Assignment 1 - System Categroization
CSE 4380

Group Thorin

February 28th, 2025

Members:	Obadah Al-Smadi
	Betim Hodza
	Elliot Mai
	Benjamin Niccum
	Nicholas Pratt
Instructor:	Trevor Bakker

Contents

List of Figures

List of Tables

1 System Description

1.1 Purpose and Capabilities

1.2 System Components

1.2.1 Software Components

1.2.2 Third-Party Components/Services

1.3 Stakeholders

1.4 Operational Environment

2 Data Flow Analysis

2.1 Data Identification

2.1.1 Types of Data Processed

2.1.2 Data Classification

2.2 Data Flow Diagrams (DFDs)

2.2.1 Level 0 (Context Diagram)

High-level representation of external interactions with ground control, cloud storage, and third-party services.

2.2.2 Level 1 DFDs

Detailed flow between onboard sensors, processors, storage, and communication systems.

2.3 Interfaces

2.3.1 Types of Interfaces

2.3.2 Protocols & Security Features

3 Security Categorization

3.1 Reference Standards

- FIPS 199: Security categorization for federal systems.
- NIST SP 800-60: Mapping security categories to information types.

3.2 Impact Levels (Confidentiality, Integrity, Availability)

Information Types	Confidentiality	Integrity	Availability
Power Supply/ Battery	L minimal impact due to information only of the battery itself	L Due to loss of Integrity	H severe impact to the mission can no longer operate drone without power
Rotors / ECU	L Due to loss of Confidentiality	L Due to loss of Integrity	L Due to loss of availability, severe impact to the mission capability
FILL	L Due to loss of Confidentiality	L Due to loss of Integrity	L Due to loss of availability, severe impact to the mission capability
FILL	L Due to loss of Confidentiality	L Due to loss of Integrity	L Due to loss of availability, severe impact to the mission capability
FILL	L Due to loss of Confidentiality	L Due to loss of Integrity	L Due to loss of availability, severe impact to the mission capability
General-Information	L	L	L
System Categorization			
	Moderate	High	High

3.3 Overall Categorization

Overall Information System Impact: **High**

3.4 Justification

The SCADA system's High impact categorization derives from:

- Critical role in power distribution for military operations
- Potential for catastrophic consequences including infrastructure failure and loss of life
- Remote control capabilities affecting physical systems
- Real-time processing requirements for energy management

4 Risk Management & Compliance

Alignment with Risk Management Framework (RMF) per NIST SP 800-37. Categorization informs security control selection (NIST SP 800-53). Ongoing assessment and mitigation per FIPS 200 minimum security controls.

5 Deliverables

- **System Description Document**: A comprehensive report covering all aspects outlined in Section 1.
- **Data Flow Diagrams**: Level 0 and Level 1 DFDs with annotations.
- **Security Categorization Whitepaper**: Detailed analysis and justification of the security categorization. See section 4.5 of NIST Special Publication 800-60 Volume I Rev. 1.