DOI: 10.36163/aon-2024-0004

CYBERSECURITY OF UNMANNED SURFACE VESSELS: IMECA BASED ASSESSMENT AND PROTECTION AGAINST AI POWERED ATTACKS

Oleg Ivanchenko
Naval Institute of the National University "Odessa Maritime Academy"
Odesa, Ukraine
o.ivanchenko@khai.edu

Vyacheslav Kharchenko
National Aerospace University "Kharkiv Aviation Institute"
Kharkiv, Ukraine
v.kharchenko@csn.khai.edu

Nataliia Smyrynska
Naval Institute of the National University "Odessa Maritime Academy"
Odesa, Ukraine
nataliia.smyrynska@gmail.com

Olena Veprytska
National Aerospace University "Kharkiv Aviation Institute"
Kharkiv, Ukraine
o.verytska@csn.khai.edu

ABSTRACT

The study is devoted to the analysis of cyber security and its impact on the efficiency and safety of the applying single Unmanned Surface Vessels (USVs) and USV swarms (USVS). Based on a review of modern USV systems, a generalized architecture and model are proposed, and the impact of the cyber and physical environment is analyzed. The types of cyberattacks on USVs are systematized taking into account the use of artificial intelligence (AI). The set of scenarios identified as "AI powered attacks against AI powered protection" is clarified considering features of USV/USVS application. Assessment of cyber security of USV/USVSs is carried out using the IMECA (Intrusion Modes and Effects Criticality Analysis) technique and Security Informed Safety (SIS) approach. Illustrative examples of IMECA based analysis of USV cyber assets/digital systems are provided taking into account specific threats, vulnerabilities, attacks and their effects for systems security and safety.

Keywords – unmanned surface vessel, threats and vulnerabilities, IMECA, AI powered attacks, countermeasures

1. INTRODUCTION

Developing and deploying Unmanned Surface Vessels (USVs) and USV swarms (USVS) enhances efficiency, safety, and cost-effectiveness across civil and military sectors. The study is devoted to the analysis of cyber security issues and their impact on the efficiency and safety of the applying USVs and USVS. Objectives are to suggest and illustrate applying a risk-oriented method of USVs/USVS cybersecurity analysis and choice of countermeasures according to criteria "acceptable risk/minimal cost" considering AI powered attacks and protection.

2. METHODOLOGY

The methodology involves a comprehensive review of contemporary USVS, leading to the formulation and analysis of a generalized architecture and model [1], while considering the influence of both cyber and physical environments. Categorization and analysis of potential cyber threats targeting USVs, particularly those employing AI, are systematically conducted. Special attention is given to refining previously identified

scenarios labeled as "AI-powered attacks against AI-powered protection"[2] to suit the specific characteristics of USV/USVS applications. Furthermore, the cybersecurity assessment of USV/USVSs employs the IMECA technique and the Security Informed Safety approach [1].

3. IMECA

The development of an IMECA table and risk matrix for AI-powered USVs entails a thorough analysis to gauge the associated risks [1,2]. This analysis encompasses factors such as the nature of potential threats, system vulnerabilities, types of attacks, expected consequences, likelihood of occurrence, severity of impacts, and overall risk assessment. By systematically evaluating these elements, organizations operating USVs can gain valuable insights into the specific risks they face and prioritize mitigation efforts effectively to ensure the safety and security of their vessels and maritime operations. The results of the IMECA analysis of attacks on AI-powered USV shown in table 1.

Table 1. IMECA analysis of attacks on AI-powered USV (with satellite interaction)

№	Threat	Vulnerability	Attack	AI for Attack Enhancement	Effects	Countermeasures
1	Incorrect operation of the system due to a compromised AI system	The unreliability of AI systems is due to the misconception that the training data will always match the actual data	Adversarial Attacks (Generative AI)	Eg. AI-generated Telemetry/GPS Spoofing	Potentially misinterpretation of the environment, navigation errors, or compromised decision-making capabilities	1. AI Regulation & Standardization 2. Anomaly Detection 3. Adversarial Training 4. Partial Human Control Systems
2	Autonomous USVs	AI-powered Autonomous USVs exploit vulnerabilities when subjected to hacking attempts	Hacking of USV or AI components	Using AI models from untrusted sources that may contain pre-biased or backdoor behavior	Data leak/loss. Use for malicious purposes, privacy invasion, weaponization, or carrying out cyber and physical attacks etc.	1. AI Regulation 2. Intrusion Detection Systems (IDS) 3. USVs Licensing 4. Forensics Techniques Usage
3	USV Failure (Availability Violation)	Limited USV resources on board	DoS/DDoS, Flooding	-	Communication disruption, network congestion, performance degradation, compromising the USVs' functionality	1. IDS: Rule-Base, Signature-Based, Anomaly-Based 2. Standardization of USVs Security Measures
4	Interception of signals from the satellite	Open frequencies Weak encryption Insufficient authentication	Eavesdrop-ping	-	Leakage of confidential information	1. Data encryption 2. PLS-Based Secure Communications in Satellite Internet 3. PLA (Physical Layer Authentication)

Based on the results of the analysis of attacks, a matrix of criticality (cyber risks) of the systems was built before and after (see Table 2) the implementation of countermeasures.

Table 2. Criticality matrix of cyber risks of systems before(a) and after(b) implementation of countermeasures

a)

		Severity		
		Low	Medium	High
Probability of occurrence	Low			
	Medium		4	1,3
	High			2

b)

		Severity		
		Low	Medium	High
Probability of occurrence	Low			1
	Medium	4	3	2
	High			

4. CONCLUSION

The main contribution is methodology, IMECA-based technique and tool to assess USVS cybersecurity and choose the countermeasures (CMs) according to criteria “acceptable risk-minimal cost”. Future research will be dedicated to development of software for support of USVS security/safety analysis and insurance.

REFERENCES

1. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., & Di Giandomenico, F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy 25.8 (2023) 1123.
2. Veprytska O., Kharchenko V., Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining, IntelITSIS'2024 (2024).