Autonomous **I**nteractive **R**obot for Air Hockey (**AIR**)

Hazard Analysis

SFWR ENG 4G06 / MECHTRON 4TB6

GROUP 3

Nima Akhbari

Daniel Chaput

Nicholas Cianflone

Michael Rowinski

Joshua Segeren

Evan Skeete

Contents

Table of Figures

Revisions

Version	Date	Authors	Revision Description
0.1	2015-01-05	Nima Akhbari Daniel Chaput Nicholas Cianflone Michael Rowinski Joshua Segeren Evan Skeete	Initial revision.
0.2	2015-01-09	Nima Akhbari Daniel Chaput Nicholas Cianflone Michael Rowinski Joshua Segeren Evan Skeete	Updated context diagram and FMEA worksheet.
1.0	2015-03-03	Michael Rowinski	Addressed shortcomings of V0.2 as discussed by TAs 1. Updated sections 3.1, 3.2, 3.7 2. Removed sections 3.5, 3.6, 3.10 3. Added reference numbers to FMEA worksheet
1.1	2015-03-04	Joshua Segeren Michael Rowinski	Minor revision; documented implemented safety mechanisms, additional feedback addressed Updated FMEA worksheet sections 4.1.4.1, 4.2.2.0

1 Introduction

An important part of every system design is ensuring that the final product meets and exceeds all safety requirements. In consideration of whether a system is safe to use, the hazards associated with the system must be determined. This can be done through the use of various hazard analysis techniques available. The Failure Modes and Effects Analysis (FMEA) method was used in developing a hazard analysis for the robotic system AIR. In the sections that follow, comprehensive considerations were taken to ensure user/system safety while including analysis of the various system failure states that may occur. The focus on user perspective led to a better understanding of the system as a whole and allowed for design considerations to be made that promote safe and more consistent usage of the AIR system.

2 Overview

2.1 Component Overview

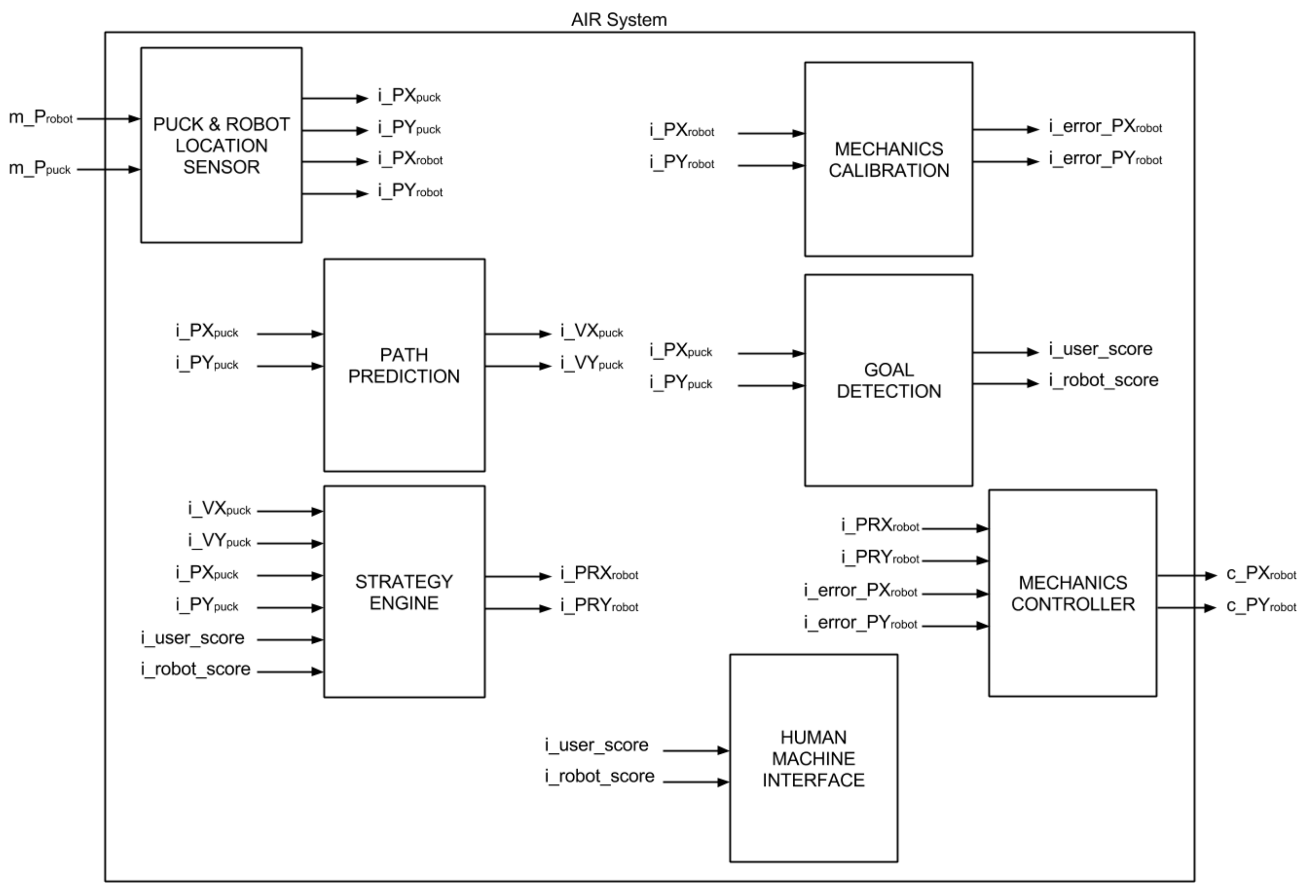

Figure 1 - System Functions

2.2 Component Descriptions

2.2.1 Puck & Robot Location Sensor

This component detects the location of the puck, the robot mallet, and the frame of reference used to identify the coordinate plane origin.

2.2.2 Path Prediction

This component determines the path and trajectory of the puck by using puck location data (over time) to predict the puck motion and velocity. This component is integral for the system to react and strike the puck at an appropriate location and time.

2.2.3 Strategy Engine

This component determines the type of reaction the robot will have to the puck. The engine selects various offensive and defensive gameplay strategies based on the flow of the game.

2.2.4 Mechanics Controller

This component interfaces with the motor controller to control the position, velocity, and acceleration of the mallet. Using the required position calculated by the strategy engine and the current error as seen by the mechanics calibration component, the mechanics controller controls the stepper motors by way of a PWM signal to the motor controller.

2.2.5 Mechanics Calibration

This component provides feedback to the Mechanics Controller by continuously calculating the deviation between the desired robot mallet position and the actual position.

2.2.6 Goal Detections

This component utilizes the puck's location in the coordinate plane to determine when the puck has entered the goals.

2.2.7 Human Machine Interface

This component provides a communication layer between the AIR system and the user using a seven-segment display.

3 Safety Considerations

The safety of the user is paramount therefore special care was taken when determining all modes of failure that may negatively affect the user. The air hockey table itself is not within the scope of this hazard analysis. Users who wish to use the AIR system should be aware of any risks associated with normal air hockey play. The robot component of the AIR system was analyzed thoroughly for any safety hazards it introduces to the game of air hockey. The hazards associated with the robot can be seen below with a description of the issues along with solutions to prevent injury.

3.1 Power Supply Failure

Issue:

- System no longer has power or function and all previous commands, actuations or movement will continue without system intervention.
- There exists a potential damage to equipment.

Solution:

- Hardware safety circuit implemented to terminate robot motion if the robot leaves its workspace
- Hard stops on the track will prevent the robot from over travelling and potentially harming the user.

- System will need to be rebooted.

3.2 Collision/Projectile Hazard

Issue:

- Puck/debris collides with user/spectator on or off the table (ricochets off the table).

Solution:

- Limit force exerted on the puck by the robot ensuring puck remains on the table
- Keep surface of table free of defects and debris
- Implement mallet handling mechanism that compensates for uneven table surface to ensure proper motion and puck contact
- User or spectators are assumed to know the potential risks when playing air hockey.

3.3 Pinch/Moving Parts Hazard

Issue:

- Robot component (i.e. axes carriages) is exposed and presents a potential pinch hazard. This could occur if a user places body part within workspace of the robot, along table edges, or otherwise near moving parts (including the motors and fans).

Solution:

- Players/spectators will be notified about the pinch/moving parts hazards both verbally before playing and via signage.
- Danger/warning signs will be put in the areas where pinch/moving parts hazards are present.

3.4 Motor Belt Snapping

Issue:

- If the belt snaps under load there is a potential for the belt to hit the user.
- Belt poses a pinch hazard to the user.

Solution:

- Ensure that the belt has been tensioned correctly and that the potential energy in the belt is in an acceptable range.
- Belt should not be tensioned past the point where slip no longer occurs on the pulley.

3.5 Burn Hazard

Issue:

- Electrical components may become hot during system use. If user touches circuit boards, power supplies, or motors the user may be burned.

Solution:

- Mount electrical systems far from the user where applicable

- Enclosures will be used where applicable
- Demarcate the hazards and notify the user of the hazard.
- Ensure sufficient ventilation is supplied to the components where applicable.

3.6 Loose wire

Issue:

- The user can be electrocuted and injured by exposed wires.

Solution:

- Ensure wires are mounted properly before starting the game.
- Minimize or eliminate loose wires and prototyping boards to prevent wires from becoming loose.
- Demarcate the hazards and notify the user of the hazard.

3.7 Exposed Power Terminals

Issue:

- Shock and/or electrocution if terminals are touched

Solution:

- Cover exposed terminals with finger protection.
- Ensure wire is properly secured and demarcate the hazards

3.8 Ergonomics

Issue:

- If there is a height mismatch between the player and table (i.e. dimensions proportions are not optimal), or excessive reaching is entailed in gameplay, there is a long-term ergonomic risk to the user.

Solution:

- Since this is considered a standard risk inherent in table-based sports, including regular air hockey, no active solution is required.
- Dimensioning the table to the standard proportions will best serve general user needs.

4 FMEA Worksheet

Design Component	Ref. #	Failure Modes	Causes of Failure	Effects of Failure	Detection	Controls	Recommended Action
Puck & Robot Location Detection	- 4.1.1.0	- Puck not detected	- Puck removed from or leaves table for sufficient duration - Camera hardware failure - Video interface/stream failure	- Robot stops moving	- Software check with duration tolerances	- Camera mounted to prevent/ minimize movement (i.e. ensure structural integrity) - Ensure puck remains on table	- Error output to user; system pauses and enters safe state for manual diagnosis - Ensure camera clear of obstruction and not pushed out of position
	- 4.1.1.1	- Incorrect object detected as puck - Multiple pucks detected	- Debris or other objects enter the workspace	- Erratic and unpredictable system behaviour	- Software check based on controls feedback - Visual check	- Supply only one puck to users - Limit detectable objects	- System pauses and enters safe state until table cleared - Clear debris and unwanted objects off the table

Path prediction	- 4.1.2.0	- Puck path cannot be predicted, or is not correctly predicted	- Incorrect or no puck detection - Software crash or failure	- Robot decreases in accuracy or becomes completely inaccurate - Game is delayed	- Software check based on consecutive misses (controls feedback)	- Software fall-back to defensive and/or real-time strategy (i.e. operational under no prediction)	- Restart game
Strategy Selection	- 4.1.3.0	- Strategy selection stuck between modes or not selected	- Software crash or failure	- Game is delayed	- Software and visual check	- Designate a default strategy	- Restart game
Goal Detection	- 4.1.4.0	- Goal is not detected	- Camera is blocked - Location of puck is lost	- Goals not updated; game unable to finish and decide winner	- Software check to determine if the camera is failing.	- Extensively test goal detection prior to release of system to the public	- Obstruction of camera must be cleared before the continuation of gameplay
	- 4.1.4.1	- Goal is falsely detected	- Software failure - Faulty switch	- User or robot gains an extra point	- Visual check	- Extensively test goal detection prior to release of system to the public	- User to decide whether to reset the game or continue playing - Replace switch if required

Mechanics Calibration	- 4.1.5.0	- Frame of reference not found	- Camera fails - Reference markers for detection are not found	- Robot accuracy decreases	- Software check	- Camera mounted in a way to prevent movement	- Ensure camera clear of obstruction and not pushed out of position
Mechanics Controller	- 4.1.6.0	- Connection to stepper motors lost	- Cable damaged or otherwise fails - Cables removed from terminals	- Robot would be unable to move in desired direction - Robot or other equipment may become damaged	- Visual check of the cables prior to system start - Software check; if no motion is detected from the robot in a given time stop the system	- Limit use of prototyping boards and ensure strong build quality - Prevent ability to damage cables where possible	- Shutdown system and perform necessary maintenance
Mechanics (robot)	- 4.1.7.0	- Robot carriage exits workspace	- Proper momentum exceeded - External force applied to carriage - Unexpected collision occurs - Belt/frame failure	- Robot, carriage table or belt damaged	- Visual detection; system stops	- Limit switches & hard stops on structure tracks to prevent/mitigate mechanical damage	- Reset carriage manually; shut down system and restart

Human-Machine Interfacing	- 4.1.8.0	- Display stops working	- Display burns out - Display damaged - Communication to display fails	- Unable to see score and normal system diagnostics (including warning/error reporting)	- Visual check of display upon starting the system and/or scoring goal	- Validate display prior to installation - Ensure display is operational before beginning a game	- Replace display and repair any broken connections
		User Perspective Hazard Considerations					
Power Supply Failure	- 4.2.1.0	- System no longer has power	- System power is disconnected	- System loses power and control - System comes to a complete halt	- Visual detection that games has stopped or power supply is damaged	- Power supply is protected from tampering	- User reconnects power and restarts the game
	- 4.2.1.1	- Damage to equipment affects system power	- Damage to power supply has removed power from system or a specific component				- Damaged supply is replaced

Collision/Projectile Hazard	- 4.2.2.0	- Puck or debris collides with user/spectator (on or off table)	- User has body parts on table during play - Puck or debris is knocked off the table into user	- Potential injury to user - User dissatisfaction with system	- Visual detection	- Extensive system testing to verify puck will remain within the confines of table - Keep unnecessary objects away from and off the table - Mechanism to keep robot mallet on workspace surface	- Users understand risks when playing air hockey -
Pinch/ Moving Parts Hazard	- 4.2.3.0	- Exposed robot parts present a moving or pinch hazard	- Exposed robotic parts	- Potential injury to user - User dissatisfaction with system	- Visual detection	- Extensive system testing to demarcate the hazards to user (verbally and via signage)	- User is notified of potential hazards verbally and via signage (demarcate the hazards - Unqualified users kept away from robot side of table

Motor Belt Snapping	- 4.2.4.0	- Robots driving belt(s) snap/break	- Belt is overly tensioned - Wear on the belt causes it to fail	- Robot loses control of actuating parts - Potential injury to user - User dissatisfaction with system	- Visual detection	- Extensive system testing to ensure belts have been tensioned properly and safely	- Damaged belt is replaced
Burn Hazard	- 4.2.5.0	- Electrical components become hot during use	- Overuse of the system - Damage to electrical components	- Potential injury to user - User dissatisfaction with system	- Visual detection	- Ensure ventilation to components that may heat during use - Demarcate hazards to user	- Gameplay is temporarily stopped to allow parts to cool
Loose Wire/Exposed Power Terminals	- 4.2.6.0	- Exposed wires that are live - Exposed power terminals	- Tampering with system - Damage to system	- Potential injury to user - User dissatisfaction with system - Power or component is compromised	- Visual detection	- Ensure systems wires and power supplies are properly mounted/covered - Demarcate hazards to user (verbally and via signage)	- Stop gameplay until repairs have been made to the system

5 Conclusion

In order to reach a system design that ensures user as well as system safety, a thorough hazard analysis must be completed at the appropriate development stage. Using the FMEA method a comprehensive list of considerations were documented and recorded for use in further design iterations or AIR. As stated before the safety and wellbeing of the end user is of utmost importance to the team and care has been taken to identify and remove/mitigate potential hazardous scenarios. Time and budget constraints have made it impossible to completely remove all hazards. In cases where hazards cannot be completely removed, adequate warnings have to be put in place so that the user is aware of the safest ways of interacting with the machine. Application of this hazard analysis will ensure this system adheres to safe and acceptable standards of design as development of AIR proceeds.