Hazard Analysis
Software Engineering

Team 5, GradSight
Willie Pai
Hammad Pathan
Wajdan Faheen
Henushan Balachandran
Zahin Hossain

Table 1: Revision History

Date	**Developer(s)**	**Change**
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Contents

1 Introduction

The word "hazard," in this context, means any latent condition or fault that can interact in a way that is threatening safety, functionality, or even data integrity or user privacy. It means either software failures, security vulnerabilities, faulty hardware components, or even poor user-induced errors that may threaten the entirety of system performance or even disclose private data.

Current risk analysis searches for potential hazards that may exist within the given system boundary, considering further software and hardware components that threaten the digital composite display system. Because this is a system intended for a public environment on campus, one may make valid assumptions about substantive requirements for data protection, security access, and reliability operations about the touchscreens. This includes research in both the interface digital interface and data management protocols to confirm the McMaster University Security and Privacy Regulations.

A structured approach to identification, classification, and mitigation using FMEA will be applied for deep analysis in each and every mode of failure that could potentially occur. The review will aim at minimum risk by adopting effective mitigation measures so as to guarantee safety, dependability, and security for all users of the system.

2 Scope and Purpose of Hazard Analysis

This hazard analysis is supposed to find, evaluate, and alleviate all types of risks associated with the GradSight digital composite interface project. In this document, the word 'hazards' will refer to every potential threat with regard to user privacy, data security, system functionality, and overall user satisfaction. As the GradSight system will be dealing with sensitive material in the form of images and profiles of students and alumni, one would want to attach great importance to data integrity and security. This includes a hazard analysis for software and hardware problems that focuses on such failures in which the system will not work within expected parameters due to software bugs, breaches in data security, or breakdown in the communication of hardware.

This would involve security gaps concerning custom software components making up the backend and database and hardware components making up touchscreen displays and mini-PC's. As much of the system's data is currently within the public domain, the addition of the LifeTouch images requires particular attention being given to the issues of privacy and ensuring that this system is compatible with McMaster University's security policies and its standards for the protection of data.

This analysis will consider the various configurations that could be deployed and the associated risk with each configuration. This may include things like risks regarding hardware communications failure, data privacy due to unauthorized access, and or limitations from the use of public third-party libraries. For example, if the addition of data from LifeTouch was to be added, the system should use privacy policies prescribed by LifeTouch itself. If more technologies were to be used, such as machine learning for image processing, the assessment would depend on the security features of the manufacturer, such as documentation of TensorFlow.

It also involves the roadmap for different phases of project development where implementation

stages have been planned for features of privacy, security, and system robustness. Otherwise, placeholder data alternatives or system interaction modifications would also be in consideration depending on the availability of data from LifeTouch during such a scenario when the intended integration of LifeTouch data is not possible. Keeping all the factors in consideration, the GradSight system will still be secure and reliable with compliance for the alumni, students, and other members of the McMaster University campus community.

3 System Boundaries and Components

Hardware Component: The system will either use a large touchscreen display provided by McMaster University or Raspberry Pi as an alternative. Additionally, with the usage of multiple displays, the devices can be scattered throughout campus and will allow students and alumni faculty to browse the composites. With that being said, the hardware is susceptible to physical damage and network failures from time to time.

Software Component: The software based system will be hosted on McMaster University's internal servers, which already contains secure communication between applications. A component of the system will provide composite data such as photos and metadata. Additionally, the functional system will allow users to search, zoom in on composites, and interact with individual profiles. Software should contain boundaries regarding availability and accessibility. The system should have uptime of 98% while the rest accounts for network failures and shortages.

External Systems: The system shall integrate with external systems and data, such as Lifetouch. Lifetouch provides the graduation photos for the university's faculty. With the addition of external systems, security and privacy should be a large factor when communicating between these systems. With lifetouch holding proprietary rights over these images, we need to comply with their usage terms. This could be resolution limitations or watermarking.

4 Critical Assumptions

Several critical assumptions underpin this analysis. These assumptions will guide the development and mitigation strategies:

- **LifeTouch's Privacy and Data Handling:** LifeTouch, the external provider of graduation photos, is responsible for ensuring that their images meet all necessary privacy standards. Our system will not need to revalidate these standards, but we are responsible for protecting these images once they are integrated into our database.
- **McMaster's IT Security Infrastructure:** McMaster University's servers, which will host the system, are assumed to have robust security measures in place. Our role is to ensure that our custom back-end components (e.g., the database and user management system) follow McMaster's security protocols.
- **Final Hardware Selection:** The final hardware for the system has not yet been chosen. We assume that all hardware options, including Raspberry Pi, will meet the system's needs.

However, we must account for potential issues like overheating, connectivity problems, and hardware incompatibility.

- **Existing Libraries:** If we use TensorFlow for Optical Character Recognition (OCR), we assume that its developers have already addressed any potential privacy issues. We will not need to validate TensorFlow ourselves, but we must ensure that our implementation does not introduce any new risks.

5 Failure Mode and Effect Analysis

Table 2: Table 5.1: Failure Mode and Effect Analysis (FMEA)

Component	Failure Mode	Causes of Failure(s)	Effects of Failure(s)	Recommended Action(s)	SR	Ref.
Authentication System	Unauthorized Data Access	Insufficient authentication or lack of access control	Compromised data integrity, and access to university systems	Enforce strict access control, maintain a detailed access log for user activities, and conduct routine access reviews.	SR-15.1, SR-15.4	H1
Touchscreen Display	System Outage	Mini-PC hardware failure, network disruption	Inaccessibility, potential user frustration	Schedule regular maintenance checks, and implement automatic system restart upon hardware disconnection or failure detection.	SR-15.5	H2
Image Retrieval System	Inaccurate Image Display	Improper database linking, data retrieval errors	Incorrect images or alumni information shown to users	Implement data validation protocols, use consistent database linking checks, include error-handling mechanisms, and schedule regular data consistency audits to verify linkage accuracy.	SR-15.5	H3
LifeTouch Data Integration	Privacy Breach (LifeTouch data)	Improper handling, lack of specific LifeTouch privacy compliance	Potential privacy violations, legal repercussions	Use LifeTouch-specific data protocols, ensure data masking or anonymization where possible, and document all data-handling processes to track compliance with LifeTouch's guidelines.	SR-15.1	H4
Server and Network	Slow System Response	Network latency, inadequate processing power	Reduced user engagement due to delayed responses	Optimize code, enhance data retrieval processes, utilize caching.	SR-15.5	H5
Mini-PC and Display Connection	Hardware / Communication Failure	Intermittent connections, outdated firmware	Complete or partial loss of display functionality	Conduct regular hardware health and firmware update checks.	SR-15.5	H6
Image Processing and Display	Image Processing Error	Low memory capacity, software bugs in image handling	Partial or corrupted images displayed	Optimize image processing algorithms, increase memory allocation if necessary, run image data tests frequently, and use caching to reduce load.	SR-15.5	H7
Data Synchronization	Failure to Update Records	Delay in syncing alumni data due to network issues	Outdated information displayed to users	Set up automated data sync alerts, add manual override for critical data sync issues, schedule regular sync intervals, and have a fallback update mechanism to handle urgent data updates when necessary.	SR-15.5	H8
Data Storage System	Data Loss from System Crash	Lack of adequate data backup measures	Permanent loss of important alumni data	Implement backups to both local and cloud-based storage, and ensure backup verification.	SR-15.5	H9
Compliance with Legal Standards	Legal Non-Compliance	Failure to adhere to LifeTouch and McMaster privacy standards	Risk of legal penalties or litigation	Consult McMaster's legal advisors, document all processes involving data, and educate team members on compliance protocols, particularly with respect to handling third-party data.	SR-15.3	H10

6 Safety and Security Requirements

To ensure system integrity and protect user data, we will implement the following safety and security measures:

- **SR-1. Access Control:** Role-based access control will be used to restrict access to sensitive features. Students, alumni, and faculty will have different levels of access, ensuring that only authorized personnel can make changes to the composite data.
- **SR-2. Audit Logging:** The system must keep detailed logs of all user interactions, especially those involving access or modifications to sensitive data. These logs will help trace any security breaches and ensure accountability.
- **SR-3. Downtime Resilience:** The system must be able to handle hardware downtime without significantly affecting functionality. This includes having backup service available and ensuring that the system can be quickly reset or replaced in the event of a failure.

7 Roadmap

Phase 1: Foundation

1. **Role-Based Access Control (RBAC)**
   - Define distinct user roles, and restrict data access based on roles to prevent unauthorized modifications.
2. **Audit Logging**
   - Log user interactions related to access and modification of sensitive data.

Phase 2: Reinforcement

1. **Data Backup and Recovery**
   - Set up automated backups with local/cloud-based storage.
2. **Hardware Security**
   - Secure physical touchscreen devices to prevent tampering.

Phase 3: Security Enhancement

1. **Continuous Vulnerability Scanning**
   - Set up automated vulnerability scans for software libraries and dependencies.
2. **Scalability and Load Balancing**
   - Optimize security to support increased traffic and data.

Phase 4: Long-Term Implementation

1. **Recovery Plan**
   - Implement protocols for major system failures, such as redundant servers/databases in case of unexpected outages (e.g., loss of internet).

2. **Scalable Security Infrastructure**
   - Expand security framework to accommodate future needs.

8 Reflection

1. **What went well while writing this deliverable?**
   During the writing of this deliverable, one of the key aspects that went well was our team's ability to collaboratively identify and address potential hazards. Our use of version control and regular meetings helped streamline the process of gathering and organizing the information necessary for the hazard analysis. Each team member took ownership of specific sections, which allowed us to efficiently complete the analysis while ensuring thoroughness across different areas such as data privacy, hardware, and system scalability. Additionally, the team's early focus on security allowed us to integrate key safety features, such as role-based access control, without having to revisit foundational aspects of the project later on.

2. **What pain points did you experience during this deliverable, and how did you resolve them?**
   One of the main pain points we encountered was uncertainty around the hardware we would be using, especially when it came to potential communication failures or hardware malfunctions. Initially, we didn't have a clear idea of which touchscreen devices or mini-PCs (like Raspberry Pi) would be available for the project, so we couldn't accurately assess potential hazards tied to the hardware's reliability. We resolved this by considering multiple configurations and creating alternative plans, which helped us avoid delays and allowed us to proceed with the hazard analysis while still accounting for possible hardware-related risks.

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?**
   Before writing this deliverable, our team had already identified several key risks, particularly around data privacy and the potential for unauthorized access. Given that we would be working with alumni photos and personal information, we knew from the outset that encryption, access control, and audit logging would be essential to mitigate security risks. However, while working on this deliverable, we realized additional risks related to data synchronization and system responsiveness. Specifically, the risk of displaying outdated information due to a network failure or delayed sync emerged during the hazard analysis. This risk came to light as we considered scenarios in which the system might lose connection with the server, leading us to propose backup solutions and regular sync intervals to minimize 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 significant risk in software products is data security because the potential risk for sensitive data (such as alumni photos and personal information) leaking can lead to breaches that damage user trust and result in legal ramifications. Ensuring that encryption and access control measures are robust is crucial to protecting this data and maintaining compliance with privacy regulations.

Another important risk is system downtime or unavailability because if the system goes offline or becomes unresponsive—whether due to hardware failure, network issues, or software bugs—it can lead to user frustration and disrupt service delivery. Downtime also risks data loss if backups are not properly maintained, so building resilience into the system through redundancy, regular maintenance, and recovery protocols is essential for ensuring reliable and uninterrupted service.