Hazard Analysis

Mechtron 4TB6 • Prof. Alan Wassyng

Group 34

Authors:

Ahmed Afifi

Abdulrahman Elgendy

Mina Ghaly

Omar Mouftah

Table Of Contents

1. Table Of Revisions

Version	Date	Authors	Description Of Revision
0	3/12/2021	Abdulrahman Elgendy Ahmed Afifi Mina Ghaly Omar Mouftah	Initial revision of the hazard analysis document

2. Introduction

The purpose of this document is to provide information regarding possible failures and safety considerations for Intellux. Component purposes and potential failures and their mitigations will be discussed on a high level along with possible safety concerns that users may need to take into consideration.

3. Component Overview

Our Intellux system can be divided into the following hardware and software components described below.

3.1 Hardware Components

3.1.1 Mechanical Blinds Rotation System

The mechanical part of the rotation system consists of the stepper motor and gears. The stepper motor is connected to the gear system while the beads slip on the gear teeth to facilitate the movement of the blinds.

3.1.2 Microcontroller

The microcontroller is responsible for running the control software in charge of automating the blinds as per the user's preferences. It will also host the user application locally, which can be accessed through any Internet-enabled device as long as the device and microcontroller are connected to the same network.

3.1.3 Lux Sensors Setup

This component consists of the two lux sensors that will provide brightness information to our Intellux system. One lux sensor will be used to measure the current brightness of the room and the other lux sensor will be used to measure the external brightness. By measuring the internal and the external brightness, Intellux would be able to determine if the user's desired brightness level is possible. Once it determines that it is possible, the blinds will automatically be rotated to achieve the user's desired brightness.

3.1.4 Mechanical Enclosure

The mechanical enclosure is the box that confines the entire Intellux apparatus. It will host all the physical parts in a single box including the rotation system, microcontroller, sensors and power circuit to ensure a barrier between the user and any moving or electrical parts.

3.1.5 Power Circuit

The main power circuit will supply power to the microcontroller and other electronic equipment attached. The circuit will be battery powered for safety concerns and ease of use.

3.2 Software Application

3.2.1 User Interface

The user interface will provide users the ability to interact with the Intellux apparatus. It consists of on-screen commands and functionality that allow the user to send, retrieve, and view data regarding the operation of Intellux. This will be possible by connecting the user interface to the database and backend of the system.

3.2.2 Control Algorithm

This component consists of the control algorithm that determines the instructions to be provided to the Intellux apparatus based on inputs from the user and lux sensors. The control algorithm ultimately determines the blinds angle to try and achieve the user's desired brightness.

3.2.3 Database

The database will store information input by the user through the user interface. This will include all CRUD functionality to create, retrieve, update, and delete information in the database. This data will be used to help Intellux operate autonomously without consistently requiring user input.

4. Safety Considerations

4.1 Hardware Components

4.1.1 Mechanical Blinds Rotation System

Risks:

1. One of the gears could snap and lose contact with the beaded wire
2. The stepper motor could burn or overheat due to faulty power supply
3. The motor and gears are moving parts and could present a hazard if not properly enclosed
4. The beads of the blinds could break and splatter inside the apparatus
5. The beads wire could slip off the gear groove, creating unpredictable behaviour

Mitigations:

1. Avoid 3D printing gears if possible as they might not be of good enough quality
2. If 3D printing gears is the only option then ensure the use of a good quality filament
3. Reduce the motor's running current ***
4. Ensure every component of the rotation system is secured in place
5. Set speed limits on the motor as to not overstress the beaded wires of the blind
6. Ensure the gear teeth perfectly fit the bead size

4.1.2 Microcontroller

Risks:

The concerns regarding the microcontroller are:

1. The microcontroller overheating
2. Any short circuits within the microcontroller
3. Crashing or failure of the locally hosted software application

Mitigations:

1. Design proper cooling of the microcontroller within the mechanical housing
2. Using limiting resistors where necessary and ensuring the device has no loose connections

3. Running the application service with backup services to reboot the application service if a crash occurs.

4.1.3 Lux Sensors Setup

Risks:

The following issues can affect the functionality of the sensor, and the control system may obtain incorrect sensor values as a result

1. Sensor contamination or obstruction
2. Sensor falling from attached position in the enclosure
3. Manufacturer Error
4. Sensor operating outside the recommended operating environment (For example: sensor used in an environment with temperature outside the recommended temperature range)

Mitigations:

The following mitigations will be used to address the issues mentioned above

1. Specifically instruct the user not to obstruct the sensor that are mounted on the enclosure, and attempts will be made in the software to try and predict if a sensor is blocked or contaminated
2. Design the mechanical enclosure with extra support for the sensors so that they can be properly mounted and supported without falling off
3. Rigorously test all sensors purchased before installing them in the Intellux system to ensure that they function correctly
4. Clearly label the optimal and recommended operating environment in the user manual for the Intellux system so that the users don't use the system in incompatible environments

4.1.4 Mechanical Enclosure

Risks:

1. The wires inside the eclouse could be exposed if not safeguarded properly
2. The enclosure could break and expose moving parts or electrical components
3. Improper mounting of the apparatus could result in unpredictable risks

Mitigations:

1. Ensure all wires are of proper length and are tied down
2. Create a enclosure from good quality materials
3. Perform stress test on the mechanical enclosure to ensure dexterity and durability
4. Create an easy to follow mounting tutorial to ensure proper mounting by any user of the apparatus

4.1.5 Power Circuit

Risks:

There are a couple of inherent risks involved with the power circuit and they are:

1. Spontaneous lithium-ion battery fire hazard
2. Power supply failure (i.e. battery supply dying without warning)
3. Exposed power terminals

Mitigations:

1. Minimizing spontaneous combustion of lithium-ion batteries will be done by designing a proper battery mount and by including a battery cooling system to prevent overheating.
2. Include a battery level indicator on the microcontroller to warn the user of low-battery levels
3. Fully enclosing all wires within the housing of the apparatus

4.2 Software Application

4.2.1 User Interface:

Risks:

1. Loss of connection to microcontroller
2. Communication lag

Mitigations:

1. Alert user when connection is unstable
2. Inform user if the device is out of range

4.2.2 Control Algorithm:

Risks:

1. Software bugs which can lead to inaccurate control decisions
2. Control outputs that are unachievable due to the limits of the Intellux system

Mitigations:

1. Perform unit tests, integration tests, regression test during the development of the control algorithm to ensure that the algorithm works as expected
2. Always limit the output of the controller to what is achievable by the Intellux system

4.2.3 Database:

Risks:

1. Database Liable to threat

Mitigations:

2. Host locally

5. FMEA Worksheet

Design Component	**Ref #**	**Failure**	**Effect of Failure**	**Severity of failure (0-10, 0 being least severe)**	**Cause Of Failure**	**Likelihood of occurrence (0-10, 0 being least likely)**	**Recommended action**
Mechanical blinds rotation system	4.1.1.1	Gears snap/lose contact	Loss of function	10	Poor gear manufacturing or overtesting	1	Invest in 3D printing filament
	4.1.1.2	Motor overheats	Controller unable to turn blinds	8	Improper power supply	2	Create a circuit to ensure no extra wattage
	4.1.1.3	Motor and gears not properly enclosed	None	6	Enclosure break	1	Create extra testing criteria for the mechanical enclosure
	4.1.1.4	Beads break	Unexpected behaviour	10	Poor blind manufacturing or overuse	2	None
	4.1.1.5	Beaded wire slips off gear	Unexpected behaviour	10	Improper mounting from user	2	Create gears with longer teeth
Microcontroller	4.1.2.1	Microcontroller overheating	Possible crashes, unexpected behaviour or complete shutdown	10	Improper cooling or storage in a hot environment	1	Replace batteries, allow microcontroller to cool, store in a cool dry place
	4.1.2.2	Short circuits	Unexpected behaviour or complete shutdown	10	Loose connections or faulty design	1	Turn off device, ensure no loose wiring and contact supplier for support
	4.1.2.3	Application control software crash / freeze	User unable to use system	10	Software failure	2	Restart device
Lux sensors setup	4.1.3.1	Sensor contamination or obstruction	Affects the functionality of the sensor, and the control system may obtain incorrect sensor values as a result	8	Incorrect mounting	4	Provide clear mounting instructions
	4.1.3.2	Sensor falling from attached position in the enclosure	Affects the functionality of the sensor, and the control system may obtain	8	Packaging / handling error	2	Provide sensors with extra support in apparatus enclosure

			incorrect sensor values as a result				
	4.1.3.3	Manufacturer Error	Affects the functionality of the sensor, and the control system may obtain incorrect sensor values as a result	8	Manufacturing error	1	Contact supplier for support / replacement
	4.1.3.4	Sensor operating outside the recommended operating environment	Affects the functionality of the sensor, and the control system may obtain incorrect sensor values as a result	10	Mounting sensor in improper environment	3	Provide clear mounting instructions
Mechanical Enclosure	4.1.4.1	Wires exposed	Possible loose wires and failure of circuits	4	Poor insulation and wire management	2	Use small clamps to ensure no loose wires
	4.1.4.2	Enclosure breaks	Loose components	5	Cheap case material	1	Invest in strong plastic type
	4.1.4.3	Improper mounting	Unexpected behaviour	9	User error	3	Improve instruction manual
Power Circuit	4.1.5.1	Spontaneous Lithium-ion Battery failure	System shutdown	10	Battery Failure	1	Replace batteries
	4.1.5.2	Power supply dying without warning	System shutdown	10	Power supply failure	4	Regularly check power levels
	4.1.5.3	Low-voltage shock	Exposed power terminals	3	Exposed terminals	1	Ensure power terminals are not exposed
User Interface	4.2.1.1	User interface freezes	User cannot interact with user interface	10	Software failure	2	Restart user interface
	4.2.1.2	User input data fails to reach backend/database	User data not saved in database	10	Software failure	2	Re-input data
	4.2.1.3	User interface does not output correct information	User is misinformed about current Intellux state	10	Software Failure	2	Restart user interface
Control Algorithm	4.2.2.1	Software bugs	Leads to inaccurate	10	Software Failure	2	Provide detailed feedback and await software upgrade

			control decisions				
	4.2.2.2	Control outputs that are unachievable due to the limits of the Intellux system	Leads to inaccurate control decisions	10	Calibration failure	1	Reset system
Database	4.2.2.3	Does not record input data from user correctly	Fails to store data correctly	10	Software Failure	2	Delete incorrect data and input correct data

6. Conclusion

A thorough hazard analysis has been conducted at this stage in development to ensure the system safety of the Intellux apparatus design for its users. A detailed set of concerns was established and recorded using the FMEA approach for use in subsequent design iteration. An effort has been made to identify and mitigate any possible dangerous hazards as a result of failures from the apparatus or user software. Where dangers cannot be totally eliminated, suitable warnings must be provided so that the user is informed of the safest methods to interact with the equipment. The use of this hazard analysis will guarantee that the Intellux system design complies to the safety standards required to be used by any blind owner.