Hazard Analysis

Cyclops Ride Assist: Real-time bicycle crash detection and blindspot monitoring.

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

2. Introduction

This document is the hazard analysis of Cyclops Ride Assist (CRA) system. Cyclops Ride Assist(CRA) will be an easily mountable, and quick to set up system that adds modern car safety features onto any bike. These features include rear vehicle detection and alert, a continuous loop of the last 60 seconds of camera, accelerometer, and Lidar data, and crash identification and response. CRA is aimed at cyclists of all levels that frequently traverse road and gravel terrains. CRA is not designed to be used on extreme terrain such as downhill mountain biking.

3. Scope and Purpose

The scope of the hazard analysis as outlined in this document will be kept within the physical/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.

This document identifies 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 the safety and security requirements which emerge as a result of this knowledge.

4. Definition of Hazard

A hazard is any property of the CRA system that has the potential to cause harm in both the user and the various systems that make up CRA. In CRA, there are hazards in safety (video logging, vehicle detection) and physical (mount, enclosure). A hazard is differentiated from an error in that an error simply results in degraded system performance but does not have the potential to cause harm.

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. 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 temperature of the outside environment can cause extreme temperature conditions inside the housing.
- Rain and snow from the outside environment can introduce water into the housing.
- Accidentally dropping the device from the height of bike handlebars can damage the housing.
- A loose mounting bracket can cause the device to tilt/shift when mounted on the handlebars.
- A bike crash can cause the housing to release from the mounting bracket.
- Poor ergonomics can strain the user after prolonged use.

6.2. Software System Boundary

6.2.1. Physical Hazards

- A faulty microcontroller can cause the software to malfunction.

6.2.2. Software Hazards

- Unanticipated errors can cause the software process to crash.
- A memory leak can cause the software process to crash after prolonged use.
- A poor image-recognition implementation can result in improper recognition of vehicles in the blindspot.
- Bottlenecks in the process can cause slow response and processing times.
- Poor code upkeep can decrease code readability and maintainability.

6.3. Microcontroller System Boundary

6.3.1. Physical Hazards

- Poor mounting can cause the microcontroller to toss around within the housing.
- Openings in the housing can introduce water and dust onto the microcontroller.
- A power supply failure can damage the hardware on the microcontroller.

6.3.2. Software Hazards

- A power supply failure can cause the software process to terminate at an illegal state.
- Damage to the microcontroller board can cause the firmware to malfunction.

6.4. Peripherals System Boundary

6.4.1. Physical Hazards

- Agitation can cause the peripheral cables to come loose from the microcontroller.
- Agitation can cause peripherals to come loose from their mounting points.
- Flawed part manufacturing can cause peripherals to fail unexpectedly.
- Openings in the housing can introduce water and dust onto the peripherals.
- A power supply failure can damage the peripherals.
- Exposed wires can inflict electrical shock to the user.

6.4.2. Software Hazards

- Loose peripherals can contaminate the data being collected by the accelerometer and cameras.
- Requiring the peripherals to operate outside of their effective range can result in unexpected behaviour or damage.

6.5. Camera System Boundary

6.5.1. Physical Hazards

- Rain, mud, and dust can obscure the lens of the front- and rear-view cameras.
- Poor lighting can affect the clarity of the captured footage.
- A bike crash can cause the camera lenses to shatter.

6.5.2. Software Hazards

- Excessive image compression can cause grainy/unclear footage.

6.6. Memory System Boundary

6.6.1. Physical Hazards

- A memory card with improper contact to the port can cause unexpected interruptions in operation.
- Physical damage to the memory card can corrupt the card.

6.6.2. Software Hazards

- Slow file writing can be a bottleneck, especially for large video files.
- Running out of memory on the memory card will cut off the ability to save files.
- A power supply failure during file writing can corrupt the card.

6.7. Headlamp System Boundary

6.7.1. Physical Hazards

- A loose switch can cause the headlamp to turn on/off unexpectedly.
- Poor ergonomics can impede the operation of the switch in extreme conditions.
- Shining light into the user's face can cause visual impairment.

7. Failure Modes and Effect Analysis

7.1. Hazards Out of Scope

Hazards out of scope can generally be categorized into three groups: outer environment, society, and user error. Examples of outer environment hazards include bicycle hazards, road conditions, and environmental factors outside of the housing of CRA. Examples of hazards due to society include city design, video recording laws, and theft. Examples of hazards caused by user error include improper use, excessive carelessness, and low battery. These hazards out of scope will not be considered in the Failure Modes and Effect Analysis.

7.2. Failure Modes and Effect Analysis Table

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 system 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
	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 g forces, tipping).	a. Same as H1-1a b. Allow user to cancel video loop logging with a button.	a. SR-1 b. AR-1
Video Logging	H2-1	Storage device cannot accommodate the loop of video attempting to be logged.	Video loop will not be logged to the storage device.	a. Video loop is too large to be logged on the storage device.	a. Log the most recent half of the current video loop, and halve the length of the video loop going forward. When sufficient storage is available on the storage device, standard video loop length should be reinstated.	a.SR-3

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
	H2-2	Obscured front/rear facing camera.	Camera footage will be void or non-optimal in the event of a camera loop logging.	a. Debris obstructs the camera's view. b. Complete camera or camera feed failure.	a. Place the camera in a position unlikely to be impacted by debris (eg. not on underside of downtube) b. Perform a camera feed check when the system is turned on. Indicate an issue if one is detected.	a. IR-1 b. SR-1
	H2-3	Corruption of video files.	Video files are lost or become unreadable.	a. Physical damage to the memory card. b. Improper contact between the memory card and the memory slot. c. Multiple files being written concurrently. d. Power supply failure.	a. Design a physical barrier that prevents damaged cards from being inserted into the memory slot. b. Write software that validates that the memory card is connected properly before performing operations on it. c. Only allow one video to be written to the SD card 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
Blind Spot Detection	H3-1	False negative blind spot detection.	A vehicle exists in the users blind spot, but they are not alerted.	a. The vehicle is not recognized by the computer vision program. b. The rear facing camera is obstructed by debris. c. The rear facing camera or camera feed fails.	a. Provide a separate lesser warning for non-vehicles that are detected in the users blind spot. b. Same as H2-2a c. Same as H2-2b	a. SR-4 b. SR-1 c. SR-1

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
	H3-2	False positive blind spot detection.	A user is alerted that a vehicle exists in their blindspot when no vehicle is present	a. Debris obstructs the rear facing camera's view.	a. Same as H2-2a	a. SR-1
Housing To Protect Hardware	H4-1	Housing integrity is violated.	Internal hardware components are damaged or destroyed.	a. Housing is submerged in water (e.g. rain, puddle lake). b. Housing is violently rattled. c. Housing is dropped to the ground.	a. Make housing waterproof b. Protect the microcontroller from vibrations using damping. c. Make the housing robust and resistant to damage due to shock.	a. IR-1 b. SR-2, IR-1 c. SR-2
	H4-2	Poor ergonomics.	User is susceptible to repetitive strain injuries.	a. Housing obstructs usage of bicycle handlebars. b. Switches on the exterior of the housing are hard to use.	a. Provide detailed instructions on how to mount the device in a non-obstructive way. b. Design switches to be visible, tactile, and easily accessible.	a. SR-2 b. AR-2
Bicycle Mount For Housing	H5-1	Mount failure.	Housing is dropped to the ground.	a. Mount is impacted by debris. b. Rattling loosens mount grip.	a. Place mount in a position unlikely to be impacted by debris (eg. not on underside of downtube) b. Instruct user to firmly tighten the mount to their bicycle. Line the gripping portion of the mount with rubber.	a. SR-2, IR-1 b. SR-2, IR-1

Design Function	Ref #	Failure Mode	Effects of Failures	Causes of Failure	Recommended Action	SR
System Firmware	H6-1	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
	H6-2	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 rear facing camera could result in unexpected blind spot detection behaviour (false positives or false negatives). A problem with the front or 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
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	H4-1b, H4-1c, H4-2a, H5-1a, H5-1b
SR-3	**System self-assessments will optimize video storage to ensure there is enough space to hold two 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 CV Vision will be checked on startup by the system to ensure that all required apps, images can still be accessed and used**

SR-4	**The CV Vision will be checked on startup by the system to ensure that all required apps, images can still be accessed and used**
Rationale	This is to ensure that the cameras are able to differentiate between vehicles and other objects
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.**
Rationale	The design of the device should feel seamless without interfering with the user experience for cyclists with accessibility needs.
Associated Hazards	H4-2b

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, H4-1b, H5-1a, H5-1b, H6-1b
IR-2	**The housing will protect its interior from undesired foreign bodies.**
Rationale	This will keep damaging substances like water, mud, and dust out while allowing access to necessary components like memory cards 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.**

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, H6-1a

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	H6-2a

PR-2	**Code will be open-sourced, but only select individuals will be allowed to contribute to the master branch of the main repository.**
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	H6-2b

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 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.

10. Appendix