

Ensuring steganosystem robustness in the cyber-physical control loop of a maritime autonomous surface vessel as a necessary condition for its functioning *

Alla Kobozieva^{1,†}, Kateryna Tryfonova^{1,†}, Olena Lebedieva^{1,†}, Viktoriya Zorilo^{1,†}

¹ Odesa National Maritime University, Mechnikova str. 34, Odesa, 65029, Ukraine

Abstract

Historically, priority in the maritime industry was given to means of ensuring the purely physical and navigational safety of vessels, while cybersecurity issues were regarded as secondary. The consequence of such systemic complacency toward cybersecurity was a cascade of devastating cyberattacks on the critical infrastructure of the global fleet and seaports. The problems of ensuring information and cybersecurity in the field of autonomous shipping are acquiring decisive relevance. Today, information and cybersecurity constitute the primary, foundational element of the overall survivability of MASS, without which the practical operation of an unmanned fleet is impossible. Among all areas of cybersecurity for autonomous shipping, steganography occupies a special place, since here the control command from the shore-based control center is the sole source of decision-making in an off-nominal situation, and concealing the fact of its transmission is critically important. The properties of the covert (steganographic) communication channel are determined by the properties of the underlying steganosystem, for which one of the primary requirements is that of robustness. The existing robustness criteria of a steganosystem have been formulated without accounting for the specificity of its use as part of a real-time cyber-physical system. The objective of this study is to ensure the possibility of designing a robust steganosystem for use as part of a cyber-physical control system for an autonomous vessel, through the creation of a complete system of robustness criteria that accounts for detection vectors specific to the steganographic channel within this particular domain of application. This objective was achieved by determining the criterion of steganosystem robustness of highest priority for MASS, and by identifying additional criteria of steganosystem robustness specific to its application under MASS conditions. The most significant outcome of this study is the development and scientific substantiation of a methodological basis for constructing high-speed, real-time steganosystems capable of integration into the deterministic cyber-physical control loops of MASS.

Keywords

cybersecurity, maritime autonomous vessel, steganosystem, steganosystem robustness, cyber-physical system

1. Introduction

The maritime industry constitutes a foundation of the state's geopolitical sovereignty, defense capability, and national security, while also serving as the main artery of global supply chains and international trade, thereby designating its transport infrastructure and fleet as strategic assets of the highest priority, upon whose uninterrupted operation the vital functioning of the country critically depends.

Historically, the maritime industry has exhibited a high degree of conservatism, with priority traditionally given exclusively to the physical and navigational safety of vessels. For a considerable period, the pace of maritime digitalization outpaced the development of robust information security

* ADT-ISMDCC 2026: *Advanced Digital Technologies: Intelligent Systems, Modeling, and Data-Driven Control*, September 22–24, 2026, Odesa, Ukraine

¹ Corresponding author.

[†] These authors contributed equally.

✉ alla_kobozieva@ukr.net (A. Kobozieva); trifonova@op.edu.ua (K. Tryfonova); lebedeva.onmu@gmail.com (O. Lebedieva); vikazorilo@gmail.com (V. Zorilo)

 0000-0001-7888-0499 (A. Kobozieva); 0009-0004-4468-1618 (K. Tryfonova); 0000-0001-5459-0251 (O. Lebedieva); 0000-0002-4802-7347 (V. Zorilo)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

measures, while cybersecurity issues were largely perceived by shipping company management as purely secondary, "office-bound" IT tasks, disconnected from actual technological processes at sea.

On the one hand, the maritime domain can, of course, be regarded as "special" with respect to cyber threats, given its potentially great distances from shore and its reliance on long-range communication systems and specialized positioning, navigation, and timing tools. On the other hand, the cyber threats themselves, along with the means and methods of cyberattacks, are not unique to this domain [1], yet still require close attention and proactive countermeasures. Crucially, the human factor, as is the case everywhere, plays a fundamental role in the effectiveness of cyberattacks, representing a significant vulnerability for maritime companies [2, 3].

The consequence of such systemic complacency toward cybersecurity manifested in a cascade of devastating cyberattacks on the critical infrastructure of the global fleet and seaports [4]. These incidents resulted in substantial financial losses, estimated in the hundreds of millions of dollars, and demonstrated that the modern vessel operates as a critically vulnerable digital node. At present, it is evident that localized protection of individual computing systems is insufficient, the approach to maritime cybersecurity must be systemic and comprehensive in scope, extending from the physical-layer encryption of onboard sensor signals to global satellite-based control loops.

Concurrently, a certain interdisciplinary gap can be observed within the scholarly-practical domain [5]. Contemporary cybersecurity specialists predominantly operate either in complete isolation from the specificities of the maritime industry, or confine themselves to general declarative theses regarding the "importance of information protection at sea" [6, 7], while attempting to apply standard corporate IT security templates. However, such templates prove ineffective within the specific field of the maritime industry, which is governed by stringent time constraints, unstable satellite communication channels, the complete isolation of the vessel at sea.

The aforementioned factors acquire critical, hypertrophied significance during the transition to maritime autonomous surface ships (MASS). Recent advancements in robotics, information technology, and artificial intelligence have driven the evolution of the transport industry toward intelligent transport systems, of which autonomous vessels constitute one of the components [8]. On the one hand, the emergence of maritime autonomous surface ships creates opportunities to reduce both capital and operational expenditures, as well as to reduce environmental impact through the use of eco-friendly technologies. On the other hand, it increases the urgency of addressing a range of problems, including technical issues associated with MASS operation: encompassing questions of safety in the operation of conventional vessels, the emergence of new risks related to port security, failures of onboard equipment or communication systems, errors associated with information exchange, and the inadequate provision of information and cybersecurity [8, 9]. The latter issue is of particular relevance. Until recently, the vector of research in the field of autonomous shipping was almost entirely oriented toward solving problems of physical safety (navigation, automated collision avoidance with other vessels, and obstacle avoidance). However, at the current stage of development, such an approach is not merely methodologically obsolete, but hazardous. The transition to higher levels of autonomy has transformed the vessel from a purely mechanical object into a highly integrated cyber-physical system that is critically dependent on continuous data streams (incoming sensor information and external control commands). The possible complete absence of an onboard crew deprives the system of the "last line" of manual defense, making any unauthorized informational interference (attacks on communication channels, coordinate spoofing, or telemetry modification) a trigger for the cascading destruction of the vessel's physical security [10].

Thus, information and cybersecurity today constitute the primary, foundational element of the overall survivability of MASS, without which the practical operation of an unmanned fleet is simply impossible. Today, the physical safety of an autonomous vessel is merely a derivative of its

information security. The vessel sails if the data is protected, if the data is compromised, the vessel perishes.

The relevance of this research is significantly heightened by the entry into force, as of July 1, 2026, of the International Code of Safety for Maritime Autonomous Surface Ships (IMO MASS Code). This foundational instrument establishes for the first time at a global level the requirement that digital connectivity, software reliability, and cybersecurity are inseparable elements of a vessel's overall survivability.

The MASS Code did not emerge in isolation. With regard to cybersecurity, it directly references the primary current resolution of the International Maritime Organization (IMO) on cyber risk management – Maritime Cyber Risk Management in Safety Management Systems. Resolution MSC.428(98), adopted on 16 June 2017 [11], thereby duplicating the already outdated methodology of the Resolution, which was developed for conventional crewed vessels and did not account for the specific characteristics of real-time autonomous AI-driven control, as a result, the MASS Code currently fails to offer concrete, practical solutions in the field of cybersecurity, despite their critical relevance and importance.

Another foundational instrument that contributed to the cybersecurity component of the MASS Code is the Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2 (2022) [12], which states that risk management, including cyber risk management in particular, is of fundamental importance for safe and secure shipping operations, a matter closely tied to the industry's growing reliance on digitalization, integration, automation, and networked systems. However, the document itself is of a declarative, recommendatory character.

Because the MASS Code is based on a Goal-Based Framework and does not prescribe specific engineering solutions, a severe methodological vacuum has emerged within the maritime community. Specifically, existing cybersecurity standards fail to account for the cascading impact of minor information perturbations (such as micro-anomalies in sensor data or covert interference in satellite communication channels) on the vessel's physical trajectory. This necessitates the development of new mathematical approaches, and the adaptation of existing ones, to verify the integral stability of autonomous vessels' information security systems in accordance with IMO requirements.

Among all directions of cybersecurity for autonomous shipping, steganography occupies a special place, which is due to the unique specificity of an autonomous vessel as an object of protection. Unlike a crewed vessel, where the loss or compromise of a control command can often be compensated for by the crew's decision on site, an autonomous vessel is frequently deprived of this possibility, especially in the case of a fully unmanned vessel – the control command from the shore control center is the sole source of decisions in an emergency situation.

In practice, this generates a fundamentally new requirement for the security of the control channel: it is necessary to conceal the very fact of communication, since an adversary monitoring the communication link, upon detecting control traffic, acquires the capability to destroy or spoof it, with direct consequences for the safety of the vessel, cargo, and the environment.

It should be noted that covert channels in the maritime environment are already a reality [13], but so far predominantly as a tool of the adversary: studies demonstrate the feasibility of covert channels based on the Automatic Identification System (AIS) for organizing attacks on maritime infrastructure. This only underscores the relevance of a symmetrical application of steganographic methods in the interest of protecting the control channel of an autonomous vessel.

The steganographic channel [14], which ensures the concealment of the fact of control information transmission, is the most adequate response to this specific threat, which determines the relevance of steganography as an independent direction of cybersecurity for autonomous shipping.

The properties of the organized covert (steganographic) communication channel will be determined by the properties of the underlying steganographic system. One of the main requirements for a steganosystem is the requirement of robustness, which here has multiple components [15-17]. However, the totality of all these components is not exhaustive, and therefore is not guaranteed to be sufficient to ensure the robustness of the steganosystem in MASS. Existing robustness criteria for steganosystems have been formed without accounting for the specifics of their use as part of a real-time cyber-physical system. The strict temporal regulation of information flows in autonomous vessel control systems, as well as the likely, with high probability, automated nature of container generation for covert transmission of control information, open up new vectors for detecting the steganographic channel that are not covered by existing robustness criteria. A steganographic system designed without considering these vectors, without accounting for the comprehensive set of robustness criteria remains vulnerable, in the context of autonomous shipping, this directly entails the compromise of the vessel's control channel, with direct physical consequences.

It is indicative that even among the few specialized studies at the intersection of steganography and MASS protection, such as [18], which proposes concrete algorithmic solutions (in particular, based on chaotic mapping and neural-network encoding), none relies on a unified system of steganosystem robustness criteria. Each such study addresses its own engineering problem in isolation, and this is characteristic not only of MASS protection efforts [19]. The isolated character of such solutions is a consequence of the insufficient methodological maturity of this subject area. In the absence of a unified system of criteria, the robustness of the steganographic channel in each individual solution is determined by its developer, which, in the general case, does not make it possible to establish whether the proposed solution genuinely addresses the full spectrum of MASS-specific threats of steganographic-channel compromise.

The purpose of this work is to enable the design of a robust steganosystem for use as part of a cyber-physical control system of an autonomous vessel, by creating a system of robustness criteria that accounts for the specific detection vectors of the steganographic channel in this application domain. To achieve this goal, the work addresses the following tasks:

1. to determine the highest-priority robustness criterion for a steganosystem for MASS;
2. to determine additional specific robustness criteria for a steganosystem when applied under MASS conditions.

2. Relationships between steganosystem robustness criteria under MASS operational conditions

Let us examine in more detail the existing steganosystem robustness criteria, the block diagram of which is presented in Fig. 1 [15-17]:

- resistance to detection of the fact of existence of hidden information (criterion K_1);
- resistance to extraction of the hidden information (criterion K_2);
- resistance to the imposition of false messages via the steganographic channel (imitation resistance) (criterion K_3);

- resistance to recovery of the steganosystem's secret key (criterion K_4);
- resistance to attacks against the embedded message (criterion K_5).

Ensuring each of these criteria is necessary for a steganosystem used within the structure of MASS. Indeed, if an adversary identifies a specific data stream as a steganographic control channel, they acquire the ability to target it specifically: to block, spoof, or destroy control commands. Criterion K_1 ensures the indistinguishability of the steganographic channel from legitimate traffic, depriving the adversary of the ability to make such an identification, from which follows the necessity of criterion K_1 . Given that control commands constitute critically important information, their disclosure allows the adversary to obtain a complete picture of the vessel operator's intentions and actions, which indicates the necessity of ensuring criterion K_2 . An uncrewed autonomous ship, in the case of a complete absence of a crew, unconditionally executes the commands it receives. The imposition of a false control command directly results in the vessel performing actions in the interest of the adversary. Ensuring criterion K_3 serves to prevent this. Compromise of the steganographic key (Fig. 1) leads to complete compromise of the steganosystem – the adversary knows everything about this system and can undertake both active and malicious actions, which indicates the necessity of ensuring criterion K_4 . Destruction or distortion of a control command under autonomous ship conditions means loss of control, which can have critical negative consequences for its functioning and justifies the necessity of ensuring criterion K_5 . Among the existing set of steganosystem robustness criteria $K=\{K_1, K_2, K_3, K_4, K_5\}$ for ensuring the nominal operation of MASS, the most critical, in the authors' opinion, is K_3 . Let us examine this in detail.

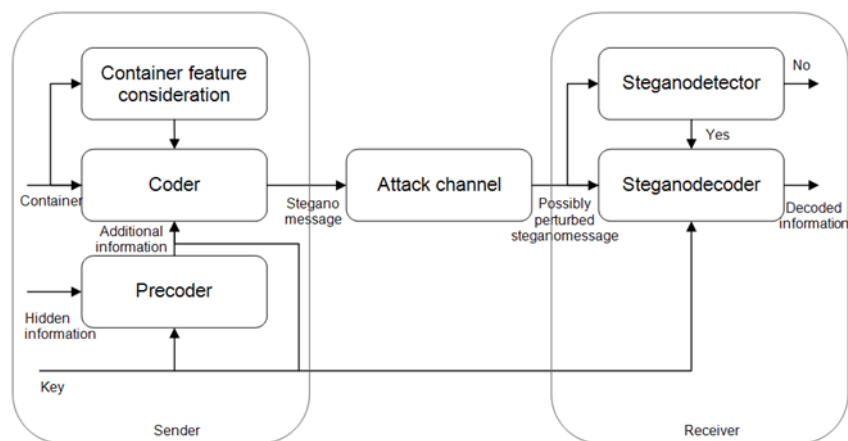


Figure 1: Generalized structural diagram of the steganosystem

The primary methodological distinction between MASS and conventional information systems lies in the fact that it constitutes a cyber-physical object [20]. Here, informational compromise becomes significant when it leads to a change in the vessel's physical state [21]. The risk assessment concept for MASS differs substantially from traditional IT patterns. For a cyber-physical object such as an autonomous vessel, information compromise (including via covert communication channels) is regarded as a critical threat exclusively when it leads to a destructive change in its physical state (motion parameters, trajectory, etc.). If an adversary's information interference does not induce anomalous responses in the actuating mechanisms, such an attack does not breach the object's survivability. In view of this, a comparison of steganosystem robustness criteria $K=\{K_1, K_2, K_3, K_4, K_5\}$ within the specific field of maritime autonomous navigation makes it possible to demonstrate the unconditional priority of the imitation resistance criterion (K_3).

Unlike the criteria K_1 and K_2 , which correspond to a passive adversary, it is specifically the breach of K_3 that leads to the active hijacking of the object's control and an unauthorized alteration of its physical state. The compromise of the key recovery robustness criterion K_4 , which, in accordance

with Kerckhoffs's principle, forms the baseline defense of the steganosystem, establishes the potential possibility of breaches, whereas the destruction of K_3 transforms this possibility into an irreversible physical accident. A violation of K_5 results in a loss of communication (which, as discussed below, may also lead to negative physical consequences), whereas a violation of K_3 leads to the legitimization by the vessel's systems of falsified navigational data.

Remark 1. In order to achieve the objective of this study, a clear distinction must be drawn between the mathematical architecture of the steganosystem and the survivability criteria of MASS as a cyber-physical object. Undoubtedly, from the standpoint of the fundamental theoretical basis of steganography, Kerckhoffs's principle, the key recovery robustness criterion K_4 is determinative (a first-cause criterion): its compromise leads to the complete compromise of the steganosystem. However, in the context of ensuring the security of autonomous shipping, it is specifically K_3 that constitutes the most critical criterion. This is due to the fact that the compromise of K_4 constitutes an informational event (the acquisition of the key by an adversary) which, in itself, does not yet disrupt the vessel's motion or state. By contrast, the destruction of imitation resistance (K_3) constitutes a direct destructive impact (the imposition of false commands), which instantaneously transforms an informational attack into a physical accident.

Remark 2. In order to ensure the objectivity of selecting the highest-priority robustness criterion of the steganosystem for MASS, a distinction must be drawn between the physical consequences caused by the destruction of the hidden message (K_5) and the consequences of a breach of imitation resistance (K_3). A violation of K_5 , in accordance with the requirements of regulatory standards, typically results in the initiation of a safe emergency shutdown protocol, thereby minimizing the risks associated with active maneuvering. By contrast, a breach of imitation resistance (K_3) results in the covert imposition of false information. As a consequence, MASS continues to move actively along a false trajectory, perceiving the destructive commands as legitimate. Accordingly, whereas a violation of K_5 leads to a passive system failure, the compromise of K_3 constitutes a trigger for the active hijacking of control over the object. Thus, it is specifically K_3 that constitutes the most critical robustness criterion of the steganosystem in terms of its consequences for the survivability of MASS. The designation of the imitation resistance criterion (K_3) as the highest-priority criterion in no way negates the necessity of comprehensively ensuring the entire set of security requirements $K=\{K_1, K_2, K_3, K_4, K_5\}$ for MASS. However, in the context of designing and synthesizing complex cyber-physical systems that operate in real time under stringent resource constraints (onboard computational capacity, satellite channel bandwidth, and etc), the task of multi-criteria optimization arises. The presence of a highest-priority criterion makes it possible to define K_3 as the principal mathematical constraint in the synthesis of steganosystems. This means that, when calculating the parameters of a steganosystem, the "mathematical margin" of imitation-protection stability is established as the highest priority. Ensuring K_3 as a primary requirement, already at the model level, reduces the probability of an informational attack transitioning into a physical accident involving MASS.

3. Defining the specific robustness criteria of a steganosystem for application within MASS

The specificity of autonomous shipping as an environment for the application of a steganosystem is determined, above all, by the nature of the information flows into which the hidden information is embedded. Unlike classical steganography application scenarios, in which the choice of container is relatively unconstrained (with the container being either fixed or streaming in nature) and the temporal characteristics of steganomessage transmission are not always critically constrained, a steganosystem operating as part of MASS functions within a strictly deterministic temporal environment. The control protocols of autonomous vessels presuppose strictly regulated data transmission intervals, any deviation from which constitutes a standard indicator of an off-nominal condition and is immediately detected by monitoring systems. Undoubtedly, under real-world MASS

operating conditions (particularly within external satellite communication channels), a degree of fluctuation in the transmission delay of data packets across the network is present – a natural temporal jitter attributable to interference, the specific characteristics of the wave-propagation medium, and similar factors [22, 23]. However, the bounds of this jitter are strictly deterministic. Any micro-deviation from the standard temporal profile (including one induced by steganographic embedding algorithms) is instantaneously detected by monitoring systems as an anomalous delay.

Thus, in order to ensure the non-detectability of the hidden (steganographic) channel, the additional delay introduced by the steganographic transformation process must be smaller than the natural jitter of the network. Otherwise, an adversary monitoring the autonomous vessel's communication channel gains the ability to detect the steganographic channel not through traditional content-based steganalysis (K_1), but through the analysis of the traffic's temporal characteristics – an attack fundamentally distinct from those addressed by the existing robustness criteria, and one specific precisely to a real-time environment governed by strict temporal regulation.

Thus, for a steganosystem employed within the architecture of MASS, an additional, specific robustness criterion is required, hereinafter denoted as K_6 , the criterion of chronometric robustness: the capacity of the steganosystem to perform the steganographic transformation of a given container within the temporal parameters established by the technological process, such that the additional time expenditure does not exceed the bounds of the network's natural time-delay fluctuation and does not generate temporal anomalies detectable by monitoring systems.

Let us examine the relationship between the introduced criterion K_6 and the criterion K_3 , which holds the highest priority for the steganosystem under MASS conditions, from the standpoint of steganosystem synthesis.

To achieve a high degree of imitation resistance (K_3) in a steganosystem, it is, as a rule, natural to employ complex mathematical transformations [24], as well as additional verification procedures in the organization of the hidden channel, however, each additional step increases the processing time of the content [25].

The criterion K_6 imposes temporal boundaries. The "build-up of resistance" in accordance with K_3 can proceed only insofar as the corresponding steganographic algorithm remains within the allotted time limit without generating delays in the vessel's traffic, that is, K_6 functions here as a "regulator and censor" for the mathematical methods by which K_3 is ensured. What must be sought here is a mathematical balance at which a high degree of imitation resistance fully satisfies the requirement of chronometric robustness. Thus, it can be considered that the criterion K_6 serves as the decisive engineering "filter" in the selection of the mathematical apparatus for ensuring K_3 : within the steganosystem, the process that ensures a high degree of imitation resistance must possess low computational complexity.

It should be noted that ensuring low computational complexity in a steganosystem constitutes a general problem in contemporary steganography, given that streaming containers operating in real time are increasingly employed in practice today, however, for a steganosystem forming part of MASS's information security system, this problem becomes pivotal. For classical steganography, whose primary objective is to preserve the secrecy of the existence of the hidden message, the criterion K_1 , resistance to steganalysis, is frequently regarded as the principal one. However, upon closer examination of the conditions under which a steganosystem is applied within MASS's information security system, it becomes evident that stringent temporal constraints may render classical steganalysis not merely difficult for an adversary to perform, but altogether infeasible: under conditions of a real-time streaming container, an adversary is, in all likelihood, unable to carry out classical steganalytic attacks, with the exception of subjective steganalysis, resistance to which requires only ensuring the reliable perceptual quality of the steganomessage – namely, that the

empty container and the steganomessage remain visually indistinguishable. This points to a further distinctive feature of the MASS steganosystem in its practical application: ensuring resistance to steganalysis here loses its priority status, however counterintuitive this may seem at first glance.

Classical steganography categorizes all containers into random, selected, and imposed types. For any steganosystem, the most effective means of satisfying its requirements is afforded by the use of a selected container. The priority accorded to container selection stems from the fact that its internal structure and statistical properties constitute one of the limiting factors for the steganosystem as a whole. To account for this, a "Container Feature Consideration" block has been introduced into the structural diagram of the steganosystem (Fig. 1), although this block is not mandatory, thereby permitting the organization of a covert communication channel using either a random or an imposed container. In general, the nature of the container (its entropy, degree of texturedness, and etc) determines the maximum throughput capacity of the resulting channel, the choice of the mathematical apparatus for data embedding, and the resistance to steganalysis of the corresponding steganomessage. In principle, it is possible to select a container in such a way that, in accordance with the secret key employed, it already contains within its composition additional information – a digital sequence resulting from the operation of the steganosystem's precoder (Fig. 1) without introducing any perturbation of the container during the steganographic transformation. This makes it possible to obtain a steganomessage that cannot be detected by any steganalysis method.

This finding is, today, one that is prompting specialists to devote increasing attention to methods of adaptive and selective steganography [26-28] in the process of obtaining a steganomessage. However, both the selection of the container and the selection of its subregions most suitable for the embedding of the additional information require the expenditure of additional time, which, as already discussed above, is undesirable or indeed infeasible for a steganosystem forming part of MASS's information security system. Consequently, the most suitable approach to container selection here may be its generation by means of AI, taking into account the steganographic key employed and the control information being covertly transmitted, for the sake of concreteness, certain images specific to MASS operations, for example. At present, there exists a considerable probability of obtaining, as the resulting image, a variant that is optimal with respect to the embedded additional information, yet far from optimal with respect to semantic context, for instance, the presence of an object's shadow oriented in an unnatural direction. Analysis of such an image would almost instantaneously reveal the process of its artificial generation, even without recourse to any specialized software tools (for which, evidently, there is no time under MASS operating conditions), and this may be regarded as an indirect indicator of steganographic embedding. Indeed, why else would an autonomous vessel generate such unnatural images in the first place.

The attack under consideration, directed at the semantic plausibility of content, has no analogue in classical steganography, it constitutes an entirely novel type of attack, whose emergence is attributable to the following factors:

- the advent and rapid expansion of AI-generated informational content, which has, in recent times, come to be widely employed as a steganographic container: digital images, digital video;
- the fact that the classical principles of steganalysis were developed prior to the era of AI integration into all spheres of human activity.

Thus, the necessity for semantic analysis of informational content is a direct consequence of the development of AI technologies.

All of the foregoing leads to the necessity of introducing yet another robustness criterion for the steganosystem in the context of its application as a component of MASS's information security

system: the criterion K_7 , defined as resistance to contextual analysis: the impossibility of detecting the existence of a steganographic channel through an analysis of the correspondence between the container/steganomessage and the standard functional processes of the system within which the steganosystem is employed, or with natural physical phenomena (in the case of digital images and digital video). The incorporation of K_7 does not alter the priorities of the existing robustness criteria of the steganosystem within MASS's information security system: K_3 retains the highest priority here, since its violation directly entails the vessel's execution of an adversary's commands, with direct physical consequences, whereas the failure to ensure K_7 constitutes merely a precondition for (possible) subsequent attacks. The final composite set of robustness criteria for the steganosystem within MASS's information security system is presented in Fig. 2.

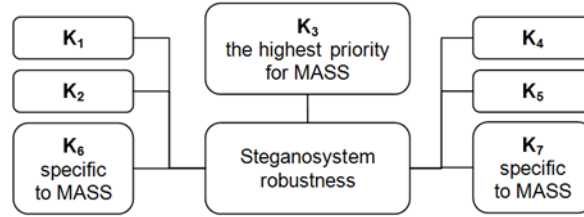


Figure 2: The set of robustness criteria for a steganosystem forming part of MASS's information security system

The incorporation of K_6 and K_7 into the system of steganosystem robustness criteria carries fundamental practical significance for the design of a steganosystem as a component of MASS's information security system. The criteria existing up to this point $K_1, \dots, K_5$ contain no explicit requirements pertaining either to the temporal characteristics of the implementation of the steganographic transformation or to the contextual plausibility of the container/steganomessage within the specific domain of application. This means that a steganosystem formally satisfying all previously existing robustness criteria may nonetheless prove vulnerable to attacks specific precisely to MASS – traffic timing analysis and contextual analysis. It should be noted here that, for a contemporary steganosystem, the criterion K_7 is relevant to any domain of its application, given the widespread use today of AI-generated informational content, for MASS, however, this criterion assumes exceptional importance owing to the exclusion of the possibility of employing adaptive, selective steganography, as discussed above, a consideration which, in this sense, renders it specific to MASS. The newly introduced criterion K_6 obliges the designer to explicitly account for the temporal characteristics of the steganographic transformation and to ensure their conformity with the standard characteristics of the vessel's control protocols – a requirement that, in the absence of an explicit K_6 , could readily have been overlooked in the design of the steganosystem. The criterion K_7 obliges the designer of the steganosystem to explicitly ensure the capacity to assess the contextual plausibility of the selected container (or the resulting steganomessage) with respect to the operating conditions of MASS, thereby excluding or restricting, in particular, the use of AI-generated images whose semantic artifacts render the existence of a steganographic channel inferable from context alone, without recourse to any steganalysis of the content itself. Thus, K_6 and K_7 transform the implicit vulnerabilities of a steganosystem within MASS into explicit requirements for its development, a necessary condition for creating a genuinely robust protection system for an autonomous vessel's control channel. To illustrate the necessity of incorporating additional robustness criteria for a steganosystem as a component of MASS's information security system, let us consider a model example. As the baseline model of cyber-physical interaction, we select the critical control loop of an autonomous vessel, defined in accordance with the methodological provisions of the International Code of Safety for Maritime Autonomous Surface Ships (MASS Code) [29]: the shore-based Remote Operations Center (ROC) – the satellite communication channel – the onboard steering-gear controller of the MASS. This loop operates under conditions of instability in its temporal transmission parameters [22, 23]. The periodicity of packet transmission within MASS's

critical navigation loops is rigidly determined by the technological regulation. In accordance with the sampling-rate requirements of industrial motion-control controllers and real-time data transmission standards, the nominal interval between successive packets ΔT is on the order of 50 ms [30, 23]. Any deviation beyond this interval, arising from the computational latency of protection algorithms, disrupts the stability of the automatic control loop.

Scenario A. Design of a steganosystem without accounting for K_6 and K_7 . A steganosystem is developed for the covert transmission of control information, with the emphasis placed solely on the classical criteria $K_1, \dots, K_5$. In order to increase the probability of ensuring imitation resistance (K_3), the developer implements a computationally "heavy" algorithm (for example, one based on the singular value decomposition of a digital-video frame's matrix, which, for an $n \times n$ -times frame alone, requires $O(n^3)$ operations, or spread-spectrum techniques [31]. Let us assume that the additional information embedding procedure on the shore-based server takes 12 ms, while the extraction and verification procedure on board the vessel takes 18 ms. The total computational delay here is $\Delta t_{stego} = 30$ ms. The values of 12 ms and 18 ms in this scenario are conventional parameters, provided for the purpose of demonstrating the problem under consideration, it is taken into account here that the shore-based center (ROC) is equipped with powerful server-grade processors, whereas the onboard computer of the MASS is typically constrained in computational power relative to the shore-based server (owing to requirements pertaining to power consumption, vibration resistance, and reliability), and that, accordingly, the embedding of the additional information occurs more rapidly than its extraction. The total packet delay in the communication channel (Δt_{total}) is then calculated according to the formula:

$$\Delta t_{total} = \Delta t_{network} + \Delta t_{stego} , \quad (1)$$

where $\Delta t_{network}$ is the network delay of the satellite channel.

For contemporary satellite systems (Starlink), the average network delay is 30–40 ms, however, owing to changes in satellite positioning and weather conditions, it fluctuates continuously within the range of 25 to 45 ms [32]. Then, in the best case, from (1) we obtain: $\Delta t_{total} = 25 + 30 = 55$ ms, whereas in the worst case: $\Delta t_{total} = 45 + 30 = 75$ ms. Thus, even under the most favorable network conditions, the total packet delivery and processing time (55 ms) already exceeds the technological threshold for real-time automation (50 ms). The onboard MASS controller expects a new packet every 50 ms. Because the computationally "heavy" protection algorithm consumed 30 ms, the packet is chronically delayed by 5–25 ms. For a real-time industrial controller, a delay of even a few milliseconds constitutes a critical failure. The vessel's automation system interprets this as a loss of communication with the shore, placing the vessel into an emergency mode (for example, emergency braking or course-holding), and legitimate control is blocked. Thus, although the protection mechanism functioned as intended, the vessel lost controllability. Safety was compromised by the protection system itself. In other words, under MASS conditions, the system proves vulnerable with respect to K_6 : traffic timing analysis reveals the presence of the steganographic transformation. Traditional steganosystems, oriented primarily toward the criterion K_1 , disregard the logical content of the digital video or image, thereby enabling an adversary to conduct successful steganalysis on the basis of detecting physical and contextual anomalies in the generated content. Thus, under MASS conditions, the system proves vulnerable with respect to K_7 : contextual analysis reveals the existence of the steganographic channel.

Scenario B. Design of a steganosystem with K_6 and K_7 taken into account. The incorporation of K_6 compels the developer to establish, from the outset, a constrained time budget:

$$\Delta t_{stego} \leq P , \quad (2)$$

where P is a certain threshold value that allows the steganographic transformation process to be entirely "dissolved" within the background network jitter and not to induce temporal anomalies, that is, it ensures that

$$\Delta t_{total} < \Delta T, \quad (3)$$

The specificity of K_6 lies in the fact that the threshold constraint P is not a fixed value. It represents a dynamic balance among a set of steganographic factors: the volume of the message being concealed, the informational capacity and physical nature of the container employed, and the computational complexity of the steganographic algorithm itself. Under MASS conditions, the protection system must continuously solve the problem of ensuring imitation resistance (K_3) amid changing container parameters, while rigidly maintaining the total computation time within the dynamic real-time limit (3). Recognition of this design constraint eliminates computationally complex steganographic methods from consideration, leaving as viable for use in organizing a covert channel only those methods for which condition (2) is satisfied. Accounting for the criterion K_7 in the development of a steganosystem ensures semantic control: the system evaluates the contextual correctness of container generation (in particular, the conformity of lighting, shadows, and object geometry to the physical laws of the real world). The embedding of the steganomessage is permitted only within containers that fully correspond to the standard processes and operational logic of MASS, thereby rendering the disclosure of the hidden channel through contextual analysis impossible, a consideration entirely absent from the first scenario. The example presented clearly demonstrates the fundamental insufficiency of the existing robustness criteria $K_1, \dots, K_5$ for a steganosystem operating as part of MASS's information security system. The steganosystem examined under Scenario A, which proved fully acceptable from the standpoint of the existing system of robustness criteria, was found, under real-world operating conditions as part of MASS, to be vulnerable along two directions simultaneously, directions not accounted for by the existing criteria. This demonstrates the necessity of introducing the additional criteria K_6 and K_7 , which account for detection vectors specific to the steganographic channel within this particular domain of application. The introduction of K_6 and K_7 is not a purely theoretical exercise: it closes real vulnerabilities that, in the absence of an explicit formulation of these criteria, would have gone unnoticed at the design stage of a steganosystem for MASS.

Remark 3. A certain "antagonism" exists between the introduced criteria K_6 and K_7 : ensuring the contextual plausibility of the container (K_7) in the case of AI-generated content presupposes verifying the semantic correctness of the generated image or video prior to its transmission – an operation requiring additional computational expenditure. However, any additional delay comes into conflict with the requirement of K_6 – the non-detectability of the steganographic embedding through traffic timing analysis. Thus, the more rigorous the verification of contextual plausibility, the higher the probability of detecting the steganographic channel through timing analysis, and vice versa. This antagonism is specific to MASS and has no analogue in classical steganographic theory. The contradiction identified between K_6 and K_7 requires separate consideration in the design of a steganosystem for MASS.

The practical value of the antagonism established between K_6 and K_7 lies in the fact that it obliges the designer of a steganosystem for MASS to consciously choose a compromise between the temporal imperceptibility of the steganographic transformation and the contextual plausibility of the container/steganomessage. Explicit recognition of this antagonism at the design stage constitutes a necessary condition for creating a balanced and practically applicable steganosystem as part of MASS's information security system.

Remark 4. Considering the viability of employing a steganographic approach to protect MASS in light of the discourse on disclosure versus secrecy in security [33, 34], it should be noted that Swire's

proposed resolution of the "security through obscurity" paradox links the effectiveness of secrecy to the nature of potential attacks: secrecy is justified where an attack incurs high costs and precludes repeated, "unpunished" execution, whereas transparency is preferable where an attack is (relatively) low-cost and can be frequently iterated. An attack on the real-time control channel of a specific MASS corresponds to the former scenario: it requires access to the communication link within a specific time window of a given voyage under dynamic transmission conditions, thereby ruling out low-cost, low-risk probing by an adversary. Consequently, applying steganographic concealment to the transmission of control commands in this context aligns with Swire's resolution of the paradox rather than contradicting it, while the underlying steganographic transformation mechanism and key secrecy remain fully compliant with Kerckhoffs's principle.

4. Conclusions

This study resolves an important scientific and practical problem that of ensuring the possibility of designing a robust steganosystem for use as part of a cyber-physical control system for an autonomous vessel, through the development of a system of robustness criteria $K_1, \dots, K_7$ that accounts for detection vectors specific to the steganographic channel within this particular domain of application. In the course of achieving the objective of this study, it has been established that:

- the process of forming a systemic, comprehensive approach to the problem of ensuring the cybersecurity of autonomous shipping is at an early stage of its development: the regulatory and legal framework is only beginning to take shape, while technical solutions are being actively developed. It is shown that steganography occupies a distinctive place among the priority directions for ensuring the information and cybersecurity of MASS, as the sole instrument capable of concealing the very fact of the transmission of control information, a consideration of fundamental importance specifically for an autonomous vessel, which lacks the capacity to compensate for a compromise of the control channel through crew decision-making;
- the existing robustness criteria of a steganosystem are necessary but insufficient for a steganosystem operating as part of MASS's information security system. The specificity of MASS as a real-time cyber-physical system gives rise to two additional detection vectors for the steganographic channel, not accounted for by the existing criteria: traffic timing analysis and contextual analysis of the container/steganomessage.

This work substantiates the priority of the imitation resistance criterion K_3 for steganosystems deployed within MASS, establishing a formal rule for resolving conflicts among robustness criteria under the real-time resource constraints inherent to MASS – that ensuring imitation resistance serves as the primary constraint in steganosystem design, to which all other criteria must adapt.

Furthermore, two novel robustness criteria specific to real-time cyber-physical systems are introduced and substantiated for steganosystems applied to MASS: K_6 – resistance to traffic timing analysis, and K_7 – resistance to contextual analysis of the container/steganomessage. An example has been presented demonstrating that a steganosystem formally satisfying all previously existing robustness criteria proves, in practice, to be vulnerable under MASS conditions precisely with respect to the newly introduced criteria, thereby confirming the fundamental necessity of their introduction.

An antagonism has been established between K_6 and K_7 , one specific to MASS and having no analogue in classical steganographic theory. The practical value of this established antagonism lies in the fact that it obliges the designer of a steganosystem to consciously choose a compromise between K_6 and K_7 at the design stage.

The incorporation of K_6 and K_7 extends the system of steganosystem robustness criteria as applied to the domain of autonomous shipping and establishes a foundation for the design of steganosystems that are genuinely robust under MASS conditions.

This study lays the conceptual and substantive foundation for a new system of steganosystem robustness criteria for MASS cybersecurity. Naturally, the task of constructing a fully fledged, comprehensively substantiated methodology for designing robust steganosystems for such a specific and complex subject area cannot be exhaustively accomplished within a single paper. The authors regard this study as a starting point for a new research direction, the further development of which entails both the deepening of the theoretical apparatus and its subsequent practical validation. In particular, a promising direction for further research is the formalization of the introduced criteria and their priority relation into a rigorous logical apparatus (through the explicit definition of predicates of the physical consequences of violating each criterion and the dominance relations between them), which will make it possible to transform the qualitative justification presented in this work into a system of strict formal statements. Moreover, the goal of the authors' subsequent research is the development of specific steganographic methods, along with their validation, oriented toward operation within real-time cyber-physical systems, taking into account the derived system of steganosystem robustness criteria.

Declaration on Generative AI

During the preparation of this work, the authors used Claude in order to check grammar and spelling. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

- [1] S. J. Nash, H. Jahankhani, Defining the maritime cyber adversarial taxonomy of tactics and techniques, in: H. Jahankhani, S. Kendzierskyj, S. Pournouri, M. A. Pozza (Eds.), *Space Governance, Space Law and Policy*, Springer, Cham, 2024, pp. 41–74. doi:10.1007/978-3-031-62228-1_2.
- [2] J. I. Alcaide, R. G. Llave, Critical infrastructures cybersecurity and the maritime sector, *Transportation Research Procedia* 45 (2020) 547–554. doi:10.1016/j.trpro.2020.03.058.
- [3] D. C. Chupkemi, K. Mersinas, Challenges in maritime cybersecurity training and compliance, *Journal of Marine Science and Engineering* 12 (2024) 1844. doi:10.3390/jmse12101844.
- [4] H. Yu, Q. Meng, Z. Fang, J. Liu, Literature review on maritime cybersecurity, *The Journal of Navigation* 76 (2023) 453–466. doi:10.1017/S0373463323000164.
- [5] V. G. Piadyshev, Issues of improving cybersecurity of maritime transport, *Maritime Security and Defence* 1 (2023) 78–86. (In Ukrainian). doi:10.32782/msd/2023.1.10.
- [6] H. V. Aloslyn, O. V. Kolomiitsev, Cybersecurity and information technologies, V. S. Ponomarenko (Ed.), *TOV "DISA PLIUS"*, Kharkiv, 2020. (in Ukrainian).
- [7] V. A. Lakhno, Improving the cybersecurity of transport information and communication systems, *Ukrainian Scientific Journal of Inf. Security* 22(1) (2016) 44–50. (in Ukrainian).
- [8] K. Heffner, Ø. J. Rødseth, Enabling technologies for maritime autonomous surface ships, *Journal of Physics* 1357 (2019). doi:10.1088/1742-6596/1357/1/012021.

- [9] I. Yoon, J. Choi, K. Seo, Technology Assessment: Autonomous Ships (summary), Korea Institute of Marine Science & Technology (KIMST), 2018.
- [10] H. Karahalios, Cybersecurity threats of remote autonomous ships while approaching ports, *Journal of Transportation Security* 18 (2025). doi:10.1007/s12198-024-00289-1.
- [11] International Maritime Organization, Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems, adopted 16 June 2017, London, 2017. URL: <https://www.dohle-yachts.com/wp-content/uploads/2021/05/MSC.42898-2.pdf>.
- [12] International Maritime Organization, MSC-FAL.1/Circ.3/Rev.2 – Guidelines on Maritime Cyber Risk Management, 7 June 2022. URL: <https://www.imorules.com/GUID-605EA6AC-0722-413D-9185-32AE56328FCF.html>.
- [13] A. Amro, V. Gkioulos, From click to sink: utilizing AIS for command and control in maritime cyber attacks, in: V. Atluri, R. Di Pietro, C. D. Jensen, W. Meng (Eds.), *Computer Security – ESORICS 2022, Lecture Notes in Computer Science*, vol. 13556, Springer, Cham, 2022, pp. 535–553. doi:10.1007/978-3-031-17143-7_26.
- [14] I. Bobok, A. Kobozieva, Localization of disturbance region of formal parameters of steganographic cover to ensure steganosystem stability, *Radioelectronics and Communications Systems* 67 (2024) 396–409. doi:10.3103/S0735272724090024.
- [15] A. V. Chunarova, Ye. O. Potapenko, Methods to increase stability steganosystem from unauthorized access, *Science-Based Technologies* 22(2) (2014) 196–199. (in Ukrainian). doi:10.18372/2310-5461.22.6819.
- [16] I. Bobok, A. Kobozieva, N. Kushnirenko, S. Sokalskiy, Increasing the resistance of the steganosystem to attacks against an embedded message by selection of container blocks, in: 2024 IEEE 5th International Conference on Advanced Trends in Information Theory, Lviv, Ukraine, 2024, pp. 264–269. doi:10.1109/ATIT64324.2024.11222497.
- [17] M. O. Nassar, StyleStego: a novel paradigm for high-capacity steganography using per layer noise maps in StyleGAN for cross-domain robustness, *Multimedia Tools and Applications* 85 (2026) 561. doi:10.1007/s11042-026-21718-4.
- [18] M. Gao, C. Jia, J. Liu, X. Geng, G. Ding, P. Shi, Y. Xia, S. Chen, Z. Kang, A. Zhang, Swarm of MASSs cyber-security for anti-hijack system based on blockchain and chaotic-steganography using VRF-PBFT and encoder-decoder deep neural networks, *IEEE Transactions on Intelligent Transportation Systems* 26 (2025) 21758–21768. doi:10.1109/TITS.2025.3616187.
- [19] Y. Hao, Z. Wang, X. Zhang, X. Li, Model steganography during model compression, *IEEE Transactions on Dependable and Secure Computing* 23 (2025) 4301–4309. doi:10.1109/TDSC.2025.3645268.
- [20] National Institute of Standards and Technology (NIST), Cyber-Physical Systems Public Working Group, Framework for Cyber-Physical Systems: Volume 1, Overview, NIST Special Publication 1500-201, Version 1.0, Gaithersburg, MD, 2017. doi:10.6028/NIST.SP.1500-201.
- [21] A. A. Cárdenas, S. Amin, S. Sastry, Research challenges for the security of control systems, in: *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec '08)*, USENIX Association, 2008.

- [22] S. Chen, X. Xiong, Y. Wen, J. Jian, Y. Huang, State compensation for maritime autonomous surface ships' remote control, *Journal of Marine Science and Engineering* 11 (2023) 450. doi:10.3390/jmse11020450.
- [23] B. Reitz, A. Munari, F. Lazaro, D. Höhn, Optimizing satellite communication for Maritime Autonomous Surface Ships (MASS) monitoring: overview of the role of age of incorrect information in preventing data channel congestion, *Journal of Physics: Conference Series* 3123 (2025) 012039. doi:10.1088/1742-6596/3123/1/012039.
- [24] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, Cambridge, 2010.
- [25] M. O. Honcharov, O. P. Nariezhnii, S. V. Malakhov, Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures, *Modern Information Security* 3 (2025) 37–47. (in Ukrainian). doi:10.31673/2409-7292.2025.030518.
- [26] I. I. Bobok, S. M. Hryhorenko, A. A. Kobozieva, K. L. Yavorska, Improving steganosystem efficiency as an integral part of ensuring the routine operation of energy infrastructure facilities, *Problems of the Regional Energetics* 2 (70) (2026) 78–93. URL: <https://journal.ie.asm.md/ru/contents/electronni-jurnal-270-2026>.
- [27] A. Kobozieva, I. Bobok, O. Laptiev, V. Savchenko, Application of graph theory to ensure the reliability of steganographic message perception in the creation of a covert communication channel, *CEUR Workshop Proceedings* 4048 (2025) 94–108.
- [28] I. Bobok, A. Kobozieva, S. Sokalsky, The problem of choosing a steganographic container in conditions of attacks against an embedded message, *Problemele Energeticii Regionale* 4 (2022) 74–88. doi:10.52254/1857-0070.2022.4-56.07.
- [29] International Maritime Organization, International Code of Safety for Maritime Autonomous Surface Ships (MASS Code), Resolution MSC.595(111), Maritime Safety Committee (MSC), adopted 22 May 2026, entered into force 1 July 2026.
- [30] J. Bauer, A. Klein, B. Schütz, J. Stoppe, Investigating the impact of communication delays and bandwidth restrictions on remote operations of unmanned systems, in: *Proceedings of the 1st International Conference on Drones and Unmanned Systems (DAUS)*, Granada, Spain, 2025.
- [31] H. Guo, X. Niu, Robust attack-aware spread spectrum watermarking in real scenes, *Neurocomputing* 635 (2025) 130060. doi:10.1016/j.neucom.2025.130060.
- [32] F. Michel, M. Trevisan, D. Giordano, O. Bonaventure, A first look at Starlink performance, in: *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*, Association for Computing Machinery, New York, NY, 2022, pp. 130–136. doi:10.1145/3517745.3561416.
- [33] P. Swire, A model for when disclosure helps security: What is different about computer and network security?, *Journal on Telecommunications and High Technology Law* 3 (2004) 163. doi:10.2139/ssrn.531782.
- [34] P. Swire, A theory of disclosure for security and competitive reasons: Open source, proprietary software, and government agencies, *Houston Law Review* 42 (2006) 101. URL: <https://ssrn.com/abstract=842228>.