Robotic Vehicle Design Project: A Cybersecurity Risk Analysis Approach Using ISO/IEC 27001:2022

PROJECT DESCRIPTION – This document presents a detailed 2-page analysis of a university engineering project, integrating key principles from data security, cybersecurity, and information security. The goal is to demonstrate how technical systems, such as autonomous or remote-controlled vehicles, can be evaluated through the lens of modern security frameworks to identify vulnerabilities and apply risk mitigation strategies.

Project Summary

During an engineering course in my early college years, I participated in a semester-long team-based capstone project focused on the design and development of a robotic vehicle using the Arduino platform. The objective was to build a remote-controlled or autonomous vehicle capable of navigating an obstacle course and retrieving wooden pillars placed throughout it. Teams competed to see whose robot could collect and return the most pillars to the starting zone within a five-minute time window.

Our development process followed a structured sprint model inspired by Agile and Scrum methodologies. Each sprint introduced a new technical challenge, such as implementing line-following behavior, integrating obstacle detection via sensors, or refining structural stability. The team structure rotated every two weeks, allowing each member to experience key roles: team lead, quality assurance engineer, and software engineer. As a result, I gained first-hand experience managing deliverables, conducting validation testing, and programming sensor-based logic using the Arduino IDE.

Our team progressed successfully through multiple tournament-style rounds and ultimately secured first place in the final competition. However, our performance in the final round exposed a hardware fault in the front-facing sensor, which highlighted the importance of resilience and real-time diagnostics in embedded system design.

Transitioning to a Cybersecurity Perspective

During my current cybersecurity internship at FIS as an IT Security Analyst, I revisited this project and explored it from a risk-based, cybersecurity-driven perspective. While the original project was academic in nature, it represented a miniature version of many real-world IoT and embedded systems. These systems often play critical roles in sensitive environments, ranging from industrial automation and healthcare robotics to military applications.

This retrospective allowed me to ask a key question:
“If this robotic system were deployed in the real world, how would we secure it against adversarial threats?”

I began by identifying potential attack surfaces:

- **Wireless communication link**: If left unencrypted, this connection could be intercepted or hijacked, allowing a malicious actor to override commands, introduce false signals, or disable the vehicle entirely.
- **Sensor spoofing**: False inputs to sensors could manipulate the robot’s behavior, creating a risk of property damage or unauthorized access to restricted spaces.
- **Firmware or application layer attacks**: Poor input sanitization or insecure coding practices in the Arduino firmware could open the system to injection attacks, privilege escalation, or logic manipulation.

- **Unauthorized access**: In more advanced systems with onboard cameras or environmental data logging, a breach could result in privacy violations or exposure of sensitive information.
- **Lack of authentication mechanisms**: Without proper access control, the system could be operated or reconfigured by unauthorized personnel.

These scenarios directly relate to violations of the Confidentiality, Integrity, and Availability (CIA) triad, which is foundational to cybersecurity.

Applying ISO/IEC 27001:2022 Annex A Controls

To approach this risk evaluation systematically, I created a formal risk register and control matrix aligned with the ISO/IEC 27001:2022 Annex A security domains. This professional framework allowed me to:

- Document technical and operational risks associated with robotics in unsecured environments.
- Map those risks to specific ISO control categories, such as:
    - A.5: Organizational Controls (e.g., policies for secure use and updates)
    - A.6: People Controls (e.g., training and responsibilities)
    - A.7: Physical Controls (e.g., secure storage of the robot when inactive)
    - A.8: Technological Controls (e.g., encryption, authentication, firmware validation)
- Assign control owners and response strategies, ensuring traceability and accountability.

The output included both a spreadsheet-based risk register and a visual mapping chart that tied identified threats to actionable control recommendations. This exercise not only deepened my familiarity with ISO 27001, but also demonstrated how even simple systems like student-built robots can become entry points for meaningful security analysis.

Takeaways and Broader Implications

This project gave me hands-on exposure to embedded system design while also allowing me to apply advanced cybersecurity frameworks to evaluate and improve the system's resilience. It demonstrated the importance of designing with security in mind from the start, regardless of how small or seemingly harmless a system might be.

More importantly, it helped me bridge the gap between engineering functionality and cybersecurity governance—something I now aim to bring into every future role I pursue in the cybersecurity field.

Whether in IoT, critical infrastructure, or autonomous systems, this project reflects my growing capability to not only identify threats but also to align solutions with global standards like ISO/IEC 27001:2022, making security actionable, measurable, and scalable.