Journal of Engineering for THERMAL ENERGY AND POWER

ISSN: 1001-2060
Vol. 23 No. 2, 2020

CYBERSECURITY CHALLENGES IN AUTONOMOUS ENGINEERING SYSTEMS

Sourabh Bansal
Professor and HOD, Department of ECE, NGCE, Manialumoodu, India

Received: 05/09/2020

Revised: 19/10/2020

Accepted: 22/11/2020

DOI:
10.12060/jet-ep-v23.i2-2

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Abstract

Autonomous engineering systems—ranging from autonomous vehicles and unmanned aerial systems to industrial robotics—are transforming modern infrastructure, manufacturing, and transportation. However, rapidly increasing autonomy, connectivity, and complexity also significantly expand the cyber-attack surface, creating profound cybersecurity challenges. These systems integrate heterogeneous components such as sensors, actuators, communication networks, and AI decision modules, making them susceptible to adversarial manipulation, remote exploitation, data breaches, and denial of service attacks. This research paper examines the major cybersecurity threats, architectural vulnerabilities, and defense strategies in autonomous systems, with a focus on real-world operational constraints and safety requirements. A mixed methodology combining literature analysis, threat modeling, and case study insights shows persistent gaps in security frameworks, standardized practices, and mitigation mechanisms. The paper concludes with recommendations for comprehensive cybersecurity integration in autonomous engineering design.

Keyword: Autonomous Systems, Cybersecurity, Attack Surface, Threat Modeling, Autonomous Vehicles, Industrial Robotics, Secure Architecture

1. INTRODUCTION

Autonomous engineering systems are engineered to operate with minimal human intervention by leveraging advanced sensing, computation, and networked communication. Applications include self-driving vehicles, industrial robots, drones, smart manufacturing systems, and autonomous ships. While autonomy promises enhanced efficiency and safety, it exposes systems to evolving cyber threats as attackers target communication links, control modules, AI perception systems, and decision logic.

Compared to traditional systems, autonomous platforms combine real-time control with networked connectivity, markedly increasing their **attack surface** and the complexity of defending against cybersecurity threats. A compromised autonomous system can lead not only to data loss but also to physical harm—making cybersecurity fundamental to reliable engineering design. Robust security measures must span multiple layers: hardware, software, communication protocols, and AI/ML components.

ISSN: 1001-2060
Vol. 23 No. 2, 2020

2. LITERATURE REVIEW

2.1 Autonomous Systems and Cybersecurity Landscape

The advent of autonomy introduces new dimensions of cybersecurity risk. Autonomous vehicles (AVs), for example, depend on interconnected sensors, inter-vehicle communication, and cloud services, making them susceptible to sensor spoofing, remote hijacking, and network-level attacks. The breadth of cyber threats across autonomous systems was systematically analyzed in a recent review of autonomous navigation systems, which identified significant gaps in attack and defense research across domains like automotive, drone, and robotic systems.

2.2 Vulnerabilities in Autonomous Architectures

Security challenges arise at multiple layers, from physical sensors to decision systems. For example, adversarial inputs can deceive vision-based autonomy, leading to misclassification and erratic system behavior. This has been the subject of recent taxonomy-level analyses showing how adversarial threats affect perception and control systems.

2.3 Sector-Specific Challenges

Autonomous aerial systems (UAVs) rely on wireless connectivity for real-time control, exposing them to spoofing and unauthorized access without strong encryption or authentication.

In autonomous ground vehicles, interconnected transport systems are vulnerable to remote hacking, data integrity attacks, and denial of service due to their reliance on wireless protocols and AI decision logic.

2.4 Standards and Security Frameworks

Automotive cybersecurity standards such as ISO/SAE 21434 are being deployed to guide secure lifecycle engineering, but broader industry-agnostic frameworks for autonomous systems are still evolving.

3. METHODOLOGY

3.1 Research Objectives

This paper investigates cybersecurity challenges across autonomous engineering systems by:

1. Reviewing existing literature to map threat landscapes.
2. Analyzing architectural vulnerabilities and attack vectors.
3. Synthesizing defensive strategies and best practices.
4. Proposing a holistic security model aligning with safety requirements.

3.2 Data Sources and Selection

Peer-reviewed journals, conference proceedings, and open access resources were systematically reviewed. Studies were selected based on relevance to autonomous systems and cybersecurity, ensuring inclusion of diverse domains such as automotive, UAVs, and robotics.

3.3 Analytical Framework

The analysis adopts a **multi-layer threat model** covering:

- **Physical Layer**: sensor and actuator vulnerabilities.
- **Network Layer**: communication protocols and interfaces.
- **Application/AI Layer**: decision algorithms and ML models.
- **System of Systems**: integration and interoperability risks.

ISSN: 1001-2060
Vol. 23 No. 2, 2020

Threat vectors were categorized and cross-referenced with defensive measures such as encryption, intrusion detection, and attack mitigation techniques.

4. PROCESS

4.1 Review and Categorization

Key threats were extracted and categorized, including sensor spoofing, network hijacking, denial of service, firmware manipulation, and adversarial AI attacks. The categorization followed established threat modeling frameworks like STRIDE and MITRE ATT&CK adapted for autonomous contexts.

4.2 Case Analysis

Representative use cases from autonomous vehicles and UAV networks were analyzed to illustrate how vulnerabilities manifest in real systems and how defense mechanisms perform under various scenarios. Defensive solutions examined include intrusion detection systems, secure communication protocols, hardened control units, and AI-based anomaly detection.

5. RESULTS

5.1 Identified Vulnerabilities

- **Wide Attack Surface**: Numerous interconnected components and interfaces increase exploitation opportunities.
- **Sensor and Perception Vulnerabilities**: Vision and lidar systems are susceptible to adversarial manipulation.
- **Communication Risks**: V2X and wireless data links can be intercepted or manipulated.
- **Software and Firmware Attacks**: Compromised over-the-air (OTA) updates can introduce malicious code.

5.2 Defense Mechanism Assessment

- **Encryption and Authentication**: Essential but may introduce latency in real-time control.
- **Intrusion Detection Systems (IDSs)**: Machine learning–driven IDSs improve detection but demand computational resources.
- **Safety-Security Integration**: Aligning security measures with functional safety standards enhances robustness.

5.3 Gaps and Challenges

Significant gaps remain in cross-domain threat analysis, standardized security frameworks beyond automotive, and resource-efficient defense mechanisms for real-time autonomous operations.

6. DISCUSSION

Autonomous engineering systems are complex cyber-physical systems where cybersecurity and safety are deeply interconnected. Traditional IT security models are insufficient, as real-time control and physical safety impose stringent performance requirements. Balancing security overhead against system responsiveness remains a key research challenge. Collaborative efforts across industry, academia, and regulatory bodies are necessary to establish resilient standards and comprehensive threat-aware design principles.

ISSN: 1001-2060
Vol. 23 No. 2, 2020

7. CONCLUSION

Cybersecurity for autonomous engineering systems is a critical and evolving field. This paper outlined major threats, architectural vulnerabilities, and emerging defense paradigms. Results show that while significant progress has been made in understanding risks, substantial challenges persist in developing scalable, efficient security solutions and standardized engineering practices. Future research should focus on cross-domain threat synthesis, resource-aware defense techniques, secure system integration, and formal security certification for autonomous systems.

REFERENCES

1. M. Hamad et al., "Cybersecurity Challenges of Autonomous Systems," Design, Automation and Test in Europe Conference Proceedings, 2025.
2. "Cyberattacks and defenses for Autonomous Navigation Systems: A systematic literature review," Computer Networks, vol. 267, 2025.
3. S. Dommari, "Cybersecurity in Autonomous Vehicles: Safeguarding Connected Transportation Systems," Journal of Quantum Science and Technology, 2025.
4. S. Ramswami and M. Nandy, "Cybersecurity Challenges in Autonomous Unmanned Aerial Vehicle Networks," Int. J. Basic and Applied Sciences, 2025.
5. "Securing (vision-based) autonomous systems: taxonomy, challenges, and defense mechanisms against adversarial threats," Artificial Intelligence Review, 2025.
6. White & Thompson, "Cybersecurity challenges in autonomous systems," Journal of Cybersecurity Research, 2017.
7. "Security strategy for autonomous vehicle cyber-physical systems using transfer learning," Journal of Cloud Computing, 2023.
8. Issa Morad & Yousef Yako, "A Systematic Literature Review on Cybersecurity in Autonomous Vehicles," Jönköping University report, 2025.
9. ISO/SAE 21434: Road vehicles — Cybersecurity engineering, international standard.
10. "Challenges in Securing Highly Autonomous Systems and Robotics," Internet article on security risks and standards, 2025.
11. G. Bendiab et al., "Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence," IEEE Trans. Intelligent Transp. Systems, 2023.
12. "Autonomous Response Systems in Cybersecurity: A Systematic Review," Communication in Physical Sciences, 2025.