Traffic & Transportation

Simulating a Cyber-Attack on the Mass Thruster Controllers at Low-Speed Motion

Igor ASTROV[1], Sanja BAUK[2]

Original Scientific Paper
Submitted: 29 June 2024
Accepted: 15 Oct 2024

[1] igor.astrov@ieee.org; igor.astrov@taltech.ee, Tallinn University of Technology, Department of Software Science
[2] Corresponding author, bsanjaster@gmail.com; sanja.bauk@taltech.ee, Tallinn University of Technology, Estonian Maritime Academy

Publisher:
Faculty of Transport and Traffic Sciences, University of Zagreb

ABSTRACT
The aim of this paper is to highlight the vulnerability of Maritime Autonomous Surface Ships (MASS) to cyber-attack and to illustrate, through a simulation experiment on a testbed, how to mitigate a cyber-attack on the MASS thruster controllers during low-speed motion. The first part of the paper is based on a scoping review of relevant articles in the field, including some MASS projects, related cyber threats and modelling techniques to improve cyber resilience. In the second part of the paper, a cyber-attack on the MASS thruster controllers at low speed motion is illustrated along with the impact of the attack on the trajectory motion. The Kalman filter, as an additional device to the thruster controllers, is used as a cyber-attack mitigation aid. Under the conditions of a simulated intrusion on the input and output signals of the thruster, the experiments conducted in the MATLAB Simulink environment provide an insight into the behaviour of the MASS propulsion subsystem from the perspective of the low-speed trajectory, with and without the Kalman filter.

KEYWORDS
MASS; cyber-attack; thruster; PID controller; Kalman filter; state-space method.

1. INTRODUCTION

The maritime industry is undergoing a revolution thanks to smart shipping, which uses automation, big data and artificial intelligence to make shipping more competitive, safe and environmentally friendly. Numerous data-collection sensors, on-board data processors and data-driven deep learning algorithms facilitate optimisation and decision-making in contemporary shipping. Ships can be remotely monitored and operated thanks to good connectivity. However, ongoing technological advancements have made it feasible for ships to operate independently. A ship can navigate by itself or call for crew assistance based on information gathered by sensors [1]. Namely, the advent of Maritime Autonomous Surface Ships (MASSs) as cyber-physical systems became possible by innovative maritime information and operation technologies. Operation technology includes a wide range of programmable controllers that enhance the convergence of cyber and physical systems. On the other hand, information technology is responsible for managing administrative operations and data. Notwithstanding, both operation and information technologies are vulnerable to cyber-attacks [2, 3].

It is possible to design MASSs to be more fuel-efficient, lighter, less expensive to operate and more wind-resistant and streamlined. However, the trend toward MASSs development is not without the difficulties. For instance, crew ships are in the focus of the Convention on the International Regulations for Preventing Collisions at Sea (COLREG), therefore it is not possible to apply concepts like “good seamanship” (rule 8) and “proper look-out” (rule 5) to MASSs [4]. Furthermore, the International Ship and Port Facility Security (ISPS) Code, which essentially forbids crew-less vessels, mandates the presence of a security officer on board (A/2.1.6). Human factors associated with programming and coding errors, remote control, along with the

ignorance of a MASS response in certain critical situations are among the challenges. Interaction with (un)manned vessels in congested areas, including the inability to detect small objects, are also the drawbacks of MASSs. Relations with the natural environment during unfavourable weather conditions, such as strong winds, high tides and thick ice, can cause additional problems. System failures can create difficulties, as well. These include operating systems or communication lines failures. Problems can also be caused by equipment failure, such as sensor malfunction, power failure, loss of propulsion or rudder function. Cyber incidents, whether deliberate (security) or accidental (safety) are inherent to MASSs and can have negative effects on human lives, vessels, marine infrastructure and the environment. These pose big challenges to practitioners, as does the absence of countermeasures if these attacks succeeded. Commonly, cyber-attacks compromise the information and operation technology infrastructure on board, spoof or jam data and signals from the Global Navigation Satellite System (GNSS) or (Satellite-)Automatic Identification System ((S-)AIS), and break communication links with control centres ashore, while the most insurance policies do not cover these risks [5]. Since cyber-threats change quickly, it is important to have backups, firewalls, monitoring systems, anti-virus software, encryption, regular audits, the newest software versions and to develop permanently efficient mechanism to protect MASSs against these threats, while ensuring cyber-resilience [6].

2. STATE OF THE ART

Within the environmental and literature scan, we will start with a review of the autonomous ships that have been developed so far for research, commercial and military purposes. We will then give a brief overview of the most common cyber-attacks on the vessels' navigation systems, including cyber-worthiness and resilience, so that we can then give an example of a cyber-attack and its neutralisation upon the propulsion sub-system of the MASS, whose mathematical model has been developed and used in the previous research works [7, 8].

2.1 Maritime Autonomous Sea Surface (MASS) vessels

Space travel marked the beginning of the use of unmanned vehicles. Then, commercial use of rail unmanned transport devices was implemented to carry freight and people. Further applications take place in air transport for both military and civil purposes. Commercial use of autonomous cars and trucks on generally accessed roads are still under the development. The situation is similar for maritime transport [9], although some MASSs are in operation. Notwithstanding, the idea of designing and developing Autonomous Underwater Vehicles (AUV) is not new. The first AUV was developed in 1957 at the Applied Physics Laboratory of the University of Washington (USA). This vehicle operated at 2–2.5 m/s to a depth of 3600 metres. In the 1970s, a few AUVs were developed at MIT and also in the Soviet Union [10]. These early underwater robots were heavy, expensive and inefficient. Today's AUVs have six degrees of freedom, move faster than 20 m/s, accurately detect obstacles and map the seafloor at depths of up to 6000 metres. They are more sophisticated, less expensive and therefore accessible to a wider range of uses such as fishing, sport, tourism, entertainment, and so on. However, AUVs still have a long way to go to become fully autonomous and capable of exploring deep and hazardous underwater habitats [11].

Prior to the deployment of unmanned and autonomous sea vehicles, several organisational, legal and technological issues must be addressed. The International Maritime Organisation (IMO) deals with the legal matters in this regard [12]. In order to guarantee that MASS operate safely alongside conventional ships, the IMO is drafting a legislative code governing these autonomous vessels. Based on the progress made thus far, the international maritime authority anticipates that in May 2025, a non-mandatory MASS Code will be finalised and adopted. The IMO's Maritime Safety Committee (MSC) states that this is a step in the long process of establishing a comprehensive mandatory regulatory code that will take effect after 2030 [13]. The IMO Maritime Safety Committee formed a working group to deal with safety concerns at and around locations where autonomous and unmanned vessel tests are conducted. A white paper "Cyber-enabled ships: Ship Right procedure – autonomous ships" was issued by Loyd's Register in 2016. The Loyd's Register Code for Unmanned Marine Systems was announced in 2017. It sets the goals and objectives for various unmanned vehicles [14]. It is important to note that Loyd's Register classifies marine vehicles into seven autonomous levels (AL0-6): AL0 means that all operations are manual with the lack of autonomous functions; AL1 refers to on-vessel decision support, where crew members have access to data; AL2 includes off-vessel decision support, where monitoring occurs on land; AL4 involves human-in-the-loop, with semi-autonomous vessels, where crew members can intervene in the case of need; AL5 refers to the autonomous vessels, where human control is possible; and AL6 applies to fully autonomous vessels that do not require human intervention. The

term unmanned refers to a class of ships on the lower ends of this scale that are remotely operated, meaning that no one is on board [15].

Today, some autonomous and unmanned ships are used for research, commercial and military purposes. We will shortly introduce here Yara Birkeland, Zhu Hai Yun, Large Unmanned Surface Vehicles (LUSVs), eXtra Large Unmanned Undersea Vehicles (XLUUVs), SEA-KIT's Unmanned Surface Vessel (USV) Maxlimer, Mayflower autonomous vessels, including KASS and Rolls-Royce Advanced Autonomous Waterborne Applications (AAWA) projects. Namely, some of the MASSs currently used in research, defence and transport are mentioned below:

- Together with Kongsberg, Yara designed the self-sufficient vessel Yara Birkland, which is an autonomous, short-range, zero-emission cargo vessel [16]. It travels along the Norwegian coast and has a capacity of 120 twenty equivalent unit (TEU) containers. The purpose of this self-sufficient vessel is to move mineral fertilizer from Yara's Porsgrunn production plant to Brevik, a nearby export port. Its length is 80 meters and maximum speed is 15 knots.
- SEA-KIT's USV Maxlimer is another autonomous vessel that successfully completed its first voyage between the UK and Belgium in 2019. Its length is 11.75 meters. In 2021, it became the first ship of its kind to receive certification for unmanned marine systems from the Loyd's Register [17].
- The US Navy is creating Extra Large Unmanned Undersea Vehicles (XLUUVs) and Large Unmanned Surface Vehicles (LUSVs) to transport various kinds of military payloads [18].
- In this context, it is also important to mention the Chinese autonomous mother ship Zhu Hai Yun, which can launch swarms of unmanned aerial, surface and underwater vehicles for monitoring and research. The aluminium hull of Zhu Hai Yun measures 88 meters in length and 14 meters in width, with a gross tonnage of 2548 tonnes. The diesel-electric propulsion system, which consists of two generators, two azimuth thrusters and emergency batteries, allows the vessel to reach the speed of 18 knots [19].
- Not to be overlooked is the Mayflower autonomous vessel, which was constructed by IBM and MarePro. This is a research vessel. It successfully completed a 40-day journey from Plymouth (UK) to Halifax (Nova Scotia), in 2022, without the need for a crew. The ship is 49 feet long by 20 feet wide, weighs approximately 5 tonnes, and is built of aluminium and composite materials. Interested parties had access to an online dashboard with a plethora of real-time information, including live video, energy consumption, speed and weather, after the 3500-mile journey of the Mayflower. Although this autonomous ship is designed to conduct scientific experiments, and its primary objective is oceanographic research [20].
- In addition, until 2025, the autonomous surface ship KASS, being built in South Korea, is in the development process [21].
- The Rolls-Royce AAWA multipurpose ocean-going reduced crew ship also deserves to be mentioned here. By 2035, it is anticipated that this vessel will be fully autonomous [22, 23].
- Finally, the Tallinn University of Technology (Estonia), together with the start-up company MindChip, has developed a MASS called "Nymo". This is a catamaran for cargo transport and environmental monitoring. This 2.5 metre long, 200 kg vessel has a maximum load of 100 kg and a range of 50 km. The mathematical model of this MASS is used in this work for simulation experiments with thruster controllers' cyber-attack intrusion and neutralisation [24].

2.2 Cyber-attacks

The most frequent cyberattack target in marine navigation is the Global Positioning System (GPS), which is one of the Global Navigation Satellite Systems (GNSSs), along with the Automatic Identification System (AIS). When a cyber-attack occurs and the ship needs to be navigated on a specific course, one method to compensate for the loss of satellite positioning data is to rely on the mathematical model of the ship, its surrounding and safe on-board sensors. The ship should be able to navigate without GPS if there is an accurate model for both the ship and natural influences on it caused by wind and currents.

Malfunctioning of a GPS receiver may occur for several reasons. For example, the GPS receiver may have been damaged or incorrectly plugged in, or the cable between the antenna and the receiver may be broken. However, GPS receivers are susceptible to several kinds of malevolent cyber-attacks, like spoofing and jamming [25]. Typically, jamming relies on a tiny transmitter operating at nearly the same frequency as the satellites. This noise can disable the receiver. Notwithstanding, certain GPS receivers can recover the original signal by filtering out jamming signals by using machine learning and artificial intelligence capabilities [26].

Another, more advanced form of GPS receiver disruption is spoofing. When this occurs, an emitter sends out signals that the GPS receiver can interpret as coming from a satellite and use it as an entirely false line of position. Spoofing has the potential to seriously confuse every receiver within the range. Compared to anti-jamming, anti-spoofing needs more sophisticated equipment and expertise. Furthermore, the receiver may mistake it for multipath, making it challenging to distinguish as an external source of error.

Alternative solutions, such as hybrid receivers combining different GNSSs as GLONASS, GPS, BeiDou, Galileo, or one of two regional satellite navigation systems, such as Indian RNSS and Japanese QZSS, can be used to mitigate the harmful effects of jamming and spoofing. More specifically, when extreme precision is needed, specialised GNSS receivers should be employed. These receivers can, for instance, track both GPS and GLONASS satellites concurrently and switch between the two systems based on the constellation's satellites' position accuracy and availability. A system like Kongsberg's Seatex DPS-232 can be used for such a purpose [27]. Among the components of this system is the European Geostationary Navigation Overlay System (EGNOS), a satellite-based augmentation system, comprising two mission control centres, forty positioning stations and three geostationary satellites [28]. An additional antenna is included with this cutting-edge GNSS receiver, Seatex DPS-232, so that it can receive corrections from the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA). When the receiver is used for demanding offshore operations, it has an external interface that supports Dynamic Positioning (DP). The system is connected to a gyro compass and a modernised radio-hyperbolic system like Enhanced Loran (e-Loran), which is used to support navigational safety and security.

Besides radio and inertial navigation, which is in the focus of our research, other systems and devices that can support GNSS functionality include augmentation-smart support systems, stable clocks in the receivers, micro electromechanical sensors, and the like. Although some of these solutions are expensive, they should be taken into consideration when satellite systems are utilised for particularly important operations. Additionally, a coded Precise Positioning Service (PPS) in the GPS is available for military use, providing highly accurate military positioning, velocity and timing at a minimum of 95% accuracy. However, commercial GPS users cannot access the cryptographic keys included in the PPS, which counteract the effects of spoofing and selective availability [29].

Some example of common cyberattacks on commercial crewed ships are given below, but the same attacks are inherent to MASSs as well, while they can cause serious damages.

For instance, the Atria tanker's master reported in June 2017 that, while off the coast of Novorossiysk (Black Sea), his GPS indicated, due to spoofing attack, that the ship was twenty nautical miles offshore, near the Gelendzhik Airport. At least twenty nearby ships were detected by navigation systems to be in the same location on the land side later. Thus, many vessels' Closest Point of Approach (CPA) alarms, which were, of course, false alarms, announced an impending collision [30, 31]. Regarding the extreme danger of this scenario, it is necessary to double-check the position and utilise every other option besides GPS to fix it accurately. In the case of a MASS, this can be done only from the shore-based control centre or through automatic regulation on-board a vessel.

Not only GPS receivers, but also AIS devices can be targets of spoofing or jamming. In addition to being used for communication and route sharing between ships and between ships and the shore control centre, which can aid in collision avoidance, the AIS is used to identify and locate both own and other ships. As an Aid to Navigation (AtoN), virtual AIS is used to verify that the system functions as intended or to virtually replace other real AoNs, such as buoys. The radar, sophisticated camera systems used in conjunction with radar and a double check of the most recent electronic charts, can all be used to restore functionality if this system is targeted by a cyber-attack. Since AIS first emerged in the early stages of the Internet commercialisation, it has had a great deal of vulnerabilities. The most frequent ones are fraudulent misrepresentation of ships (e.g. a fishing boat can pose as a different kind of vessel), the lack of message integrity, missing timestamp information and the lack of geographic validation [25, 31]. False AIS AtoNs as green boys can direct the vessel to a shallow waterway that cannot be navigated.

While AIS and GPS are both highly developed and sophisticated technologies, they are also very susceptible to cyber-attacks. These systems are receptive to corruption by different adversaries through a variety of low-tech means, so developing defences against such attacks or coming up with other means of positioning and navigation is required. One of the key solutions covered in this study is the effort to create a navigation system on board the autonomous research vessel that is capable of operating without the assistance of GPS or AIS.

2.3 Cyber-resilience

Cyber-resilience is the capacity of an entity (in this case a MASS) to consistently produce the desired result despite cyber-attacks [32]. Operation and information technology systems, critical infrastructure, business processes, organisations, societies and nation-states all depend on their ability to withstand cyber-attacks. The same applies for MASSs, which operate in extremely complex and interdependent maritime ecosystem. Cyber-worthiness, an evaluation of a system's resistance to cyber-attacks, is a related term [33]. It can be used on a variety of hardware and software components, e.g. standalone applications, online code, browsers, military mission systems, commercial equipment or (Industrial) Internet of Things (IIoT) devices, as well as on MASSs.

The shipping sector is rather traditional. It does not embrace new technologies quickly. It is mostly linked to long-distance mass transport over vast geographic distances. It has an international aspect and involves numerous parties. Shipping industry necessitates significant investments, and as a result, it is commonly hesitant to try out novel technologies and modes of operation. On the other hand, MASSs are of interest to researchers. As a result, the number of studies conducted in this field grew gradually between 2011 and 2016, but then it started to grow exponentially. After carefully examining the literature on the dependability of MASS, Chaal et al. [34] came to the conclusion that the majority of research articles concentrate on the following problems:

— Techniques for risk assessment and safety engineering to aid in decision-making.
— Avoiding collisions and maintaining safe navigation.
— Systemic frameworks, such as System Theoretic Process Analysis (STPA), to assess the risks associated with MASSs [35, 36].
— Bayesian networks and other probabilistic modelling approaches used to mitigate MASSs vulnerabilities [37].
— Risk analysis for cybersecurity.

The Zero Trust Architecture model with the MITRE ATT&CK matrix [38, 39], which aims to develop an overall cyber security principle of "never trust, always verify" can be added to the above list. This is a critical component of a modern security strategy that enables different industries to actively assess the changing cyber threat landscape and ensure a safer and more resilient digital future. Additionally, a comprehensive analysis of cyber assets, threats, vulnerability analysis and mitigation measures for MASSs is given in [40]. This study is based on the latest guidelines on cyber security issued by the IMO and the Baltic and International Maritime Council (BIMCO). It includes HAZard Identification (HAZID)-based cyber-risk assessment that was performed according to the smart ships.

Notwithstanding, the STRIDE technique, which refers to Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege, seems to be essential. This methodology aligns the risk matrix and various components of the MASS system architecture with the threat criteria. According to the STRIDE analysis, autonomous ship controllers face a considerable risk of denial of service. But this system's functionality is vital because without it, the MASS might not be able to sail. According to Kavallieratos et al. [41], there is a high risk of spoofing because position, course, Maritime Mobile Service Identity (MMSI), and other crucial information for safe and effective navigation may be tampered by hacking of GNSS, AIS, or Global Maritime Distress and Safety System (GMDSS) data, etc. Norway, the UK, the US, France, Croatia, Greece, Germany and South Korea have contributed the most to maritime cybersecurity research, based on metrics that take into account selected Scopus-indexed publications [42].

As the level of automation, and especially autonomy, increases, so does the risk of cyber intrusion. The focus of the following will be on autonomous ships' cybersecurity resilience, in the case of intruded cyber-attack to the MASS's thruster controllers at a low-speed mode of operation.

3. PROBLEM STATEMENT

The aim of this work is to analyse the effects of cyber-attacks on the MASS "Nymo" [7] thruster controllers at a low-speed motion. To test the behaviour of the system and its trajectory under perturbations, cyber-resilience was tested by deploying the Kalman filter with certain characteristics. The parameters of the Kalman filter need to be optimised.

3.1 Methodology

The possibility of breaking into the MASS "Nymo" Supervisory Control and Data Acquisition (SCADA) system motivated us to conduct this experiment. Malicious actors can target SCADA servers that monitor, control and analyse MASS devices and processes. The SCADA enables both local and remote data collection from a MASS. It has changed dramatically over time, moving from a largely isolated environment to a highly connected network such as the Internet of Things (IoT) SCADA. In fact, IoT and cloud-based SCADA can cause several security risks, including unwarranted data and information sharing over the Internet, increased bandwidth congestion, latency and the like [43]. A cyber-attacker can use the technique known as privilege escalation to infiltrate the SCADA system and gain unauthorised access. Numerous attack vectors, including malware, social engineering, misconfiguration and stolen credentials, can lead to this malicious activity [44]. This can happen through default password configuration, improper logging of invalid authentication attempts [45], etc. The attacker can then spoof hardware devices, introduce malicious virtual noise generators and/or malicious code to compromise the system. An example of such an attack could be the introduction of malevolent influential noise into the thrusters' control circuit, which we have analysed on the "Nymo" testbed. As a key research strategy, we have used simulations. Details are provided in the following section.

3.2 Novelty of the approach

There are many applications for a robot ship like "Nymo". Examples include seabed mapping, fish stock monitoring, bird or seal counting, marine pollution monitoring, as well as maritime rescue, border patrol and defence solutions. In the Nordic countries, mail and parcel services or waste transport to small islands or from islands to the mainland, or both, could be considered. The "Nymo" MASS can therefore be used for any of these services with appropriate modular hardware and software adaptations. However, "Nymo" has a specific mathematical model that describes it and, to the best of our knowledge, this is the first time that anyone has analysed a cyber-attack on its SCADA system, embodied in an amplified noise intrusion that disrupts the operation of the rudder control system. This type of cyber-attack can cause the MASS to deviate from its intended path, i.e. to collide, crash, ground or sink. These are all fatal consequences for the vessel itself, its cargo and the environment. It is therefore important to ensure that such cyber intrusions into the control system of an autonomous vessel are avoided or neutralised. This is what this research is all about, neutralising a cyber-attack on the MASS rudder controller.

4. SIMULATION EXPERIMENTS AND RESULTS

At the Tallinn University of Technology (Estonia), one of the areas of study for some time now has been research into the MASS [46-49]. Through mathematical and numerical simulations, we continue this research in the MATLAB Simulink environment. Below are mathematical formulations of the problem, accompanying schemes in Simulink along with the obtained results.

Consider the model of MASS (see *Figure 1*).

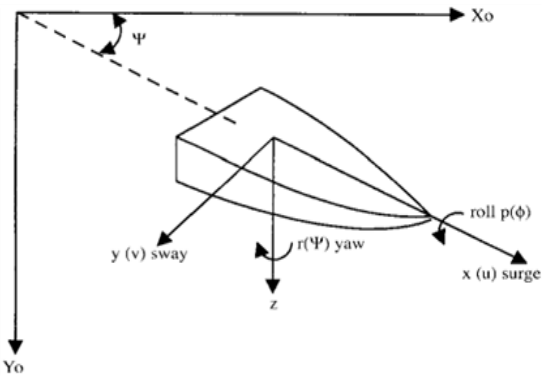

Figure 1 – MASS motion coordinate system

The state-space model of MASS can be expressed by *Equation 1* and *Equation 2* as [50]:

$$\dot{X}=AX+BU \tag{1}$$

$$\dot{Y}=CY+DU \tag{2}$$

where X, Y and U are expressed by *Equation 3*:

$$X=\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix};\ U=\begin{bmatrix}\tau_x\\\tau_y\\\tau_r\end{bmatrix};\ Y=\begin{bmatrix}u\\v\\r\end{bmatrix} \tag{3}$$

τ_x – is the required force on the ship's longitudinal axes,
τ_y – is the required force on the ship's lateral axes,
τ_r – is the required rotational force of the ship,
u – is the derivative longitudinal velocity of the ship,
v – is the derivative lateral velocity of the ship,
r – is the derivative rotational velocity of the ship.

The matrices A, B, C, D in *Equation 1* and *Equation 2* are as follows:

$$A=\begin{bmatrix}-0.0034 & 0 & 0\\0 & -0.0090 & -0.0002\\-0.0030 & -0.0100 & -0.0077\end{bmatrix},$$

$$B=\begin{bmatrix}0.0036 & 0 & 0\\0 & 0.0021 & 1.61e-05\\3e-05 & 1.15e-05 & 0.0080\end{bmatrix},$$

$$C=\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}, D=\begin{bmatrix}0 & 0 & 0\\0 & 0 & 0\\0 & 0 & 0\end{bmatrix}.$$

The kinematics of this system can be presented by *Equation 4* as follows:

$$\begin{bmatrix}\dot{x}\\\dot{y}\\\dot{\psi}\end{bmatrix}=\begin{bmatrix}\cos\psi & -\sin\psi & 0\\\sin\psi & \cos\psi & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}u\\v\\r\end{bmatrix}, \tag{4}$$

where (x,y) denotes the coordinates of the centre of mass of the vessel in the earth-fixed frame, ψ is the heading angle of the vessel, and u, v, r are the velocities of surge, sway and yaw, respectively.

Next, the centre of mass coordinates and heading angle are obtained by the integration *Equation 5*:

$$x(\tau)=\int_0^\tau \dot{x}(t)\,dt, y(\tau)=\int_0^\tau \dot{y}(t)\,dt, \psi(\tau)=\int_0^\tau \psi(t)\,dt, \tag{5}$$

where initial state $x(0)=0, y(0)=0, \psi(0)=0$.

We can see from *Equation 1–Equation 5* that the vector $(x,y,\psi)^T$ of the MASS can be computed based on given equations and initial conditions.

4.1 PID control system

The Proportional–Integral–Derivative (PID) controller is designed to ensure the smoothness and safety of the MASS's trajectory during a manoeuvre such as the proposed approach to the berth. The control system configuration for the MASS model to regulate the input variable U using PID controllers is designed to have the following structure (see *Figure 2*). The references $u_d = 0.05\ \frac{m}{s}, v_d = 0.05\ \frac{m}{s}, r_d = -0.003\ \frac{rad}{s}$ for system of *Equation 1–Equation 2* were applied during this manoeuvre. Although PID controllers exist in many forms, one possible implementation is given by the following compensator formula *Equation 6*:

$$PID(s)=K_P+K_I\left(\frac{1}{s}\right)+K_D\left(\frac{K_N}{1+K_N\left(\frac{1}{s}\right)}\right) \tag{6}$$

where $PID(s)$ is the transfer function, and K_P, K_I, K_D, K_N are proportional, integral and derivative filter coefficients of continuous-time parallel-form PID controller, respectively.

The fixed K_P, K_I, K_D, K_N parameters from *Equation 6*, which are used to tune the three controllers to a desired behaviour, are obtained by using Simulink software for tuning as follows:

$$K_{P1} = 1.2415, K_{I1} = 0.0083, K_{D1} = -13.4187,\ K_{N1} = 0.0127;$$

$$K_{P2} = 6.0052, K_{I2} = 0.1084, K_{D2} = -22.7713, \ K_{N2} = 0.0444;$$

$$K_{P3} = 1.3459, K_{I3} = 0.0209, K_{D3} = -5.3248, \ K_{N3} = 0.0385.$$

The simulation tasks for the output signals are explained in *Figures 3, 4 and 5*. The resulting XY graph of MASS's motion is shown in *Figure 6*. Note that good quality of control was achieved. The MASS makes a slow and smooth approach to the berth and mooring can be easily accomplished.

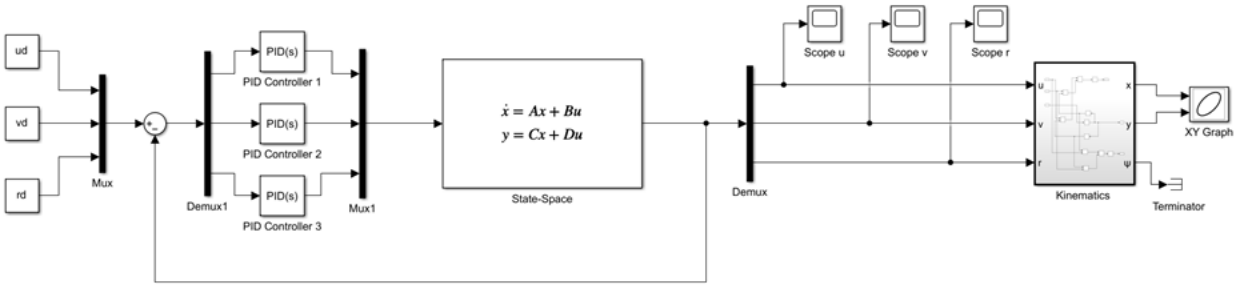

Figure 2 – Simulink-style block diagram of MASS with PID controllers without disturbances

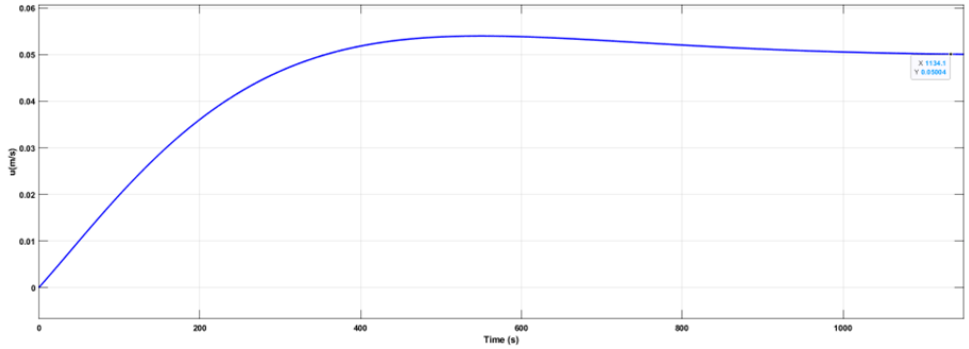

Figure 3 – Surge rate of MASS without disturbances

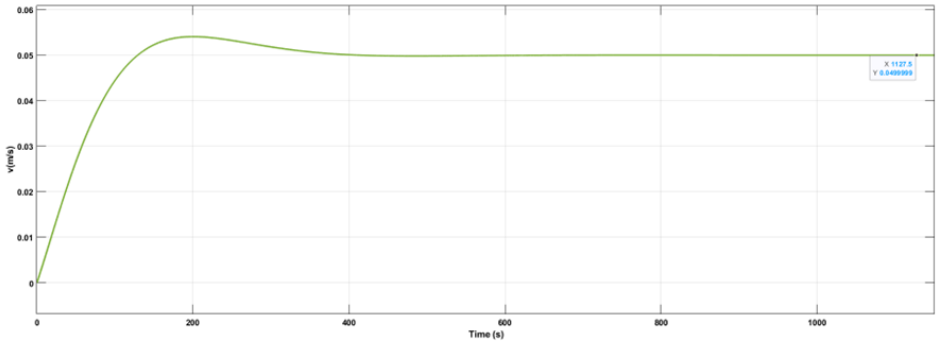

Figure 4 – Sway rate of MASS without disturbances

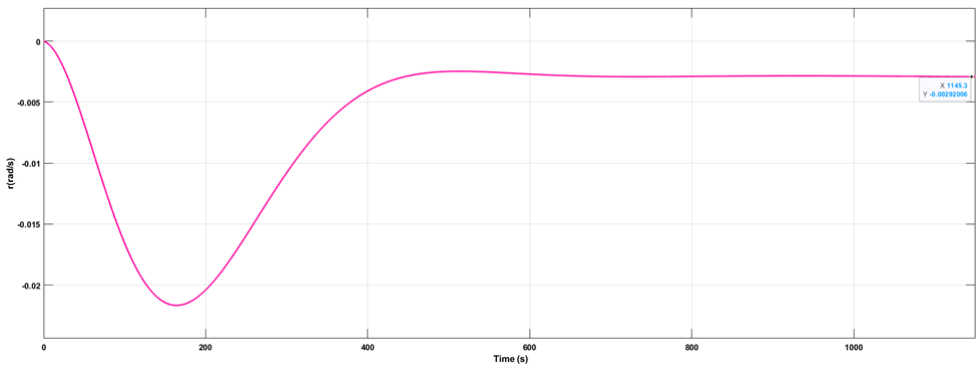

Figure 5 – Yaw rate of MASS without disturbances

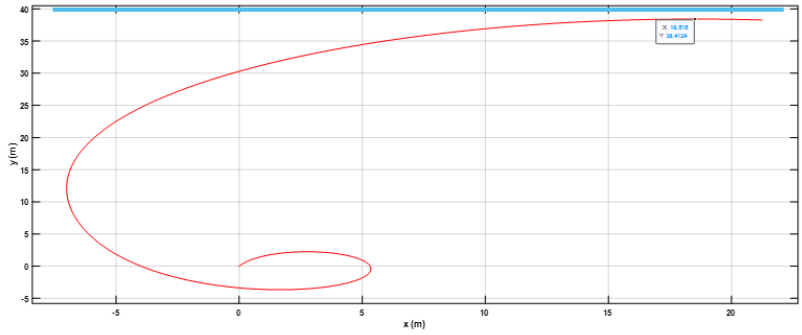

Figure 6 – Trajectory of MASS without disturbances

4.2 Simulation of a cyber-attack

The adversary can attack the system on any control system component. This attack is propagated through the control system and modifies the value of the control signal in some random manner. The effect of a cyberattack can be modelled by adding the Gaussian white noise to any control system component. The actual measurement vector Y_a is related to the desired output vector Y_d with V as a measurement noise vector, so it follows:

$$Ya(\tau)=Yd(\tau)+V(\tau) \tag{7}$$

Consider now a feedback system with a disturbance vector W occurring at the input side of the plant as illustrated in *Figure 7*.

$$Ua(\tau)=Ud(\tau)+W(\tau) \tag{8}$$

The control system configuration is the same as considered before, i.e. it is based on PID controllers (*Figure 7*). The references $u_d = 0.05\frac{m}{s}$, v_d=0.05 $\frac{m}{s}$, $r_d = -0.003\frac{rad}{s}$, the white noise powers $P_W=10^{-7}$, P_V=0.3 from *Equation 7–Equation 8* for system *Equation 1–Equation 2* were applied during this manoeuvre.

The white noise caused by a cyber-attack is much higher than the typical white noise present, so the white noise power level chosen for the input is much higher than the typical quantisation noise. Typical quantisation noise is generally assumed to be zero-mean, uniformly distributed white noise that is uncorrelated with the input signal. The signal-to-quantisation noise ratio (SQNR) can be calculated as in [51].

When the SQNR is desired in terms of decibels (dB), a useful approximation to SQNR is as follows:

$$SQNR=P(x^{\nu})+6.02\nu+4.77$$

where P (x^ν) is the signal power, ν is the number of bits in a quantised sample. Note that for each bit added to a sample, the SQNR goes up by approximately 6 dB.

Generally, quantisation noise can be, and should be, kept below the other noise sources in amplitude. Eight-bit digitisers are quite common, and this puts the quantisation noise level (1/256) below 0.5% of the total dynamic range.

Noisy output signals are shown in *Figures 8–10*. The XY graph of MASS's motion is shown in *Figure 11*. In such conditions, the MASS makes chaotic movements and becomes uncontrollable. Thus, MASS blocks the berth and creates a risk of sliding collisions with other ships.

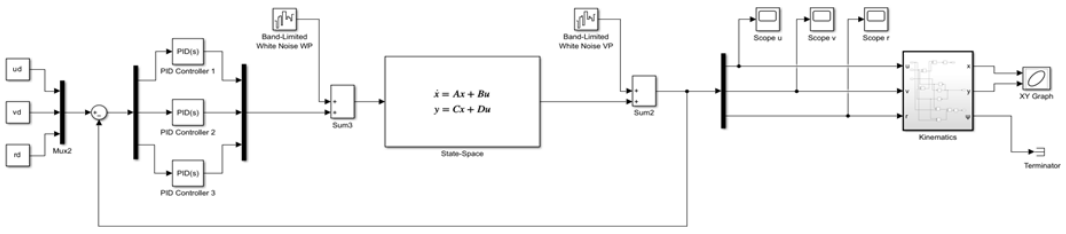

Figure 7 – Simulink-style block diagram of MASS with PID controllers with disturbances

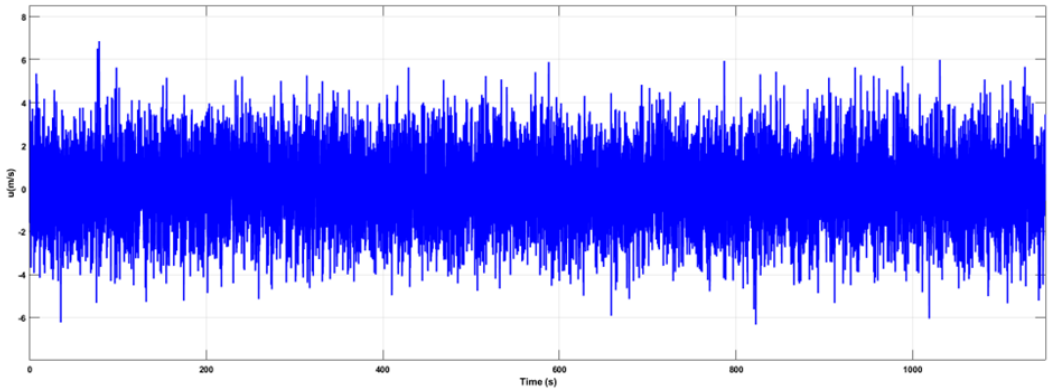

Figure 8 – Surge rate of MASS with disturbances

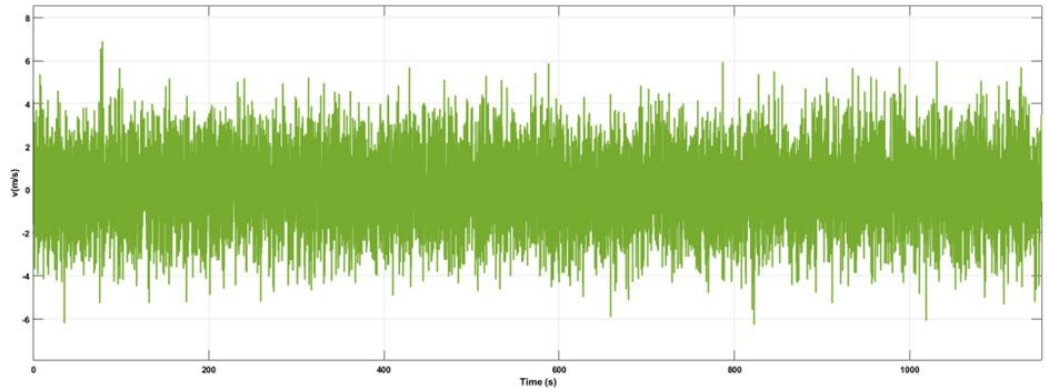

Figure 9 – Sway rate of MASS with disturbances

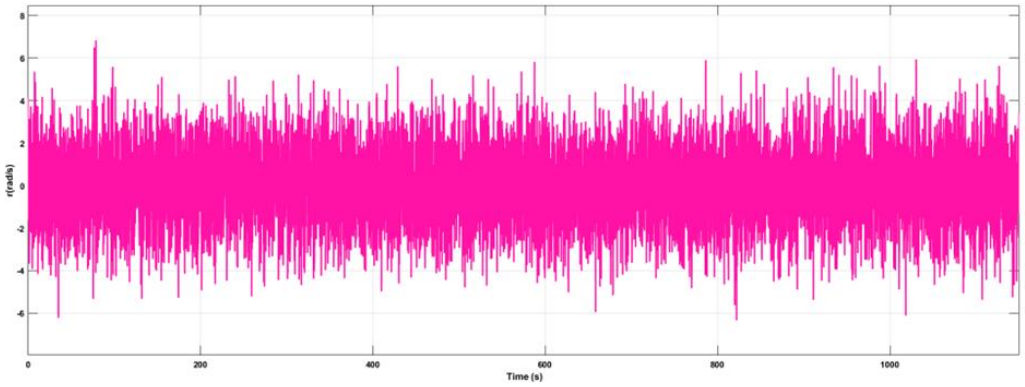

Figure 10 – Yaw rate of MASS with disturbances

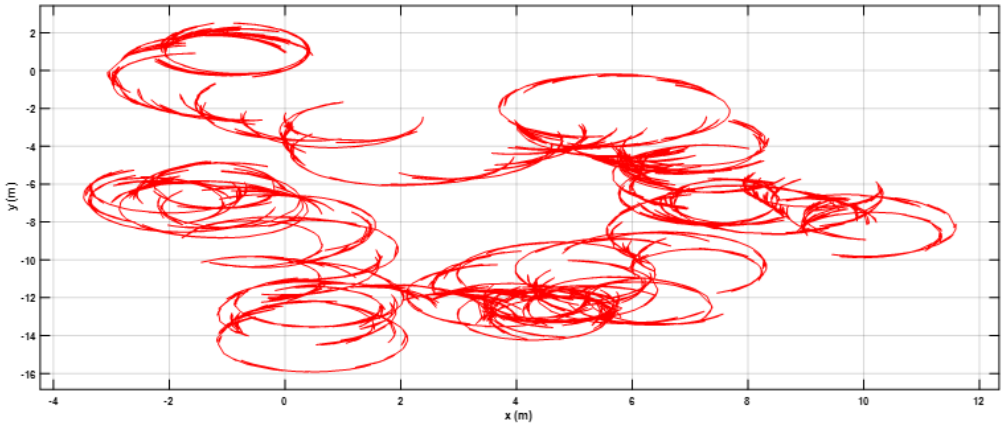

Figure 11 – Trajectory of MASS with disturbances

Trajectory of MASS with disturbances (see *Figure 11*) demonstrates the simulation result for the control system activity (see *Figure 7*) in noises conditions for chosen model of MASS.

4.3 Simulation of a cyber-attack prevention

The control system configuration is the same as considered before, i.e. it is based on the usage of PID controllers with the addition of a Kalman filter (*see Figure 12*).

The references u_d=0.05$\frac{m}{s}$,v_d=0.05$\frac{m}{s}$, $r_d = -0.003\frac{rad}{s}$, the white noise powers P_W=10^{-7}, P_V=0.3 from *Equation 7–Equation 8* for system *Equation 1–Equation 2* were applied during this manoeuvre.

The Kalman filter matrix gain L is designed so that the continuous, stationary Kalman filter:

$$\dot{X}_e = AX_e + BU + L(Y - CX_e - DU) \tag{9}$$

produces an optimal estimate X_e of vector X. The matrix L in *Equation 9* is calculated as follows:

$$L = 1e\text{-}4 \times \begin{bmatrix} 0.4922 & 0.0020 & -0.1336 \\ 0.0020 & 0.1875 & -0.1169 \\ -0.1336 & -0.1169 & 0.4162 \end{bmatrix} \tag{10}$$

Filtered output signals by the Kalman filter are presented in *Figures 13–15*. The trajectory of MASS with Kalman filtering is shown in *Figure 16*.

The usage of the Kalman filter demonstrates the ability to reduce the impact of noises caused by the influence of simulated cyberattacks on the MASS with a slight decrease in control quality.

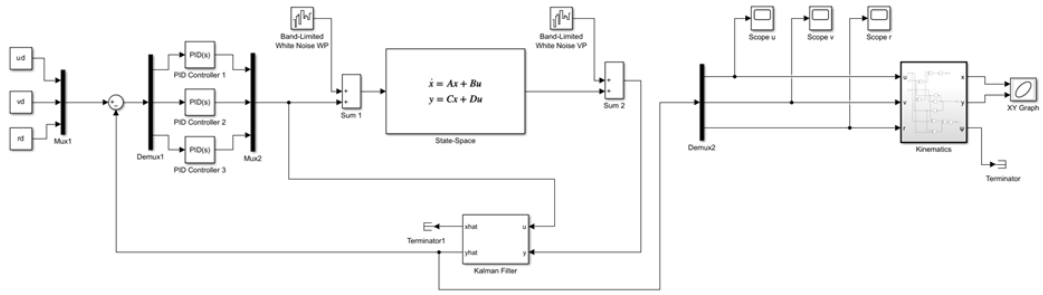

Figure 12 – Simulink-style block diagram of MASS with PID controllers with Kalman filtering

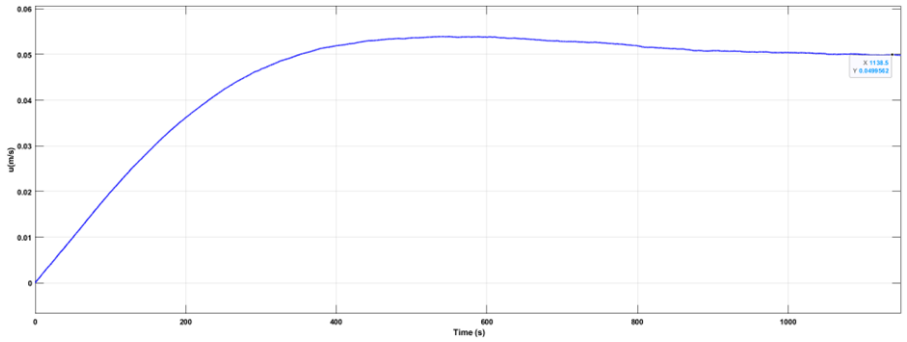

Figure 13 – Surge rate of MASS with Kalman filtering

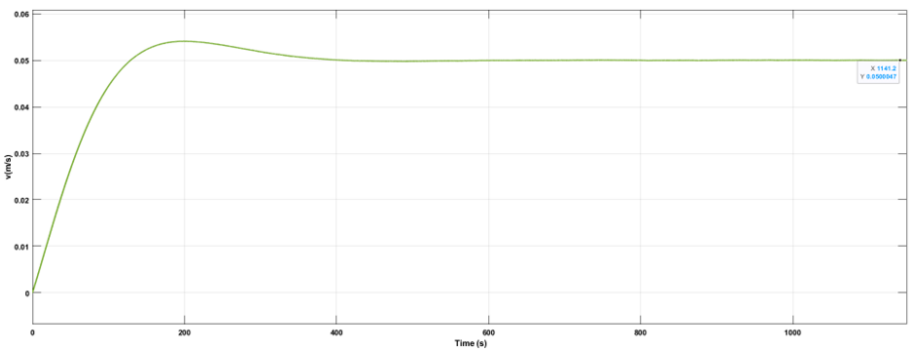

Figure 14 – Sway rate of MASS with Kalman filtering

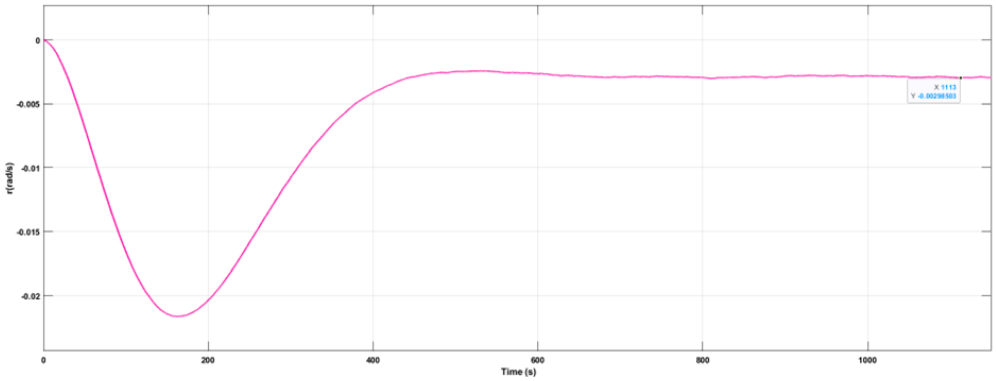

Figure 15 – Yaw rate of MASS with Kalman filtering

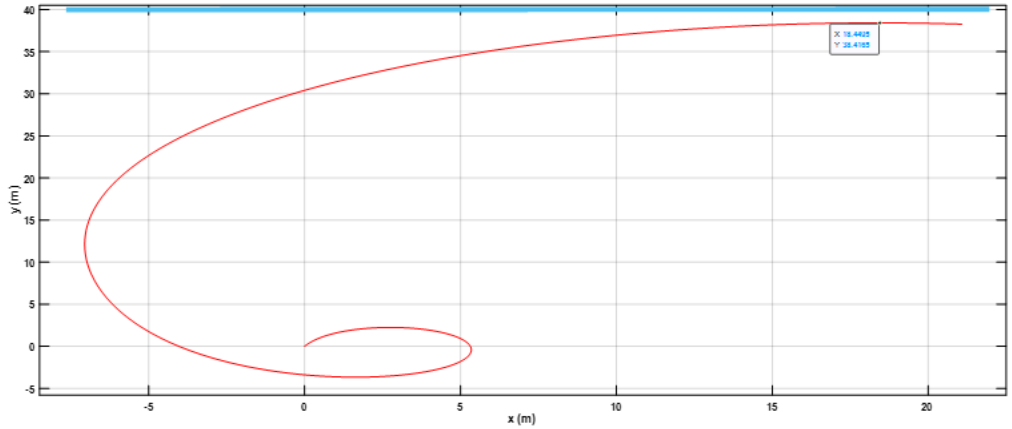

Figure 16 – Trajectory of MASS with Kalman filtering

The results of the error compensation of the controller are shown in *Table 1*.

Table 1 – Control errors' compensation

Control error	Ideal system without noise	Noisy system with Kalman filter
Surge rate (*see Figure 3*)	Y=0.05004	(0.05-Y)/0.05= -0.08 %
Surge rate (*see Figure 13*)	Y=0.0499562	(0.05-Y)/0.05= 0.0876 %
Sway rate (*see Figure 4*)	Y=0.0499999	(0.05-Y)/0.05=0.0002 %
Sway rate (*see Figure 14*)	Y=0.0500047	(0.05-Y)/0.05=-0.0094 %
Yaw rate (*see Figure 5*)	Y=-0.00292006	(-0.003-Y)/-0.003 =2.66466 %
Yaw rate (*see Figure 15*)	Y=-0.00298503	(-0.003-Y)/-0.003 = 0.499 %

The data clearly shows that the Kalman filter and the optimisation of the system parameters have achieved a sound improvement of the system, as it is normal for the relative control error not to exceed 5%.

5. CONCLUSIONS

This paper provides an overview of MASSs used for research, commercial and military purposes. The advantages of these vessels are highlighted, as well as their disadvantages, with an emphasis on cyber-

resilience. A concise overview of the most commonly used methods for risk assessment and cyberattacks prevention is also provided. Experience has shown that the most frequent target of cyber-attacks is the navigation system of vessels, so some attention is being paid to hybrid navigation methods that can be applied in the event of satellite navigation signal corruption. The emphasis has been put on using inertial navigation, which is also susceptible to cyberattacks, to provide the best vessel guidance when satellite navigation is not available. By simulating a SCADA cyber-attack on the thruster controllers' input and output of the autonomous research vessel "Nymo", designed and created by the Tallinn University of Technology and a start-up company MindChip experts, we explored the consequences and proposed attack mitigation measures by adjusting the Kalman filter parameters. More precisely, MATLAB Simulink was used to simulate a SCADA testbed cyber-attack during a manoeuvre such as the MASS's approach to the berth. The control system for the MASS is designed so that the vessel can remain close to the desired course when exposed to cyber-attacks simultaneously on the input and output of the thrusters' control circuit. This control system contains the three PID controllers and a Kalman filter as its main elements and demonstrates high efficiency for the selected manoeuvre.

The developed simulation model of cyberattacks on a given model of the MASS presents an important part of the development of software for the optimal control and exploitation of the autonomous vessel. Further studies should be conducted in different environmental conditions, simulating cyber intrusions, through varying noise types and levels, while paying special attention to the effects of wind and currents.

ACKNOWLEDGEMENTS

Research for this publication was funded by the EU Horizon2020 project 952360-MariCybERA.

REFERENCES

[1] James FA, Ioannis C. Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS). *Frontiers in Computer Science*. 2023;5. DOI: 10.3389/fcomp.2023.1151188.

[2] Bauk S, et al. Autonomous marine vehicles in sea surveillance as one of the COMPASS2020 project concerns. *Journal of Physics: Conference Series*. 2019;1357. DOI: 10.1088/1742-6596/1357/1/012045.

[3] Astrov I, et al. Simulink/MATLAB based comparison of neural and basic tracking control for an autonomous surface vessel for situation awareness applications. *Proceedings of the IEEE Joint 19th International Symposium on Computational Intelligence and Informatics and 7th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics 2019, 14-16 Nov. 2019, Szeged, Hungary*. 2019;105–110. DOI: 10.1109/CINTI-MACRo49179.2019.9105230.

[4] Astrov I, et al. Target tracking by neural predictive control of the autonomous surface vessel for environment monitoring and cargo transportation applications. *Proceedings of the 17th Biennial Baltic Electronics Conference 2020, 6-8 Oct. 2020, Tallinn, Estonia*. 2020;1-4. DOI: 10.1109/BEC49624.2020.9277115.

[5] Chang CH, et al. Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety*. 2021;207:107324. DOI: 10.1016/j.ress.2020.107324.

[6] Dupont B, et al. The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*. 2023;132:103372. DOI: 10.1016/j.cose.2023.103372.

[7] Udal A, et al. Modeling the trajectory tracking accuracy of an autonomous catamaran patrol vessel under different positional data disturbance conditions. *Proceedings of the 10th Maritime Transport Conference 2024, 5-7 June 2024, Barcelona, Spain*. 2024;1-15. DOI: 10.5821/mt.13165.

[8] Astrov I, Bauk S. Simulating a cyber-attack on an autonomous sea surface vessel's rudder controller. *Proceedings of the 13th Mediterranean Conference on Embedded Computing 2024, 11-14 June 2024, Budva, Montenegro*. 2024;558-564.

[9] Pietrzykowski Z, Hajduk J. Operations of maritime surface ships. *TransNav – The International Journal on Maritime Navigation and Sea Transportation*. 2019;13(4):725-733. DOI: 10.12716/1001.13.04.04.

[10] Sahoo A, Dwivedy SK, Robi PS. Advancement in the field of autonomous underwater vehicle. *Ocean Engineering*. 2019;181:145-160. DOI: 10.1016/j.oceaneng.2019.04.011.

[11] Bauk S, Kapidani N, Boisgard JP, Lukšić Ž. (2021). Key features of the autonomous underwater vehicles for marine surveillance missions. In: Bauk S, Ilčev SD (eds) *The 1st International Conference on Maritime Education and Development*. Springer, Cham. DOI: 10.1007/978-3-030-64088-0_7.

[12] Van Brummelen J, et al. Autonomous vehicle perception: The technology of today and tomorrow. *Transport Research Part C*. 2018;89(2018):384-406. DOI: 10.1016/j.trc.2018.02.012.

[13] Wingrove M (June 4, 2024). One year to go for IMO non-mandatory MASS Code. https://www.rivieramm.com/news-content-hub/news-content-hub/one-year-to-go-for-imo-non-mandatory-mass-code-81022#:~:text=IMO%20is%20writing%20a%20legislative,on%20the%20progress%20to%20date [Accessed on 6th September 2024].

[14] Meadow G, et al. Autonomous shipping – Putting the human back in the headline. IMarEST. Report number: 2018:1, 2018. DOI: 10.13140/RG.2.2.18628.37768.

[15] Lloyd's Register. ShipRight design and construction. Additional Design Procedures. LR Code for Unmanned Marine Systems. 2017.

[16] Yara (n.d.). MV Yara Birkeland. https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/ [Accessed on 26th June 2024].

[17] Skopljak N (September 19, 2023). SEA-KIT one step closer to developing first type-approved USV control system. https://www.offshore-energy.biz/sea-kit-one-step-closer-to-developing-first-type-approved-usv-control-system/ [Accessed on 26th June 2024].

[18] Congressional Research Service (December 30, 2023). Navy large unmanned surface and undersea vehicles: Background and issues for congress. https://sgp.fas.org/crs/weapons/R45757.pdf [Accessed on 26th June 2024].

[19] Baird Maritime (March 31, 2023). Vessel Review: Zhu Hai Yun – Chinese-built drone mothership boasts autonomous sailing systems. https://www.bairdmaritime.com/work-boat-world/specialised-fields/marine-research-and-training/vessel-review-zhu-hai-yun-chinese-built-drone-mothership-boasts-autonomous-sailing-systems/ [Accessed on 26th June 2024].

[20] Yellig J (June 14, 2023). Myflower autonomous ship makes unmanned Atlantic crossing. https://www.iotworldtoday.com/transportation-logistics/mayflower-autonomous-ship-makes-unmanned-atlantic-crossing#close-modal [Accessed on 26th June 2024].

[21] Korean Research Institute of Ships & Ocean Engineering (n.d.). Korea autonomous surface ship project detail. https://kassproject.org/en/info/projectdetail.php [Accessed on 27th June 2024].

[22] Rolls-Royce. Autonomous ships – The next step. 2016. https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/%20customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf [Accessed on 26th June 2024].

[23] Ship Technology (April 13, 2016). Rolls-Royce reveals vision of remote and autonomous shipping through AAWA project latest findings. https://www.ship-technology.com/news/newsrolls-royce-reveals-vision-of-remote-and-autonomous-shipping-through-aawa-project-latest-findings-4863708/?cf-view [Accessed on 26th June 2024].

[24] Homepage of MindChip OÜ, a spin-off company of Tallinn University of Technology. https://mindchip.ee [Accessed on 27th June 2024].

[25] Kessler GC, Shepard SD. Maritime Cybersecurity – A guide for leaders and managers. Printed in Great Britain by Amazon, 2022 (ISBN: 9798412526034).

[26] GPS World (Tracy Cozzens, 12 February 2020), ADVA tackles GNSS jamming and spoofing with AI solutions. https://www.gpsworld.com/adva-tackles-gnss-jamming-and-spoofing-with-ai-solution [Accessed on 27th June 2024].

[27] Kjerstad N. Electronic and acoustic navigation systems. NTNU, Ålesund, Norway, 2016 (ISBN: 9788292186572).

[28] EUSPA (n.d.). About EGNOS. https://egnos-user-support.essp-sas.eu/egnos-system/about-egnos [Accessed on 25th June 2024].

[29] Bauk S, et al. Satellite navigation systems' vulnerabilities and alternative solutions. Esti Laevanduse Aastaraamat 2024, p. 85-88. https://www.apollo.ee/eesti-laevanduse-aastaraamat-2024 [Accessed on 27th June 2024].

[30] Wired (Matt Burgess, 21 September 2017). When a tanker vanishes, all the evidence points to Russia. https://www.wired.co.uk/article/black-sea-ship-hacking-russia [Accessed on 26th June 2024].

[31] EUSPA (29 September, 2023). ASGARD: The ultimate response to maritime spoofing attack. https://www.euspa.europa.eu/newsroom/news/asgard-ultimate-response-maritime-spoofing-attacks [Accessed on 27th June 2024].

[32] Björck F, et al. Cyber resilience - Fundamentals for a definition. *Advances in Intelligent Systems and Computing*. 2015;353:311–316. DOI:10.1007/978-3-319-16486-1_31.

[33] Roland TL. A warranty of cyberworthiness. *IEEE Security and Privacy*. 2004;2:73-76. DOI:10.1109/MSECP.2004.1281252.

[34] Chaal M, et al. Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety Science*. 2023;167:106256. DOI: 10.1016/j.ssci.2023.106256.

[35] Wróbel K, et al. System-theoretic approach to safety of remotely-controlled merchant vessel. *Ocean Engineering*. 2018;152:334-345. DOI: 10.1016/j.oceaneng.2018.01.020.

[36] Wróbel K, et al. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliability Engineering & System Safety*. 2018;178:209-224. DOI: 10.1016/j.ress.2018.05.019.

[37] Jones B, et al. The use of Bayesian network modelling for maintenance planning in a manufacturing industry. *Reliability Engineering & System Safety*. 2010;95(3):267-277. DOI: 10.1016/j.ress.2009.10.007.

[38] Ahn G, et al. Research on improving cyber resilience by integrating the zero trust security model with the MITRE ATT&CK matrix. *IEEE Access*. 2024;12:89291-89309. DOI: 10.1109/ACCESS.2024.3417182.

[39] Kujo J. (2023). Implementing zero trust architecture for identities and endpoints with Microsoft tools. Master's thesis. JAMK University of Applied Sciences.

[40] Lim J, Yoo Y. Cyber threat and vulnerability analysis-based risk assessment for smart ship. *Journal of Korean Society of Marine Environment & Safety*. 2024;30(2):263-274. DOI: 10.7837/kosomes.2024.30.3.263

[41] Kavallieratos G, et al. Cyber-attacks against the autonomous ship. In: Katsikas S., et al. Computer Security. SECPRE CyberICPS 2018. Lecture Notes in Computer Science, Vol. 11387, Springer, Cham. DOI: 10.1007/978-3-030-12786-2.

[42] Bolbot V, et al. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection. 2022;39:100571. DOI: 10.1016/j.ijcip.2022.100571.

[43] Ding J, et al. CPS-based threat modeling for critical infrastructure protection. *SIGMETRICS Perform. Eval. Rev*. 2017;45(2):129–132. DOI: 10.1145/3152042.3152080.

[44] SI-SCADA International (2024). What does SCADA stand for? https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for,data%20from%20the%20industrial%20equipmen. [Accessed on 3rd September 2024].

[45] CWE (March 22, 2024). Common weakness enumeration. https://cwe.mitre.org/about/index.html [Accessed on 3rd September 2024].

[46] Astrov I, et al. An optimal control method for an autonomous surface vessel for environment monitoring and cargo transportation applications. *Proceedings of the IEEE 25th International Conference ELECTRONICS 2021, 14-16 June 2021, Palanga, Lithuania*. 2021;1–6. DOI: 10.1109/IEEECONF52705.2021.9467483.

[47] Astrov I, et al. Wind force model and adaptive control of catamaran model sailboat. *Proceedings of the 8th International Conference on Automation, Robotics and Applications 2022, 18-20 Feb. 2022, Prague, Czech Republic*. 2022;202–208. DOI: 10.1109/ICARA55094.2022.9738524.

[48] Astrov I, et al. Experimentally adjusted modelling and simulation technique for a catamaran autonomous surface vessel. *Proceedings of the IEEE 2nd International Conference on Electrical, Computer and Energy Technologies 2022, 20-22 July 2022, Prague, Czech Republic*. 2022;1-7. DOI: 10.1109/ICECET55527.2022.9873069.

[49] Astrov I, Astrova I. A model-based adaptive control of turning maneuver for catamaran autonomous surface vessel. *WSEAS Transactions on Systems and Control*. 2024;19:135-142. DOI: 10.37394/23203.2024.19.14.

[50] Gierusz W, Rybczak M. Effectiveness of multidimensional controllers designated to steering of the motions of ship at low speed. *Sensors*. 2020. Vol. 20, June 2020, 3533. DOI: 10.3390/s20123533.

[51] Lathi BP. Modern digital and analog communication systems (3rd ed.). Oxford University Press, 1998 (ISBN: 9780195110098).

Игорь Астров, Саня Баук

Моделирование кибератаки на контроллеры двигателей судов с автономной навигацией при движении с малой скоростью

АННОТАЦИЯ

Целью данной статьи является объяснение восприимчивости автономной навигации судов к кибератакам и иллюстрация на примере моделирования, как можно смягчить кибератаку на контроллеры двигателей судов с автономной навигацией при движении с малой скоростью. Первая часть статьи будет основана на обзоре соответствующих статей в этой области, которые будут включать некоторые проекты автономной навигации судов, связанные с ними киберугрозы и методы моделирования для повышения киберустойчивости. Вторая часть статьи будет иллюстрировать кибератаку на контроллеры двигателей судов с автономной навигацией при движении с малой скоростью вместе с воздействием атаки на траекторию движения. Фильтр

Калмана, как дополнительное устройство к контроллерам двигателей, используется в качестве средства смягчения кибератак. В условиях имитационного воздействия на входные и выходные сигналы двигателя эксперименты, проведенные в среде MATLAB/Simulink, позволяют получить представление о поведении подсистемы движения судов с автономной навигацией с точки зрения низкоскоростной траектории с фильтром Калмана и без него.

КЛЮЧЕВЫЕ СЛОВА
Автономная навигация судов; двигатель; кибератака; метод пространства состояний; ПИД-регулятор; фильтр Калмана.