CYBER SECURITY ANALYSIS OF MARITIME SURVEILLANCE SYSTEMS

Nedko DIMITROV, Chavdar ALEXANDROV, Milen TODOROV
Nikola Vaptsarov Naval Academy Varna, Faculty of Navigation
Technical University Varna, Faculty of Maritime Sciences

ABSTRACT

The authors present in the paper the main technical features of the AIS system as most popular marine traffic surveillance system. In the framework of the made cyber vulnerability analysis they shape the main cyber vulnerabilities of the system. The explanation of the vulnerabilities is connected with the possible way of their exploitation, together with the motivation of the actors. The research is conducted by applying the technical assumptions and simulations in the operational environment. The methodology allows to replay various scenarios and to outline the most typical, the most usual, the most unusual, etc. The four most typical scenarios are described and assessed based on the two factors risk assessment methodology. Groups of technicians and AIS system operators were involved in the assessment filling in a questionnaire. After the answers processing the authors define the level of cyber risk for the AIS systems for each scenario. The experts indicated controls to deal with the risk. The last part of the paper is dedicated to the ways to cover the cyber vulnerabilities of the AIS system during the real work of the system in favor of the effective and safety marine traffic control. The operators are given the awareness of how real is the situation they monitor and how to recognize possible inadequacy of the actions. The results of AIS cyber vulnerabilities analyses help the operators have to have clear understanding how much the generated operational picture on the screens represents the reality. The most important outcomes are included in the cadets' educational program.

INTRODUCTION

Modern Vessel Traffic Management and Information Systems (VTMIS) are hi-tech facilities, including the latest achievements in the field of information and communication technologies along with AIS, classical radio communication systems, radar surveillance systems and sources of hydro- and meteorological information. The majority of them are connected to external computer networks to provide information of different types and purposes to different external users by means of the so called "cloud" technologies.

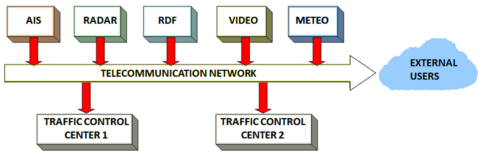

Figure 1. Typical VTMIS Architecture

CYBER SECURITY RISK ASSESSMENT METHODOLOGY AND ITS APPLICATION

The purpose of risk identification is to identify what may occur or which situations may exist, influencing the achievement of the set objectives. Using a risk identification methodology increases the chances of identifying all these elements, either by gathering verifiable evidence, by using expertise, or in another structured way. For this purpose, the following risk identification methodologies are applied:

- Brainstorming: it was useful for risks identification because the situations require a rapid response and little official data is available.
- Interview: Two groups consisting of IT experts and operators from Bulgarian Port Infrastructure Company were interviewed. A questionnaire was developed in order to collect the expert's opinion on the predefined questions / statements relevant to the AIS cyber security area;
- Scenario analysis: 4 scenarios were developed, that according to the expert's opinion are most balanced and cover the possible spectrum of source-event–reason-consequence chain of AIS cyber security risk relevance, taking into account the possible outcomes, strategies and actions leading to the outcomes (See results in Table 1.). The most widely accepted formula for quantifying risk is:

Risk = likelihood of scenario occurrence *x* severity of consequences,

so the risk matrix (fig. 2) is used to calculate the risk level of every one of the scenarios and the results are presented in the last column of the table.

Table 1. Results of the scenarios assessment

Scenario description	Consequences	Occurrence likelihood	Impact	Risk Level
S1. Attenuation or interference of signals emitted by AIS (ship and shore) stations.	Inability of AIS to receive data from other receivers and to identify the targets digitally.	3	1-2	Low
S2. Overloading of the air with false signals.	AIS works normally or close to but visualizes a lot of objects with no idea which is valid/invalid.	3	3	Mod.
S3. Placement (scattering) of real emitting objects in the area, in addition to a signal to the	AIS works normally but the operator cannot recognize which object is valid/invalid.	1	5	Mod.
S4. Sabotage of the work of the AIS by blocking or controlling the management of key com-	AIS works normally but the operator cannot recognize the intrusion and which object is valid/	5	3-4	High

POSSIBLE IMPLEMENTATION OF THE AIS CYBER SECURITY RISK MITIGATION MEASURES

Integration of information from many sensors included in the VTMIS, or data fusion is a way to deal with the disadvantages of AIS by using technical approach. The data fusion aims to confirm the existence of a real target and its location by using another sources of information and thus to verify the reliability of AIS information, i.e. information provided by the radar observation and tracking system, Radio Direction Finders (RDF) and Syntethic Apperture Radar images, or SAR images, provided by satellites. In Bulgarian VTMIS the algorithm for integration of radar data with AIS has been built into the software of operator's workplace or Operator Display Unit (ODU). Software visualizes both radar and AIS data on the ODU, as shown on fig. 3, where radar echoes, provided by two coastal surveillance radars are displayed together with AIS information. Direction finders installed in Bulgarian VTMIS have options to receive signals transmitted on VHF channels 87B and 88B and therefore to determine directions to AIS transponders. The most significant advantage of SAR technology is its global coverage and the main disadvantage is the relatively long time interval between two consecutive flights of the platform or the so called "revisit period". The SAR imaging is also affected by the Doppler effect, as a result of which the location of the target of observation changes depending on its radial velocity. On fig.4 SAR images of a target at anchor (on the left), a target moving to the west (in the middle) and a target moving to the southeast (on the right, see the arrows) can be seen with their displacement due to radial velocity. SAR image of the target, moving to the west is shifted north of the position, provided by AIS, while the image of the other moving target - southeast of the AIS position. Images are provided by Sentinel-1 A/B satellites during their ascending passes and are verified by using AIS data from Bulgarian VTMIS .

Impact

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

Figure 2. Risk Matrix used in Cyber Security risk assessment

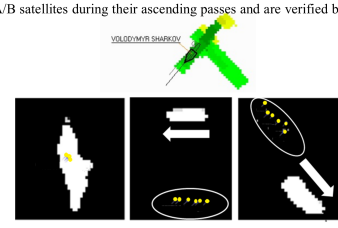

Figure 3. Integration of RADAR picture with data provided by AIS

Figure 4. SAR Images of targets with displacement depending on radial velocity

CONCLUSIONS

In this paper the main technical features, advantages and weaknesses of the AIS system as most powerful component of marine traffic surveillance systems were discussed. Authors tried to shape the main cyber vulnerabilities of the system within the framework of the made cyber vulnerability analysis. The research was conducted by applying the technical assumptions and studying in the operational environment. A number of scenarios were created in order to outline the most typical cases of cyber vulnerabilities utilization;

The cyber security of AIS system is determined when the risk assessment of the scenarios is conducted. At the end of the paper different measures for mitigation of cyber security risk were discussed. Integration of information provided by different sensor such as the radar observation and tracking system and the radio direction finder system, both included in Bulgarian VTMIS, as well as SAR images provided by Sentinel-1 satellites, was presented as the main means to compensate the vulnerabilities of AIS and thus reduce cyber security risk of coastal surveillance systems.

CONTACTS

n.dimitrov@nvna.eu
ch.alexandrov@nvna.eu
m.todorov@tu-varna.bg