Hazard Analysis
Software Engineering

Team #22, TeleHealth Insights
Mitchell Weingust
Parisha Nizam
Promish Kandel
Jasmine Sun-Hu

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 24 2024	Jasmine Sun-Hu	Added Sections 1,2,3
October 25 2024	Jasmine Sun-Hu	Added Drafts of Section 4, Reflection
October 25 2024	Promish Kandel	Created FMEA table, Added Section 6,7, Reflection

Contents

1 Introduction

This document contains the hazard analysis for Telehealth Insights, a project for a website that will help parents administer language tests at home for bilingual children with speech difficulties. A hazard is defined as a property or condition in a system that when combined with a condition in the environment has the potential to harm or damage to the system. A hazard is not limited to safety, it can also be related to system security, user sensitivity and unexpected human or technology interactions. The purpose of this document is to identify any hazards to the project, and develop newsafety and security requirements from a Failure Mode and Effect Analysis.

2 Scope and Purpose of Hazard Analysis

The hazard analysis focuses on identifying, evaluating, and mitigating any hazards that could negatively impact the speech language assessment platofrm. This includes both technical and user interaction hazards in particular since the project will include handling sensitive patient data. The analysis will cover many aspects of the system such as data handling, software stability and user sensitivity.

The purpose of the hazard analysis is to identify any risks that could affect data privacy and security, system reliability, data collection accuracy, and compliance with relevant standards. A hazzrd analysis minimizes these risks, as the loss from unaddressed hazards could involve patient safety, data breaches, and legal or financial consequences for the assessment organization.

3 System Boundaries and Components

The system referred to throughout the document consists of several major components:

1. **User Interface (UI)**: The front-end platform where users interact with the system. It allows users to navigate through the assessment, accepts inputs, and displays results.
2. **Backend Server**: The back-end platform handles data collection and processing, business logic, and communcation between all system components.
    - **Authentication**: Manages the login and access control mechanisms.
3. Assessment Recording
    - **Video Recording Module**: Responsible for capturing and transmitting video data during an assessment session.
    - **Audio Recording Module**: Responsible for capturing and transmitting audio data during an assessment session.
4. Assessment Analysis
    - **Video Analysis Model**: Processes and analyzes the video recording for disturbances and other behaviours against assessment instructions.
    - **Audio Analysis Model**:Processes and analyzes the audio recording for disturbances and other behaviours against assessment instructions.

5. **Database**: A centralized storage for all assessment results, recordings, analysis results, user data, and any other data as necessary.

The system boundary for this project includes the entire platform, consisting of the user interface, backend server, assessment recording and analysis components, and the database. Components such as the user's device (e.g. computer or tablet used for the assessment), and any third-party services used are external to the system and outside the control of the capstone team and will not be directly considered in the hazard analysis. The connections to external components however will be considered within the system boundary and may be included in the hazard analysis.

4 Critical Assumptions

1. Users have reliable internet access while using the web application.
2. The user's device is compatible with the web application and has the necessary capabilities and system requirements to run the assessment session.
3. Users will not share their password with anyone. (maybe remove? it's not about the software or the system directly -JS)
4. Any third-party services (e.g. cloud storage or hosting) used by the backend server are reliable and secure according to industry standards.
5. When a user is taking the assessment they will have a functional microphone and camera that meet the minimum requirements for recording assessment sessions.

5 Failure Mode and Effect Analysis

5.1 Hazards Out of Scope

The following are hazards that could occure outside the control of the system, thus they can't be fixed or mitigated.

- Wifi shuts down during assessment
- User hardware malfunctions during assessment

5.2 Failure Mode & Effect Analysis Table

The following FMEA table is a breakdown of the hazards that could occure within the system with a reccomended action to mitigate them.

Table 2: Failure Mode and Effect Analysis

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Database	1. SQL injection attack 2. Unauthorized access	1. Loss of confidentiality, integrity and availability of user data and assessment data. 2. Breach of sensitive patient data, violation of HIPAA.	1. Inadequate input validation or unparameterized SQL queries. 2. Administrative access is not validated and user accesses database directly.	1. Implement periodic data backups, prioritize and implement thorough database access controls, and use parameterized queries. 2. Add multi-factor authentication.	1. PR-RFT2, PR-RFT3 2. SR-AC3, SR-AC4	1. HA-D1 2. HA-D2
Authentication	1. Parent gets clinician level access 2. Users can't login	1. Unauthorized access to sensitive patient data, leading to potential HIPAA violations and data breaches. 2. Users are unable to access their accounts or data, leading to poor user experience.	1. Improper role-based access control implementation resulting in errors in user role assignment. 2. Errors in authentication logic or server downtime.	1. Do regular access audits to ensure clear separation of user roles. 2. Implement a fallback login and add error handling for feedback.	1. FR-A1,FR-A3 2. FR-A2,FR-A4	1. HA-A1 2. HA-A2

Continued on next page

Table 2 Continued from previous page

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Video Analysis Model	1. Model cannot access video recording 2. Model cannot detect user actions during analysis	1. Video-based analysis is incomplete or fails, which may hinder decision-making based on video data. 2. Reduced accuracy in behaviour detection or activity recognition.	1. Missing file permissions, incorrect file paths, or server-side issues. 2. Insufficient training data, low video resolution, or model overfitting to specific data types.	1. Validate file paths before processing, ensure proper access permissions, and log all access attempts for debugging. 2. Retrain model with more diverse data, improve preprocessing techniques like video upscaling, and evaluate model performance.	1. FR-VADA1 2. FR-VADA3	1. HA-VAM1 2. HA-VAM2
Audio Analysis Model	1. Model cannot access audio recording 2. Model cannot detect audio cues during analysis	1. Audio-based analysis is incomplete or fails, impacting the overall data analysis outcome. 2. Missed events or actions during analysis.	1. File corruption, incorrect file format, or lack of access permissions. 2. Inadequate training on diverse audio samples or background noise interference.	1. Validate audio files before analysis, provide user guidelines for supported formats, and log access errors. 2. Use noise reduction preprocessing, retrain the model with varied audio data.	1. FR-VADA1 2. FR-VADA3	1. HA-AAM1 2. HA-AAM2
Video Recording	1. Video recording is blurry	1. The video analysis model may miss critical details, leading to inaccurate analysis.	1. Low-resolution recording settings, poor camera quality, or motion blur.	1. Apply post-processing filters.	1. FR-SS3	1. HA-VR1

Continued on next page

Table 2 Continued from previous page

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Audio Recording	1. Audio recording has static	1. Poor quality audio makes it difficult for the model to detect speech or audio events accurately.	1. Faulty recording equipment, interference, or poor recording environment.	1. Filter static using software tools, and provide best practices for recording.	1. FR-SS2	1. HA-AR1
Backend Server	1. Data loss during processing 2. Server crashes due to user overload	1. Partial or complete loss of data during video/audio processing could result in incomplete analysis 2. Users may be unable to complete the assessment, or the server crashing could destory user data.	1. Server overload or incorrect handling of data transfer. 2. High traffic overload, memory leaks, or unhandled exceptions.	1. Use robust data storage solutions such as a temporary cache before saving. 2. Monitor server health and use proper exception handling to manage unexpected errors.	1. FR-DSC1, FR-DSC2 2. PR-CR1, PR-CR2, PR-CR3	1. HA-BS1 2. HA-BS2

Continued on next page

Table 2 Continued from previous page

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
User Interface	1. Error in navigation structure/flow 2. Button components aren't clickable	1. Users cannot move through the application smoothly, leading to frustration and a poor user experience. 2. Users cannot complete quizzes or perform specific actions and are unable to proceed through the interface.	1. Incorrect routing logic or implementation. 2. Errors in implementation.	1. Test navigation paths thoroughly and implement error logging for navigation failures. 2. Test UI components with different devices and browsers.	1. LF-AR2, LF-AR5 2. UH-AR1, LF-AR4	1. HA-UI1 2. HA-UI2

Concluded

6 Safety and Security Requirements

6.1 Security Requirements

HA-SER1. The system shall validate all SQL queries and ensure that input data is properly sanitized to prevent SQL injection attacks.
Rationale: Prevent unauthorized access, data corruption, and breaches of sensitive user information.
Fit criterion: All SQL queries must be parameterized, and inputs must be validated for known SQL injection vulnerabilities before execution.

HA-SER2. The system shall implement multi-factor authentication (MFA) for all users accessing sensitive patient data.
Rationale: Unauthorized access to patient data, which could lead to data breaches and violations of HIPAA.
Fit criterion: Users accessing sensitive data must pass a multi-factor authentication process within 2 minutes of a code being sent

HA-SER3. The system shall monitor server health and implement exception handling mechanisms to manage unexpected errors.
Rationale: Minimize downtime and data loss due to server crashes or overload
Fit criterion: The system should trigger a warning alert for server overload within 2 minutes, with exception handling enabling automatic recovery or failover mechanisms within 5 minutes.

7 Roadmap

The hazard analysis has identified several new security requirements that were not initially considered. However, due to the time constraints of the capstone project, not all of these requirements will be implemented at this stage. The team has decided to prioritize the implementation of requirement HA-SER1, as it is essential to ensure the security of the database. Requirements HA-SER2 and HA-SER3 will be addressed in future development phases after the capstone timeline.

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?

   The structured format and clear guidelines from both the document outline and lecture slides for writing the hazard analysis, as well as the student examples from previous years were helpful and provided a clear idea of what was expected from us for this deliverable.

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

   One of our main challenges was defining the system components and boundaries clearly, especially in deciding which external components to include or exclude in the hazard analysis. The team considered including third-party services and user devices as part of the boundary, but after further discussion, we decided to limit our scope to only include components the team can have control over. The reasoning for this is because including external components would have added complexities out of our control, such as third-party security protocols and user device management, which could vary and introduce risks that are outside our scope to address. This approach still lets us focus on designing reliable interactions with external systems, but not need to address the external components themselves.

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 conducting the hazard analysis, our team had already considered risks related to video and audio processing by asking "what if" questions, such as "What if the video is broken?" or "What if the audio is noisy?" However, during the hazard analysis, we began to explore deeper concerns related to database management and the hazards associated with it, which directly informed the new security requirements. We started by discussing the importance of securing patient data and recognized that for a software hazard analysis, database security was crucial to prevent any potential data leakage. This led to further discussions about other risks, such as SQL injection attacks and incorrect assignment of user roles, which are now captured in the updated security requirements.

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?

1. Data Security Risks: Risks such as unauthorized access, data breaches, and data leaks are critical because of the increased reliance on digital storage of sensitive information. A data breach could result in severe legal and financial repercussions, especially in healthcare applications where patient confidentiality is extremely important.

2. User Experience (UX) Risks: Things like confusing navigation or unresponsive interfaces can lead to user frustration, decreased usage, and even refusal to use the software. This is particularly important for non-technical users such as parents and children in a telehealth setting.