Hazard Analysis
Software Engineering

Team 15, SyncMaster
Kyle D'Souza
Mitchell Hynes
Richard Fan
Akshit Gulia
Rafeed Iqbal

Table 1: Revision History

Date	Developer(s)	Change
10/25/2024	Whole Team	Rev0 Hazard Analysis

Contents

1 Introduction

Hazards can be defined as either a state of the system or an action taken on the system, which causes system failures. System failures include, but are not limited to, an inability of the system to perform its required functions, loss of data, unauthorized access, or harm to users.

2 Scope and Purpose of Hazard Analysis

This document outlines a hazard analysis for SyncMaster, which is a system that manages documentation and enables administrators to verify presence of users on site. The purpose of this analysis is to identify and evaluate potential hazards, outline how they will be detected/introduced to the system, and to establish mitigation strategies. This analysis will also determine the parties responsible for each of the aforementioned points. Some of the losses that may be incurred as a result of hazards are, but are not limited to: financial loss, data loss, loss of trust, regulatory violations, and operational interruption. These losses stemming from hazards must be mitigated to ensure that the system operates securely, and in compliance with relevant regulations.

3 System Components and Boundaries

3.1 System Components

- Document Management Module: This module is responsible for handling the storage, retrieval, categorization, and versioning of the documents.
- User Authentication and Authorization Module: This module is responsible for ensuring that only authorized users can access or modify the documents.
- User Presence Verification Module: This module is responsible for tracking and verifying the presence of users on site.
- Logging and Monitoring Module: This module is responsible for generating and monitoring the logs related to system usage, document changes, and user presence verification activities.
- Notification Module: This module is responsible for sending alerts to admins about important events such as document updates or user presence verification issues.
- Database: The database stores all documents, user information, presence verification data, and logs.

3.2 System Boundaries

- User Authentication: The authentication of users will be handled through a third-party provider. The application will only interface with this provider.
- System Infrastructure: This application will be cloud-based and the underlying infrastructure including computation, storage, and network resources will be maintained by a cloud service provider.

4 Critical Assumptions

1. There are trained, trusted employees with appropriate access in the system to resolve failures should they occur.
2. There are workflows and processes in place to complete necessary tasks should the application fail.
3. External libraries used are trustworthy, secure, and will not be a cause of failure.

5 Failure Mode and Effect Analysis

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Detection	Recommended Actions	SR	Ref.
Geo-blocking	Geolocation is inaccurate	Contractor may be on site, but unable to follow entry/exit protocols	a. GPS Signal Blocked b. Use of inaccurate Geolocation API c. Out of date third-party databases d. Device does not have a GPS e. VPN usage	System provides error message to user when they get geo-blocked and sends an email to manager indicating that the user has been geo-blocked	a. User reports inaccurate location detection to manager	SR-AR1	H1-1
	GPS signal spoofing	Contractors are able to access the system and upload documents even when they are not on site	a. Use of spoofing applications b. Physical spoofing of GPS signals	System compares GPS location along with the ip address of the originating request	a. System will detect and report suspicious location activity to administrators	SR-AR1	H1-2
User Authentication	Unauthorized Access	Comprimises system security	a. Weak protocols for user authentication	Geo-blocking	a. System should require multi-factor authentication b. System should limit login attempts	SR-AR1	H2-1
	User has higher access level than they should	User may be able to view or edit documents they should not be able to causing security concerns	a. Permission issue from database failure	System maintains detailed logbook of all views and edits to documents from within the system. Managers can subscribe to a document to get a notification when it is edited.	a. Allow administrator to adjust permissions	SR-AR2 SR-AR3 SR-IR1	H2-2
	User unable to complete Two-Factor Authentication	User unable to access application	a. User name and email not in database b. User did not receive authentication email c. User unable to access email account d. Email address in database outdated or incorrect	Self-report by user	a. User to report authentication issue to manager	SR-AR1	H2-3
	Failure to revoke permissions	Contractor retains access to system after they have completed project/no longer a contractor	a. Admin fails to remove access	Access logs	a. System automates permission revocation after contractor ceases to work on project	SR-IR1 SR-AR1	H2-4
View Station Entry Protocols	Contractor Views Old Version of Entry Protocols	Contractor may view and abide by out-of-date and incorrect station entry protocols	a. Database Error	Send all documents that a contractor viewed to their manager for verification upon completion	a. Manager can reupload newer version of entry protocol documents	SR-IR2	H3-1
	Contractor Unable to Sign Documents	Contractor cannot start doing their work as they are unable to complete appropriate documentation	a. Permission issue from database failure	System provides detailed error message to user explaining that they cannot sign and guiding them on next steps	a. Allow administrator to adjust permissions	SR-AR1 SR-AR4	H3-2

Table 2: Failure Mode and Effect Analysis (FMEA) Table Part 1

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Detection	Recommended Actions	SR	Ref.
Access to web-application	User is unable to access the application through their device	User unable to use application functionality	a. Poor or no internet on device b. Device or browser unsupported or unable to run application	Self-report by user	a. User to report to Manager b. User to follow alternative workflow and processes to complete tasks on site to manager	SR-AR1	H4-1
			c. Unable to access URL (QR code damaged or missing, no camera on device, User unable to find URL)	Self-report by user	a. User to Ask Manager for URL b. Employees to provide new scannable QR code at location if applicable	SR-AR1	H4-2
Accept Contractor Document Upload	Document is valid but is uploaded in the wrong location	Poor discoverability and organization	a. Human-computer interface failure	User detects document is in the wrong category	a. Alert administrator to adjust	FR1	H5-1
	Document is malicious and should not be in the system	Malware infection	a. Malicious user gained access to system	Malware scan identifies malicious documents	a. Application removes file from system and notifies administrator	SR-AR1	H5-2
	File chosen for upload is corrupted and not able to be opened	User fails to open file	a. Failure in document chosen or upload process	Error messages to user	a. Application removes file from system and notifies administrator	SR-IR3	H5-3
	File type uploaded is not a supported type	System can't display file correctly to the user	a. Failure in file type detection b. System permitted user to attempt upload of wrong file	Error message to user	a. System notifies user of incompatible file type	FR1	H5-4
	The upload process is interrupted and the file upload is incomplete.	File upload fails	a. System connection interruption	Error messages to system	a. System notifies user	PR-SC1	H5-5
Contractor acknowl-edges document	Contractor does not acknowledge correctly and it is not saved to the system	Acknowledgement not received	a. User does not understand feedback from the application interface b. User does not agree to sign the document	Application detects unsuccessful acknowledgement state	a. System notifies user	FR7	H6-1
	Device loses power and interrupts the acknowl-edgement	Acknowledgement is not received by the system	a. Loss of power disconnects users from the application	Server side detects user disconnection	a. Save the application state and return user to previous state when they reconnect	FR7	H6-2

Table 3: Failure Mode and Effect Analysis (FMEA) Table Part 2

6 Safety and Security Requirements

SFR1. The system shall notify the facilities manager if a contractor declines to sign a document.

Rationale: The facilities manager should be aware if their contractor declines to sign a document. This creates a health and safety concern.

Fit criterion: The facilities manager receives a notification from the application identifying the contractor and the document.

7 Roadmap

All existing and new safety requirements will be implemented within the timeline of this project. All documented safety requirements are essential to the stakeholders, and must be implemented before the application can be deployed for use.

Appendix — Reflection

The purpose of reflection questions is to give you a chance to assess your own learning and that of your group as a whole, and to find ways to improve in the future. Reflection is an important part of the learning process. Reflection is also an essential component of a successful software development process.

Reflections are most interesting and useful when they're honest, even if the stories they tell are imperfect. You will be marked based on your depth of thought and analysis, and not based on the content of the reflections themselves. Thus, for full marks we encourage you to answer openly and honestly and to avoid simply writing "what you think the evaluator wants to hear."

Please answer the following questions. Some questions can be answered on the team level, but where appropriate, each team member should write their own response:

1. What went well while writing this deliverable?

   When writing this deliverable, we were able to efficiently discuss and delegate sections of the document to team members. We made good use of the issues and PR's on GitHub to track the status.

2. What pain points did you experience during this deliverable, and how did you resolve them?

   One pain point was identifying new safety requirements and determining the best way to incorporate them into the HazardAnalysis.pdf document while maintaining consistency with the SRS.pdf. The team utilized a pull request to discuss the best approach. The team decided to give each safety requirements it's own unique label to resolve this problem.

3. Which of your listed risks had your team thought of before this deliverable, and which did you think of while doing this deliverable? For the latter ones (ones you thought of while doing the Hazard Analysis), how did they come about?

   Our team had thought about poor internet signal at stations and also the risk of GPS technology not working properly. This deliverable allowed us to consider in more depths what the causes of failure could be and what actions the system should take to respond. Our team discovered new risks, including what would happen if a contractor decided not to sign a document. This led to the creation of a new safety requirement to address this issue.

4. Other than the risk of physical harm (some projects may not have any appreciable risks of this form), list at least 2 other types of risk in software products. Why are they important to consider?

One important risk to consider is the risk of poor user experience. Our application will be used by dozens of contractors, so the application must not be frustrating for the user or they will not utilize it and the benefits it has to offer.

Another important risk is the risk of malicious documents entering the system. Applications which accept the input of data are naturally at a higher risk from malicious actors. The hazard analysis allowed our team to consider the importance of scanning uploaded documents for threats instead of trusting the documents which the system receives.