Free University of Bozen-Bolzano

Requirements Engineering

Project 2

Group Members: Crystal Kwok, Matteo Ponza, Tetty-Nartey Samuel

Lecturer: Claus Pahl

Content Page

Task 1: Issues with Project Basis

1. Ambiguity in Spatial Gap Requirement for Safety

1.1 Issue description

According to the project description, it is mentioned that:

In a lane change due to a merging of lanes, the vehicle performing the change needs to ensure the availability of a sufficient spatial gap in the target lane.

A sufficient spatial gap is required between two vehicles such that the third vehicle can merge safely. This spatial gap requirement is not clearly defined. This gap will be dependent on several factors such as the speed of moving vehicles, the weather conditions and the road conditions.

1.2 Options

The viable options to identify the requirement are as follows:

- Conduct a workshop with car manufacturers to obtain feedback on safety standards
- Research on traffic laws and regulations set by transportation or road safety authorities

1.3 Decision and rationale

Although there are guidelines for merging and following safe distancing of vehicles, many of the safety standards, including spatial gap between cars, are determined based on judgement. This means that practical knowledge and experience will be more effective to identify the spatial gap requirement. Hence, the decision is to conduct a workshop with car manufacturers who are the people on the ground with practical knowledge.

2. Ambiguity in the Specification of Vehicle's Awareness of the Surroundings

2.1 Issue description

The project description for the Localized Cooperative Lane Merging mentions the following requirement:

Vehicles need to be aware of their surroundings by the exchange of status update messages.

However, it is unclear whether the cars involved in the cooperative lane merging are aware of the surroundings of other cars. Additionally, it is not specified what type of surroundings a car should be aware of and how this information can be obtained.

It is important to clarify this point since the information will be used to evaluate the cooperative lane merging manoeuvre and therefore have great implications for the safety of the system.

2.2 Options

The viable options to identify the requirements are as follows:

- Conduct an in-depth research study regarding various types of information that modern vehicles can sense
- Conduct a workshop with the car manufacturers to obtain detailed information on the types of data a vehicle can obtain
- Review the information listed with car safety experts to identify the most important surroundings information for evaluating the safety of the car

2.3 Decision and rationale

The workshop with the car manufacturer and the review of the information listed with the car safety experts are chosen. Although beneficial and suggested, the research study alone would not be sufficient to obtain the expected level of detail for this information. Given that the information obtained has implications for the safety of the system, it is a necessity to have complete clarity on the information-sensing capabilities and limitations of the vehicles.

3. Incompleteness in the Specification of Safety of Manoeuvre

3.1 Issue description

The project specifications mention that is necessary to evaluate the safety of a manoeuvre before executing it or aborting it:

A decision could be to abort the overtaking action because of an incoming emergency/not-equipped vehicle/lack of safety.

However, it is not specified what is considered a safe manoeuvre. For example, it could be characterized by maintaining safety distance between the vehicles, by the absence of incidents or sudden stops, which should also be quantified, as well as other parameters.

3.2 Options

The viable options to identify the requirements are as follows:

- Conduct technical workshop with car safety experts to identify and quantify what constitutes a safe manoeuvre
- In depth review of traffic regulations law regarding the subject
- Conduct a questionnaire to understand the societal acceptance of safety

3.3 Decision and rationale

Both the options above are chosen since having clear requirements specification for safety is key. Safety constitutes a central part of the system as well as being thoroughly reviewed and verified. It is critical that the system complies fully with the traffic regulations laws.

4. Incomplete Specification for Security of System

4.1 Issue description

Since the cooperative lane merging can be implemented locally or centrally, exchanges of status update messages are either direct between vehicles or between vehicles and centralized entity. In this situation where information is being communicated and shared, vehicles are exposed to external systems and vulnerable to attacks. However, the security requirements of the system are not stated.

4.2 Options

The viable options to identify the requirements are as follows:

- Research on strong security measures and security best practices
- Conduct a workshop with the transportation authorities to obtain feedback on the type of information required to be shared
- Review international agreements or standards between countries

4.3 Decision and rationale

All three options above are chosen. Since security is crucial and may potentially impact safety, strong security measures should be implemented in the software system. Additionally, workshops with the transportation authorities would clarify the required data needed, possibly limiting the sharing of sensitive information. Lastly, as the project involves vehicles and data crossing international borders, it would be useful to understand and review the international agreements between the countries involved in the project.

5. Lack of Specification of Availability Requirements

5.1 Issue description

In systems as critical as that of cooperative lane merging, the requirement of the system uptime should be stated clearly. The downtime of the system server, network communication or computational system should be minimized. However, the availability specification is not defined in the project.

5.2 Options

The viable options to identify the requirements are as follows:

- Conduct extensive research on industry standards and benchmarks related to system availability
- Organize focused workshops with technical experts to collaboratively outline requirements for availability of the system
- Engage system architects to obtain limitations on infrastructure of system to derive realistic availability requirements

5.3 Decision and Rationale

A comprehensive approach combining in-depth research and collaborative workshops are chosen. This decision aims to achieve a thorough understanding of industry standards while tapping into the collective expertise of technical professionals. Through collaborative workshop with technical experts, diverse perspectives and experienced insights can also be taken advantage of.

6. Lack of Specification of Network Requirements

6.1 Issue description

Requirements for the network infrastructure are not stated in the project description. In order to cater to a certain amount of traffic, a specific bandwidth requirement should be well-defined. For the users to trust that the system works as expected, the reliability requirement should also be specified.

6.2 Options

The viable options to identify the requirements are as follows:

- Conduct research to gather insights on network requirements of critical systems
- Organize technical workshops with network engineers to understand suitable network requirements

6.3 Decision and Rationale

The decision is to conduct technical workshops. Since network requirements of different systems differ greatly based on size, type and severity of system, this approach allows for a more targeted solution with the network experts providing their knowledgeable feedback directly in the perspective of the project.

Task 2: Preparation of requirements elicitation

Workshop: Safety of Cooperative Lane Merging Manoeuvre

Workshop is conducted at the early stage of the project.

Objectives	- Identify possible scenarios involved in 3 cars cooperative lane merging manoeuvre - Brainstorm and develop ideas to facilitate the manoeuvre safely - Obtain preliminary understanding of critical points that affect safety
Participants	Transportation authority X 2 Reason: Knowledge of traffic laws and regulations
	Car manufacturer X 2 Reason: Knowledge of car capabilities and manoeuvre
	Car safety expert X 2 Reason: Knowledge of strategic safety requirements
	Software Architect X 2 Reason: Knowledge of software infrastructure
	Project Manager X 2 Reason: Knowledge of project background
Facilitators	Requirement Engineer X 2 Reason: Moderate sessions and provide prompts
Format	Disney Creative Strategy
Duration	7.5 hours
Location	- Seminar Room: For presentation and sharing, large room (12 Pax) equipped with projector - Discussion Room 1: For discussion, medium room (6 Pax) equipped with white board - Discussion Room 2: For discussion, medium room (6 Pax) equipped with white board
Food and Beverage	- Light Refreshment - Lunch - Coffee and Tea

Table 1 Workshop Details and Specifications

Workshop Agenda

The details of the workshop agenda are further specified in the sections below.

Agenda	**Description**	**Duration**	**Location**
1. Introduction	- Ice Breaker - Project Introduction	40 Mins	Seminar Room
2. Workshop Introduction	- Goals - Disney Creative Strategy	30 Mins	Seminar Room
Refreshment Break	- Light refreshment - Move to respective rooms	30 Mins	Pantry
3. Workshop Kick-off	- Scenario brainstorming	30 Mins	Discussion Rooms
Break	- Participants immerse in *the dreamer* role	15 Mins	
4. The Dreamer	- Participants take on the role as *The Dreamer*	60 Mins	Discussion Rooms
Lunch Break	- Lunch	60 Mins	

	- Participants immerse in *the realist* role		
5. The Realist	- Participants take on the role as *The Realist*	60 Mins	Discussion Rooms
Break	- Participants immerse in *the critic* role	15 Mins	
6. The Critic	- Participants take on the role as *The Critic*	60 Mins	Discussion Rooms
Coffee Break	- Coffee and Tea	20 Mins	Pantry
7. Debrief	- All participants and hosts to review the ideas that were formulated in the workshop	30 Mins	Seminar Room

Table 2 Workshop Agenda and Description

1. Introduction

Ice Breaker

Duration: 30 mins

Every participant to introduce himself/herself with the following prompts: name, job and fun fact. This activity is to create a relaxed and open atmosphere, so the participants feel comfortable with one another.

Project Introduction

Duration: 10 mins

Provide a brief introduction on the 5G Carmen Project with focus on cooperative lane merging manoeuvre using the 5G Carmen promotional video in Figure 1 below.

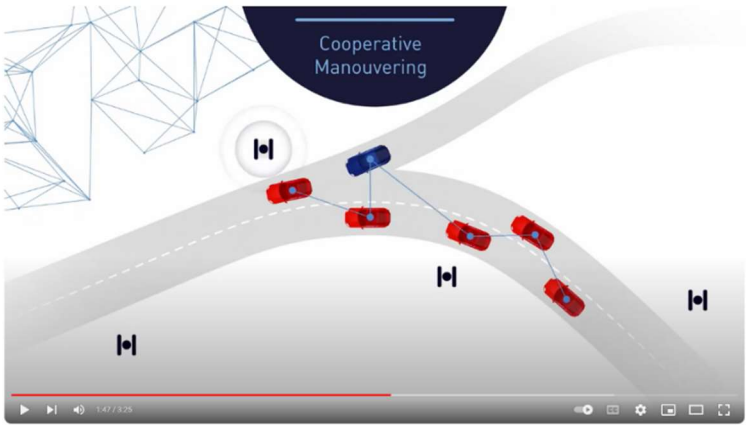

Figure 1 Project Introduction Video for Participants

2. Workshop Introduction

Goals

Duration: 10 mins

Explain the goals of the workshop to the participants:

- Identify possible scenarios involved in 3 cars cooperative lane merging manoeuvre

- Brainstorm and develop ideas to facilitate the manoeuvre safely

- Participants should be open minded and to put themselves into different mindsets according to the roles

Disney Creative Strategy

Duration: 20 mins

Following *Disney Creative Strategy*, participants should take on the roles of *the dreamer*, *the realist* and *the critic* to develop creative ideas that are realistic and with safety in mind.

Rationale: This workshop format allows participants to think out of the box to generate new and innovative ideas. Subsequently, change their perspective to make the ideas realistic and suitable in the context. Lastly, put on critical thinking hats to improve on the ideas.

Process: The participants will be divided into two teams with equal number of participants, as in Table 3 below. Two separate teams are formed in the workshop in order to obtain a broader view and varying perspectives.

Teams	Team 1	Team 2
Location	Discussion Room 1	Discussion Room 2
Participants	1 Requirements Engineer - Facilitator 1 Transportation authority 1 Car manufacturer 1 Car safety expert 1 Software Architect 1 Project Manager	1 Requirements Engineer - Facilitator 1 Transportation authority 1 Car manufacturer 1 Car safety expert 1 Software Architect 1 Project Manager

Table 3 Distribution of Participants in Two Teams

The two teams will gather in two separate discussion rooms to carry out the workshop. The team workshop includes the workshop kick-off stage, followed by the three phases - *the dreamer*, *the realist* and *the critic*, with breaks in between to allow participants to take mental breaks and switch out of the previous role.

Materials: In each of the discussion rooms, the teams will be provided with materials as listed below in Table 4.

Materials	**Rationale**
- 1 Whiteboard - 5 Sheets of A0 paper (841 x 1189 mm)	- Large canvas for participants to display ideas visible to entire group
- 3 Stacks of Coloured Sticky Notes (Pink, Yellow, Green)	- Versatile note taking or penning down individual ideas - Can be rearranged on larger surface
- 3 Sets of Whiteboard Markers (Red, Blue, Green, Black) - 6 Black Pens - 6 Pencils	- Variety of writing materials to jot down ideas - Different colours to categorize or highlight concepts
- 5 Toy Cars	- Visualisation of cooperative lane merging scenarios
- 20 Magnets	- Clip A0 paper on whiteboard
- 1 Clock	- Keep brainstorming session focused to encourage spontaneity

Table 4 Materials Provided for Each Team

Refreshment Break

Duration: 30 mins

Light refreshment provided for all participant – coffee, tea and light snacks.

Participants should move to the respective rooms for their respective teams as in Table 3 above.

3. Workshop Kick-off

Duration: 30 mins

Within the allocated time, teams should pen down possible cooperative lane merging situations involving three cars.

The facilitator in each group starts the session off by introducing the tools and getting the teams active with the clock and toy cars. If the teams are stuck, facilitators may prompt the teams with the following scenario:

- Three cars lane merging in snowy conditions
- Three cars lane merging in rainy conditions
- Three cars lane merging in heavy traffic
- Emergency vehicle behind merging car
- Object on road in front of merging car
- One of the cars in lane merging scenario is not equipped

Result: Written list of cooperative lane merging scenarios involving three cars.

Break

Duration: 15 mins

Participants to take the time to immerse into the dreamer role.

4. The Dreamer

Duration: 60 mins

Goal: Brainstorming of high-level solutions.

In this phase, participants are required to come up with solutions to the cooperative lane merging scenarios that were gathered in the session earlier. They take on *The Dreamer* role where they think out of the box and let their ideas run wild.

To inspire participants, a short 4 minutes video, in Figure 2, titled *Waymo's Approach to Building a Safe Waymo Driver* would be shown to participants at the start of the session. This video is chosen as an inspirational video as Waymo is the world's first fully driverless car that is operational in various major cities in United States of America.

Figure 2 Inspirational Video of Waymo Autonomous Driving Car

Facilitators should encourage the thinking "Nothing is impossible, and nothing is too crazy". Facilitators to note that teams should spread their time evenly between scenarios.

Result: Written texts or sketches of innovative solutions on lane merging scenarios.

Lunch Break

Duration: 60 mins

Lunch for all participants.

Towards the end of lunch break, participants to take the time to immerse into the realist role.

5. The Realist

Duration: 60 mins

Goal: Building on previous solutions

In the second phase, participants are required to review the solutions to the cooperative lane merging scenarios that were gathered in the session earlier. They take on *The Realist* role where they make sense of ideas from the previous phase. The useful and reasonable solutions are retained, and more details are added to ensure the ideas are practical.

To encourage participants, a short 2 minutes video, in Figure 3, titled *Active Lange Guiding | BMW Driver's Guide* would be shown to participants. This video is chosen as it is a realistic representation of the considerations to be taken into account during a vehicle lane change. The video clearly outlines the process of the lane changing whilst highlighting the use of appropriate technologies.

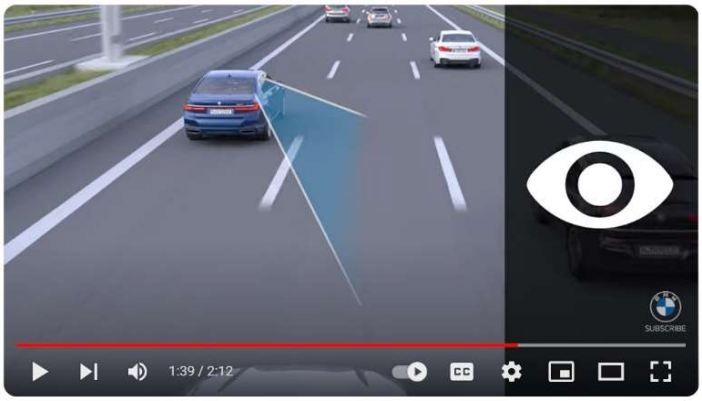

Figure 3 Thought-Provoking Video of BMW Lane Guiding Capability

Facilitators should urge the participants to take on a “How do we make this work” attitude. Facilitators to note that teams should spread their time evenly between scenarios.

Result: Written texts or sketches built on the previous solutions.

Break

Duration: 15 mins

Participants to take the time to immerse into the critic role.

6. The Critic

Duration: 60 mins

Goal: Review the previous solutions and raise safety concerns

In this phase, participants are required to analyse the scenarios that were gathered in the earlier sessions and raise concerns regarding the feasibility, soundness and safety of the proposed ideas. They take on *The Critic* role where they think analytically and look out for blind spots that may not have been considered before, with emphasis on safety.

To stimulate reflective thinking in the participants, the video, in Figure 4, titled *Why self-driving cars have stalled | It's Complicated* is shown to participants. This video is chosen as it prompts the spectators about complications in the realm of autonomous cars as well as it raises awareness on the safety concerns regarding self-driving cars.

Figure 4 Video on Problems with Self-Driving Cars to Stimulate Critical Thinking

Whenever the discussion digresses too much going into to solutioning or too narrowly into a single problem the facilitator will remind the group to maintain the focus of the session and to discuss multiple criticalities.

Result: Written texts or sketches emphasizing safety concerns.

Coffee Break

Duration: 20 mins

Coffee and Tea provided for all participants.

Participants to take the time to clear their mind.

7. Debrief

Duration: 60 mins (Per team: 20 mins presentation + 10 mins questions)

Both teams gather back in seminar room where they present their discussions and findings.

Workshop Outcome:

Requirements Engineers obtain preliminary findings from the workshop to have a high-level understanding of the possible scenarios of cooperative lane merging manoeuvre and the safety considerations involved. The materials produced will need to be reviewed to sieve out the salient points to be addressed in more details.

Task 3: Requirements Specification

Analysis

To derive the functional requirements for the cooperative lane merging manoeuvre, an analysis is conducted focusing on the safety, reliability and availability as well as security of the system.

1. Safety Analysis

As the cooperative lane merging manoeuvre involves humans and with lives at stake, safety is critical and of top priority. As such, an in-depth analysis of the safety of the system is conducted.

The safety analysis involves a three-step approach where hazard and accident are first analysed. The same list of hazards is subsequently analysed based on the probability and severity, deriving the overall risk. Finally, the possible root causes of a vehicle crash are analysed using a safety-fault tree.

1.1 Hazard-Accident Analysis

In terms of safety, only hazards that result in single or multiple vehicle crashes during cooperative lane merging manoeuvre are analysed in Table 5.

Component	**Hazard**	**Accident**
Vehicle	Punctured tyre (Mechanical failure)	Vehicle crash
Vehicle	Proximity sensor malfunction (Electrical failure)	Vehicle crash
Vehicle	Global Positioning System (GPS) sensor malfunction (Electrical failure)	Vehicle crash
Vehicle	Loss of connection (Network failure)	Vehicle crash
External	Obstacle in lane (Physical hazard)	Vehicle crash
5G Antenna	Multi vehicle loss of connection (Network failure)	Multi vehicles crash
5G Antenna	System overload (Service failure)	Multi vehicles crash
Edge Server	Cyber security attack (Service failure)	Multi vehicles crash
Edge Server	System overload (Service failure)	Multi vehicles crash
Edge Server	Human error (Service failure) (Ehtesham, 2022)	Multi vehicles crash

Table 5 Hazard-Accident Analysis

1.2 Safety Risk Analysis

With the hazards identified in Table 5, the risk of the resulting accident is then derived based on the probability of the hazard and severity of the accident. Risk can range from acceptable to ALARP (as low as reasonably practical) to intolerable. The analysis can be found in Table 6 below.

Hazard	**Probability**	**Severity**	**Risk**
Punctured tyre	Low	Medium	ALARP
Proximity sensor malfunction	Low	Medium	ALARP
GPS sensor malfunction	Low	High	Intolerable
Loss of connection	High	Medium	Intolerable
Obstacle in lane	Medium	Medium	ALARP
Multi vehicle loss of connection	Medium	High	Intolerable
5G antenna system overload	Low	High	Intolerable
Edge server cyber security attack	High	High	Intolerable
Edge server system overload	Medium	High	Intolerable
Human error in edge server configuration	Medium	High	Intolerable

Table 6 Safety Risk Analysis

From the analysis above, all hazards identified may lead to an accident with risk level of ALARP or higher. This is due to the fact that vehicle crash, with lives at stake, is never acceptable.

The hazards with intolerable risks should be handled with immediate priority and greater focus in the functional requirements in the subsequent sections. The hazard involving edge server cyber security attack will be further analysed in the security analysis.

Punctured tyre, obstacle in lane and proximity sensor malfunction are considered ALARP as they are hazards that involve a single vehicle. In order to ensure that risk level associated with proximity sensor malfunction does not increase, there should be mitigation in place to handle it in the functional requirements.

1.3 Safety-Fault Tree

As the ultimate goal of the safety requirement is to ensure that the vehicle does not crash, a safety-fault tree in Figure 5 is used to analyse the potential root causes of a vehicle crash.

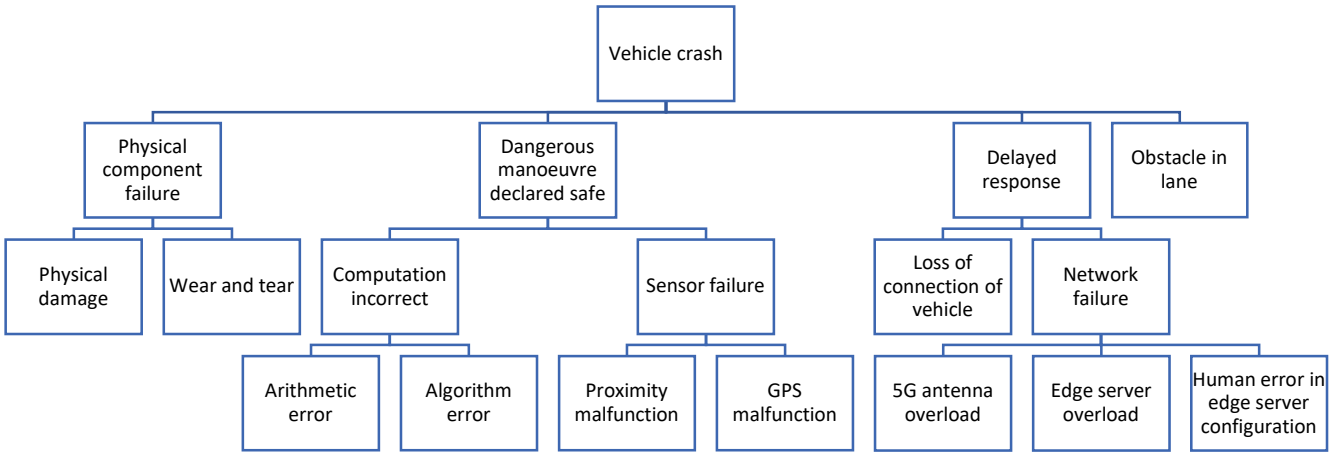

Figure 5 Safety-Fault Tree

In this project, the physical component is assumed to be independent from the system requirements.

The chosen focus would be on the root causes from sensor failure, network failure and loss of connection. These faults are congruent with the hazards identified in Table 6 above. As such, the functional requirements of the system would be targeted at these root causes.

2. Reliability and Availability Analysis

In autonomous vehicles partaking in cooperative lane merging manoeuvre, the reliability and availability of components of the vehicles and infrastructures are key in ensuring the merge is carried out safely. The analysis of system reliability and availability are conducted using the fault-failure analysis and dependability mapping.

2.1 Fault-Failure Analysis

In this analysis, the components in vehicles, 5G antenna and servers are identified in Table 7, together with possible faults and associated failures.

Component	**Fault**	**Failure**
Vehicle communication device	No signal	No connectivity
Vehicle proximity sensor	Broken	Missing or incorrect data
Vehicle GPS sensor	Not calibrated	Incorrect position
5G antenna connection to servers	Congested	Intermittent connection
5G antenna connection to vehicles	Interrupted	Loss of connection
Edge server compute unit	Hardware defect	Unable to process requests
Edge server network unit	Human error in configuration	Loss of connection
Lane merging application	Computation defect	Incorrect instructions

Table 7 Fault-Failure Analysis

2.2 Dependability Mapping

From Table 7, the more critical components are extracted and further analysed in Table 8 below.

The metrics considered are as follows:

- $AVAIL = 1 - \frac{downtime}{uptime}$
- $Probability\ Of\ Failure\ On\ Demand\ (POFOD) = \frac{number\ of\ failures}{number\ of\ requests}$
- $Rate\ Of\ Occurrence\ Of\ Failures\ (ROCOF) = \frac{number\ of\ failures}{total\ time\ of\ operation}$
- $Mean\ Time\ To\ Failure\ (MTTF) = \frac{total\ operation\ time}{number\ of\ failures} = \frac{1}{ROCOF}$

Component	**Dependability Concern**	**Metric**	**Value**
Vehicle communication device	Availability	AVAIL	0.9999
Vehicle communication device	Reliability	ROCOF	1 failure in 360 milliseconds
Vehicle proximity sensor	Reliability	ROCOF	1 failure in 1.8 seconds (0.5556)
Vehicle GPS sensor	Reliability	ROCOF	1 failure in 1.8 seconds (0.5556)
5G antenna	Availability	AVAIL	0.99999
Edge server compute unit	Availability	AVAIL	0.99999

Table 8 Dependability Mapping

The components with availability concerns use the AVAIL metric to determine the acceptable downtime of the component.

In order for vehicle communication device to be dependable, various values are considered using a three-hours travel journey. With 0.999, the component would be down for 10.8 seconds in 3 hours. With 0.9999, downtime would be 1.08 seconds in 3 hours. In this critical system, it is concluded that

downtime of 1.08 seconds in 3 hours would be acceptable while 10.8 seconds would not be acceptable.

The 5G antenna and edge server compute unit are given 0.99999 with downtime of 5.256 minutes a year. Since both the 5G antenna and edge server are centralized components, they handle large amount of traffic and would require higher availability as compared to a single vehicle. In addition, according to Amazon Web Services (AWS) cloud provider, the accepted availability standard for emergency response systems is 0.99999 or “five nines”. (Reynolds, 2020)

The rationale of using the corresponding metrics and values for reliability is detailed below with the following assumptions:

- Consider vehicle driving at a speed of 200km/h
- 100m safety distance is taken to achieve conservative calculations
- 1.8 seconds to travel 100m
- Self-driving cars take 0.5 seconds to react (Yuen, 2021)
- Consider decelerating to stop takes 1 second
- Remaining time of 0.3 seconds will be considered for the components below

1. For reliability of vehicle communication device, ROCOF is chosen since the device typically has frequent and short interactions. The calculations are as follows:
    - 1 request every 20ms
    - 15 possible requests in 0.3 seconds of remaining time
    - Not more than 5 failure is acceptable in 1.8 seconds
    - Therefore, 1 failure in 360 milliseconds
2. For reliability of vehicle GPS sensor, ROCOF is chosen since the GPS coordinates of vehicles are constantly and always immediately required. The calculations are as follows:
    - Given that the vehicle GPS refreshes every 0.1 second
    - In 0.3 seconds of remaining time, not more than 1 failure in GPS within 1.8 seconds is acceptable

3. Security Analysis

Due to the nature of the cooperative lane merging manoeuvre, communication between vehicles as well as communication from vehicles to the servers are carried out via the internet. With the system hosted on the internet, it is vulnerable to external threats and attacks. A successful attack on the system may lead to an impact on the confidentiality, integrity and availability of the data, thereby, rendering the system unsafe. Since security is a pre-requisite to system safety, reliability and availability, it is also indispensable.

3.1 Security Threat Analysis

The security risk analysis in Table 9 starts first by analysing the assets to be protected, followed by the possible exposure of the assets, in terms of confidentiality, integrity and availability. The corresponding threats, vulnerabilities and attacks are identified. Lastly, potential controls are suggested.

Asset	**Exposure**	**Threat**	**Vulnerability**	**Attack**	**Control**
Vehicle operational data	Data fabrication (Integrity)	Intruder fabrication	No proper replay attack identification	Packet replay attack	Timestamping
Vehicle operational data	Data loss (Integrity)	Intruder deletion	No proper access control	Unauthorised user accesses database	Authentication
Vehicle operational data	Data interception (Confidentiality)	Intruder interception	No proper network security	Network attack	Network access control rules
Historical data	Data loss (Integrity)	Accidental deletion	No proper backup	Accidental	Access control
Server response data	Data manipulation (Integrity)	Intruder modification	No encryption of data in transit	Packet spoofing and manipulation	Encryption
Edge server connectivity	Service unavailable (Availability)	Service interruption	No firewall	Distributed denial of service (DDoS)	Firewalls

Table 9 Security Threat Analysis

3.2 Security Risk Analysis

From the table above, the assets and exposures are further analysed, determining the asset value and threat probability. The risk level is then derived in Table 10.

Asset and exposure	**Asset value**	**Threat probability**	**Risk level**
Vehicle operational data fabrication (Integrity)	High	Medium	High
Vehicle operational data loss (Integrity)	High	Medium	High
Vehicle operational data interception (Confidentiality)	High	Medium	Medium
Historical data loss (Integrity)	Low	Medium	Low
Server response data manipulation (Integrity)	High	High	High
Edge server connectivity unavailable (Availability)	High	High	High

Table 10 Security Risk Analysis

In the above analysis, exposure in integrity and availability are more critical in terms of safety risks. Confidentiality breach does not directly lead to a safety risk.

In terms of the type of data, operational and current data is more critical that historical data. Operational data include speed and position of vehicles, which are required to be precise and accurate for the safety of cooperative lane merging manoeuvre.

With cost and time in consideration, only exposures with high risk levels are considered for the functional requirements.

Functional Requirements

Based on the analysis above, the functional requirements are obtained as below.

1. Offline Vehicle Operation Mode

Requirement	The vehicle shall implement offline operation mode during a loss of connection.
Description	When the vehicle is not connected to the network, the vehicle needs to continue operating in a safe manner.
State	The vehicle is not connected to the network.
Action	If the system recognize that it is not connected to the network, the vehicle should switch to an offline operation mode. When the vehicle is in the offline operation mode, it shall not attempt to effectuate centralized cooperative lane merging manoeuvre with the coordination from the edge cloud system. It should rely on localized communication with other vehicles (if available) or local vehicles sensor data.
Inputs	Lack of connection signal, vehicle sensor data, information exchanged locally with other vehicles.
Outputs	The vehicle switches to offline operation mode and if lane merging is required, it relies on localized cooperative lane merging manoeuvre.
Rationale	During travel journey, interruptions in the network connectivity are expected. According to the safety risk analysis in Table 6, accidents due to a loss of network connection are considered an intolerable safety risk. It is of paramount importance that the vehicle system operates safely even when it is not connected to the network.

Table 11 Offline Vehicle Operation Mode Functional Requirement

2. GPS Sensor Self-Monitoring Architecture in Vehicles

Requirement	Vehicles shall have GPS Sensor Self-Monitoring Architecture.
Description	GPS Sensor installed in the vehicles shall be built with a self-monitoring architecture. Two independent GPS sensors shall be installed and the software system shall compare the measurements from both sensors in order to detect faults. The accuracy of a single GPS sensor shall be within 3 meters. (Watts, 2023) A larger inaccuracy in measurement of vehicle position could lead to inaccurate manoeuvre, posing as a safety risk.
State	Vehicle is in operation.
Action	If one of the sensors stops producing data, the driver shall be alerted immediately with a critical alert. Meanwhile, the vehicle can continue operating using the data from the remaining sensor. If the output between the two sensors differs by more than 6 meters, the GPS sensor is considered faulty. The conductor shall be alerted, and the vehicle should stop as soon as safely possible for sensor recalibration.
Inputs	Position readings from the two GPS sensors.
Outputs	Alert indication when the sensor is faulty. Vehicle position when sensors are operating correctly.
Rationale	As identified in the fault tree analysis in Figure 5, a possible root cause of vehicle crash is the malfunction of the GPS sensor. The GPS sensor provides the position information that is required for the cooperative lane merging manoeuvre. With the self-monitoring architecture, the GPS sensor can provide better reliability, hence, higher level of safety of the vehicle.

Table 12 GPS Sensor Self-Monitoring Architecture Functional Requirement

3. Prioritize and Distribute Communication for 5G Antenna

Requirement	The 5G antenna system shall prioritize and distribute communication.
Description	The 5G antenna picks up communication traffic from 5G accessible vehicles within its vicinity. The 5G antenna system shall have a load balancer to implement dynamic load balancing for even traffic distribution. The 5G antenna system shall prioritize critical services during peak demand to maintain optimal system performance.
State	5G antenna system is operating.
Action	The 5G antenna system shall prioritize communications with emergency vehicles, followed by vehicles partaking in cooperative lane merging manoeuvre and lastly the vehicles that do not require communications with other vehicles.
Inputs	Network traffic data.
Outputs	Efficient load distribution and prioritized communication.
Rationale	According to safety analysis in Table 5 and Table 6, although there is a low probability of an overload to the 5G antenna system, the risk resulting from this hazard is intolerable. Since it may affect multiple vehicles closely located in the same geographic area, a multi vehicle crash may happen. As such, it has been analysed in Table 8 that the availability of this centralized system should be 0.99999.

Table 13 5G Antenna System Overload Functional Requirement

4. Edge Server Auto-scaling Capabilities

Requirement	The edge server shall have auto-scaling capabilities.
Description	In the scenario where there is a sudden surge in network communication, the edge server must be able to handle the network traffic. This can be done by automatically adding new servers by scaling out or increasing the size of the servers by scaling up.
State	Massive surge in network traffic to edge server.
Action	Edge server shall scale up or out to prevent overload.
Inputs	New capability limit.
Outputs	Scaled up or scaled out servers.
Rationale	During periods of heavy traffic on the road, the edge server may experience surge in network traffic. According to safety analysis in Table 6 and Figure 5, an overload in the edge server is a potential root cause to an intolerable multi vehicle crash. Furthermore, in the availability analysis in Table 8, the edge server is required to have an availability of 0.99999. To prevent an overload in the network requests and subsequently causing the server to go down, it should have the capability to handle the higher network traffic when required. On the other hand, during periods of slow network traffic, the edge server should also be able to reduce capability as needed.

Table 14 Edge Server Auto-Scaling Functional Requirement

5. Edge Server Redundancy

Requirement	Edge server shall have redundant architecture.
Description	When an edge server is down, due to server failure or natural disasters, there shall be redundant backup servers to ensure continuous availability, fault tolerance and reliability. There shall be at least three separate physical edge servers running the same operations to take over one another in case of server failure. The three edge servers shall be stored in three different datacentres.
State	Operational: High availability during edge server operations.

Action	During an edge server failure, the system shall integrate automatic failover and load balancing to distribute traffic seamlessly to active and standby edge servers.
Inputs	System architecture details and overload detection mechanisms.
Outputs	Traffic directed to active edge servers.
Rationale	In the analysis in Table 8, the edge server shall have an availability of 0.99999. In order to enhance the availability and resilience of the edge server, redundant architecture with fault tolerance is required.

Table 15 Edge Server Redundancy Functional Requirement

6. Automated Deployments on Edge Server

Requirement	The system shall have automated deployments on edge server.
Description	The system, in an actively maintained and monitored state, shall implement automated processes to maintain a state of high reliability and operational efficiency, minimizing the occurrence and impact of human errors in operational tasks. Automated deployment pipelines for software updates and system configurations shall be developed and integrated. Version control systems should be utilized to track and manage systematic changes.
State	A new version of the system needs to be deployed on the edge server.
Action	After the new version has been approved for the deployment, and the deployment process is started, the new version is deployed on the edge server without the need for further human intervention.
Inputs	Approved version change.
Outputs	The new version is deployed on the edge server.
Rationale	In the safety analysis in Table 6, human error in configuration is a potential hazard that might lead to an intolerable multi vehicle crash in the scenario where it causes network failure. With the introduction of automated deployment of the edge server, processes will minimize human errors and enhance system reliability, thereby increasing system safety.

Table 16 Automated Deployment on Edge Server Functional Requirement

7. Firewall Protection

Requirement	The cloud systems shall implement firewall protection.
Description	The system shall be equipped with robust firewall protection, specifically designed to detect, mitigate and prevent Distributed Denial of Service (DDoS) attacks. An incident response plan shall be agreed upon and reviewed by the cybersecurity team.
State	Cloud system is in operation.
Action	Request rate limiting and IP blacklisting measures are enforced to limit the impact of a DDoS attack.
Inputs	DDoS attack is detected.
Outputs	Impact of the DDoS attack is reduced.
Rationale	As identified in the security threat analysis in Table 9, DDoS pose a threat to the availability of the cloud server. Unavailability of the cloud server is a safety concern that could lead to multi vehicle crash, as identified in the safety analysis in Table 5. To safeguard the system from DDoS attacks, proactive and adaptive firewall measures are chosen to minimise the impact of such types of attack.

Table 17 Firewall Protection Functional Requirement

8. Database Authentication

Requirement	The database systems shall enforce authentication measures.
Description	The system must enforce robust authentication measures for database access as well as ensuring secure and authorized interactions with the database. In particular, different access policies for historical and operational data shall be put in practice to respond to the different security needs of the two. Different database user groups shall be configured according to the principle of least privilege, to prevent undesired access and modifications and minimise the attack surface.
State	Database system is in operation.
Action	User authentication is required to access the database.
Inputs	Password policies and database user account audit procedures.
Outputs	Enhanced database security, protection against unauthorized access and compliance with security best practices.
Rationale	As identified in the security threat analysis in Table 9, integrity and availability of the operational data is a key part in ensuring the safety of operations. To reduce the vulnerability surface of the operational data, strict database access control measure is chosen. The measure mitigates the risk of deliberate or accidental security threats.

Table 18 Database Authentication Functional Requirement

9. Server-Vehicle Communication Data Encryption

Requirement	Communication between the server and vehicles shall have data encryption.
Description	Data transmitted between the cloud system and the vehicle shall be transmitted in an encrypted form. Since the vehicle transmit and receives data over the wireless network, the communication with the server is susceptible to man in the middle attacks. In order to prevent malicious attackers from intercepting and altering the data packets exchanged, usage of encryption is required. Encryption algorithms shall be chosen according to modern industry standards and reviewed by the cyber security team.
State	Vehicle is transmitting data to cloud server or requesting coordination for cooperative lane merging manoeuvre.
Action	Data exchange should happen in an encrypted form.
Inputs	Information to be transmitted and encryption keys.
Outputs	Encrypted data packets.
Rationale	As identified in the security risk analysis in Table 10, the integrity of the data must be protected to ensure the safety of the system. Accidental or deliberate alterations of the vehicle data pose as a risk to the safety of manoeuvre.

Table 19 Server-Vehicle Communication Data Encryption Functional Requirement

10. Timestamping of Communication Packets

Requirement	System shall timestamp all communication packets.
Description	Every data packet exchanged between vehicles and cloud server shall include timestamp information. Upon receiving a new data packet, each system shall discard packets that are older than a given threshold. Timestamps shall be included with a resolution of at least a millisecond. The threshold for considering packet invalid should be computed considering a possible discrepancy between vehicle and cloud system clock as well as the maximum expected round trip time of the packets.

	The system clock of the vehicle shall periodically synchronise with the cloud system using standard clock synchronization protocols. To ensure safety of the system, we assume a maximum difference between vehicle and cloud system time of 150ms and packet round trip time of 20ms. Therefore, both systems shall discard packets that are older than 170ms.
State	Vehicle and cloud system are communicating.
Action	Packets from both parties shall include a timestamp information. If a component receives a packet that is older than 170ms, it shall be regarded as invalid and not be processed.
Inputs	Timestamp included on data packet.
Outputs	On receiver side: decision whether to process or discard the data packet based on timestamp.
Rationale	As identified in the security risk analysis in Table 10, the communication between vehicles and edge servers, even if encrypted, is susceptible to replay attacks. Malicious attackers could intercept and replay valid data packets and simulate the presence of vehicles in fictitious locations, affecting the safety of the overall system. Timestamping is chosen as control measure to protect the system integrity.

Table 20 Timestamping of Communication Packets Functional Requirement

References

Ehtesham, H. (2022, June 21). *Top 7 Major Causes of IT Downtime*. Retrieved from Externetworks: https://www.extnoc.com/blog/top-7-major-causes-of-it-downtime/

Reynolds, R. (2020, Mar 17). *Achieving "five nines" in the cloud for justice and public safety*. Retrieved from AWS Blog: https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/

Watts, J. (2023, Apr 21). *How Accurate is Vehicle Tracking Using GPS? – 2023 Guide*. Retrieved from Expert Market: https://www.expertmarket.com/uk/vehicle-tracking/accurate-gps-tracking

Yuen, D. (2021, Jan 30). *Can You React Faster than a Self-Driving Car on 5G Networks?* Retrieved from Medium: https://medium.com/predict/making-roads-safer-with-self-driving-cars-and-5g-c1e28526362c