# Hazard Analysis
# Mechatronics Engineering

Team #1, Back End Developers
Jessica Bae
Oliver Foote
Jonathan Hai
Anish Rangarajan
Nish Shah
Labeeb Zaker

Table 1: Revision History

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

# Contents

[You are free to modify this template. —SS]

# 1 Introduction

In today's society, technology and engineering solutions are simply expected to work. The multitude of complex engineering designs and systems created to meet the needs of the world are expected to be infallible in the eyes of the public. When failures do occur, society considers them it shocking. When these failures happen in engineering systems critical to an aspect of safety, health, or some other critical role, people can die. In many cases, these failures are predictable and preventable in the design phase. The causes of such failures are known as hazards.

## 1.1 Purpose of Hazard Analysis

It is therefore necessary for engineers to perform extensive and thorough assessments of the systems they design in the aim to elimate as many failures as reasonably possible. This is process is called hazard analysis.

More formally, hazard analysis is a step in the process to assess risk within an engineering system. Its aim is to identify and assess the potential conditions which may cause failure. These hazards can exist and cause failures alone, or in combination with other hazards or conditions. Once completed, a hazard analysis should provide a comprehensive assessment of the hazards within a system according to the system's components and boundaries, the assumptions critical in performing judgements regarding hazards and the scenarios they may occur in, and the requirements necessary to ensure that these hazards will be mitigated within the realm of reasonable possibility.

# 2 Scope

The purpose of this document is to perform this hazard analysis on the system to be designed by the Back End Developers. This document will first provide a description of the system boundaries and components of the system on an abstract level (both the hardware and software components), and then will list and justify the assumptions made in order to perform this hazard analysis. These assumptions will be kept to a minimum, in the hope to reduce the number of potentially overlooked hazards. The document will then describe the Failure Mode and Effect Analysis (FMEA) done by the team of the Back End Developers, and then detail the specific safety and security requirements that have been discovered in the process of performing the hazard analysis. The document will end with a roadmap describing the steps which will be taken in order to implement the novel discovered requirements, the timeline in which they will be implemented, and what considerations must be made regarding said requirements.

# 3 System Boundaries and Components

# 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 —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]