Electronic navigation challenges for autonomous ships

Wilfried Honekamp
Akademie der Polizei Hamburg

Electronic navigation challenges for autonomous ships

Wilfried Honekamp

Professor in applied computer science at the Hamburg Police University College. Braamkamp 3b, 22297 Hamburg, Germany, wilfried.honekamp@polizei-studium.org

Abstract:

Progressive automation is increasingly affecting maritime transportation. Because of cost pressure of maritime logistics and piracy threats, the autonomous ship seems to be about to make a breakthrough. The control of such ships is necessarily based on satellite navigation. The navigation relies to a considerable extent on the Electronic Chart Display and Information System. In our research project, manipulation possibilities of the ship's navigation systems were identified. It has been shown, that it is possible to introduce unnoticed manipulated nautical charts and routes into the system or to manipulate input data like that from the GPS receiver. It can be seen, that this results in a risk to shipping in a narrow fairway such as the Elbe. A collision or seagoing could be the result. The IT security on board should be given as much importance as other security measures of the ship and its crew. Therefore, a uniform standard in the IT area should be developed, in which better protection of the system should be regulated before manipulation. It is foreseeable that a worldwide international coordination will be necessary to make autonomous shipping possible. From this point of view, the security aspects of ship navigation systems need to be considered critically, before satellite navigation can be considered relentless in autonomous shipping.

JEL classification: L92, O33

Keywords: automation, autonomous shipping, IT security

1 Introduction

Control of large cargo, tank and container ships across the world by networked computer systems on board, served by data centre satellite links anywhere in the world, is known as “maritime unmanned navigation through intelligence in networks”. This subject was explored by eight institutions from, inter alia, Germany, Norway, Sweden, Iceland and Ireland in an EU project with a budget of 3.8 million euros by 2015. “The autonomous ship is the vision that leads our research leads”, say the project managers. The technology the project partners developed did not yet aim at relieving the entire crew of a ship. It is conceivable, however, that ships could be managed by a smaller crew. The bridge would no longer have to be equipped around the clock with the captain and a helmsman if this task could be done temporarily by IT. The situation is similar with the prime movers, who are supposed to drive for weeks without machine operator monitoring and maintenance (De Jong 2014).

Incidents on the Elbe river such as the emergency anchor manoeuvre of the 336 m long *NYK Olympus* in July 2015 next to the island Lühesand and the accident of the more than 400 m long *Indian Ocean* in February 2016, which has been lying on the edge of the sand for several days after a rowing outburst, make it clear that specialised personnel on board are required for the complex technology of a ship for troubleshooting. The same applies to manipulations from the outside to the networked IT systems or satellite links. In these cases, misfunctions can only be controlled if suitable personnel can take over the safe control manually. The foundations on which research on autonomous ships is based on, are already in place today, and some have already been implemented in the standards for seagoing vessels.

For example, no unmanned ship of the future finds its course over the oceans without the electronic sea-map. Even today, many ships are equipped with electronic nautical chart systems. In an event of a cyber-attack Maritime companies are at risk of not only losing critical, business-related information or valuable ships, but also risk their economic competitiveness (Masala and Tsetsos 2015, p. 24).

2 Electronic Nautical Charts (ENC)

Electronic nautical charts are prepared and published by the respective coastal regulatory authorities. For paper sea charts, the survey information and sea marks are printed on the map sheet. By looking at the nautical chart, all available information is visible. They are offered in different magnification levels. Larger scales are used for navigation in open sea areas such as from the English Channel to the Elbe estuary. They contain only the information required for this purpose (NOAA 2017).

For navigation entering the port or in the district driving, for example in the fairway of the Elbe river, much more detailed nautical charts are required, which are kept in smaller scales. If paper maps are digitized to electronic raster maps, all the information from the template is displayed on them. Commonly, they are sometimes referred to as electronic photocopies. Raster maps can be enlarged with zoom functions on the monitor, as with a magnifying glass.

If a small map scale is required for navigation, an electronic copy on a different scale, i.e. another raster map, must be called up, which then contains more detailed information. If nautically significant information of the concrete, firing or fairway changes, it must be updated individually in all maps. Today, the digital data generated during sea surveying are usually stored as arithmetic operations. These nautical charts are referred to as vector charts. If a map section is called up, software from the vectors calculates the representation of the information and its position on the monitor.

The information of a vector map can be adjusted by the software with the parameters of the ship. If the depth of water noted in the vector map falls below the draft of the ship, the software indicates to the navigator already during the travel planning by an alarm that another course is required. Areas that fall below the given draft of the ship are marked in colour on the monitor. Vectors also include information about traffic prohibitions, traffic separation areas, shoals, off-shore facilities and other important nautical information that, if ignored, triggers an alarm from the system.

3 Electronic Chart Display System

Manufacturers of Electronic Nautical Chart Systems (ECDIS) must apply for type-approval of their installations with the competent authorities. In the Federal Republic of Germany, the type examination is carried out by the Federal Maritime and Hydrographic Agency (BSH) in Hamburg. The compliance of an on-board installation with the type-approval of the building is subject to official controls, among others conducted by the water police.

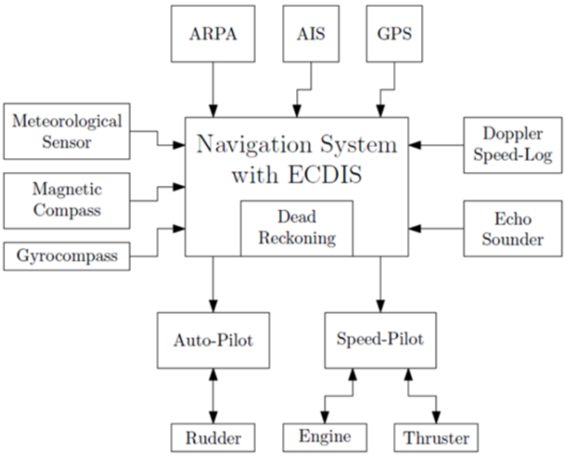


Figure 1: Relationship between sensors, actuators, and the ECDIS on an integrated bridge system (Bhatti and Humphrey 2014, p. 3)

The ECDIS consist of a monitor, via which the visualization of the information takes place. There also is an input device and a computer unit on which an operating system and the software using the ENC are running. The information of nautical sensors present on the ship, such as speed and depth gauges, compass and Global Positioning System (GPS), turn indicator, Automatic Identification System (AIS) and others are transmitted to an ECDIS and processed by the software. Like any electronic device, ECDIS processes the information available on the chart and supplied by the sensors according to the rules given in the installed software. If the sensors or ENC deliver faulty values due to defects or manipulations, misrepresentations on the ECDIS and possibly incorrect ship management decisions will be made.

Even more serious are the consequences if the data of the ECDIS is the basis for the functions of an automatic steering gear of the ship. Errors or manipulations in the position data of the compass or GPS automatically lead to changes of direction away from the planned course of the ship (Warner and Johnston 2003). By linking the electronic components, a defect in one component has a negative impact on the entire system. Not only navigation is increasing supported by IT, but also the control of drive systems, pumps and the power supply of seagoing vessels. If sensors of a steering gear report the maximum possible rudder change, the control electronics will not allow any further rudder change in this direction. If this message is created by mistake or by a manipulation of the IT, the control electronics continue to follow the rules of their programming and thus create the danger of average.

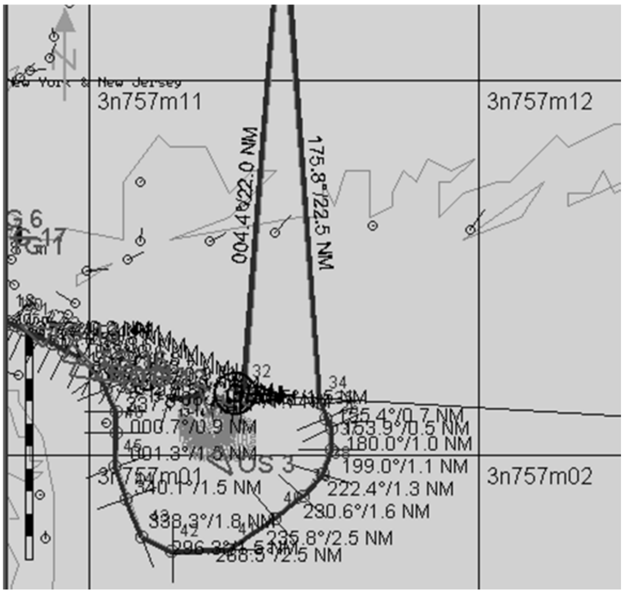
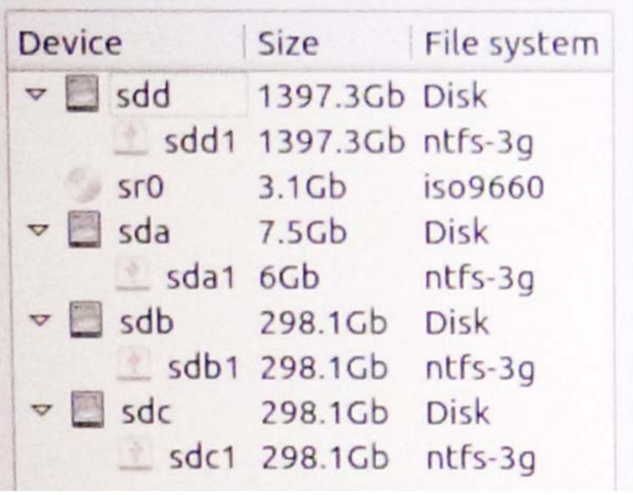


Figure 2: Manipulation of an ECDIS route (Honekamp and Mielke 2016)

4 Access to operating systems

Manipulation and unauthorized access to operating system and software are among the currently considered attack scenarios. Initially, the investigations were limited to ECDIS facilities used for test and training purposes and to installations on board official ships. There were devices and software from four different manufacturers available. It was also pointed out by the users when the devices were being presented, that the prescribed travel planning is done with the help of the ECDIS. Hereby, waypoints are set, which are headed at during the journey. Once a waypoint has been reached, the new course is set to the next waypoint.

The ECDIS software checks in the nautical chart whether the water depth over the entire selected route is greater than the draft recorded in the vessel data and whether traffic separation areas and restricted zones are bypassed at a sufficient distance. If the water depth or locked areas are insufficient, an alarm will be issued requesting the navigator to change the itinerary. On individual systems, various manipulations could be made. Since files can be saved to an external data medium via the operating system, it is also possible to transfer data back to the system. Thereby, it is possible to falsify the operating system, the nautical charts used and created routes by importing manipulated data.



Device	Size	File system
sdd	1397.3Gb	Disk
sdd1	1397.3Gb	ntfs-3g
sr0	3.1Gb	iso9660
sda	7.5Gb	Disk
sda1	6Gb	ntfs-3g
sdb	298.1Gb	Disk
sdb1	298.1Gb	ntfs-3g
sdc	298.1Gb	Disk
sdc1	298.1Gb	ntfs-3g

Figure 3: Hard disk structure of an ECDIS system

The internal dialogues also interfered with the operating system in some systems. For example, programs could be started from a USB flash drive. For almost all systems, the boot sequence could be manipulated so that the system could be started with a Linux live DVD. Subsequently, all files could be accessed and a complete system image (forensic image) could be drawn. The image could then be converted to a virtual environment and started there.

5 Conclusion

Data manipulation and data security of ship systems currently offer great potential. On the one hand, investigative authorities can secure extensive additional evidence, on the other hand, future security regulations should make it much more difficult to manipulate the facilities.

6 References

Bhatti J and Humphreys TE (2014). Covert Control of Surface Vessels via Counterfeit Civil GPS Signals. https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf (17.12.2017).

De Jong N (2014). Ohne Mannschaft auf hoher See. Deutsche Verkehrs-Zeitung 17. Juli 2014. http://www.dvz.de/rubriken/single-view/nachricht/ohne-mannschaft-auf-hoher-see.html (17.12.2017).

Honekamp W; Mielke J (2016). Schiffs-IT-Forensik. In: Honekamp, W; Mielke, J Polizei-Informatik 2016. RediRoma-Verlag Remscheid.

Masala C; Tsetos K (2015). A Demanding Challenge for the Maritime Industry. Look-Out 2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives. http://elib.dlr.de/98812/1/Look-Out%202016_web.pdf (18.12.2017).

NOAA (National Oceanic and Atmospheric) (2017). Electronic Charts (ENC). http://www.charts.noaa.gov/InteractiveCatalog/nrnc.shtml#mapTabs-2 (17.12.2017).

Warner JS; Johnston RG (2003). A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-2384 (17.12.2017).