AR:IN

Autonomous Robotics: Intersection Navigation

GROUP 11
Hazard Analysis (Revision 0)

Derek Arts - 1329017
Jonathan Klawunn -1320342
Kate Keskikyla - 1300693
Kerianne Rikley - 1309336
Nabil Hamza - 1317929
Trent Stevenson - 1314633

Table of Contents

List of Tables

0 Revision History

Table 1: Revision History

Revision Number	Date	Revision Description
0.0	09/01/2017	Initial Revision and Document Creation

1 Introduction

In order to ensure safety on the roads for people in autonomous and non-autonomous vehicles, the careful consideration of the safety of using our systems in an autonomous vehicle is an essential aspect of the system design. It is crucial to determine the hazards of the system not only when assessing whether or not the system is safe to use, but also for the process of setting the system's safety requirements. These safety requirements are an important aspect of system design and it is necessary to ensure that the end final system to meet and exceed these requirements. In order to determine the hazards of the system, there are various different methods that can be used. In the development of AR:IN autonomous vehicle for intersection navigation, the Failure Modes and Effects Analysis (FMEA) method has been used. This document will provide a comprehensive outline and analysis of various system failures that may occur and the considerations taken in order to ensure the safety of the both the user and the system.

2 Overview

2.1 Component Descriptions

2.1.1 Object Detection Sensors

This component detects vehicles and other obstructions on the road and determines distance. Used as a redundancy for camera.

2.1.2 Image Recognition Camera

This component captures image for use by image processor in lane detection, obstacle detection and path correction..

2.1.3 Image Recognition Processor

This component analyzes image from camera and computes course for lane following and obstacle avoidance.

2.1.4 Inter-Car Communication System

This component handles all communication between the other autonomous cars. This is an integral part of intersection behaviour as it both receives and sends all stop and go messages.

2.1.5 Vehicle Movement Controller

This component controls speed and steering of vehicle. Contains control loops that work with image recognition processor and inter-car communication to ensure vehicle turns, accelerates and decelerates smoothly.

3 Safety Considerations

3.1 Power Supply Failure

Issue:

- System no longer has control of the vehicle, cannot change the speed or direction of motion
- Vehicle can collide with other objects causing damage to the vehicle or the object.

Solution:

- If power to motors are cut vehicle will steer off to the side
- If power to the controller is cut off no commands can be implemented so the body will be made to cushion collisions
- System will need to be restarted

3.2 Collision Hazard

Issue:

- The vehicle colliding with a person or another vehicle

Solution:

- Keep the speed of the vehicle low enough to not cause significant damage if a collision occurs
- Keep the speed low enough so that the system can control the vehicle

3.3 Burn Hazard

Issue:

- Electrical components of system can become hot and possibly burned if touched

Solution:

- Allow sufficient ventilation where applicable
- Mark where potential burn risks are to help avoid touching them
- Use enclosures where appropriate

3.4 Exposed Electrical Component

Issue:

- Someone could be electrocuted

Solution:

- Minimize the number of wires used and make sure they are all properly attached
- Cover power source terminals

4 FMEA worksheet

Table 2: FMEA

Design Component	**Ref. #**	**Failure Modes**	**Cause of Failures**	**Effects of Failure**	**Detection**	**Controls**	**Recommended Action**
Object Detection Sensors	4.1.1	-does not detect object - detect object that doesn't exist	-sensor hardware failure	-car could collide with object -car could stop moving indefinitely	-check camera feed and other sensors, compare inputs	-test all sensors at start up -always compare sensor inputs to other sensors and camera	-if only one sensor fails then operation can continue but passenger will be notified -if multiple sensors have conflicting feeds then pull of to side and attempt to calibrate sensors
Image Recognition Camera	4.1.2	-camera feed fails	-hardware failure	-car could no longer do lane following	- camera feed stops transmitting	-make sure camera and all wiring is secure at start up	-system goes into safe state and waits for maintenance
Image	4.1.3	-incorrectly	-software error	-car could go	-compare	-if image is	-wait one cycle

Recognition Processor		identifies object or lines -does not identify existing object or lines	 - poor quality input from camera -processor hardware failure	outside lane or collide with objec -car could do unnecessary course correction	camera input to sensor inputs -check resolution of image at time of processing	of poor quality wait until next image capture -use other sensor inputs to supplement picture	to see if image improves - go into safe state and wait for maintenance -reprocess image
Inter-Car Communicatio n	4.1.4	-fails to send or receive a message -sends or receives corrupted message	-software error -communication interference -hardware failure	-others cars could be unaware of cars presence causing collision -could be stalled at intersection waiting for message	-cyclic redundanc y check - test message other vehicles	-perform crc checks on all messages -test message sending and receiving on start up	- resend message or ask for it to be resent -go into safe state and wait for maintenance
Vehicle Movement Controller	4.1.5	- The desired speed or orientation are incorrectly calculated	-Controller miscalculating the output speed or orientation -The controller receiving incorrect data from sensors	-The car will not move in the intended way	-Use image recognition to recognise if car is off path	-Recalculat e speed and orientation if vehicle	-Reset position of car -Adjust formula for calculating speed or orientation
User Perspective Hazard Considerations							
Power Supply Failure	4.2.1.0	-System no longer has power	-Power source is disconnected	-System loses ability to control speed or direction -System starts to decelerate	-Controller will recognise unplanned decrease of speed	-Protect the power supply	-Reconnect and restart system
	4.2.1.1	-The system is damaged limiting the power	-Damage to system has limited the power				-Replace supply and
Collision Hazard	4.2.2.0	-Vehicle Collides with another vehicle or object	- Vehicle speed or pathing is incorrect	-Vehicle is not controlled as intended and collides with a vehicle or object	-Visual Detection or IR sensor	-Use IR sensor as a redundancy -Emergency stop if path is not found	- Place car back on path -Ensure sensors are working
Burn Hazard	4.2.3.0	-Electrical	-Faulty	-Potential	-Visually	-Include a	-System will

		component heats up	components -System has been on for too long	injury if touched	detect	temperature sensor	have to be turned off so parts can cool
Exposed Electrical Component	4.2.4.0	-A live electrical component is exposed	-Wire becomes unattached -Damage to the system	-Potential injury if touched -System may not work or deteriorate in effectiveness	-Visually detect	-Attach all wires properly and enclose hardware if needed	-Turnoff system and repair

5 Conclusion

Autonomous driving is a nuanced field that comes with a high standard for safety, which makes a hazard analysis even more impactful. The reason why there is this high standards because the repercussions of a failure could have drastic effects on the user. In order to avoid this with regards to AR:IN, this hazard analysis was completed with detail and an in depth consideration of the consequences. This analysis describe safety considerations for AR:IN that detailed the glaring problems that could be encountered. The FMEA worksheet specifies design components with respect to how they fail, the effects of the failures and the recommended actions necessary to fix the components. AR:IN during its development and implementation will completely adhere to the standards set by this hazard analysis in order to ensure a safe environment when complete.