THE UNIVERSITY OF WESTERN AUSTRALIA

Software Approach to Autonomous Vehicle Safety Systems

GENG5511/GENG5512 Engineering Research Project

Student:

Jason Chu (21300674)

Master's of Professional Engineering (Software)

The University of Western Australia

Supervisor:

Prof Dr. Thomas Bräunl

School of Electronic and Computer Engineering

The University of Western Australia

Word Count: 7,364

Table of Contents

Nomenclature 3
Project Abstract 4
Acknowledgements 5
Table of Figures 6
1.0 Introduction 7
2.0 Scope 7
2.1 Project Identification 7
2.2 Objectives 8
2.3 Resources 9
3.0 Literature Review 11
3.1 Safety on Autonomous Vehicles 12
3.1.1 Non-Line-of-Sight Conditions 12
3.1.2 Socially Acceptable Collision Avoidance 12
3.1.3 Elastic Band Theory 12
3.1.4 Passenger Safety 13
3.2 Dread Risk and Public Confidence in Autonomous Vehicles 13
3.3 Engineering Safety & Redundancy 13
3.3.1 Triple Modular Redundancy 13
3.3.2 N-Version Programming 14
4.0 Design Process and Final Design 14
4.1 The nUWAy Shuttle Bus 14
4.2 Design Considerations 15
4.2.1 The Software 15
4.2.2 Current Implementation of PLC Safety Curtain 16
4.3 Application of Reviewed Techniques & Concepts 16
4.4 Final Design 17
4.5 Watchdog Nodes 17
4.6 The Speed Scaling System 18
4.7 The User Interface 20
5.0 Results 21
5.1 Risk Assessment 21
5.2 Discussion & Improvements 23
6.0 Conclusions 24
6.1 Further Investigations 25
7.0 References 26

Nomenclature

SAE	Society of Automotive Engineers
ROS	Robot Operating System
nUWAy	UWA Autonomous Shuttle Bus
PLC	Programmable Logic Controller
LiDAR	Light Detection and Ranging
REV	Renewable Energy Vehicle
GPS	Global Positioning System
IMU	Inertial Measurement Unit
NLOS	Non-Line-of-Sight
V2P	Vehicle-to-Pedestrian
DSRC	Dedicated Short Range Communication
VRU	Vulnerable Road User
TMR	Triple Modular Redundancy
NVP	N-Version Programming
UI	User Interface

Project Abstract

Following advancements in new technology for autonomy in driving, several vehicles can now achieve the status of self-driving or autonomous driving. The removal of human interventions in driving changes the economy of safety to consider during vehicular use, especially for public transport and matters involving pedestrians and public passengers. The shift in safety concerns involving driving decisions that are now to be dictated by computers and sensors have been rarely addressed, and now, in the absence of educating human drivers, new precautions must be undertaken to increase the level of safety concerning both passengers and pedestrians. The University of Western Australia's nUWAy shuttle bus is a vehicle that has been undertaking autonomous driving research and development. The singular safety system of a digital Light Detection and Ranging Sensors (LiDAR) emergency stop curtain remains insufficient for public use. This research aims to discuss and create new solutions for safety applications on the nUWAy shuttle bus. It discusses vehicle safety concepts that are important to autonomy, hazard prevention, passenger, and pedestrian safety, and focus on software safety practices. It follows the implementation and limitations of the onboard SICK Safety Programmable Logic Controller (PLC) and potential improvements, and how this can be provided on a software level. Alternative software features and methods have been taken to increase degrees of safety through the shuttle's Robot Operating System (ROS) framework and examines how the data passthrough of the system can be harnessed to improve status feedback for both development and public use. An onboard watchdog software node and system has developed for use on the nUWAy shuttle bus, covering multiple points of failure experienced during autonomous testing during the system's continued development.

Acknowledgements

I would like to thank Professor Thomas Bräunl for his role as supervisor and director of the REV Project. He has guided and advised me greatly in the field of Robotics and Automation. I would also like to thank all members of the REV Research Team, especially Daniel Trang, Farhad Ahmed, Kyle Carvalho, Yuchen Du, Jai Castle and Zack Wong. They have been an integral part of my time on this project, and I could not have achieved this without them. I would also like to thank the PhD students who volunteer their free time around the lab, helping us in our tasks for the nUWAy shuttle bus.

Table of Figures

Figure 1. The nUWAy Shuttle Bus 9
Figure 2. EZ10 LiDAR Vision 10
Figure 3. EZ10 Lidar Vision (Overhead) 10
Figure 4. ROS Architecture. Adapted from 11
Figure 5. Simplified nUWAy Node Architecture 11
Figure 6. Socially Acceptable Distance 12
Figure 7. Triple Modular Redundancy 14
Figure 8. N-Version Programming 14
Figure 9. PLC Safety Curtain Range 15
Figure 10. Watchdog Node System Integration 18
Figure 11. New Stopping Ranges 19
Figure 12. Pedestrian Stopping Node Integration 20
Figure 13. The User Interface 21

Table 1. Risk Matrix 21
Table 2. Original Risk Register 22
Table 3. Projected Risk Register 22

1.0 Introduction

With the rising progression in technological application for the benefit of the public, the large field of autonomy for research and development remains at the forefront. The exciting proposition of autonomous control over facets of life such as menial tasks in the workplace or travel have been fast accelerating with many universities and companies seizing the new field of opportunity for investigation and experimentation. Autonomous driving has quickly become a large social presence in technology in recent years, with many publicly available cars becoming a status of luxury among the public.

Although this is a rising trend – there are multiple issues with the movement from human driven machines to full or partial autonomy. One facet of autonomous driving that this project will explore is the concept of safety. The concept of autonomous safety is heavily researched for public on-road use – however there are other applications of autonomous driving that can be investigated and pursued; public transport, air travel and lower speed high pedestrian density areas such as university campuses.

The University of Western Australia has recently received an EasyMile model EZ10 shuttle bus – it's aim to drive at level 4 autonomy [1] for student and public use on the university campus. The EZ10 shuttle bus is equipped with components essential for autonomous use, and contains combination of components and technology that is common in many autonomous vehicles that address machine logic, vision, self-localisation and drive by wire controllers.

The ambitious nUWAy project has allowed the Renewable Energy Vehicle (REV) Project Team at The University of Western Australia to pursue the research of practical full scale autonomous driving. It allows the project team to research and develop many aspects of autonomy in supporting the project goal of fully autonomous daily use on campus to assist students, staff and visitors and supply an exciting and technologically advanced method of transport around campus.

2.0 Scope

2.1 Project Identification

The impetus behind the shuttle bus project development stems from the University receiving the EZ10 shuttle bus figuratively empty, that is, no software was retained on its arrival to the university campus. Only the lowest level of safety remained on board – a separate Programmable Logic Controller that is preprogramed and not among the currently implemented main network of systems. As the addition of autonomous public transport is still a new venture, there is no baseline to issue or follow to create a safe enough driving system on this level of campus. It is difficult to assess the risks and performance metrics needed to create an appropriate baseline for comparisons [2]. The high volume of people the university campus and speed limits in small tighter spaces restrict the use of other existing autonomous driving technologies, such as line tracking for lane detection [3] and traffic roadmaps [4]. The different environment requires the full use of the vehicles own components and computation to safely travel and stop around campuses.

This project's goal is to raise the safety level of the nUWAy shuttle bus sufficiently, that is to support the autonomous driving system to ensure that when the shuttle bus is open to campus use,

we are able leave the shuttle to true autonomy without fear of fault or failure affecting its lifetime and reputation in daily use. This constitutes a level of safety where sufficient precautions will react safely should a failure or hazard approach. Explicitly, in the hazard failure, the object detection or avoidance of the autonomous path planning system has failed, and an undetected or unplanned collision is likely to occur. In theory, object avoidance techniques aboard an autonomous vehicle perform at full capacity to avoid every single obstacle detected, however in reality, accidents will and do occur. In the planned application scenario, the shuttle bus is not the only aspect of collision and accidents – unforeseen situations involving the pedestrian, or the secondary party is unavoidable from the development and safety precautions of the first party. Though some risk is impossible to fully mitigate it is up to the development team to reduce the likelihood of this risk to its absolute minimum. Additionally, the nUWAy is an intended public transport vehicle that will often contain passengers. A priority on passenger safety should be considered for the intended purposes of autonomous driving, as the fault of unfortunate accidents may eventually lie with its developers.

2.2 Objectives

The objectives of this project follow the outline that was identified in the previous section. The EZ10 shuttle received in its initial condition was not in an acceptable level of safety and hazard assessment, so it is vital for a safety system be created that can be sustained for additional development and to improve on the safety level of the system. The progression of the driving software is also in constant development as the shuttle bus project team continues work – so it is imperative that the safety control system on board remain open to scaling and expansion for inclusion of additional features and systems. Consistent with this, the main focuses of these objectives with respect to the software will specifically pinpoint node failures that have repetitively occurred during the nUWAy projects development which will be discussed in the design section.

Additionally, in support of the raising of safety and security standards of the bus, the shuttle bus needs to support an appropriate and sufficiently safe proximity safety feature. As object avoidance is not always the solution and unforeseen accidents are a real time occurrence in practical applications, a secondary system of emergency stopping, or collision avoidance is required. An example of this is a pedestrian riding a bike, or distracted pedestrian accidentally colliding or approaching the moving vehicle. Another objective of this project is to fulfill these requirements through software. This may be treated as logical reasoning due to the initial blank state condition the EZ10 shuttle bus has been received in, we in the REV Team are free to research and design the system in the architecture we desire. Finally, this project will address the communication standards of safety in autonomous vehicles to the public, as the primary objective of the nUWAy project is public transport application. Although seemingly secondary – it is still an important task that ties into the core values of safety that is discussed in this project. These objectives have been outlined with the factor of limited resources of the bus and the campus environment in mind. Development and research in autonomous vehicles on public roads is fairly common in the current age of autonomous development, but techniques for safety priority and considerations differ in a high urban density campus environments.

2.3 Resources

After outlining the purposes and scope for this project, it is important to highlight the available resources during the development of this project. The accessibility and function of these resources on the original EZ10 shuttle influences the methods of planning and development of the proposed design solution.

Figure 1. The nUWAy Shuttle Bus

The base EZ10 shuttle bus received for the project currently consists of:

- 8 LIDARs for the purposes of vision and navigation
  - 4 single layers 270 degree SICK Safety LiDARs
  - 2 180-degree Velodyne Puck model LiDARs
  - 2 four-layer IBEO LUX Localisation LiDARs
- SICK Programmable Logic Controller
- Basic onboard PC
- NovAtel GPS IMUs
- Two interactive touch screens

among additional components [5]. The few that are highlighted here will be discussed and are vital to the design of the safety system.

The LiDAR vision of the base EZ10 shuttle bus is represented in Figure 2 and 3.

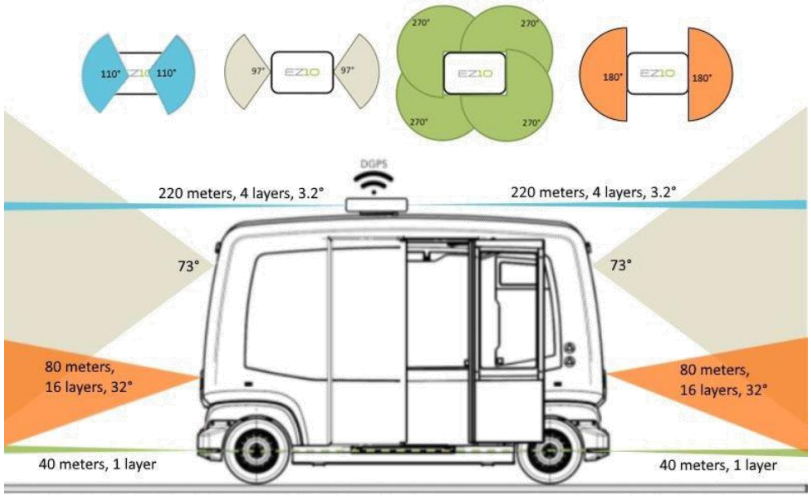

Figure 2. EZ10 LiDAR Vision [5]

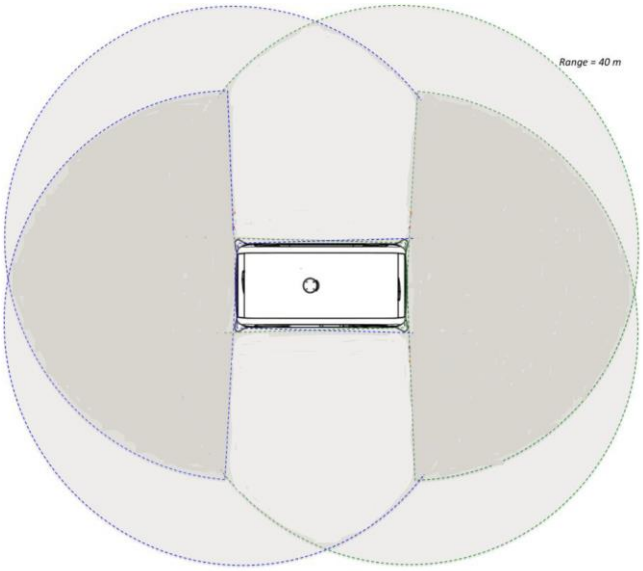

Figure 3. EZ10 Lidar Vision (Overhead) [5]

With respect to software, the nUWAy bus operates on the open-source Robot Operative System (ROS) Framework [6] and is run on a Lubuntu Operating System. ROS is described as a meta-operating system with capabilities including hardware abstraction, implementation of common robotic functionality including localisation and path planning and is intended for development of machines in fields including obstacle detection and driving autonomy. ROS operates in an architecture akin to a publishing and subscribing pattern of initialising data streams into topics that are communicated between process nodes. This architecture can be seen in Figure 4, which is a quick ROS architecture of the basic function of a vehicle's movement from sensor vision to the motor controllers. These nodes can perform multiple actions based on retrieval of data from subscribed topics and can perform tasks vital for autonomous driving. Open-Source packages that contains functions to support autonomous driving and often implemented include:

- Localisation

- Mapping
- Path Planning / Navigation
- Odometry
- CAN bus Communication

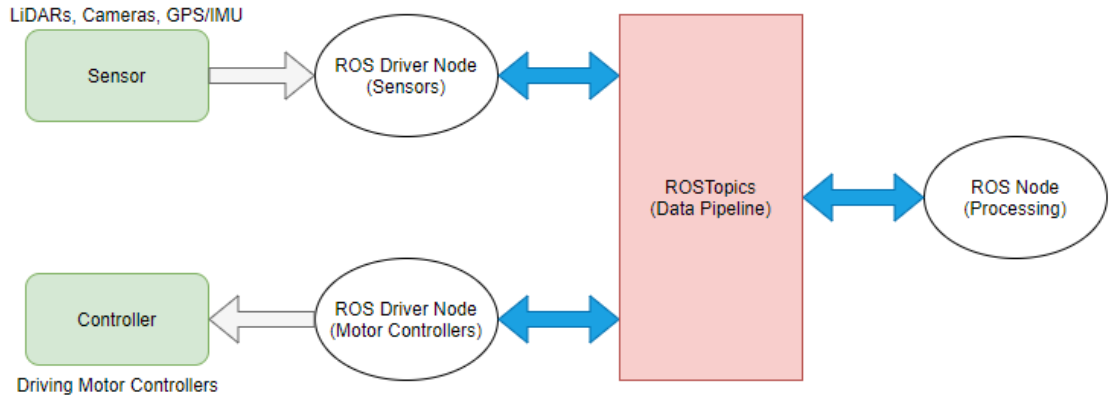

Figure 4. ROS Architecture. Adapted from [6]

The nUWAy architecture in its current implementation employs the use of user developed nodes in combination with the open-source package ROS Cartographer [7]. ROS Cartographer is used for the path planning of the vehicle and extends its received inputs to each LiDAR drivers onboard the vehicle, as well as the GPS and IMU components to perform localisation and odometry. It is key to note that ROS Cartographer will constantly output its path planning and map transformations unless it does not receive any of its required inputs, in which it will warn the system in terminal and stop outputting data on its topics. This may lead to some hazards and risks that will be identified and discussed in a future section.

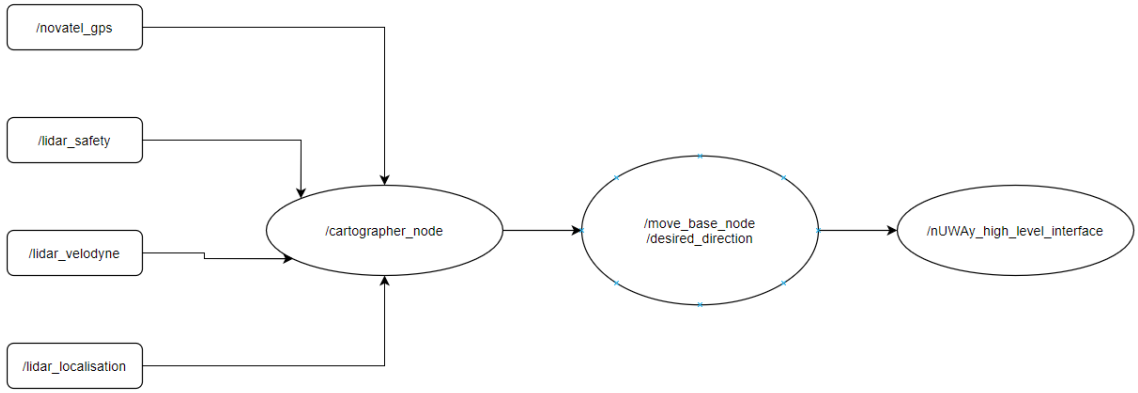

Figure 5. Simplified nUWAy Node Architecture

3.0 Literature Review

This section will focus on these facets of safety in respect the project scope and aim, that is in relation to autonomous driving and safety systems thereof. The section follows several safety considerations to be undertaken when developing under autonomous vehicles. Additionally, it will explore various engineering terms and techniques to address safety and safety in redundancy relevant to the level that is pursued in the listed project objectives. The idea is to build on the

progression of safety concepts and exploration into potential engineering practices useful to address the ongoing safety development on the shuttle bus.

3.1 Safety on Autonomous Vehicles

As the nUWAy shuttle bus is in preparation for function in high pedestrian density areas, it is necessary to explore conceptual safety with respect to pedestrian and passengers – the two remaining key participants in practice of autonomous vehicles. Multiple methods and considerations prioritising walking pedestrian and hazards of a campus scenario are discussed below.

3.1.1 Non-Line-of-Sight Conditions

Safety in Autonomous Vehicles follow is a newly developed concept that combines the traditional road vehicle safety concepts and the addition of safety concepts that must be followed in the development of path planning and decision making. A representation of this is the new consideration of Non-Line-of-Sight (NLOS) conditions. The dependency autonomous vehicles have on their immediate vision based on sensory LiDAR or cameras lead to unknown obstacles arriving from obstructed areas of vision and is seen as a major drawback of autonomous vehicles [8]. In cases like these, it is not difficult to imagine an unfortunate collision scenario that a local path planner may struggle with, therefore a secondary system of collision avoidance may be necessary. A proposed method of secondary system is the addition of Vehicle-to-Pedestrian (V2P) communications, to detect obstructed obstacles from a different source of communication [8]. However, this method demands enabled Dedicated Short Range Communication (DSRC) devices such as a compatible smartphone on a pedestrian, and can be seen as impractical in an publicly available campus environment due to this compatibility requirement.

3.1.2 Socially Acceptable Collision Avoidance

Another method of collision avoidance that prioritises a moving pedestrian obstacle is the Socially Acceptable Collision Avoidance Algorithm [9]. This method prioritises the urban environment and alters the path planning algorithm to respect the distances of both Vulnerable Road User (VRU) and the vehicle itself. It displays a concept that the behaviour of path planning is different once the pedestrian, which is more than a simple stationary object, moves with intent and requires a defined social space to feel safe and comfortable around vehicles in close proximity. It is expressed as seen in Figure 6, where the calculated total safety distance considers the intent of VRU, required social distance of the VRU and the safe distance of the vehicle itself.

$$d_{safety} = d_{VRU} + d_{social} + d_{vehicle}$$

Figure 6. Socially Acceptable Distance [9]

3.1.3 Elastic Band Theory

The Elastic Band Theory serves as the basis for many object avoidance algorithms. It refers to the concept of a path planning technique that is modified by external forces acting on the band or path. It is a mix of internal forces that keep the band together, while external forces act to keep the band away from obstacles. The theory originates from the robotics field and can be applicable in more modern situations of road collision avoidance [8] [10]. It can be further adapted to suit urban environment situations where the forces incurred from perceived obstacles have a defined social space considered for safety [9], as discussed in the previous section. This concept of each obstacle contributing to interacting internal and external forces altering an avoidance algorithm

can be explored to create a system that is adaptive to unexpected obstacles discussed previously [11].

3.1.4 Passenger Safety

The goal of the nUWAy project is to provide a method of public transport around the university campus, as such it is important to research the importance of passenger safety – as the primary customers of public transport are those that are travelling inside the vehicle. This involves standing and sitting passengers. It was identified that in a 3-year observation that up to a quarter of injuries sustained on public transport have been non collision [12]. That is, the sudden braking and acceleration of vehicles – specifically in emergency situations have led to injuries to passengers aboard the involved vehicle. This can be rooted to the inertial deceleration and acceleration caused by unexpected travel speeds. There remains the need to ensure the safety of passengers, specifically on autonomous shuttle buses, where the purpose is the publicly available method of transport.

3.2 Dread Risk and Public Confidence in Autonomous Vehicles

In a poll of 4500 people conducted in 2020, it was found that 60% of polled individuals felt unsafe as a pedestrian around autonomous vehicles, with the highest concern of growth being safety concerns [13]. With the higher than half percentage of people taking a risk averse approach to autonomous vehicles there is an underlying fear of the methodology of trusting a machine to make vital decisions. This can be defined as dread risk [14], defined as the heightened perception of risk when there is a level of uncontrolled, or non-understandable situations, or in this case, technology that is present. This affects public perception of autonomous driving, as there is a lack of domain knowledge that most of the public does not possess that increases the dread risk of passengers on autonomous vehicles [15].

3.3 Engineering Safety & Redundancy

With the development of the nUWAy shuttle bus there is a need to explore engineering safety concepts. Redundancy is one of these concepts, as it is a common technique applied in engineering to cover safety critical systems. This section will discuss approaches to safety in redundancy for application in both autonomy and software practices.

3.3.1 Triple Modular Redundancy

Triple Modular Redundancy (TMR) is the effect of triplicated hardware components to create 3 identical copies working in parallel that output a majority vote of the cloned components as a form of hardware redundancy. It is a form often used in engineering for its high fault tolerance and efficiency [16]. TMR concepts emphasise the modularity of the three systems, and the faults or failures that can occur in a singular system, will not easily be replicated in all three cloned systems at once. It is a technique often used in drive-by-wire or fly-by-wire systems [17], and can be applicable to the nUWAy shuttle motor-controlled system.

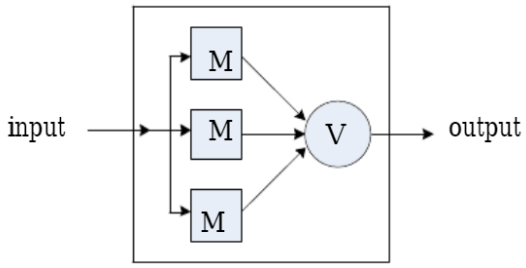

Figure 7. Triple Modular Redundancy [16]

3.3.2 N-Version Programming

N-Version Programming (NVP) is a software redundancy concept that explores an N-creations of the systems based on the same specifications. NVP systems follow a dissimilar design, and emphasise the independence of faults and failures between sister systems of the same specifications [18].NVP has inspired previous fusion decision systems modelled from neural network models to increase resilience and reliability in path planning algorithms [19].

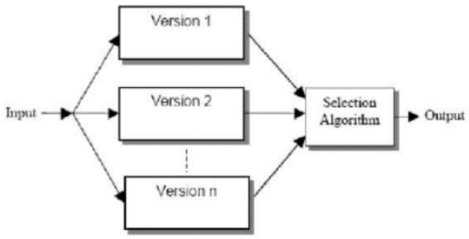

Figure 8. N-Version Programming [18]

4.0 Design Process and Final Design

This section will cover firstly the initial status of the nUWAy Shuttle Bus and the considerations that have influenced the design phase, followed by the final design of the project.

4.1 The nUWAy Shuttle Bus

In its base condition, an EZ10 shuttle bus contains the only an extremely limited safety stopping trigger. The range of this curtain trigger is presented in Figure 4. This curtain range is controlled by the Programmable Logic Controller and customisation of this is limited to the default ranges when the bus was received. This will be referred to as the PLC Safety Curtain, and triggers at a measured 1 meter ahead of its front two SICK LiDARs, and approximately 20cm off the cabin wall on the vehicle's sides. It is important to specify that the approximate 20cm side range extends from the wall of the shuttle cabin and reaches little beyond the corner lidars which themselves extend about 20cm further off the cabin. This combined with the 1m frontal rectangle that is fairly short in practice, it can be assumed that the range of the PLC curtain is prioritising self-preservation, in terms of assured physical collisions occurring at that range, over the early stopping obstacle and collision avoidance that is common for low level autonomous vehicles.

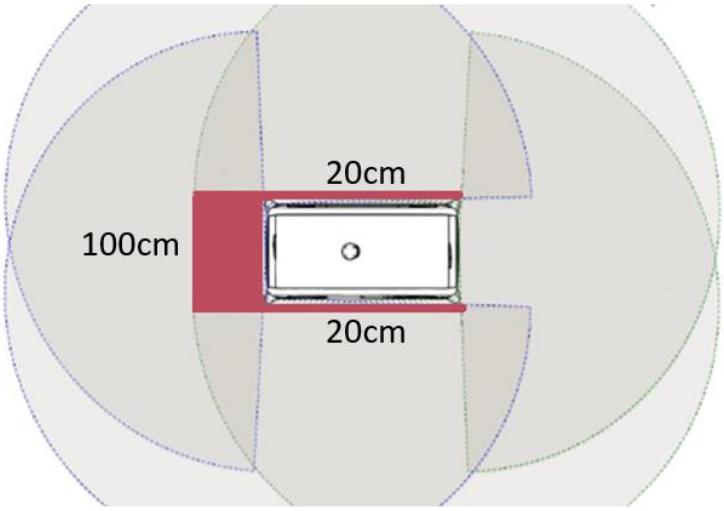

Figure 9. PLC Safety Curtain Range

An outstanding risk that has been identified is turning of the vehicle at this range. The vehicle can turn very quickly if desired, and due to the nature of the PLC Safety Curtain, the front range of emergency stopping may not be wide enough to encounter a moving pedestrian beside the vehicle, effectively turning into the pedestrian with an imminent collision between the side of the cabin and the forward walking pedestrian.

4.2 Design Considerations

The development of all aspects of the shuttle bus ranging from navigation and planning to odometry and sensor reception have been plagued with common issues that arise from the lack of high-level safety and self-diagnostic system onboard the nUWAy shuttle. Common software and hardware issues identified, and solutions designed in this project will be discussed in this section.

4.2.1 The Software

Many of the software issues that occur in the ROS framework and are often trackable and controllable from the developers. The ROS frameworks freedom of loose node coupling, and nature of a distributed framework allows for abstraction of function for autonomous vehicles. This also means that errors and faults experienced during development, which are common, are easily identifiable through the assessment of nodes function during experimentation and trials. Throughout development the nUWAy bus has experienced difficulties with its computational power. The original dated PC that was supplied with the shuttle bus struggled to maintain the computational needs of cartographer ROS, the path planning package that has been utilised during trials and testing of the shuttle bus's autonomous drives. Nodes of considerable importance have repetitively failed as a result of the lowered computational capabilities and have left the shuttle bus in compromising situations, including failures to start after stopping, failure to detect obstacles, and most critically, failure to stop when approaching an obstacle.

Often these node faults and node shutdowns occurred without the REV team's knowledge and have led to multiple trials and tests of undiscovered faults to failures. As there is no natural heartbeat or status monitor involved with some ROS libraries, it is difficult to diagnose a node that has simply failed. Without the immediate knowledge of a node failure, it was difficult to continue development, as discovering the node failures took a considerable amount of system

assessment. This in turn slowed testing as the solution would often require a full shutdown and restart of the entire shuttle bus system. The addition of a Jetson Xavier kit to supplement the computational power on the shuttle bus has seemingly resolved the node crashes during testing. There is continuing development on the nUWAy's system, and it can be foreseen that the computational requirements will increase over time, as such to avoid a similar situation, another method of solution is required. Therefore, the result of the situation has increased the immediate need for monitoring aboard the nUWAy shuttle architecture.

4.2.2 Current Implementation of PLC Safety Curtain

The current implemented PLC Safety Curtain has been previously deemed as insufficient for practical use. A 1-meter distance stopping curtain is not sufficient for safe vehicle practice and can still lead to collisions with moving obstacles. In a campus scenario, there are many types of pedestrians to consider, often on university campuses, there are distracted pedestrians [20]; on cell phones, carrying objects that obstruct view, or simply pedestrians with low situational awareness. Therefore, a new technique that has an increased level of safety must be considered. Failure to address these issues will lead to many failures and exposure to hazards that the team has experienced during development of the path planning and autonomous driving experiments. Additionally, if the PLC Safety Curtain is triggered, there is a need for manual re-arming of the vehicles driving components. This circumstance alone violates the level 4 Autonomy that the nUWAy project aims to achieve.

The newly designed stopping system is required to at minimum, stop at a confident and safe distance away from potential obstacles and stop at a distance that does not trigger the PLC Safety Curtain. Although theoretically, local path planning and obstacle avoidance measures should prevent a collision situation, safety should not be based on perceived function of components and should be planned for truthfully occurring faults of reality that will lead to unfortunate failures and accidents.

4.3 Application of Reviewed Techniques & Concepts

Following the research and review of engineering techniques in addressing a guideline for an efficient and available choice of technique that was readily supported in our available ROS framework. The design of this project was to follow the concept of Triple Modular Redundancy combined with the N-Version Programming that is common in software systems [18]. The proposed system mainly addresses two high priority safety hazards that have been identified and experienced during both navigation and automation development of the shuttle bus architecture and software.

Following the case of ROS node failures, it was apparent that a monitoring system that correctly reported the status of all nodes – including the monitoring node itself was required. This is important because the failure of a single vital node would render the entire system incapable of performing its task, causing a total failure, and potentially causing an unmonitored collision. Monitoring these nodes in a redundant fashion allows for full function and recovery of a node should another software failure occur. The ROS Framework holds the capability of restarting nodes [21] , and should the system experience a node failure, the monitoring system can safely recover from this failure without the need to stop and reset the system, and without violating the level 4 automation requirement of driver intervention.

The insufficient single PLC Stopping Curtain can be improved by adding a preventative measure. It should regard the existing stopping curtain as the final resort to emergency stopping and collision avoidance. The solution will prioritise prevention and take inspiration from the replicating and multiple redundancy concepts of TMR and NVP, while approaching the socially acceptable collision algorithm discussed in the literature review of this report. This is included in the design to respect the social and comfortable distance of pedestrians to increase the reputation of autonomous vehicles and lower the dread risk experienced by pedestrians.

Additionally, in practical use, the nUWAy shuttle bus will enable boarding passengers to stand for the duration of travel. As seen, it is imperative that the standing passengers and those sitting closely remain safe in unexpected circumstances of inertial change, whether it be emergency stopping or alterations in the local path. Therefore, the proposed solution must consider preservation of the passengers in addition to outside pedestrians when coming to an emergency stop or avoiding an unforeseen obstacle.

4.4 Final Design

For the final design, both proposed redesigned systems will employ a system that is triplicated for redundancy, akin to the explored Triple Modular Redundancy concept. This will enable three levels of fault tolerance and reduce the risk of failure of both considered components – the software node failure, and safety curtain stop. Both systems also take inspiration from NPV programming, in which the emphasis is on replication of system requirements, but independence in design implementation. This is to reinforce and cover different points of failure across each replication of the system.

The software node system failure and PLC curtain stopping are both considered due to their failures leading to certain failures in the system. However it is needed to clarify that triggering the PLC Safety Curtain is not deemed a failure in terms of collision avoidance, in fact, triggering the PLC Safety Curtain can be seen as a successful safety system. However, for the purposes of overall system function, it will shut down the shuttles driving functionality, requiring a re-arming of the shuttle bus. Although it is critical that the shuttle bus never hit a pedestrian if avoidable, we would like to avoid triggering the PLC Curtain.

4.5 Watchdog Nodes

The watchdog system is designed is an extension of cartographer. As previously discussed, the cartographer node acts as a fault tolerance measure to failure, as it will not continue to plan paths or function should it fail to receive an input. The secondary and third redundant measures are continued in the newly developed watchdog nodes. These two nodes take advantage of the ROS Diagnostics package [22]. The diagnostics package has an aggregation feature that can allow publishing of node heartbeat and diagnostics information. The implementation of the watchdog nodes allows us to aggregate node heartbeat, data publish rate, and data validation for all LiDAR driver, movement, and path planning nodes.

Each of the two watchdog nodes will both replicate aggregation of all node status diagnostics, with the addition of the secondary watchdog including the node diagnostics of the first. This will ensure that even should the watchdog die, the system will be aware of the situation. This method ensures replication fault tolerance, while also allowing for NPV fault tolerance, in differing in design from the cartographer node fault tolerance. If cartographer fails to receive an input from

its required LiDAR or input nodes, it will not create valid data, alerting the watchdog nodes. These watchdog nodes will also be receiving the failed nodes incorrect data and the cartographer node's invalid data, and lowered publishing rate. The watchdog nodes can then recover the system by restarting relevant nodes if possible. Additionally, the watchdog nodes can alert the development team of the system or node failure through the newly developed User Interface integration. Figure 8 illustrates the addition of the two watchdog nodes.

Move_base_node and desired_direction nodes have also been integrated into the watchdog system. As these nodes are user written by the REV team, we are able to include the addition of diagnostics publishing into the node functions.

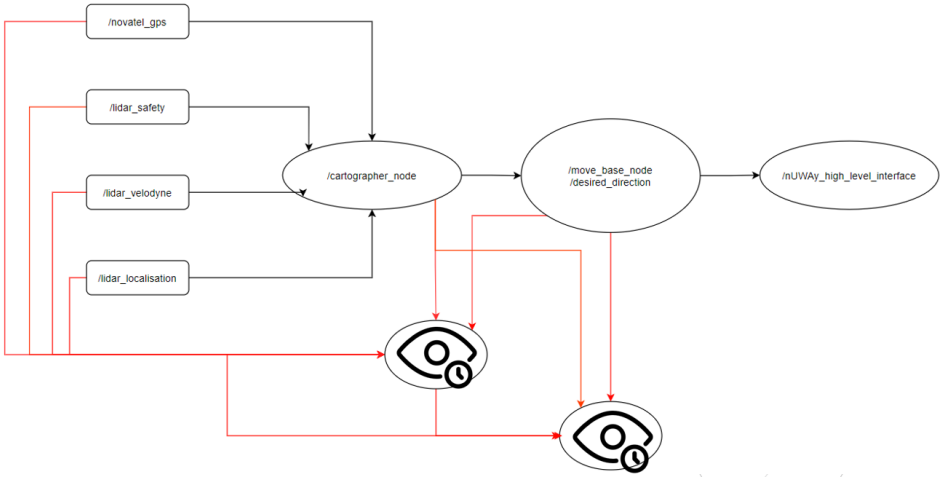

Figure 10. Watchdog Node System Integration

It should be noted that the high-level interface in Figure 8 is its own self-contained system that implements self-contained diagnostics and employs its own failure handling without affecting the core ROS system, and therefore is not included in the design of this watchdog system.

4.6 The Speed Scaling System

The safety curtain system will be extended by two extra components. In combination with the existing safety curtain system – there will be triple redundancy in collision avoidance. The design of the safety curtain includes a speed scaling feature, as well as a soft stopping feature. These will run together in a node and operate functionally differently from the PLC Safety Curtain. All three redundancies run from the same inputs from the four SICK safety LiDARs, however the PLC Safety Curtain does not have the ROS node driver passthrough that the speed scaling feature experiences and will still activate in the unfortunate event of safety LiDAR drivers failing.

The speed scaling feature follows inspiration from Socially Acceptable Collision Avoidance and slows down for approaching pedestrian or obstacles and comes to a complete stop if the pedestrian or obstacle continues to come into the stopping range of the vehicle. The scaling of the speed is based on percentage of a detected obstacle between two thresholds, a starting distance and a stopping distance. The scale will drop from 100% speed to 0% speed, as the detected obstacle approaches the stopping distance. This new stopping range is a distance further than the PLC Stopping Curtain and is currently set to 2 meters in front of the vehicles moving direction in a wide cone shape. The PLC Stopping Curtain is only active when the bus is in a moving state and

will not trigger an emergency stop if an obstacle is within its curtain range while stationary. As such the new stopping feature has been called a soft stop – due to the stop not triggering the PLC Safety Curtains hard system stop.

The current speed scaling node begins scaling the speed of the vehicle at 4 meters from any direction. This speed scaling is a form of both safety in practicality and safety in perception. As previously discussed, a quarter of injuries sustained on public transport buses occur from non-collision accidents, specifically from falling or minor collisions inside the cabin of the bus. These occur from the sudden stopping and inertial change of the bus coming to a complete stop with high deceleration. The new speed scaling serves to alleviate the change in the jerk when coming to an emergency stop, thus reducing passenger incidents from within the cabin. The secondary safety in perception is pedestrian being in reduced perceived danger due to the lower speeds when approaching or within the vicinity of the nUWAy shuttle bus. This can serve to alleviate the dread fear and increase trust of autonomous vehicles as something that is taking appropriate safety measures in regards to pedestrian preservation.

Figure 9 illustrates the new stopping distances of the Speed Scaling node. Its threshold distances are currently 4 meters to begin speed scaling, and 2 meters to soft stop. This is an experimental distance that is changeable and is further discussed in a later section.

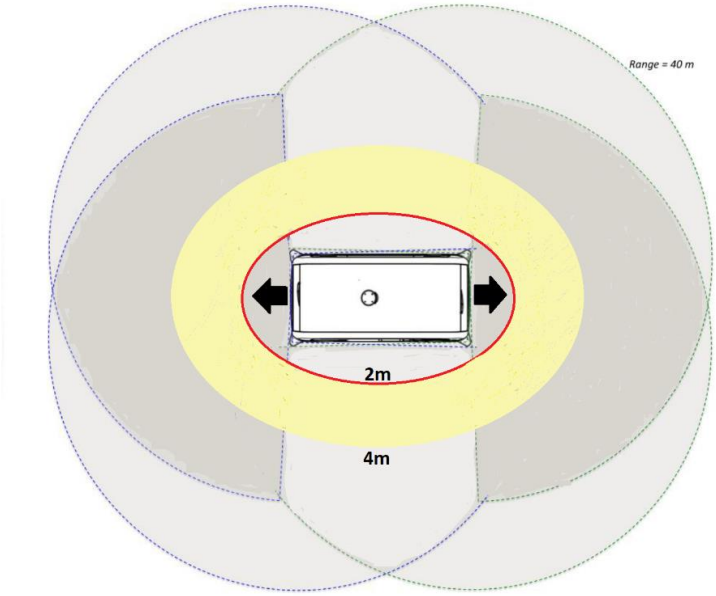

Figure 11. New Stopping Ranges

Figure 10 illustrates the Speed Scaling node integration into the nUWAy's ROS architecture. Its addition will be included in the diagnostics aggregation and includes functions to publish its own diagnostics to the aggregation watchdog nodes.

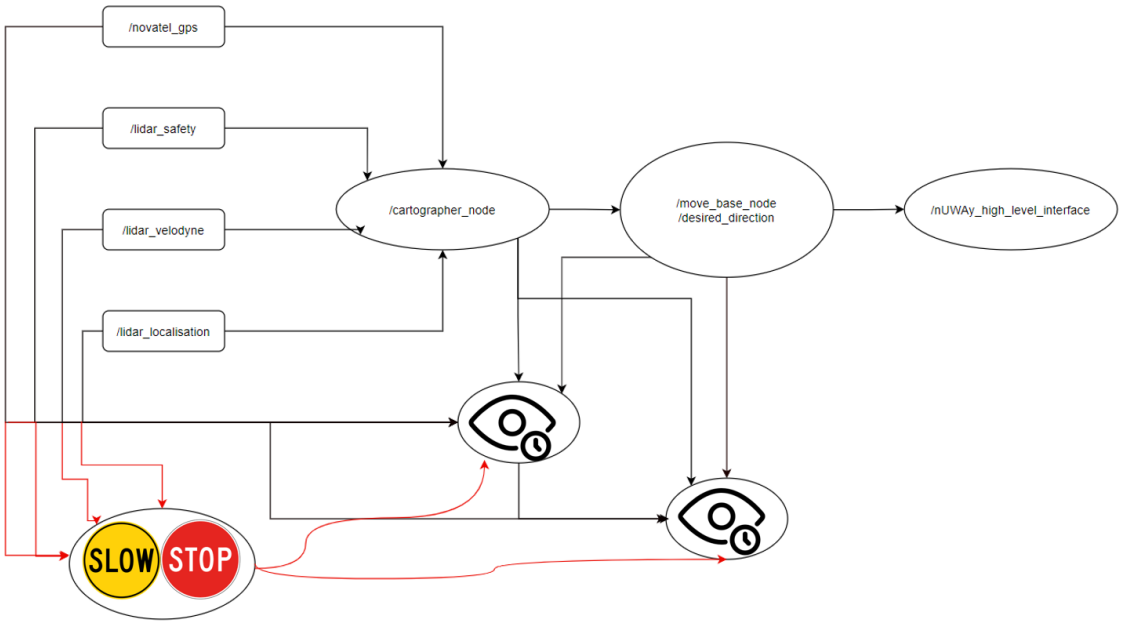

Figure 12. Pedestrian Stopping Node Integration

4.7 The User Interface

As a part of the REV Team, I was additionally tasked with creating a User Interface (UI) for the system, that was to be appealing and appropriate for its purpose of travelling to and from stations around campus. As discovered during the research phase of this project, it was apparent that there is a dread risk related to the lack of domain knowledge and from the unknown technology [14]. As such, it was beneficial to include the status and aggregate diagnostics to publish to the passengers as well as the developers of the system. Although intended to be for developer use in diagnostic tracking during testing, being able to communicate the unknown factors of the autonomous vehicle to the passengers may serve to alleviate dread risk and increase trust in autonomous vehicles. Figure 13 illustrates the UI, with the inclusion of status trackers at the bottom of the figure. As an autonomous vehicle can act as a mysterious and unknown machine to some, we can now educate some passengers on the status of nUWAy shuttle bus should it come to a stop. The naming convention is changed when represented on the UI, as the lack of domain knowledge prevents use of terms specific to ROS or the architecture of autonomous vehicles, so names chosen to be simple and concise have been used.

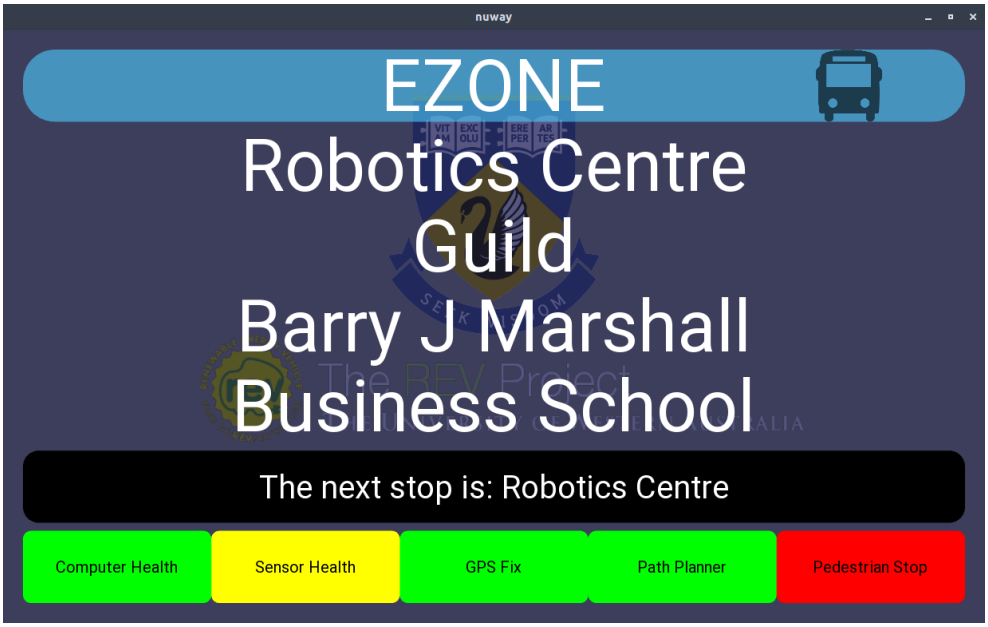

Figure 13. The User Interface

5.0 Results

5.1 Risk Assessment

Considering the design and application aspect of this project – it is a suitable assessment to view the level of risks and hazards that are on the bus at any time. Table 1 represents the Risk Matrix used during assessment. The listed consequences were made with respect to injury in persons - pedestrian or passenger. In a low-speed autonomous vehicle, the severe consequence will represent a death due to the vehicle, Major being a disability or severe injury incurred, while Moderate and Minor represent mild and minor injuries at most. In the cases of node failures – consequence is a measure of system failure, where Severe is a complete shutdown of systems, leading to at least multiple days of downtime, Major is a shutdown of systems requiring a hard restart, followed by reducing levels of inconvenience, such as Moderate being a shutdown before restarting the nodes, Minor being a short delay, and Insignificant meaning the bus can continue its tasks with no effect.

Table 1. Risk Matrix

		Consequence				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Likelihood	Almost Certain (5)	Medium	High	High	Extreme	Extreme
	Likely (4)	Medium	Medium	High	Extreme	Extreme
	Possible (3)	Low	Medium	Medium	High	Extreme
	Unlikely (2)	Low	Low	Medium	Medium	High
	Rare (1)	Low	Low	Low	Medium	High

Table 2 describes the risk register prior to the project design, displaying risks relevant to the projects design, where only the limited PLC Safety Curtain is implemented. We can see the highest risk of injury due to collision is turning into a pedestrian and a collision occurring, with

all other risks having a high likelihood – either from the lack of appropriate emergency stopping, or software nodes crashing and system failure. The highest risk to the shuttle bus system is the activation of the PLC Safety Curtain shutting down all systems, requiring a manual re-arm of the system, and is a Major consequence to the system. All these failures can result in some level of injury incurred by either a collision or abrupt stopping.

Table 2. Original Risk Register

Risks	**Likelihood**	**Consequence**	**Overall Risk**	**Risk Level**
	1-5	**1-5**	**1-25**	
Failure to stop resulting in head on Pedestrian Collision	2	4	8	Med
Turning into a Pedestrian and being involved in a collision	4	3	12	High
Passenger collision inside vehicle from abrupt stop	4	2	8	Med
Single Node (Drivers, Cartographer) Failure	4	3	12	High
Bus continues without correct path planning	3	3	9	Med
System shutdown due to emergency stop from PLC Safety Curtain	4	4	16	Extreme

There is no immediately quantifiable result to achieve with this risk assessment and risk register approach, although a true full assessment of the experienced risks will take time to discover the true likelihood and consequence of each risk. As such, Table 3 represents the intermediately experienced and projected Risk Register of the nUWAy shuttle bus with the addition of the newly designed safety systems. All likelihoods have and should stay lowered, dropping to rarely occurring. In the cases of collisions, the speed scaling system will have reduced the speed of the vehicle or stopped it entirely in situations in which the original system will have continued movement into a collision. This is especially true with the turning into a pedestrian collision, due to the much larger side and front cones of detection for stopping. Node and software failures will also have dropped in likelihood due to the watchdog nodes' ability to stop the vehicle and recover the system successfully, so the likelihood of incidents caused by dying nodes will not have collisions.

Table 3. Intermediate & Projected Risk Register

Risks	Likelihood	Consequence	Overall Risk	Risk Level
	1-5	1-5	1-25	
Failure to stop resulting in head on Pedestrian Collision	1	4	4	Med
Turning into a Pedestrian and being involved in a collision	1	4	4	Med
Passenger collision inside vehicle from abrupt stop	1	2	2	Low
Single Node (Drivers, Cartographer) Failure	1	2	2	Low
Bus continues without correct path planning	1	2	3	Low
System shutdown due to emergency stop from PLC Safety Curtain	1	4	4	Med

5.2 Discussion & Improvements

The high likelihood of the discussed risks has been mitigated as we have seen intermediately in Table 3. This is in no way a comprehensive list of risks for the entire nUWAy project, and only a list of those relevant to the projects design and objectives outlined in the earlier objectives section of this report. Reducing the risk level of these risks has been achieved through mitigation of likelihood with new software nodes. Both the Watchdog nodes and Speed scale nodes have actively reduced the likelihood of each relative risk to drop most of the overall risk to rare likelihood.

It is important to note that the consequence of collision risks remain unchanged, as there remains the chance of collision in some cases. Reducing the likelihood of these cases is near impossible as there is only so much that can be done from a likelihood mitigation standpoint of the shuttle bus, there remains some risk involved from the secondary party of the collision that is unmitigable from the shuttle bus. Alternative methods of risk mitigation such as gaining the attention of distracted may be suitable but are not in the scope of the objectives of this project.

The consequences of software node failures have reduced, due to the integration of the watchdog nodes' alerting users and developers of the failure of nodes. This reduces the consequence of software failure risks to reduced downtime of the faulted system. We can see the moderate consequences of Single Node Failure and Bus Continuing without path planning have dropped to

Minor, as the watchdog nodes will alert the users and developers only leaving short delay in time lost without the system shutting down.

The speed scaling node can see improvements through further testing in trial runs of practical application. Currently, the distances of 4-meter and 2-meter thresholds for the speed scaling have been chosen based on preliminary testing between the REV Team members. The threshold distances have yet to be fully tested for the most efficient application due to the differences between development and application scenarios. During full application, the shuttle bus will see a potentially high density of pedestrians moving along the campus paths, where a 2-meter scaling window may become insufficient, and the shuttle bus will constantly travel at a significantly lowered scale speed despite the reasonable distance of pedestrians. Additionally, the method of design for the scaling may be improved through the addition of the Elastic Band Theory, where the obstacles contribute to the sum of active forces, altering the scaling algorithm proactively as the number of surrounding pedestrian increases.

The ROS Cartographer is currently not considered as a diagnostic in the watchdog system during integration. ROS Cartographer is a sourced package, and it is difficult to insert diagnostic on what was originally treated as a black box component. There has been attempts to create diagnostics from its transformation topic output but has shown to not accurately depict the true diagnostics of the node, as publishing rate has been shown to be inaccurate during preliminary testing. As such further improvements can be made to the watchdog nodes if we were able to devise a way to create and aggregate diagnostics from the source code of the cartographer node.

True Triple Modular Redundancy is not achieved here in the system. Although the current system has taken inspiration from the concept, it is due to limited resources such as budget and computational restraints. The objective of this project contained the ability to create these systems with the given resources, without expenditure into a new separated systems that will bring independent point of failures. that the level of true independency between triplicated systems cannot be achieved. Similarly with N-Version Programming, neither of the systems N-versions replicated have true independent failure modes from another. Specifically, both watchdogs operate on the same network, and share the entire system point of failure, and the speed scaling and soft stopping functions operate on the same node, both sharing the node failure point of failure.

6.0 Conclusions

The Project has led to the design of successfully created safety systems, fulfilling the objectives of supplementing the nUWAy shuttle bus project with a safer system, improving on the bare systems that existed on arrival on the University of Western Australia campus. Although true assessment of the system will take time, intermediate results show the risk likelihood has been mitigated, though the consequences of collision cannot be mitigated. Software system failures have reduced since the inclusion of the system.

Additionally there has been integration into the UI of the watchdogs alert system that will alleviate the potential dread risk of some untrusting passengers.

The final design still has room for improvement and can be further expanded to include additional nodes during continued development of the shuttle project. This project's watchdog and speed scaling systems may be chosen to be re-assessed at a later date once full integration into the finalised nUWAy shuttle system has been achieved.

6.1 Further Investigations

Further Investigations is advised to continue the development and improvement of the safety system, these include:

- Improvements that have been previously stated in Section 5.2, that is:
    - Further testing of the system over time, and in practical trial scenarios. The speed scaling thresholds will most likely require tweaking when the shuttle bus is ready for full deployment.
    - If ROS Cartographer is continuing to be used in the development of the nUWAy shuttle bus, there must be a method devised to integrate diagnostics publishing and aggregation.
- Investigation into seamless restarts of dying nodes, without the need to come to a complete stop. This will investigate the ability of spoofing continued input data for cartographer to continue path planning while the failed node recovers or finding an alternative to movement with reduced integrity of input nodes.
- Alternative methods of Triple Modular Redundancy or N-Version Programming, that follow the defined true independency of both theories. That is, a fully triplicated and independent system for TMR, and truly independent failure modes present in NVP.
- Integration with nUWAy's high level interface. Although the inclusion of this system was treated as separate and out of scope, logically to include the complete working system, the high-level interface nodes should be integrated into the watchdog system, completing its full integration into the entire system of the shuttle bus.

7.0 References

[1] "SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles," 11 12 2018. [Online]. Available: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles. [Accessed 30 4 2021].

[2] J. Cregger, M. Dawes, S. Fischer, C. Lowenthal, E. Machek and D. Perlman, "Low-Speed Automated Shuttles: State of the Practice," U.S Department of Transportation, 2018.

[3] Z. Wu, K. Qiu, T. Yuan and H. Chen, "A method to keep autonomous vehicles steadily drive based on lane detection," *International journal of advanced robotic systems,* vol. 18, no. 2, 2021.

[4] C. Wang, H. Huang, Y. Ji, B. Wang and M. Yang, "Vehicle Localization at an Intersection Using a Traffic Light Map," *IEEE transactions on intelligent transportation systems,* vol. 20, no. 4, pp. 1432-1441, 2019.

[5] EasyMile, EasyMile EZ10 User Manual, Toulouse, 2016.

[6] ROS.org, "ROS Documentation," 11 06 2020. [Online]. Available: http://wiki.ros.org/. [Accessed 14 06 2021].

[7] The Cartographer Authors Revision, "Cartographer ROS Integration," 2021. [Online]. Available: https://google-cartographer-ros.readthedocs.io/en/latest/. [Accessed 12 06 2021].

[8] S. Y. Gelbal, B. Aksun-Guvenc and L. Guvenc, "Collision Avoidance of Low Speed Autonomous Shuttles With Pedestrians," *International Journal of Automotive Technology,* 2019.

[9] H. Wang, "Control System Design for Autonomous Vehicle Path Following and Collision Avoidance," ProQuest Dissertations Publishing, The Ohio State University, 2018.

[10] Ö. Ararat and B. A. Güvenç, "Development of a Collision Avoidance Algorithm," in *The International Federation of Automatic Control*, Korea, 2008.

[11] J. Hilgert, K. Hirsch, T. Bertram and M. Hiller, "Emergency path planning for autonomous vehicles using elastic band theory," in *Proceedings 2003 IEEE/ASME International Conference on Advanced Intelligent Mechatronics* , Kobe, 2003.

[12] A. P.Silvano and M. Ohlin, "Non-collision incidents on buses due to acceleration and braking manoeuvres leading to falling events among standing passengers," *Journal of Transport & Health,* vol. 14, 2019.

[13] H. Jones, “The Social Ethics of Self-Driving Cars: Public Perceptions and Predictions of Autonomous Vehicle Safety Risks.,” *Contemporary Readings in Law & Social Justice,* vol. 12, no. 1, p. 37043, 2020.

[14] J. D. Lee., “Exploring Trust in Self-Driving Vehicles Through Text Analysis,” *Human Factors: The Journal of the Human Factors and Ergonomics Society,* vol. 62, no. 2, pp. 260-277, 2019.

[15] M. Raue, L. A. D'Ambrosio, C. Ward, C. Lee, C. Jacquillat and J. F. Coughlin, “The Influence of Feelings While Driving Regular Cars on the Perception and Acceptance of Self-Driving Cars,” *Risk Analysis,* vol. 39, no. 2, 2019.

[16] S. A. Shernta and A. A. Tamtum, “Using Triple Modular Redundant (TMR) Technique in Critical Systems Operation,” in *The First Conference for Engineering Sciences and Technology*, 2018.

[17] Y. Yeh, “Triple-triple redundant 777 primary flight computer,” in *IEEE Aerospace Applications Conference*, 1996.

[18] G. M. Nayeem and M. J. Alam, “Analysis of Different Software Fault Tolerance Techniques,” *Journal of Engineering and Science (JES),* vol. 1, no. 1, 2009.

[19] A. Wu, A. H. M. Rubaiyat, C. Anton and H. Alemzadeh, “Model Fusion: Weighted N-Version Programming for Resilient Autonomous Vehicle Steering Control,” in *2018 IEEE International Symposium on Software Reliability Engineering Workshops*, Memphis, 2018.

[20] D. Stavrinos, K. W. Byington and D. C. Schwebel, “Distracted walking: Cell phones increase injury risk for college pedestrians,” *Journal of safety research,* vol. 42, no. 2, pp. 101-107, 2011.

[21] ROS.org, “roslaunch,” Open Robotics, 23 10 2019. [Online]. Available: http://wiki.ros.org/roslaunch. [Accessed 12 06 2021].

[22] ROS.org, “diagnostics,” Open Robotics, 06 03 2018. [Online]. Available: http://wiki.ros.org/diagnostics. [Accessed 12 06 2021].