Risk Documentation

Smart House System

Revision History

Date	Version	Description	Author
2026-02-08	1.0	Initial potential risks for the Smart House System	Daniel Marcarini

Risk List

Risk Description	Priority
R1. Integration Complexity Between System Components	High
R2. Scalability and Performance Limitations	Medium-High
R3. Incomplete or Over-Ambitious Innovation Scope	High
R4. Unclear Requirements or Changing Requirements	Medium
R5. Unauthorized Access or Security Vulnerabilities	High
R6. Data Privacy Concerns	Medium-High
R7. Uneven Work Distribution	Medium
R8. Time Constraints and Deadline Pressure	Critical
R9. Insufficient Testing	High

Risk Handling Plans

Contents

Risks – SG4 Innovation

1 Introduction

This section identifies and evaluates the key risks associated with the SmartHouse project, particularly those related to innovation, system complexity, and technical integration. Since SG4 focuses on innovation and refinement, several technical and project-related uncertainties must be considered to ensure successful implementation and delivery.
Each risk is evaluated in terms of:

- **Description**
- **Likelihood** (Low / Medium / High)
- **Impact** (Low / Medium / High)
- **Mitigation Strategy**

Technical Risks

Risk 1: Integration Complexity Between System Components

Description:
The SmartHouse system consists of multiple interacting components (e.g., sensors, controllers, user interface, backend logic, possible IoT simulation). Integration between these modules may introduce unexpected behavior, compatibility issues, or architectural inconsistencies.

Likelihood: Medium
Impact: High

Mitigation Strategy:

- Use a modular architecture with clearly defined interfaces.
- Apply early integration testing instead of postponing integration until late stages.
- Follow consistent design principles and coding standards.
- Conduct peer code reviews.

Risk 2: Scalability and Performance Limitations

Description:
Innovative features (e.g., automation rules, real-time monitoring, event handling) may increase system complexity. If not properly designed, the system may experience performance degradation as the number of devices or rules increases.

Likelihood: Medium
Impact: Medium to High

Mitigation Strategy:

- Use efficient data structures and algorithms.
- Perform early performance testing with simulated load.
- Avoid unnecessary polling or blocking operations.
- Refactor performance-critical sections when identified.

Risk 3: Incomplete or Over-Ambitious Innovation Scope

Description:
Since SG4 emphasizes innovation, there is a risk that the team attempts to implement overly complex or experimental features that exceed the time or technical capacity of the group.

Likelihood: Medium
Impact: High

Mitigation Strategy:
- Prioritize core functionality before innovative extensions.
- Define a Minimum Viable Product (MVP).
- Time-box experimental features.
- Regularly evaluate progress against deadlines.

Risk 4: Unclear Requirements or Changing Requirements

Description:
Smart house systems often involve evolving user expectations. Changes in requirements during development may cause rework and architectural instability.

Likelihood: Medium
Impact: Medium

Mitigation Strategy:
- Clearly document functional and non-functional requirements.
- Use version control for requirement changes.
- Apply incremental development with frequent feedback.
- Maintain traceability between requirements and implementation.

Security and Privacy Risks

Risk 5: Unauthorized Access or Security Vulnerabilities

Description:
A smart house system may simulate or implement authentication, device control, and user data handling. Weak security design may lead to vulnerabilities such as unauthorized access or manipulation of devices.

Likelihood: Medium
Impact: High

Mitigation Strategy:
- Implement proper authentication and authorization mechanisms.
- Validate all user inputs.
- Avoid hard-coded credentials.
- Follow secure coding practices.

Risk 6: Data Privacy Concerns

Description:
If the system stores user preferences, logs, or sensor data, there is a risk of mishandling sensitive information.

Likelihood: Low to Medium
Impact: High

Mitigation Strategy:
- Minimize stored personal data.
- Apply encryption if sensitive data is stored.
- Clearly define data storage policies.
- Restrict access to stored data.

Project Management Risks

Risk 7: Uneven Work Distribution

Description:
In group-based software engineering projects, some members may become overloaded while others contribute less, affecting quality and deadlines.

Likelihood: Medium
Impact: Medium

Mitigation Strategy:
- Clearly define responsibilities.
- Use task tracking tools.
- Hold regular team meetings.
- Ensure transparency in workload distribution.

Risk 8: Time Constraints and Deadline Pressure

Description:
Innovation often requires experimentation and iteration, which may conflict with fixed academic deadlines.

Likelihood: High
Impact: High

Mitigation Strategy:
- Create a detailed project timeline.
- Prioritize essential features.
- Reserve buffer time for testing and debugging.
- Monitor progress weekly.

Quality Risks

Risk 9: Insufficient Testing

Description:
Due to focus on innovation and feature development, testing may be deprioritized, resulting in unstable functionality.

Likelihood: Medium
Impact: High

Mitigation Strategy:

- Implement unit testing for core components.
- Perform integration testing before delivery.
- Use test cases derived from requirements.
- Automate testing where possible.

Summary

The SmartHouse project involves technical integration, innovative feature development, and collaborative software engineering. The most critical risks relate to integration complexity, time constraints, and over-ambitious innovation goals. By applying structured planning, modular design, continuous testing, and clear team coordination, these risks can be significantly reduced.

Proper risk management ensures that innovation enhances the project rather than jeopardizes delivery, quality, or maintainability.