Hazard Analysis
Software Engineering

Team 13, Speech Buddies
Mazen Youssef
Rawan Mahdi
Luna Aljammal
Kelvin Yu

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 7, 2025	Kelvin Yu	Added Sections 1-4
Date2	Name(s)	Description of changes
...	...	...

Contents

1 Introduction

In the context of VoiceBridge, a hazard is any condition or event that could lead to harm, system failure, or loss of functionality during the collection, processing, and communication of speech data. The purpose of this analysis is to identify, evaluate, and propose mitigations for potential hazards before and during the system's lifecycle.

2 Scope and Purpose of Hazard Analysis

Our hazard analysis identifies potential risks that could compromise the VoiceBridge system throughout its development lifecycle and operational use.

Potential losses that could result from identified hazards include:

- Loss of user trust due to poor accuracy, delayed feedback, or confusing interactions.
- Loss of confidentiality if sensitive voice data, transcripts, or credentials are leaked.
- Loss of availability caused by hardware, software, or network failures that make the system unusable.
- Loss of integrity if documents or transcripts are modified, duplicated, or misinterpreted.

This scope ensures that both technical and human-interaction factors are considered when evaluating safety and usability risks.

3 System Boundaries and Components

VoiceBridge is a multi-component software system designed to convert and interpret speech reliably while protecting user data.

The main components analyzed for hazards are:

- Input Devices: Microphones and recording interfaces used to capture audio.
- ML Model Pipeline: The models responsible for phoneme recognition, intent detection, and command processing.
- Database/Storage: Secure repositories for user data, transcriptions, and system logs.
- Communication Layer: Real-time streaming, API connections, and message handling.

- User Interface: The front-end application where users interact and receive feedback.
- Third-Party Libraries and Services: External dependencies for authentication, hosting, and model frameworks.

Each of these components forms a boundary for potential hazards and has been evaluated for risks such as data loss, model inaccuracy, or accessibility failures.

4 Critical Assumptions

The following assumptions define the environment in which VoiceBridge operates and help focus this analysis on realistic and manageable risks:

- User devices and microphones are assumed to function normally, though temporary access loss or permission issues may occur and must be handled gracefully.
- Internet and cloud services are assumed to be available most of the time, but brief outages may happen. VoiceBridge must recover automatically.
- Users may provide imperfect audio (e.g., background noise or unclear pronunciation), and the system must tolerate and adapt to such inputs.
- Data storage systems and APIs are protected by authentication and encryption, reducing but not removing data-breach risks.
- Third-party and open-source libraries are assumed to be maintained and free from critical vulnerabilities, though version control and verification are required.

5 Failure Mode and Effect Analysis

[Include your FMEA table here. This is the most important part of this document. —SS] [The safety requirements in the table do not have to have the prefix SR. The most important thing is to show traceability to your SRS. You might trace to requirements you have already written, or you might need to add new requirements. —SS] [If no safety requirement can be devised, other mitigation strategies can be entered in the table, including strategies involving providing additional documentation, and/or test cases. —SS]

6 Safety and Security Requirements

[Newly discovered requirements. These should also be added to the SRS. (A rationale design process how and why to fake it.) —SS]

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

Appendix — Reflection

[Not required for CAS 741 —SS]

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