

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	Added Introduction, Scope and Purpose,
Date2	Name(s)	Description of changes
...

Contents

1	Introduction	1
2	Scope and Purpose of Hazard Analysis	1
3	System Boundaries and Components	1
4	Critical Assumptions	1
5	Failure Mode and Effect Analysis	2
6	Safety and Security Requirements	2
7	Roadmap	2

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 platform. 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 hazard 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

[Dividing the system into components will help you brainstorm the hazards. You shouldn't do a full design of the components, just get a feel for the major ones. For projects that involve hardware, the components will typically include each individual piece of hardware. If your software will have a database, or an important library, these are also potential components. —SS]

4 Critical Assumptions

[These assumptions that are made about the software or system. You should minimize the number of assumptions that remove potential hazards. For instance, you could assume a part will never fail, but it is generally better to include this potential failure mode. —SS]

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?