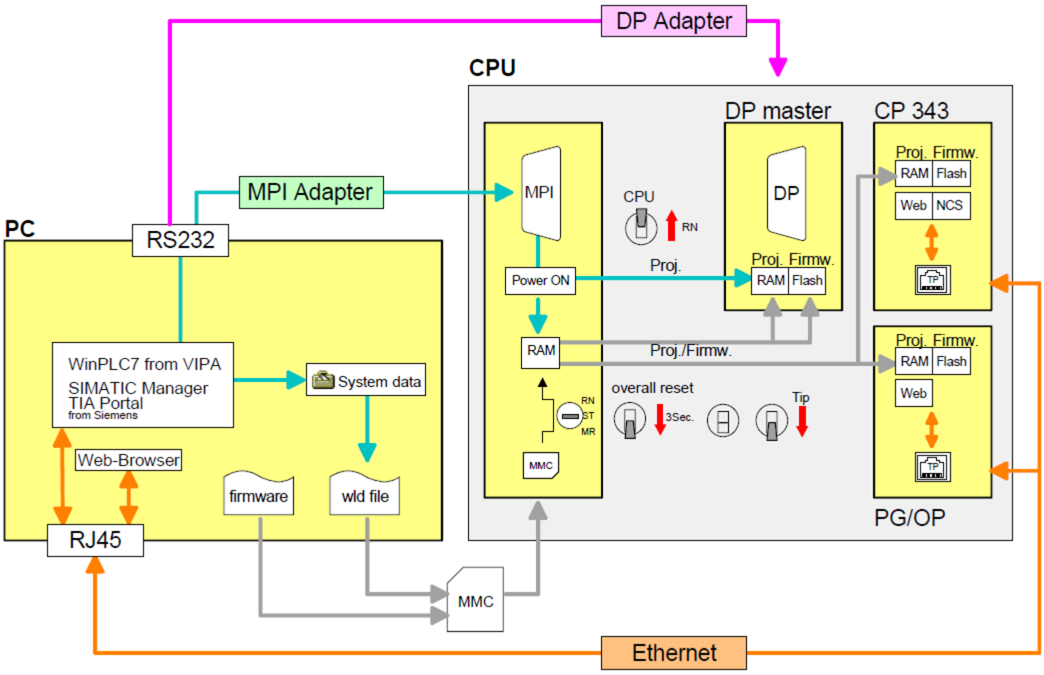
The expert asked a machine operator to use the crane and some other equipment from the bridge and from the movable crane. Once the tests have shown that the equipment was successfully operated, the operating consoles were shut down in order to proceed with the PLC programs extraction.

3.2. Extracting the programs

As already mentioned, the ship has two PLCs: one in the bridge, and the other in the engine room. These PLCs are based on the System 300S SPEED7 from VIPA. They are programmed using the Siemens STEP©7 framework which supports different language: Ladder Logic, FBD (Function Block Diagram), STL (Statement List), S7- Graph and SCL (Structured Control Language).

A schematic of the PLC architecture, taken from [12], is presented in **Figure 2**.

Figure 2. Standard VIPA System 300S SPEED7 architecture



The PC part of this architecture (block on the left) is used to program or monitor the CPU part (the actual PLC). The firmware and the user's project files are transferred from the PC to the CPU via a MMC (Multimedia Memory Card). The PLC cannot operate without the MMC, although when the system is running all the firmware and project files are loaded into the different CPU memories and the MMC is no more accessed. The native communication protocol is PROFIBUS, but Ethernet is also supported as well as direct access via RS232 and patch cable (through RJ45 socket).

The first step of the extraction was to forensically image the MMC cards. This was done quite easily using FTK imager from Access Data and dedicated hardware.

The second step was to extract the program from the PLCs memory itself. This was done using Siemens Simatic Step 7, after company X introduced secretly the PLC password to log in the PLC. The extraction of the two programs was possible from the bridge PLC, since the engine room PLC was connected to the bridge PLC.

The third step was to extract the software from the operating consoles. The consoles software is stored on a SD (Secure Digital) card. The first SD card was forensically imaged using FTK imager from Access Data and dedicated hardware. Unfortunately, during the forensic imaging of the SD card, multiple errors were found on the device. These errors have not been detected prior to the investigation. As a matter of fact, at that time, the expert learnt from the crew that the operating consoles were powered on at the beginning of operations and were left powered on during the several months or years of operation. The program on the SD card was loaded into the console RAM once at the beginning, and then stayed in the RAM until the end. The SD card, although of an industrial grade, underwent harsh conditions and suffered.

The problem with the SD card was not the copy itself, but the fact that it was not possible to power on the console again. And the expert learnt that no spare SD card, with the console software, was available on board. No MMC backup either was stored on the ship.

Fortunately, the SD card in the movable crane console was error prone, forensically imaged correctly and the expert was able to restore this image on a new SD card that he brought with him. Both operating consoles were then powered on and the ship could resume her operation. The reader can be assured that the expert was relieved for this outcome.

3.3. Comparing the PLC programs

The whole PLC programs comparison is not part of the scope of this paper, but a small part of it is relevant. The PLC programs were updated regularly the two first years of the ship operations. However, the programs did not have a release version, nor a release date. The programs were modified by the manufacturer to correct bugs but no versioning was done. And the programs were common to several ships. It was then very complicated to determine which version of the program was last installed on this particular ship, and also if a version of this program was kept unchanged at the constructor's premise.

Moreover, it happened that company X went bankrupt after the investigation, and its software is no more available.

4. Lessons learned

The investigation aboard a ship is different from traditional forensic investigation in many ways.

First, each ship is very different from another, and the knowledge of the information system is not shared among the crew. This is also true with companies, but crew turnover on vessels is, from the expert experience, much higher than on land, and knowledge is diluting rapidly.

Second, when a ship is at sea, the expert cannot rely on close by suppliers in case of necessity. Moreover, the access to a data network at sea can be damageable in two aspects: (1) it opens a channel for unwanted actions, for example an accomplice could wipe a device using the established link, or simply a remote operator can make an error and (2) transmission can override more important messages related to the ship safety.

Of course, new provisions in recommendations [3] and guidelines [13] stress the need of trained staff, and protection of IT/OT systems. But OT systems are still quite ignored, or their operational modes are less known, by cybersecurity professionals.

For vessels running PLCs, it is of upmost importance to have backup copies of all removable media that are crucial for ship operation. Even with industry grade mass storage, the conditions (weather, temperature in the engine room, accident, error from the crew) at sea can severely damage the device. These backup copies also need to have indication of the software versions they hold. Moreover, in case of software supplier disappear, there is no guarantee to find another copy of the software.

A log register of all the software updates made on the PLCs or other equipment is also mandatory. It the present case, it was a matter of intellectual property, but it can be crucial to track down errors in the ship operation or simply the introduction of a malware.

Then, but it is common practice in IT security, inward communications to the information system should be logged, as well as accesses.

5. Conclusion and recommendations

In this paper, we described the digital forensic investigation of PLCs aboard a ship. PLCs are part of the OT (operational technology) system and communicate with the IT (information technology) through the CS (communications systems).

The case is an alleged PLC hacking and concerns the ship manufacturer and the ship owner. The OT forensic investigation is detailed and shows that it is extremely important to:

- Define a procedure that ensure that the PLC program that is extracted for further analysis is precisely the PLC program servicing the ship equipment. This is done by testing the equipment prior of the PLC program extraction.
- Prepare for a failure of PLC parts, in that case the SD card holding the operating console program.
- Prepare for lack of documentation about the ship IT/OT infrastructure due to lack of knowledge from the crew.
- Prepare for lack of support (forensic software or hardware suppliers) when at sea.

From the lessons learned, this paper recommends that an addition to the SOLAS - Safety Of Life At Sea - convention or one of other IMO (International Maritime Organization) conventions should be made. In this addition, it should be explicitly stated that all removable media that are crucial for OT ship operation should have a backup, in the same removable media format, aboard the ship and that a log of all the software versions should be kept onboard. As a matter of fact, some OT systems can be crucial for the preservation of life at sea and should be able to operate at any time.

These simple recommendations are of course supplementary to the traditional cybersecurity guidelines and codes of practice.

References

[1] "International Convention for the Safety of Life at Sea (SOLAS), 1974." [Online]. Available: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx. [Accessed: 15-Mar-2019].

[2] Hugh Boyes, *Code of Practice Cyber Security for Ships*. 2017.

[3] IMO - Maritime Safety Committee, "Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3," 05-Jul-2017.

[4] Norman Dahl, NightWatch Industries, "PLCs in Marine Monitoring," 2010.

[5] DNV GL, "Cyber security resilience management for ships and mobile offshore units in operation, DNVGL-RP-0496," Sep-2016.

[6] Siraj A. Shaikh, "Future of the Sea: Cyber Security," Aug-2017.

[7] Niko Pajunen, "Overview of Maritime Cybersecurity," Bachelor's Thesis, South-Eastern Finland University of Applied Sciences, 2017.

[8] Sotiria Lagouvardou, "Maritime Cyber Security: concepts, problems and models," Master Thesis, Department of Management Engineering, Technical University of Denmark, 2018.

[9] Bénédicte Pilliet, "La cybersécurité dans le milieu maritime : un impératif stratégique," *cybercercle.com*, vol. 1, no. 1, Oct-2018.

[10] M. Piccinelli and P. Gubian, "Modern ships Voyage Data Recorders: A forensics perspective on the Costa Concordia shipwreck," *Digit. Investig.*, vol. 10, pp. S41–S49, Aug. 2013.

[11] "SOLAS XI-2 ISPS Code." [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx. [Accessed: 15-Mar-2019].

[12] VIPA, "SPEED7 - CPU, 315-4NE13, Manual," Nov-2012.

[13] International and Chamber of Shipping, "The Guidelines on Cyber Security Onboard Ships," 07-Dec-2018.