Hazard Analysis

Cyclops Ride Assist: Real-Time Monitoring System.

Team 9
Aaron Li (lia79)
Amos Cheung (cheuny2)
Amos Yu (yua25)
Brian Le (leb7)
Manny Lemos (lemosm1)

Table Of Contents

List of Tables

List of Figures

1. Revision History

Table 1.1: Revision History

Date	Developer(s)	Change
2022-10-19	Aaron Li, Amos Cheung, Amos Yu, Brian Le, Manny Lemos	Document created
2022-10-20	Amos Yu	Improved formatting
2022-11-06	Amos Yu	Addressed peer review suggestions
2023-03-25	Aaron Li	Updated document, incorporate TA and peer feedback for Rev1

2. Introduction

This document is the hazard analysis of the Cyclops Ride Assist (CRA) system. The CRA is an all-in-one, easily mountable, and quick to setup system that adds modern car safety features onto a bicycle or motorcyle. These features include rearview detection, crash detection, and automatic video and data capture with upload.

3. Scope and Purpose

The scope of this document will be kept within the physical and software space of the CRA system boundary. Hazards imposed by the outer environment, society, and user error will be considered out of the scope for this document. At each major phase of production, this document will be updated to reflect any hazards that come up. Phases of production will include software design and implentation, hardware design and implementation, software and hardware testing, etc.

The purpose of this document is to identify potential hazards which arise due to failures in the hardware and software used in the CRA system, the causes and effects of these failures, plans for hazard mitigation and potential elimination, and the safety and security requirements which emerge as a result of this knowledge.

4. Definition of Hazard

A hazard is any property or condition in the CRA, that combined with environmental conditions, has the potential to cause harm to both the user and the various systems of the CRA. In the CRA, there are physical (mount, enclosure, wiring) and software hazards (video logging, vehicle detection) that will be mitigated to ensure safety-criticalness. A hazard is differentiable from an error in that an error results in degraded system performance but does not have the potential to cause harm. Hazards of the CRA will be discussed extensively in this document.

5. Critical Assumptions

There are no critical assumptions that were made.

6. System Boundary

The system boundary consists of all components within and on the surface of the physical space of the housing and mounting bracket. Although the system's environment can affect or be affected by the CRA, it will not be considered to be within the system boundary. Thus, the hazards can be classified by subdividing the system boundary into sub-systems and domains.

6.1. Housing System Boundary

6.1.1. Physical Hazards

The physical hazards within the housing system boundary are listed below.Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system. Some possible environmental factors were also acknowledged.

Hazard	Possible Consequences
Temperature of Exterior Environment	This can cause extreme temperature conditions with the housing which may damage certain components of the housing.
Environmental Factors	Water can be introduced into the housing via holes, screwholes, etc, leading to housing damage.
Accidental Drop of Housing	The housing can be damaged by the surface upon which it has fallen (concrete, wood, glass, dirt, etc).
Inconsistent Mounting	Tilting and shifting of the bracket can occur, leading to instability of the system on the handlebars.
Significant Car Accident	A signficant external force applied to the housing (ex. a major crash, weight of the vehicle) can cause the housing to break.
Ergonomic Design	After prolonged use, the user may feel strained due to repeated movements. Possible repetitive movement can lead to further injury including carpal tunnel syndrome.
Clamp Design	Improper clamping can lead to possible damage to the housing. Since the force is high, physical harm can be caused to the user if clamped onto a finger or other body part.

6.1.2. Software Hazards

Since the housing is a completely mechanical system, there are no software hazards within the housing system boundary.

Hazard	Possible Consequences
-	-

6.2. Software System Boundary

6.2.1. Physical Hazards

The physical hazards contained within the software system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Microcontroller Failures	Errors such as wiring issues, shorts, etc. can cause the microcontroller to become defective, leading to software malfunctions. This may lead to improper output of the system.
Cable Connections	Cables held within their own casing may become defective due to wear and tear, leading to communication issues and software errors. This is especially important at manually soldered areas.
LiDAR Recognition Failure	A faulty LiDAR sensor can lead to incorrect data being inputted into the software. The LEDs will then display the incorrect information of objects approaching.
Accelerometer Inaccuracies	An inaccurate accelerometer reading can lead to false detections of a crash. This can lead to the software incorrectly identifying accidents vs non-accidents, which can be hazardous if the storage of the flash drive becomes filled unexpectedly.

6.2.2. Software Hazards

The software hazards contained within the software system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Error Handling	Unanticipated errors can cause the software process to behave unexpectedly, leading to bugs or crashes during operation.
Memory Leak	A memory leak can cause the software process to crash after prolonged use.
Cable Mismanagement	Crossing wires may become shorted or loose, leading to incorrect inputs and outputs if wires or pins accidentally touch improper connectors.
Algorithm Bottlenecks	Bottlenecks in the process can cause slow response and processing times. Having different processes run over a certain runtime can lead to even greater processing times.
Code Upkeep	Poor code upkeep can decrease code readability and maintainability. In the event of an error, hazards can arise from debug oversights.

6.3. Microcontroller System Boundary

6.3.1. Physical Hazards

The physical hazards contained within the microcontroller system boundary are listed below. Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system.

Hazard	Possible Consequences

Hazard	Possible Consequences
Faulty Microcontroller Mounting	Improper mounting can cause the microcontroller to move around in the housing, damaging the controller and the housing.
High Microcontroller Temperature	High operating temperature can lead to damage to ports or connections.
Environmental Factors	The microcontroller can malfunction if introduced to enough dust, water, etc.
Power Failure	A power supply failure or surge can cause damage to various components on the microcontroller.
Physical and Static Force	Excessive force from an external factor such as a finger can damage components. Static force can induce a current that could cause damage to components.

6.3.2. Software Hazards

The software hazards contained within the microcontroller system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Power Failure	A power supply failure or surge can cause the software processes to terminate at an unexpected state.
Microcontroller Damage	Damage to the microcontroller board via physical, static force can cause the firmware to malfunction.

6.4. Peripherals System Boundary

6.4.1. Physical Hazards

The physical hazards contained within the peripherals system boundary are listed below. Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system.

Hazard	Possible Consequences
Cable Agitation	Constant agitation can cause the peripheral cables to come loose from the micontroller or LiDAR sensor. Agitation can also cause the peripherals to fall from their mounting points. This will lead to unconnected cables and connections while the CRA is in use.
Exposed Wiring	Exposed wires with a current can inflict an electric shock to the user.
Environmental Factors	The peripherals can become damaged if exposed to enough water, dust, etc, leading to the failure of the CRA's features.
Power Failure	A power supply failure or surge can damage the peripherals with a high voltage.

6.4.2. Software Hazards

The software hazards contained within the peripherals system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Loose Peripherals	Peripherals can become loose, contaminating the data being collected by the accelerometer, LiDAR, and camera.
Cable Mismanagement	The cables of the peripherals can become intertwined with the bike's wires which could lead to falls.
Peripheral Boundary Limits	Software can exceed the limit as set out by the manufacturers of the peripheral, leading to unexpected behaviour.

6.5. Camera System Boundary

6.5.1. Physical Hazards

The physical hazards contained within the camera system boundary are listed below. Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system.

Hazard	Possible Consequences
Environmental Factors	Rain, dust, vehicle fumes, etc. can obscure the view on the lens of the camera, leading to improper footage capture which can not be used for further analysis.
Bicycle Collision	A bicycle collision leading to severe contact between the camera and the surface can cause the front lens of the camera to shatter.

6.5.2. Software Hazards

The software hazards contained within the camera system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Video Compression	Excessive compression of the video can lead to unclear or grainy footage, leading to improper footage capture which can not be used for further analysis.

6.6. LiDAR System Boundary

6.6.1. Physical Hazards

The physical hazards contained within the LiDAR system boundary are listed below. Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system.

Hazard	Possible Consequences

Hazard	Possible Consequences
Cable Mismanagement	The cable of the LiDAR can become intertwined with the bicycle's regular cabling which could lead to dangling or hanging wires.
Environmental Factors	Various environmental factors can cause the LiDAR to crash, leading to electrical issues.
LiDAR Mounting	The clamp that the LiDAR is located on has a strong clamping force that can become a hazard if tightened improperly on unintended surfaces such as body parts.

6.6.2. Software Hazards

The software hazards contained within the LiDAR system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Software Misreads	Rain, dust, vehicle fumes, etc. can obscure the LiDAR's view, leading to inaccurate distance information provided to the software.
Environmental Factors	If the LiDAR sensor is exposed to enough factors including temperature, water, dust, the connections and pins make render useless, making the software behave unexpectedly.

6.7. Memory System Boundary

6.7.1. Physical Hazards

The physical hazards contained within the camera system boundary are listed below. Consideration was given to components of the CRA that could lead to possible physical hazards to the user and system.

Hazard	Possible Consequences
Improper Contact	A flash drive with improper contact can cause unexpected interruptions during operation
Flash Drive Damage	Physical damage to the flash drive can lead it to not be properly plugged in to record footage.

6.7.2. Software Hazards

The software hazards contained within the memory system boundary are listed below. Consideration was given to components of the CRA that could lead to possible software hazards to the user and system.

Hazard	Possible Consequences
Long File Write Time	Video may take more time to upload, creating a bottleneck in the system.
Storage Overflow	Too many files located in the memory can cause the system to overheat if writes continue to occur.

Hazard	Possible Consequences
Power Supply Failure	A power supply failure or surge during file writing can corrupt the card.

7. Failure Modes and Effect Analysis

7.1. Hazards Out of Scope

Hazards Out of Scope will not be considered in the Failure Modes and Effect Analysis listed below in Section 7.2.

Group	Example
External Environment	Bicycle hazards (brakes, cabling, frame), road conditions (construction zones, potholes, traffic), other factors (precipitation, temperature, air quality)
Society	City and rural design, video recording laws, theft, damage (graffiti)
User Error	Improper use and installation, excessive carelessness during handling, low battery, low storage, and low maintenance upkeep

7.2. Failure Modes and Effect Analysis Table

The Failure Modes and Effect Analysis Table (FMEA) Table indicates the failure modes associated with certain design functions and the optimal response to minimize harm to the user or product. The FMEA able thus outlines the recommended course of action required for the CRA team to eliminate as many hazards or failures for its users.

Table 7.2.1: Failure Modes and Effect Analysis

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
Crash Detection	H1-1	False negative crash detection.	The current loop of video will not be logged to the storage device.	a. Sensor failure (bias, drift, complete failure, precision degradation). b. Crash was not violent enough to trigger a crash detection sequence.	a. Perform a sensor calibration and test when the CRA is turned on. Indicate an issue if one is detected. b. Allow users to force video loop logging with a button.	a. SR-1 b. AR-1

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
	H1-2	False positive crash detection.	An unnecessary loop of video will be logged to the storage device.	a. Sensor failure (bias, drift, complete failure, precision degradation). b. A non-crash event had trademark features of a crash (e.g. high force, tipping).	a. Same as H1-1a b. Alert the user through the LED display that a video has started. Do not stop the video recording in the event of an accident.	a. SR-1 b. AR-1
Video Export to Storage	H2-1	Insufficient memory in storage device	Video loop will not be logged to the storage device.	a. Video loop is too large to be logged on the storage device or there is insufficient space on the storage device.	a. Notify the user that there is an insufficient amount of storage space on boot. In the event of a storage overflow, remove the oldest capture folders to accomodate for the incoming footage.	a. SR-3
	H2-2	Obscured front-facing camera footage.	Camera footage will be void or non-optimal in the event of a camera loop logging. Footage cannot be used for review and analysis as required.	a. Debris or dust obstructs the camera's view. b. Complete camera or camera feed failure.	a. Create a housing that will allow for the complete camera to be covered. Place the camera in a location where it is unlikely to be impacted by any debris. b. Perform a camera and camera feed check when the CRA is turned on. Indicate an issue if one is detected.	a. IR-1 b. SR-1

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
	H2-3	Corruption of video files.	Video files are lost or become unreadable.	a. Physical damage to the flash drive. b. Improper contact between the flash drive and the memory slot. c. Multiple files being written concurrently. d. Power supply failure.	a. Design a physical barrier that prevents a damaged flash drive from being inserted into the memory slot. b. Alert the user in the case that there is no detected memory device inputted. If connected, alert the user if the drive cannot be written to. c. Only allow one video to be written to the memory drive at a time. d. Use a reliable power supply with a reliable connection.	a. IR-2, AR-1 b. IR-1 c. SR-3 d. IR-3
Rear Vehicle Detection	H3-1	False negative rear vehicle detection.	A vehicle exists in the user's rear view, but they are not alerted.	a. The vehicle is not detected by the LiDAR sensor. b. The LiDAR sensor is obstructed by debris. c. The LiDAR connection or feed fails.	a. Perform a sensitivity check on bootup to ensure that the LiDAR is connected properly through a debug mode. b. Same as H2-2a c. Same as H2-2b	a. SR-4 b. SR-1 c. SR-1
	H3-2	False positive rear vehicle detection.	A user is alerted that a vehicle exists in their rear view when no vehicle is present.	a. Debris obstructs the LiDAR's view.	a. Same as H2-2a	a. SR-1

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
Rear Vehicle Alerting	H4-1	Incorrect LED lights.	A vehicle exists in the user's rearview but the rear vehicle alerting system does not identify the distance correctly. The opposite also occurs.	a. Debris obstructs the LiDAR's view. b. The connection pins between the LiDAR and system have failed. c. The LED has disconnected from some of the pins on the microcontroller.	a. Same as H2-2a b. Perform a sensitivity check on the LEDs when powering the system on. c. Perform a sensitivity check on the LEDs when powering the system on.	a. IR-1 b. SR-1 c. SR-1
	H4-2	Missing LED lights	The LED system does not light up at all when powered on.	a. The connection between the LiDAR system and the main system has failed. b. The LED system has come off the microcontroller.	a. Perform a sensitivity check on the LEDs when powering the system on. b. Perform a sensitivity check on the LEDs when powering the system on.	a. SR-1 b. SR-1
Hardware Housing	H5-1	Housing integrity is violated.	Internal hardware components are damaged or destroyed.	a. Housing is submerged in water (e.g. rain, puddle, body of water). b. Housing is violently rattled. c. Housing is dropped to the ground.	a. Create a water-proof housing with minimal holes b. Secure the microcontroller using screws, nuts, and bolts to the housing. Secure the housing to the frame through a designed clamp. c. Make the housing robust and resistant to fall damage. Secure the housing to the frame through a designed clamp to minimize impact.	a. IR-1 b. SR-2, IR-1 c. SR-2

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
	H5-2	Poor ergonomical and accessible design.	User is susceptible to repetitive strain injuries.	a. Housing obstructs usage of bicycle handlebars. b. Buttons on the exterior of the housing are hard to use. c. Housing cannot be put together or taken apart easily.	a. Provide detailed instructions on how to mount the device in a non-obstructive way. b. Design buttons to be visible, intuitive, tactile, and easily accessible. c. Design housing using the same nut and bolt size and with intuitive mounting holes of where pieces should be placed. Create a user manual to aid installation.	a. SR-2 b. AR-2 c. AR-2
Bicycle Mount For Housing	H6-1	Mount failure.	Housing is dropped to the ground.	a. Mount is impacted by debris. b. Rattling loosens mount grip.	a. Place the mount in a position unlikely to be impacted by debris. b. Instruct user to firmly tighten the mount to their bicycle like the metal frame bar. Line the gripping portion of the mount with rubber to increase friction and fit.	a. SR-2, IR-1 b. SR-2, IR-1
System Firmware	H7-1	Hardware malfunction.	The microcontroller is unable to execute the software as intended.	a. Power supply failure. b. Poor mounting of the microcontroller.	a. Same as H2-3d b. Design a durable mount for the microcontroller, and test the reliability during crashes.	a. IR-3 b. IR-1
	H7-2	Software malfunction.	The real-time software running on the microcontroller does not behave as intended.	a. Unanticipated errors in software. b. Poor code upkeep.	a. Run the software process for a prolonged period of time. b. Enforce readable, maintainable code.	a. PR-1 b. PR-2

8. Safety and Security Requirements

8.1. Safety Requirements

SR-1	**A system welfare check will be conducted each time the CRA is powered on to verify that all cameras and sensors are successfully communicating with the microcontroller.**
Rationale	A problem with the LiDAR sensor could result in unexpected rear view detection behaviour (false positives or false negatives). A problem with the rear facing camera could result in footage of a crash being lost. A problem with crash detection sensors could result in unexpected crash detection behaviour (false positives or false negatives).
Associated Hazards	H1-1a, H1-2a, H2-2b, H2-3b, H3-1b, H3-1c, H3-2a, H4-1b, H4-1c, H4-2a, H4-2b
SR-2	**Safety instructions will be created to ensure that the CRA is properly equipped and mounted for the user.**
Rationale	Instructions will allow the user to properly mount and maintain their system.
Associated Hazards	H5-1b, H5-1c, H5-2a, H6-1a, H6-1b
SR-3	**System self-assessments will optimize video storage to ensure there is enough space to hold videos and will alert the user if the space is insufficient.**
Rationale	In the case that the storage memory device is full, videos will be cut short to ensure that the user has the footage of the latest accident that they have been involved in.
Associated Hazards	H2-1a, H2-3c
SR-4	**The camera, LiDAR, camera feed will be checked on startup by the system to ensure that all required software is connected and usable.**
Rationale	This is to ensure that the camera is able to create and log video data as required on vehicle collision. This is also to ensure the LiDAR sensing is able to detect distances of objects accurately.
Associated Hazards	H3-1a

8.2. Access Requirements

AR-1	**CRA will allow the users to access their videos freely from an external hardware storage drive.**
Rationale	This is to allow the user to connect it to their own personal systems to view, delete their videos. There is no need for encryption as this would complicate the process.
Associated Hazards	H2-3a
AR-2	**CRA will be ergonomically designed to accomodate all cyclists, including cyclists with special physical accessibility needs.**

AR-2	**CRA will be ergonomically designed to accomodate all cyclists, including cyclists with special physical accessibility needs.**
Rationale	The design of the device should feel seamless without interfering with the user experience for cyclists with accessibility needs.
Associated Hazards	H5-2b, H5-2c

8.3. Integrity Requirements

IR-1	**The mounting system will be made with solid and sustainable material to ensure mechanical integrity.**
Rationale	This will be able to withstand changes in weather and temperature, accidental drops, and debris.
Associated Hazards	H2-2a, H4-1a, H5-1b, H6-1a, H6-1b, H7-1b
IR-2	**The housing will protect its interior from undesired foreign items.**
Rationale	This will keep damaging substances like water, debris, and dust out while allowing access to necessary components like memory and charging ports
Associated Hazards	H2-3a
IR-3	**The components that are sourced from third-parties will be upheld to a quality level corresponding to their importance.**
Rationale	As we cannot economically create every part of the device ourselves, we will need to source basic parts from third-party manufacturers. These parts need to be reliable enough to operate as intended.
Associated Hazards	H2-3d, H7-1a

8.4. Privacy Requirements

PR-1	**CRA will not be connected to the internet but will be used and trained locally for CV purposes.**
Rationale	This is to ensure that the footage of accidents will not be posted on the internet without the consent of the user. Instead all footage will be saved to an external hardware storage device.
Associated Hazards	H7-2a
PR-2	**Code will be open-sourced, but only select individuals will be allowed to contribute to the master branch of the main repository.**

PR-2	**Code will be open-sourced, but only select individuals will be allowed to contribute to the master branch of the main repository.**
Rationale	This will ensure that the code running on the device follows the coding standards and is peer-reviewed by members of the team.
Associated Hazards	H7-2b

9. Roadmap

The roadmap of CRA is a projection of the safety and security requirements listed above. The majority of these requirements will be implemented on the initial prototype and final application due to the nature of the system and its functionalities. Requirements will be constantly reevaluated with several factors in consideration such as time and project constraints. Towards the end of the project, the Hazard Analysis document will be an evaluation over the project to get an understanding of what risks have been successfully mitigated and which ones will still require work.

With the conclusion of the CRA approaching, the Hazard Analysis was reconsidered to accomodate for any changes or additions. Changes included the introduction of camera and video logging for the rear vehicle detection camera, the LiDAR sensor along with the rear vehicle alerting LED system, as well as the removal of the use of computer vision. Throughout the design process and verification and validation phase, the Hazard Analysis was repeatedly considered which allowed the team to miitigate all risks outlined in this document. Further addendums or updates will be created in the case any discrepancies that arise.

10. Appendix