

Hazard Analysis v1.0

Group 4: Autonomous Foosball Table

|  |  |
| --- | --- |
| Ryan Ma | 1147335 |
| Chenhe Li | 1158035 |
| Taha Hussain | 1200349 |
| Viktor Smirnov | 1154392 |
| Roland Zhou | 1216063 |
| Alvin Li | 0957972 |

# 

# **1 REVISIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0 | Dec 26, 2015 | Ryan Ma,  Chenhe Li,  Taha Hussain,  Viktor Smirnov,  Roland Zhou,  Alvin Li | Initial version |
| 0.1 | Dec 27, 2016 | Ryan Ma,  Chenhe Li,  Taha Hussain, | - Added STPA |
| 1 | Feb 27, 2016 | Taha Hussain,  Ryan Ma,  Chenhe Li,  Roland Zhou,  Alvin Li | - Added severity rating and added additional failures  - Updated format |

Table 1. Revisions

# 

# 

# **2 TABLE OF CONTENTS**

|  |  |
| --- | --- |
| [Revisions](#h.jn80cq2zvfe3) | 1 |
| [Table of Contents](#h.ddx98bh1tboj) | 2 |
| [List of Figures](#h.xa6jscwllanc) | 3 |
| [List of tables](#h.6wu6oulp10n3) | 4 |
| [Introduction](#h.l3ahpe1ue1gi) | 5 |
| [Purpose](#h.t4ewuay0clr5) | 5 |
| [Scope](#h.wk1jtpdgin3v) | 5 |
| [Background](#h.6jlu7j5sdn6h) | 5 |
| [Roadmap](#h.dmwexrwi4p1l) | 5 |
| [Overview](#h.4kwod21bhct9) | 7 |
| [STPA](#h.bcppzbvgxcgo) | 8 |
| [Introduction](#h.ma9tbw1vv7v6) | 8 |
| [System Schematic](#h.8jcd69dqzajn) | 8 |
| [STPA Diagram](#h.gkfsn4qgfc20) | 9 |
| [STPA Chart](#h.9beqbkdc9ftr) | 9 |
| [FEMA](#h.3rvfeujmaa5j) | 11 |
| [Introduction](#h.dnjg5enrjq1l) | 11 |
| [FEMA Chart](#h.vo3z4ulbh04) | 11 |

# 

# 

# **3 LIST OF FIGURES**

[Figure 1. Roadmap](#id.r4e2kmqg0k09)

[Figure 2. Function Overview](#id.66kc29n5iww0)

[Figure 3. Control Diagram of Autonomous Foosball Table](#id.prs692yhsjv1)

[Figure 4. Control Diagram of Autonomous Foosball Table with Hazard](#id.ngmketmoiel6)

# 

# 

# **4 LIST OF TABLES**

[Table 1. Revisions](#id.90fttjcu423p)

[Table 2. Potentially Inadequate Control Actions](#id.3zj87tfm0f85)

[Table 3. FMEA](#id.g7adsj33mt25)

# 

# 

# **5 INTRODUCTION**

## **5.1 Purpose**

The purpose of this document is to assess and describe the potential risks involved in the use of the autonomous foosball table. Hazard analysis is performed in order to identify different types of hazards and conditions that can potentially cause a functional failure or accident.

## **5.2 Scope**

This document focus on identifying different types of hazards scenarios that a user could face during when operating the system. These are specific safety issues that were considered to improve the design of the system. General failures will be considered as well. [System Theoretic Process Analysis (STPA)](#h.bcppzbvgxcgo) and [Failure Modes and Effects Analysis(FMEA)](#h.3rvfeujmaa5j) are used in this document to perform such systematic analysis and assess the various risks involved with Autonomous Foosball Table

## **5.3 Background**

The autonomous foosball table is a foosball table that offers a robotic opponent which can challenge human players. It allows one to play foosball without the need of finding another human opponent and play with AI on different difficulty levels.

## **5.4 Roadmap**

[Figure 1](#id.sqli33oa3ily) below is the roadmap for this project. (For detailed version click this [link](https://docs.google.com/spreadsheets/d/1D8vNFgQwGkfuoN6klKOyD6agbPdgBtAi7UDL9EPomso/edit?usp=sharing) )

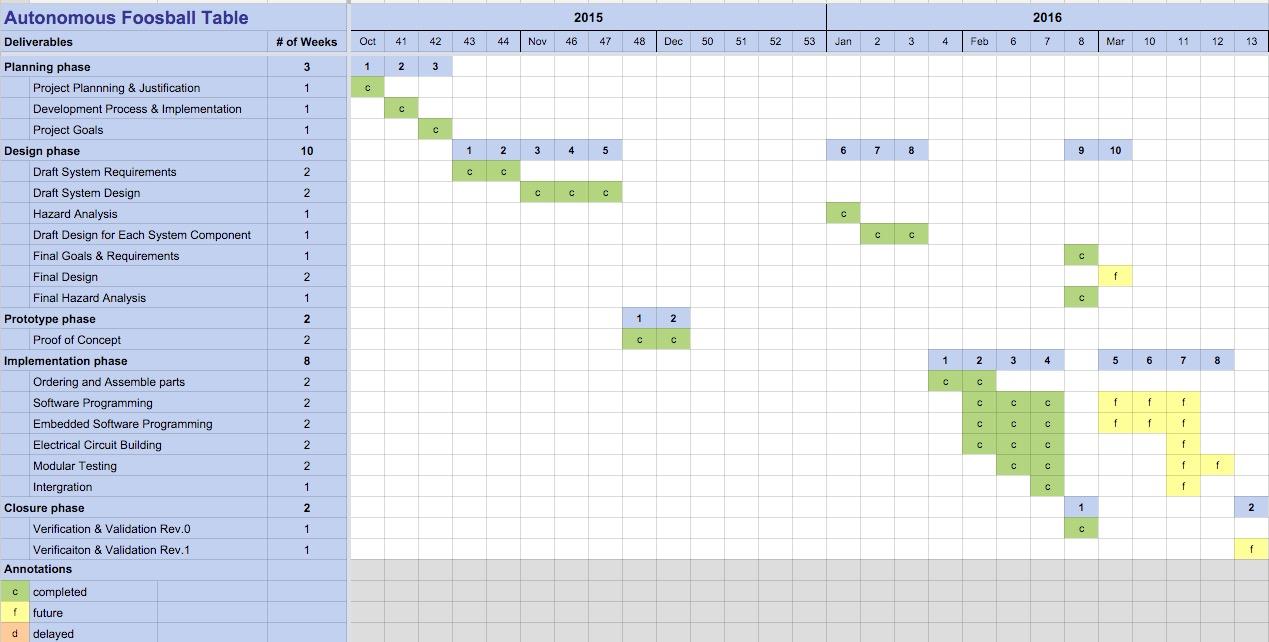


Figure 1. Roadmap

# 

# 

# **6 OVERVIEW**

A general overview of the system design is highlighted in this section. This gives an insight into how the system is interfaced. The core functions are broken down and shown in the [diagram below.](#id.ctm4szumupnh)

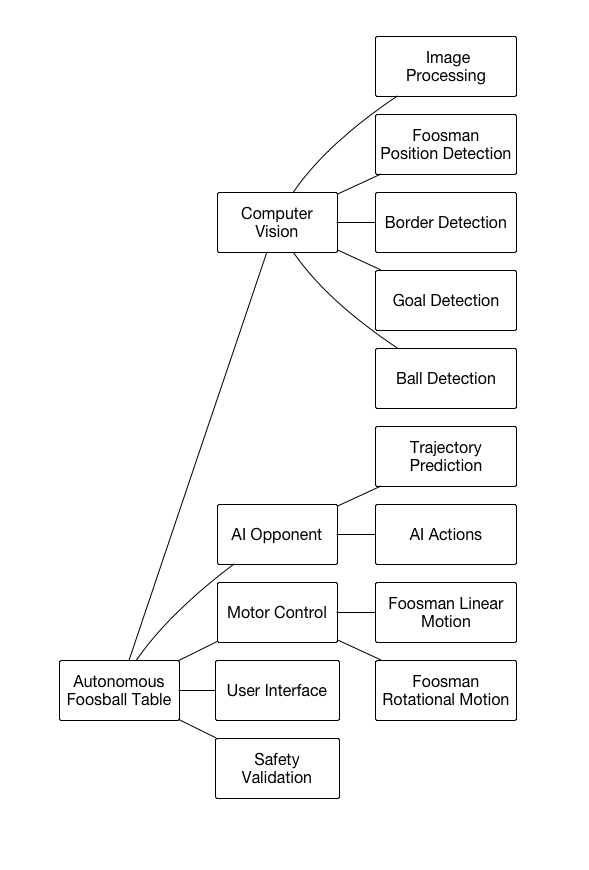


Figure 2. Function Overview

# **7 STPA**

## **7.1 Introduction**

The [STPA diagram](#h.gkfsn4qgfc20) is designed to analyze the various components of a system to detect any potential failures or faults that may arise and the possible impacts that may occur due to those failures.

## **7.2 System Schematic**

[Figure 3](#id.ipbvtb4hyp2i) below is a simple representation of the system schematic.

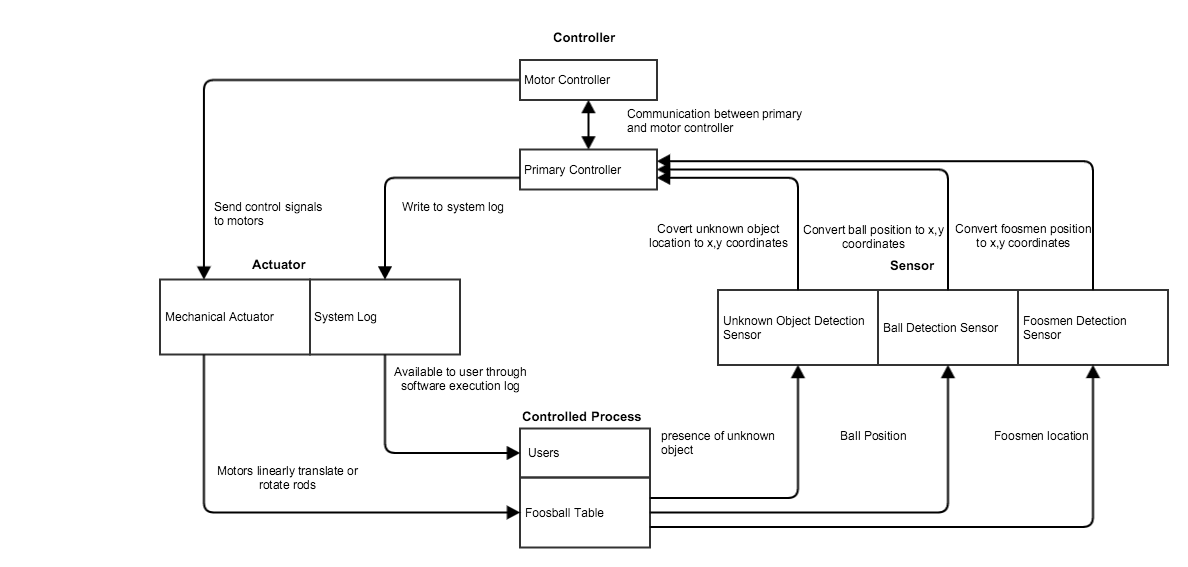


Figure 3. Control Diagram of Autonomous Foosball Table

## **7.3 STPA Diagram**

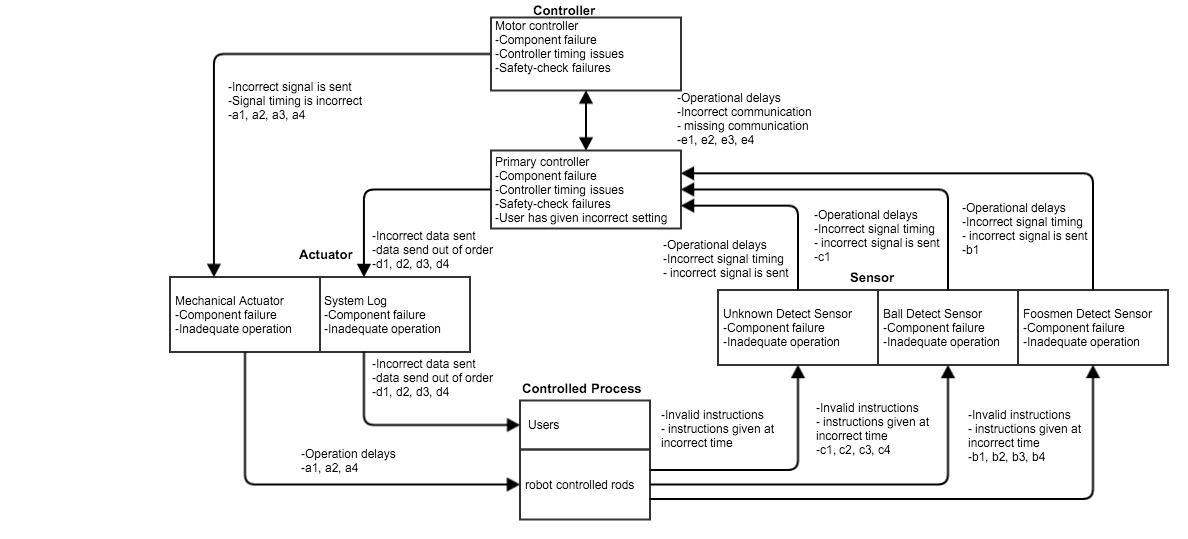


Figure 4. Control Diagram of Autonomous Foosball Table with Hazard

## **7.4 STPA Chart**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Action** | **A control action required for safety is not provided or is not followed.** | **An unsafe control action is provided that leads to a hazard** | **A potentially safe control action is provided too early, too late, or out of sequence** | **A safe control action is stopped too soon** |
| Foosmen Actuator | System does not output foosmen’s speed or position when desired.(a1) | System outputs incorrect foosmen’s speed or position.(a2) | Foosmen could move to the desired location too early or too late and not hit the ball. Foosmen could also move to incorrect location.(a3) | Foosmen move to incorrect location.(a4) |
| Get Foosmen Position Feedback | Input foosmen position is incorrect.(b1) | Incorrect foosmen position is entered.(b2) | Foosmen position is incorrect.(b3) | Incorrect foosmen position is transmitted.(b4) |
| Get Ball Position Feedback | Input ball position is incorrect.(c1) | Incorrect ball position is entered.(c2) | Ball position is incorrect.(c3) | Incorrect ball position is transmitted.(c4) |
| Logging Information | System fails to write information to the log.(d1) | The information that is being logged or shown is incorrect.(d2) | Logging information is recorded out of sequence could write incorrect information to the log.(d3) | Logging operation ends before it finishes.(d4) |
| Communication between controllers | Data transmits between controllers is incorrect.(e1) | Incorrect data transmits between controllers.(e2) | Data transmits too early, too late, or out of order could lead controller do wrong action.(e3) | Incorrect data transmits between controllers.(e4) |

Table 2. Potentially Inadequate Control Actions

# 

# 

# **8 FEMA**

## **8.1 Introduction**

The FMEA is designed to analyse equipment and systems to detect failure and its effect on the system. The chart is broken up into two main categories, the issues that result from failure (how it can harm the user or the system), and the steps in place to reduce the damage said failure cause on the system (how user is kept safe)

## **8.2 FEMA Chart**

**Severity ratings:**

* A high severity rating implies this failure will cause damage to human player or surrounding environment. High severity failures should be avoided at all cost.
* A medium severity rating implies that this failure will cause damage to the entire system but will not hurt the human player or damage the surrounding environment. Parts of the system may need to be replaced in order to recover from a medium severity failure.
* A low severity rating implies the failure will cause the system to malfunction but will not cause permanent damage to the system, human player or surrounding environment. A reset of the system shall fix a low severity failure.

**Detection ratings:**

* A high detection rating implies this failure is being continuously checked and there are several ways of monitoring the device or function.
* A medium detection rating implies this failure is being continuously checked but there is only one way of monitoring the device or function.
* A low detection rating implies that this failure is not being continuously checked and can only be detected by manual inspection.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item/**  **Function** | **Failure Modes** | **Effects of Failure** | **Cause of Failure** | **Detection** | **Controls** | **Severity rating** | **Detection rating** | **Recommended Action** |
| Robot controlled rod | -Mechanical structure  deforms  - Linear  actuator gets damaged | User can be hurt by the movement of the rod | Rod is not covered on user side and  robot controlled rod is moving linearly or rotationally | Continuously checking  monitored inputs against sensor  operating range | - Send stop signal to motor controller  - System goes to stop state | High | Medium | -Cover user side robot controlled rod with acrylic cover |
| User interface | - Input device malfunction  - Value delayed | - User input is undetected  - System  unresponsive  - Mistaken input | - Input device malfunction  -Communication cable damages  - Loose connection  - Controller overload | -Initialization system with safety check  - Continuously checking  monitored inputs | - Input devices verification prior to installation  - System goes to stop state | Low | High | - Restart system |
| Rotational motion | - Rotational stepper  motor  malfunction  - Motion restricted de to obstacles | Foosmen’s rotational movement is undesired or incorrect | - Internal mechanics failure  - Control system failure  - Motor malfunction  - Loss of power  -Excess power | -Continuously checking foosman’s angular position and compare if they are within a certain tolerance  -Continuously checking outputs from controller | - Actuator verification prior to  installation  - System goes to stop state  - Software  range checking | High | High | - Perform maintenance by technican  - Conduct repair protocols  - Press emergency stop  button |
| Image processing | Camera malfunction  - Image data transmission delayed  - No image  - Low image quality  - Defective camera | Ball position and unknown detection are misjudged and the  system acts erratically | - Defective camera  - Defective cable  - Loss of communication to controller  - Insufficient lighting | -Initialization safety check  -Continuously checking  monitored inputs against sensor  operating range | - Sensor verification prior to  installation  - System goes to stop state  - Software restricts linear and rotational motion | Medium | High | - Perform maintenance by technican  - Conduct repair protocols  - Press emergency  button  - Restart system |
| Power supply | -Power supply malfunction  - No power  - Not enough power  - Excessive power | - System freezes  - System overheats | - Loose connection with power supply  - Power outage  - Power overload  - Power short circuit | - Visual inspection  - System no response | - Internal safety built into power supply for current protection  - LED on power supply indicates power status | High | Low | - Replace power supply  - Perform maintenance by technican |
| Foosmen position detection | - Image processing malfunction  - User program malfunction  - Communication blocked | Reaction of system is incorrect or system is non responsive | - Losing connection  - Defective sensor  - Controller overload | -Continuously checking  monitored inputs against sensor  operating range  -Initialization safety check | - Sensor verification prior to  installation  - System go to safe stop | Low | Medium | - Confirm camera meets design specification. If not, replace camera  - Restart system |
| Ball detection | - Image processing malfunction  - User program malfunctions  -Communication blocked | reaction of system is incorrect or system is not responsive | - Low quality image inputs  - Detection algorithm failure  - Long processing time | -Continuously checking the inputs from camera | -System goes to stop state | Low | Medium | - Make the room brighter  -Improve ball detection algorithm |
| Unknown object detection | - Image processing malfunction  - User program malfunction  -Communication blocked | - Not able to detect unknown object  - May cause damage to human or system  - False alarm | - Low quality image input  - Detection algorithm fail  - Long processing time | - Manual checking and testing conducted by user | -System goes to stop state | High | Medium | - Press emergency stop button  - Perform maintenance by technican  - Conduct repair protocols  - Restart system |
| Linear motion | -Stepper  motor malfunction  -Interrupted communication | Linear movement is incorrect  Stepper motor skips steps | - Stepper motor cannot handle the frequency of the input signal  - Invalid motor inputs  - Motor malfunction | -Continuously checking linear motion controller to compare their values within a certain tolerance  -Continuously check processor outputs | - Lower signal frequency  - Software linear position correction through feedback sensors  -excess current protection enabled on controller | High | High | - Press emergency stop button  - Remove obstacles hindering motor movement  - Check motor inputs boundaries |
| Linear motion | Stepper  motor malfunction | Linear movement is incorrect or restrict | - Defective motor  - Motor loses Loss connection to Stepper driver  - Stepper driver loses connection to controller  -Stepper Driver malfunctions | -Continuously checking linear motion controller to compare their values within a certain tolerance  -Continuously checking processor outputs | - Actuator verification prior to  installation  - System goes to stop state | High | High | - Press emergency stop button  - Perform maintenance by technican  - Conduct repair protocols |
| Safety  validation | Safety validation malfunction | Loss of synchronization | - Faulty MCU  - Loss of connections  - Loss of power | - System going to emergency stop mode | -Verification prior to installation | High | Medium | - Press emergency stop button  - Perform maintenance by technican  - Conduct repair protocols |
| Communication | Communication malfunction | -Loss of synchronization  -transmission between controllers. | - Loose connections  - Faulty MCU  - Sending incorrect data  - Loss power | -Controllers handshake every 100ms  -Adding parity bits for checking correctness | Verification prior  to installation | Low | High | - Restart system  - Conduct repair protocols |

Table 3. FMEA