CYBER SECURITY ANALYSIS OF MARITIME SURVEILLANCE SYSTEMS

Nedko Dimitrov[a], Chavdar Alexandrov[a], Milen Todorov[b]
[a]Nikola Vaptsarov Naval Academy, Varna 9000, Bulgaria
[b] Varna Technical University, Varna 9000, Bulgaria
n.dimitrov@naval-acad.bg

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 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.

Keywords: **AIS, cyber threats, cyber vulnerabilities, risk assessment, marine surveillance, traffic control**

1. 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 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 (see Fig. 1).

Among the most important issues to be addressed in these cases are those related to the security of these systems in terms of unauthorized access and external impact, both on specific sensors and on integrated system information.

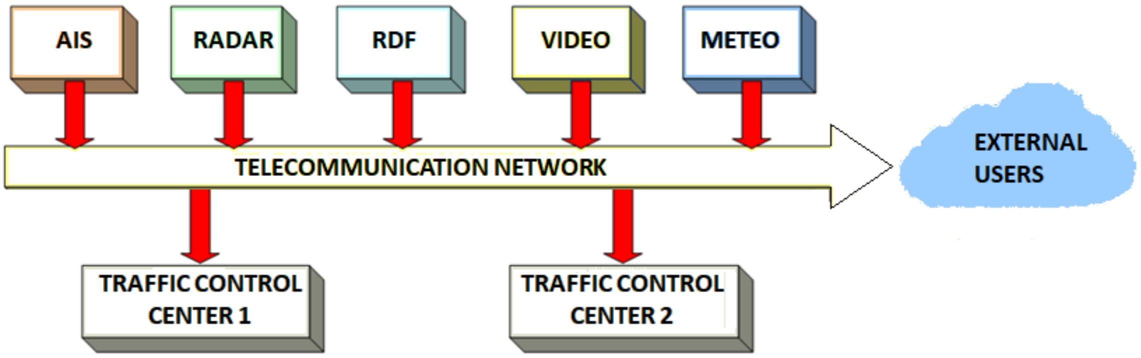


Figure 1. Typical VTMIS Architecture

In this paper, authors attempt to evaluate the degree / the level of threats of a different nature on specific subsystems and sensors, included in the complex VTMIS systems and propose solutions to increase protection against cyberattacks. The scenario based risk assessment methodology is applied using qualitative assessment by experts in area of operational use and technical support of the VTMIS system. The main contribution of the paper is the answer of the question – how to cover the cyber vulnerabilities of the AIS (Automatic Identification System) system and to create as realistic as possible maritime operational picture.

2. Technical aspects of maritime surveillance systems cyber security

The VTMIS structure integrates the following subsystems:

- Universal Automatic Identification System (AIS)
- Radar Observation and Tracking System (RADAR)
- Closed-circuit television system for video monitoring of ports areas (VIDEO)
- Radio Direction Finders System (RDF)
- Hydro- and Meteorological Sensors (METEO)
- Radio Communication System in VHF and MF/HF frequency bands
- Telecommunication Network, the backbone of the VTMIS
- Data processing system
- System for monitoring and control of the above components

AIS is the newest and most powerful system in terms of information capabilities. It is a vessel information and vessel location reporting system, providing information about vessels identity, position, speed, course, and other information to coastal states and to another ships in the vicinity on a common VHF channel, named VHF Data Link, VDL (ITU VHF Channels 87B and 88B). Information provided to another ships can be used mostly for collision avoidance, while when integrated with VTMIS, the AIS information can be used for monitoring and managing the traffic in coastal waters and port areas.

Despite AIS being the most powerful source of information for VTMIS, some of its serious limitations must be taken into account. First of all, there are conventional limitations, arising from IMO requirements that this system is mandatory to be used only by so-called SOLAS vessels. Non SOLAS vessels, i.e. vessels under 300gt may have no AIS equipment installed onboard and as such may remain "invisible" for the coastal surveillance systems and for VTMIS. Another limitation is relatively small coverage area, related to the way of propagation of VHF radio waves – up to the line-of-sight or to about 40nm from the coast. And last but not least, the transmission of correct AIS information depends on the status of onboard equipment and qualification of people, responsible for proper operation. In [1], three main types of incorrect AIS data were identified: errors, falsifications and spoofing.

The errors, having an impact mostly on the static data (ship's ID, size and antenna position, type of ship), dynamic data (co-ordinates of the ship, COG and SOG), or voyage related data (the ship's draught, hazardous cargo type, destination and ETA), can be caused by transponder deficiency, an incorrect data entered manually, erroneous pieces of information that come from external sensors, etc. In [2], more than 20% of AIS data is incorrect due to these errors.

The falsifications is the modification of a correct value of any parameter by a false value, or by stopping the broadcast of messages, made in order to mislead the ships sailing nearby and the coastal authorities, responsible for the management of the traffic, i.e. VTS authorities, port authorities, etc. Unlike the errors, in falsifications the wrong data is broadcasted intentionally. According to [3], about 1% of the vessels broadcast falsified data, including theft of identity, broadcast of false coordinates or disappearances, statements of a wrong activities, etc.

The spoofing activities include broadcasting of externally generated and / or modified AIS data by an outsider. In order to mislead the ships sailing nearby and the coastal authorities, the outsider creates ghost vessels or aids to navigation, or broadcasts false emergency messages intentionally, similar to falsifications.

Based on the world wide published research results for the AIS operation in different type of environment [3,5,6,7,8] the authors conducted cyber security risk analysis of Bulgarian AIS as part of VTMIS operated by Port Infrastructure company.

3. Cyber security risk assessment methodology and its application

The purpose of risk identification[1] is to identify what may occur or which situations may exist, influencing the achievement of the set objectives. Given the cyber security of AIS systems, for the purpose of the research the objective is *to keep the situational awareness of the operator as real as possible in order to achieve the safety of navigation and security of the infrastructure*. In order to identify all the possible risks for the AIS cyber security a risk description was developed, that contains the following main elements:

- Sources of risk: elements of the scenario that, isolated or combined, have the potential to affect the expected results (signal attenuation or interference, etc.)
- Event: a specific set of circumstances (overloading the air, placement /scattering of real objects radiating signals for unreal objects, etc.)
- Reason: the initial state that triggers the event (illegal activities that has to be covered, hacking curiosity, etc.)
- Consequence: the result of the event affecting the target (loss of data, invalid objects, etc. affecting the correct situational awareness of the operators)

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:

[1] According to ISO 31010: 2012 - "Risk Management - Risk Assessment Techniques" [10]

- Brainstorming: it was useful for risks identification because the situation requires a rapid response and few 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. They are as follows:

S1: Attenuation or interference of signals emitted by AIS (ship and shore) stations - the system works by digital transmission of VHF data, as frequencies are known and can be simulated or attenuated.

S2: Overloading of the air with false signals - submission of data for invalid objects, which are accepted by the system along with the real ones.

S3: Placement (scattering) of real emitting objects in the area, which, in addition to AIS signal should also generate marks from the ships' own sensors or the coastal services.

S4: Sabotage of the work of the AIS by blocking or controlling the management (hacking) of key components of the system such as base stations, network devices, power supply, etc. via the Internet or other electronic connectivity.

As the main AIS cyber security risks are described in scenarios the risk assessment is conducted in the process of playing the scenarios (by the same experts) and answering specific questions composed in a short interview. Answering the questions, both groups of experts had to take into account the source-event–reason-consequence logical construction and to assess the two factors of the cyber security risk: scenario occurrence likelihood (rating is ranged from 1 - most unlikely to 5 - most likely) and impact / severity of the consequences (rating is ranged from 1 – negligible to 5 - severe). This method was chosen because of difficulties in determining the likelihood of occurrence, as there is lack of statistical information for defined types incidents in past. The results are presented in the table 1.

During the scenario playing the experts express and take into account the following considerations:

- S1 is an easily feasible scenario from an organizational point of view, associated with a relatively easy unnoticed deployment and power supply of jamming equipment, but requires availability and activation of specific equipment, as well as trained professionals to handle it. The AIS malfunctioning is an easy-to-identify problem, and the safety of navigation is ensured by other options such as visual surveillance, own sensors, radio and other communications between the various participants of shipping.
- S2 - Each AIS transceiver looks for free time slots and can be set to fill them with false information - invalid virtual objects. A standard transmitter can transmit data for only one object, but a base station can transmit a number of objects such type. It is relatively easy to implement from a technical point of view, but it is necessary to mobilize a specialized technical resource as well as trained specialists to handle it.

It is relatively difficulty to identify the problem. It will also take time and the involvement of well-trained professionals while filtering out invalid from real objects, during which period of time it may be necessary to take action to divert vessels or traffic in general, leading to financial losses. It is not clear to what extent ship crews will be able to identify and deal with the problem and whether this will not lead to immediate safety threats.

Table 1. Results of the scenarios assessment

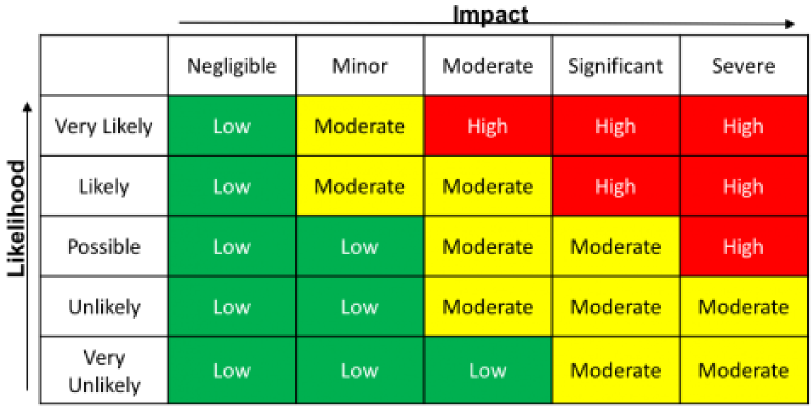
Scenario description	**Consequences**	**Occurrence likelihood**	**Impact**	**Risk level**
S1. Attenuation or interference of signals emitted by AIS (ship and shore) stations - the system works by digital transmission of VHF data, as frequencies are known and can be simulated or attenuated.	Inability of AIS to receive data from other receivers (ship and shore) and the inability to digitally identify the targets.	3	1-2	low
S2. Overloading of the air with false signals - submission of data for invalid objects, which are accepted by the system along with the real ones.	AIS works normally or close to normally but the visualization does not reflect the real situation at sea. A lot of objects with no idea which is valid/invalid	3	3	Mode-rate
S3. Placement (scattering) of real emitting objects in the area, which, in addition to a signal to the AIS, should also generate marks from the ships' own sensors or the coastal services.	AIS works normally but the visualization does not reflect the real situation at sea. The operator cannot recognize which object is valid/invalid.	1	5	Mode-rate
S4. Sabotage of the work of the AIS by blocking or controlling the management (hacking) of key components of the system such as base stations, network devices, power supply, etc. via the Internet or other electronic connectivity.	AIS works normally but the visualization does not reflect the real situation at sea. The operator cannot recognize the intrusion and which object is valid/invalid.	5	3-4	High

- S3 - The hidden circulation in the area by vessels to locate physical objects would be associated with a large technical and financial resource and a very complex organization at various levels to overcome the monitoring and control of the vessels movement. Vessels with low detection probability can be used, research of the possibilities of the monitoring systems has to be done in advance, specialists and / or insiders have to be engaged, etc.

The presence in the navigation waters of physical objects that have unclear origin and destination would require adoption of the resolute measures such as reorganization and redirection of all traffic, measures for inspection and deactivation of objects deployed in the in the water area. This generates a waste of time and money and can pose a real threat to the safety of vessels and the safety of facilities.

- S4 - It can be applied remotely by accessing the system via the Internet. There are many levels at which the system can be manipulated this way - from malfunctioning (a lighter option in terms of consequences) to taking the control (option with many possible consequences - false targets, navigation errors when submitting false information for real objects, etc.)

There are many different formulas for risk, but perhaps 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 Table 1.


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 [11] used

At the final step of the assessment the experts team was requested to address the deficiencies identified in order to reduce the significance of the likelihood and impact as risky factors. Summary risk management measures described by the team include but are not limited to:

- Training of navigational staff for ships identification (generally – objects) without using AIS - through behavior analysis, communications etc.;
- Increased surveillance and tracking to control the activities of small vessels, that can be used for placement (scattering) of real emitting objects in the area;
- Establishment of protection and appropriate architecture of the Internet environment where AIS operates, training of cybersecurity specialists and counteraction to hacker actions;
- Establishment of the maritime operational picture using different sources, data fusion.

4. 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 mentioned above by using technical approach. According to the IMO Resolution A.917 (22) AIS should become a useful source of supplementary information to that derived from navigational systems. 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. The appropriate parameter such as ship's position, speed over ground (SOG), course over ground (COG), track history, etc., and an appropriate threshold corresponding to the accuracy requirements should be defined. To confirm the existence of a real target, the difference between the measured parameters should comply with the inequality (1):

$$|C(Sensor) - C(AIS)| \leq \delta, \qquad (1)$$

where *C(Sensor)* is the parameter (coordinates, COG, SOG etc.), provided by any other sensor, such as radar observation and tracking system, RDF, etc., and δ is the threshold value of the criterion [4, 5].

Integration of information provided by the radar observation and tracking system with AIS data is the main tool in this process [6, 7]. 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 (yellow and green colored), provided by two coastal surveillance radars are displayed together with AIS information, which includes the name of the vessel, her size and velocity vector. The essential information for traffic control however is based on radar data processing.

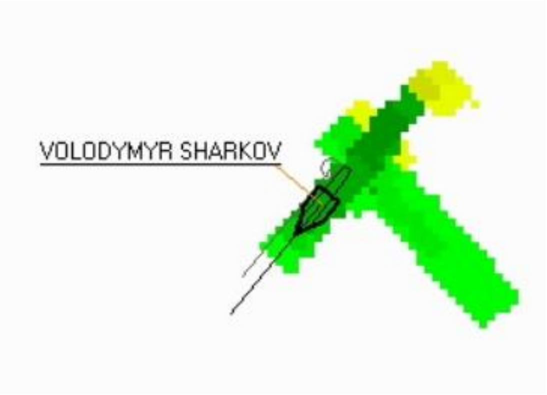


Figure 3. Integration of RADAR picture with data provided by AIS

Radio Direction Finders (RDF) can be used to confirm the existence of real targets as well. Having a network of coastal RDF installations in the composition of a coastal VTS, the position of a transmitting object can be determined by using radio-triangulation scheme. The locating accuracy of this technology is poor, but it is very useful for the purposes of Search and Rescue operations at sea to detect small objects such as life boats or life rafts equipped with only portable VHF radios, transmitting on Ch. 16 and/or 406MHz satellite EPIRBs. Direction finders installed in Bulgarian VTMIS have also options to receive signals transmitted on VHF channels 87B and 88B and therefore to determine directions to AIS transponders.

Synthetic Aperture Radar images, or SAR images, provided by satellites may also be used to verify the reliability of AIS information. The most significant advantage of this 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”. For medium latitudes for example, the revisit period is about 48 to 72 hours using the acquisitions of one of the Sentinel-1 A/B satellites only, and 24 to 36 hours using the acquisitions of both satellites. The SAR imaging in this case 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. If it is assumed that area of observation is relatively small and within this area the Earth surface is flat, the azimuth offset or displacement, δ_x, e.g., the difference between the actual moving target location and its location on the SAR image, can be determined by using Eq. (2):

$$\delta_x = \frac{u_r.R}{V}, \tag{2}$$

where u_r is the radial velocity of the target, R is the slant range to the target and V is the platform velocity [6Graziano, …] 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 (AIS position is visualized by using yellow pins), 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 [9].

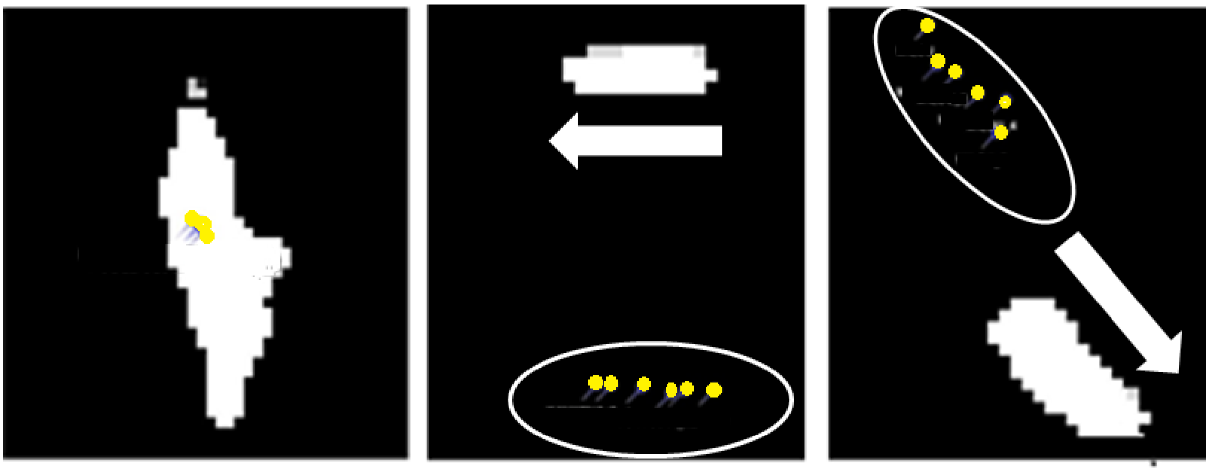


Figure 4. SAR Images of targets with displacement depending on radial velocity

5. Conclusion

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 shaped the main cyber vulnerabilities of the system within the framework of the conducted 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 scenarios risk assessment 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.

References:

[1] Cyril Ray, Clément Iphar, Aldo Napoli. Methodology for Real-Time Detection of AIS Falsification. Maritime Knowledge Discovery and Anomaly Detection Workshop, Jul 2016, Ispra, Italy. pp.74-77 - ISBN 978-92-79-61301-2.

[2] Sotirov St., Ch. Alexandrov, Improving AIS data reliability, 18th Annual General Assembly of the International Association of Maritime Universities - Global Perspectives in MET: Towards Sustainable, Green and Integrated Maritime Transport, IAMU 2017, Vol. 1, pp. 237–244

[3] Harati-Mokhari, A., Wall, A., Brooks, P. and Wang J., Automatic Identification System (AIS): a human factors approach. J. Navig. Vol 60(3), Cambridge University Press, 2007

[4] Angelova A., Ch. Alexandrov, Comparison between information provided by radar and AIS in the integrated vessel traffic systems, 16th Conference on Electrical Machines, Drives and Power Systems, ELMA 2019 - Proceedings, 2019

[5] V. Atanasov and Y. Sivkov, "Data Fusion for IoMT in Shipping," 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), 2020, pp. 1-6, doi: 10.1109/SIELA49118.2020.9167126

[6] Kastilieris F., Braca P., Coraluppi S., Detection of malicious AIS position spoofing by exploiting radar information, Conference: Proc. of the 16th International Conference on Information Fusion (FUSION 2013), Istanbul, Turkey, 2013, pp. 1196 – 1203

[7] Alexandrov Ch., Bulgarian vessel traffic information system and education and training of VTS personnel in Bulgaria, Proceedings, 16th Annual General Assembly of the International Association of Maritime Universities IAMU AGA 2015, Rijeka, Croatia, pp. 13–20

[8] Graziano M., Renga A. and Moccia A., Integration of Automatic Identification System (AIS) data and single-channel Synthetic Aperture Radar (SAR) images by SAR-based ship velocity estimation for Maritime situational awareness, *Remote sensing*, 2019, 11, 2196

[9] Kolev N., Alexandrov Ch., Tsvetkov M., Sentinel – 1 SAR SLC image ship detection and motion estimation, 16th Conference on Electrical Machines, Drives and Power Systems, ELMA 2019 - Proceedings, 2019

[10] ISO 31000 Risk Management – Principles and Guidelines, [online] available on:
https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines

[11] System Risk Analysis, [online] available on:
https://itsecurity.uiowa.edu/resources/everyone/determining-risk-level