Hazard Analysis
Mechatronics Engineering

Team # 34, ParkingLotHawk
Fady Zekry Hanna
Winnie Trandinh
Muhammad Ali
Muhammad Khan

Table 1: Revision History

Date	**Version**	**Notes**
October 19, 2022	1.0	Initial Revision
November 2, 2022	2.0	Removing malfunction button requirement, changing low battery threshold.
March 4, 2023	3.0	Added clarification on actions to take when using redundant sensors. Added faults on visual perception system.
March 4, 2023	3.1	Requirements updated in response to change in where the parking lot bounds are computed (Drone vs PC). Moved secondary sensor implementation requirements into Phase IV.

Contents

List of Tables

List of Figures

1 Introduction

Safety is a key feature of almost all products and services used. In order to determine safety features, a Hazard Analysis is typically done to generate, understand, and resolve key hazards that may come up during operations. For this document, a hazard is defined as a property or condition within the physical or virtual constraints of the system, together with a condition in the environment that has the potential to cause harm or damage. A Hazard Analysis of the ParkingLotHawk is presented in this document.

2 Scope and Purpose of Hazard Analysis

The purpose of the Hazard Analysis is to find, understand and finalize resolutions to the various hazards that may occur.

The product, ParkingLotHawk, is an autonomous aerial drone used to gather live images and data within the confines of any given outdoor parking lot. The user of such a product is the Parking Lot Operator (called Operator for short), who communicates with the Aerial Drone using an application running on their PC.

The scope of this Hazard Analysis is related to hazards that occur when the Parking Lot Operator is using the final product in the typical real-world use case: investigating an outdoor parking lot. For example, Hazards related to the development and prototyping of the product are not analyzed in this document.

The document starts by breaking the system into components, followed by identifying hazards for each component using the Failure Modes and Effects Analysis (FMEA) method, and then finally generates new safety requirements to resolve the various hazards. This method will help minimize any unsafe behavior in the system by finding any possible causes of the said failure and determining the proper response for it.

3 System Boundaries and Components

The systems referenced in this document for conducting ParkingLotHawk's hazard analysis are defined within the System Components Table:

Table 2: System Components Table

Components	Description
Main Drone Application	The Main Drone Application contains an implementation of the Finite State Machines specified in the Software Requirements Specification. This component also communicates with the Operator's PC Application to receive user commands and send relevant parking lot information.
Flight Operations	This component is responsible for calculating the optimal propeller speeds to stabilize and move the drone in accordance with movement commands from the Main Application. This component consists of the flight controller hardware, the external sensors it uses, and firmware that is flashed onto the flight controller board. Internal sensors include the Inertial Measurement Unit (IMU) for estimating acceleration and angular rate, a compass for orientation, and a barometer for atmospheric pressure to determine the altitude. External sensors include the Global Positioning System (GPS), used to locate the drone's position.
Vision Perception	The Vision Perception component consists of a camera and the algorithm for detecting parking spots, making an occupancy map of the lot, and segmenting the boundaries of the parking lot. It outputs live images from that camera for the user interface to display to the operator, and outputs and detections of whether it currently sees a parking lot which is used by the user interface to create an occupancy map.
Path Planner	This software component is used for autonomous exploration; it creates a path to explore the parking lot. Its outputs are used by the Main Drone Application.
Thrust Components	The Thrust Component is responsible for spinning the propellers at the speed commanded by the Flight Operations component. The component consists of motors, propellers, and Electronic Speed Controllers (ESCs).
Frame	The Frame will hold all the physical pieces of the drone together.
Power Modules	The Power Modules will power components within the drone such as the flight controller and motors. The components consist of a battery, charging equipment, switches, and wires.
Operator's PC Application	This component is what the Operator interfaces with to get the drone up and running, in addition to how the Operator obtains the information provided by the drone. This component communicates with the Main Application running on the physical drone to send user commands and receive relevant parking lot information.

Figure 1 below visualizes all of the system components within the project.

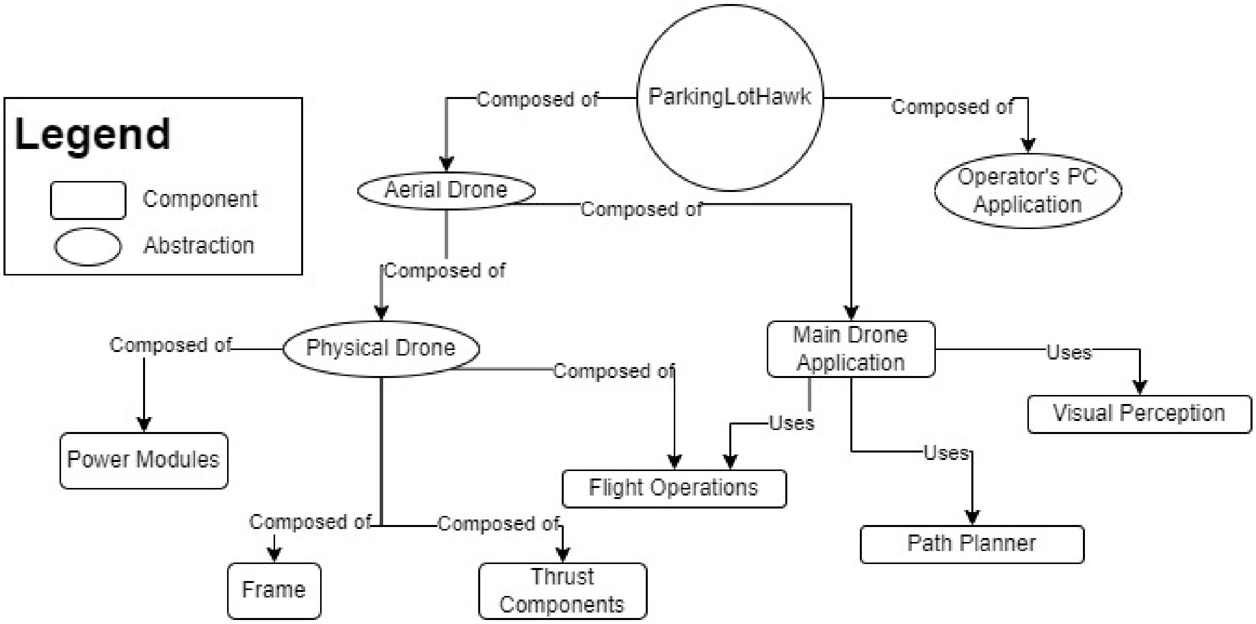

Figure 1: Systems Components Diagram

4 Critical Assumptions

There are several assumptions that help to solve and sometimes even eliminate hazards all together. Firstly, it is assumed that the Parking Lot Operator utilizing the drone has completely read the User Manual and that they utilize the drone in the way specified by the User Manual. For example, if the User Manual specifies weather conditions under which the drone should not be flown, it is assumed that the user does not fly the drone in these inclement weather conditions. Secondly, it is assumed that the Operator uses the drone solely for parking lot investigation, not for activities such as recreation, spying, etc.

5 Failure Mode and Effect Analysis

The analysis of the components outlined within System Boundaries and Components are provided through FMEA tables below, with the associated Safety Requirements attached to any applicable hazards.

The Severity, Occurance, and Detection are ranked on linear scales of 10, with 10 being the most severe. RPN then provides a combined score for the hazard, with higher RPNs being more hazardous.

With regards to H_001 and H_002, the redundant sensor will be implemented in the same way as the primary, but the sensor will be selected to provide increased robustness at the cost of accuracy. If the primary sensor has a variance above a threshold, calculated through the Extended Kalman Filter, the secondary sensor will be used instead. If the secondary sensor also produces unacceptable variances, then the drone will enter the Malfunction State.

Similarly for H_003, the height readings from the barometer will be crosschecked with the IMU readings on the Z axis. If the variance between the sensors exceed a threshold for a specified amount of time, then the drone will enter the Malfunction State.

Table 3: FMEA Table related to Flight Operation Components.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Flight Operation	IMU gives inaccurate readings.	The Drone is unable to determine angular orientation, which makes flight motion and stabilization difficult.	10	IMU damaged during flight, magnetic interference, data parsing error.	2	7	140	Implement Flight Controller with secondary IMU, providing diversity and redundancy.	SR_004	H_001
Flight Operation	Compass gives inaccurate readings.	Drone has difficulty in determining heading in space.	7	Compass damaged during flight, magnetic interference.	3	7	147	Implement Flight Controller with secondary compass, providing diversity and redundancy.	SR_004	H_002
Flight Operation	Barometer gives an inaccurate reading.	Flight controller unable to determine altitude, creates difficulty in landing.	9	Barometer damaged during flight, UV/motor backwash interference, data parsing error.	2	7	126	Add an ultrasonic sensor at the bottom of the drone, providing a secondary height estimate in the range of 0-2m for landing.	SR_005	H_003
Flight Operation	Firmware unable to make the drone hover in place. Hovering was specified as stabilizing and staying within some tolerance of a location in space for a sufficiently long time.	Drone will not be able to fly to locations or follow paths well. Drone being unable to hover means that the camera will see blurry and shaky images.	10	Flight Controller internal malfunction, inclement weather (such as high winds).	1	2	20	Mention maximum wind requirement in User Manual. Report malfunction to Operator and enter the Malfunction state.	SR_006, SR_007	H_004
Flight Operation	GPS Connection is lost or weak.	The drone will have a less accurate estimate of position, and thus won't be able to perform autonomous missions or move to a specific GPS locations.	10	GPS damaged during flight, magnetic interference.	3	7	210	Implement an alternative localization method via the camera or other range finder sensor, such as SLAM or optical flow.	SR_008	H_005

Table 4: FMEA Table related to Visual Perception.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Visual Perception	Camera gives poor quality images, delayed images, or no image at all.	The primary functionality of showing the Operator the parking lot cannot be accomplished.	2	Camera lens is foggy or has other obstructions, data communication to PC is delayed, or the camera is damaged during flight.	3	1	6	Operator will detect the low image resolution themselves while they watch the live video. Operator may choose to wait, move the drone to a new closer location, land the drone, clean the lens, restart the drone, and/or reconfigure it to fly closer to the ground.	SR_006, ??	H_006
Visual Perception	Drone fails to classify parking lot and non-parking lot correctly.	Drone is unable to create a correct occupancy map.	3	Perception algorithm performs poorly due to weather conditions, the uniqueness of the parking lot, or weakness of the perception algorithm.	2	3	18	Operator should notice from the live camera video feed (which will be annotated to show parking lot areas) that the drone is consistently failing to correctly segment the parking lot, and thus the user should ignore the occupancy map they see on the user interface.	SR_006, SR_009	H_007
Visual Perception	Drone fails to detect the boundaries of the parking lot.	Drone is unable to implement autonomous states, and can only implement manual movement commands.	5	Perception algorithm performs poorly or the uniqueness of the parking lot.	4	3	60	Operator should notice from the drone map that the drone is consistently failing to correctly segment the parking lot, and thus the drone is only useful for true manual movement.	SR_009	H_008
Visual Perception	Launching a drone without satalitte imagery.	Operator/drone software will not be able to determine if the current location of the drone is within a parking lot.	8	User attempts to launch the drone in a location without pre-downloaded satellite imagery.	4	3	96	Operator should not fly the drone or contact developers for support to fly in the specified location.	SR_001	H_019

Table 5: FMEA Table related to the Thrust Components and the Frame.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Thrust Components, Frame	An arm of the copter is unable to perform within its specifications, detected by the flight controller or noticed by the Operator.	The drone has fewer active propellers than it was tuned, trained, and designed for. This will cause difficulty in flight and stabilization.	8	The given arm has a damaged propeller, damaged motor, broken electrical connection between the motor and ESC, mechanical disconnection between the propeller and motor, or a crack on the arm to the extent of not being able to provide a rigid frame.	4	5	160	Although flight will be hindered, the firmware has the capabilities to still fly the drone under most conditions. The drone shall enter the malfunction state, trying to land at its original location. The Operator, being from a non-technical background, will need to send the drone for repair once recovered. In the user manual, it should be specified that the Operator is required to inspect the drone for damage prior to flight.	SR_002, SR_007	H_009

Table 6: FMEA Table related to the Frame.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Frame	Center of frame cracked, as seen by Operator.	Drone will have difficulty in flight. Parts of the drone may fall out if the crack is large enough.	5	Center of frame damaged during flight or storage.	2	7	70	Enclose the central base of the drone such that components do not fall out. In the user manual, specify that the Operator is required to inspect the drone for damage prior to flight. If the Operator sees any cracks during flight, they should send the drone into the malfunction state.	SR_001, SR_002	H_010
Frame	Drone is very hot.	Operator may be hurt if they touch the hot components. Drone components may also be damaged after prolonged heat exposure.	5	Overheating components due to component malfunction.	5	7	175	Add heat sinks on electrical components and specify the correct way to hold the drone in the user manual. Also specify how long the Operator must wait and let the drone cool down before making any contact with it.	SR_010	H_011

Table 7: FMEA Table related to the Power Modules.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Power Modules	Low Battery.	Drone will be unable to fly for a long duration of time. If Drone is not landed soon, it could run out of power midair and crash.	8	Drone has been flying for a long duration, or recharge is not completed before use.	7	4	224	Once the drone detects less than 3 minutes of battery remaining, it shall automatically land the drone at it's original launch location and inform the Operator.	SR_003, SR_011	H_012
Power Modules	Battery capacity low.	Drone will be unable to fly long enough to complete its functions.	8	Drone's battery life has deteriorated over time.	2	6	96	Drone should prevent flight if the battery capacity is less than 3 minutes, and the drone should convey to the Operator that it cannot fly and state the reason why. The Operator will need to purchase a new battery replacement.	SR_003, SR_012	H_013
Power Modules	Wire connections become loose.	Electrical components and system will not function correctly.	9	Wires may become loose after extended use or upon damage.	2	7	126	Solder all electrical wires and attach heat shrinks or crimps to wire-to-wire connections.	-	H_014
Power Modules	Drone smokes or ignites.	Drone is unable to function properly and the safety of the Operator is diminished.	10	Wires is short circuited due to damage, motors are damaged, or the battery is damaged or punctured.	2	2	40	Require the Operator to perform a visual inspection before flight, and ensure that the Operator has access to a Class B fire extinguisher.	SR_002	H_015

Table 8: FMEA Table related to the Operator’s PC Application.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Operator’s PC Application	Malicious user hacks into the Operator’s PC Application via login system.	Malicious users will be able to inspect the parking lot.	3	Too simple of a login password or password leaked out.	1	10	30	Require that the passwords be sufficiently complicated: at least one upper case, one lower case, one number, and one special character. Also, denote in the user manual that the password should be kept a secret from external parties.	SR_-013	H_-016

Table 9: FMEA Table related to the Path Planner.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Path Planner (also called Autonomous Explore)	Internal explore strategy malfunctions. The Operator notices the drone is not exploring the parking lot correctly.	Drone may keep exploring the same area thus wasting time, or the drone may exit the parking lot.	4	Due to the path planning algorithm not performing accurately/correctly. For faulty vision input, see FMEA Table related to Visual Perception.	4	8	128	It is upon the Operator to notice the inaccuracy of the path planning feature during the Autonomous Explore State, At which point the Operator should utilize other more accurate features instead (such as Manual Explore). This hazard is apart of a stretch goal for the product.	-	H_017

Table 10: FMEA Table related to the Operator's PC Application and the Main Drone Application.

Design Component	Failure Mode	Effect of Failure	Severity	Causes of Failure	Occurrence	Detection	RPN	Recommended Action	SR	Ref
Operator's PC Application, Main Drone Application	Drone loses connection to Operator's PC Application, or connection has deteriorated. For example, the connection has been lost for sufficiently long, the connection is very slow, weak, and/or delayed.	Drone is unable to communicate to the Operator. The drone is unable to send its data to the Operator. The drone may also miss commands from the Operator.	10	The connection is poor due to weather, distance, or network interference (such as another similar radio frequency in the nearby area). Another possible cause is the Operator's PC Application crashing.	6	1	60	Upon sufficiently poor connection detected for a sufficiently long time, the drone shall enter the Weak Connection State and convey this to the user if possible. In this state, the drone flies back to its original launch location, and if during flight it regains a sufficiently good connection for a sufficiently long time it resumes normal operation.	SR_006, SR_007	H_018

6 Safety and Security Requirements

Multiple new requirements were discovered through the generation of the FMEA table. Each requirement is referenced with the hazard that revealed it in the FMEA tables above.

Table 11: SR_001

Description	The operator shall specify the cities/regions they intend to fly the drone in prior to purchasing the product. If the operator would like to fly the drone in a city/region that they did not specify during purchase, they must contact developers for support. If the operator attempts to fly outside of this region, the drone should prevent flight and a descriptive error message on c_Log.
Rationale	The requirement ensures that the drone and Operator always have satellite imagery.
Associated Hazard	H_019

Table 12: SR_002

Description	The product shall inform the user that a visual inspection for damages is required before each use, such as through a user manual.
Rationale	The requirement ensures that the Operator is instructed to inspect the product before use for any damages that may impact its performance.
Associated Hazard	H_009, H_010, H_015

Table 13: SR_003

Description	The product shall provide a visual display of its estimated remaining battery life in minutes.
Rationale	The requirement ensures that the Operator is informed of the expected duration of operation remaining, such that the Operator can plan its operation accordingly.
Associated Hazard	H_012, H_013

Table 14: SR_004

Description	The product shall feature redundant sensors that can be used for localization.
Rationale	The requirement ensures that the product can still function within its specifications even if its primary localization sensors such as the IMU are malfunctioning.
Associated Hazard	H_001, H_002

Table 15: SR_005

Description	The product shall have a redundant method of determining its height for landing.
Rationale	The requirement ensures that the product can safely land in the event that the primary method of height determination is malfunctioning.
Associated Hazard	H_003

Table 16: SR_006

Description	The product shall inform the user of the environmental conditions where the product cannot be used, such as through the user manual.
Rationale	The requirement ensures that the Operator does not use the product within inclement weather, as the product is not designed to operate in such conditions.
Associated Hazard	H_004, H_007, H_008, H_017

Table 17: SR_007

Description	Upon entering into the Malfunction States, the product shall inform the Operator through the Operator's application if the product and application can successfully communicate.
Rationale	The requirement ensures that the Operator is aware that the product has detected a malfunction, and that it has entered the malfunction state as opposed to continuing with its normal operation.
Associated Hazard	H_004, H_009, H_017

Table 18: SR_008

Description	The product shall have a secondary localization method that can be used when the GPS is non-functional.
Rationale	The requirement ensures that the product is still able to operate within its specifications in the event that its GPS sensor is malfunctioning.
Associated Hazard	H_005

Table 19: SR_009

Description	On the user interface's satellite map, the product shall highlight the parking lot boundaries. On the live drone camera video feed, the drone should annotate the raw images with segmentations of parking lot vs non-parking lot to the Operator's application.
Rationale	The requirement ensures that the Operator is aware of how the product is perceiving its environment and can determine if the product's perception of its environment is correct or incorrect.
Associated Hazard	H_007, H_008

Table 20: SR_010

Description	The product shall inform the user of how to hold the product, such as through the user manual.
Rationale	The requirement ensures that the product is not damaged by incorrect handling, nor is the Operator harmed by the product as a result of incorrect handling.
Associated Hazard	H_011

Table 21: SR_011

Description	The product shall automatically return to its original launch location and land once the estimated battery time is less than 1.5 minutes.
Rationale	The requirement ensures that the product has sufficient battery left to safely return to its landing area and land, all while remaining within its specifications.
Associated Hazard	H_012

Table 22: SR_012

Description	The product shall inform the user if the battery capacity before launch is estimated to be less than 2.5 minutes of flight, and prevent launch of the product.
Rationale	The requirement ensures that the product is not used with excessively worn out batteries, to the extent that it cannot operate within its specifications.
Associated Hazard	H_013

Table 23: SR_013

Description	The Operator's login password shall be sufficiently complex: shall feature at least one upper case, one lower case, one number, and one special number.
Rationale	The requirement ensures that the Operator's application is safe against malicious users.
Associated Hazard	H_015

7 Roadmap

The safety requirements will be implemented through 4 main phases, and are as follows:

- Phase I: Proof of Concept - November 14, 2022
- Phase II: Revision 0 (Minimal Viable Product (MVP)) - February 6, 2023
- Phase III: Revision 1 - March 27, 2023
- Phase IV: Revision 2 - April 27, 2023

The requirements will be implemented within the respective phase as listed in Table 24.

Table 24: Safety Requirements Roadmap

Phase I	SR_002, SR_010
Phase II	SR_006, SR_007, SR_013
Phase III	SR_003, SR_011, SR_012, SR_001
Phase IV	SR_004, SR_005, SR_008, SR_009