Analysis of Safety and Security in Autonomous Vehicle Intersections

Márton Novák[1], Balázs Varga[1], Tamás Ormándi[1]

***Abstract*— Fully autonomous intersections, where traffic lights are not needed, are a long-term goal in urban traffic planning. In these types of intersections, the priority rules and the order in which vehicles can cross the intersection are determined by wireless communication. Eliminating the human factor can lead to fewer incidents; however, to achieve this, the system must operate perfectly. In the case of autonomous intersections, communication between vehicles and infrastructure must be flawless, as must the execution of the desired maneuvers (for example, avoiding emergency situations). The aim of this research is to analyze autonomous vehicles, intersections, control methods, and how failures in different components of the specified infrastructure can lead to safety and security issues. Firstly, it is necessary to categorize the different types and elements of autonomous intersections and control methods. This includes analyzing the concepts and components of centralized and decentralized intersections, the components of self-driving vehicles, communication protocols, and the topics of safety, security, and cybersecurity in autonomous systems. Potential failures are identified using the Failure Mode and Effect Analysis (FMEA) method, which categorizes and evaluates the impact of different failures in the intersection system. This analysis provides an overview of potential failures and pinpoints components that pose the highest risk. In addition, this paper conducts a simulation-based analysis to assess the severity of some critical failures. Providing comprehensive solutions to such failures is beyond the scope of this work.**

I. INTRODUCTION

Autonomous vehicles and connected traffic control could reduce the number of accidents and improve road safety and security in certain critical locations, such as intersections [1]–[3]. However, to ensure safety and security, autonomous systems must be reliable. For this reason, the safety analysis of autonomous intersections is a crucial task. The aim of this research is to identify which components have the most significant impact from a safety perspective.

This research is particularly important in the area of autonomous system safety and security because, to our knowledge, no prior studies in the literature have analyzed a complex infrastructure like an intersection by breaking it down into its components. We conducted an FMEA analysis to address this research gap.

Autonomous intersections are highly complex systems in which not only autonomous vehicles communicate with each other, but, in the case of centralized systems, the intersection is also equipped with intelligent infrastructure elements, such as Roadside Units (RSUs), which utilize Vehicle-to-Infrastructure (V2I) communication [4], [5].

[1]Department of Control for Transportation and Vehicle Systems, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics, H-1111 Budapest, Műegyetem rkp. 3, Hungary novakmarton@edu.bme.hu, varga.balazs@kjk.bme.hu, ormandi.tamas@bme.hu

In this research, the contributions are summarized as follows:

- We analyzed the possible failures of different components in autonomous intersections.
- We conducted an FMEA on the components of RSUs, autonomous vehicles, and other external factors.
- Potential failure modes, effects of failure, causes of failure, recommended actions, possible preventions, and risk factors were identified for each component.
- The FMEA was validated for certain scenarios through simulations in the Veins open-source framework [6] for vehicular network simulations.

This paper is organized as follows: Section II presents the types of autonomous intersections, communication protocols, and the safety and security features of such systems. Section III discusses the components of autonomous intersections and vehicles. Section IV introduces the FMEA for autonomous intersections. Section V describes the validation of the FMEA using the Veins framework. Finally, Section VI concludes the paper.

II. AUTONOMOUS INTERSECTIONS

Intersections are among the most dangerous elements of transportation because they are locations where vehicles cross paths. The likelihood of collisions is much higher at intersections than at other points in the infrastructure. In autonomous transportation, communication between a vehicle's On-Board Unit (OBU) and RSU is crucial. If communication functions perfectly, human errors could be eliminated, reducing accidents and improving the safety and efficiency of traffic flow. On the other hand, wireless communication between autonomous systems poses safety and security risks [7], [8]. This research focuses on simple four-way intersections; however, more realistic and complex scenarios, involving not only cars but also vulnerable road users, could lead to additional challenges. The proposed method is generalizable, as the devices used remain consistent across intersections, with only the environment or the number of lanes varying.

A. Centralized intersections

Centralized intersections may include a central traffic control device that communicates through an RSU, or the RSU itself may run a control algorithm, implementing traffic control using a single piece of hardware [9]–[12].

B. Decentralized intersections

In decentralized autonomous intersections, there is no need for a central device to determine the order because

vehicles approaching the intersection can communicate with one another, and priorities are negotiated based on predefined control logic. This approach reduces costs and complexity; however, it may face greater challenges, particularly in standardizing the negotiation algorithm across different Original equipment manufacturers (OEMs) [13].

C. Communication in autonomous intersections

The most crucial task in centralized intersections is communication between the RSU and vehicles. Various communication technologies have emerged over the years to ensure safe data exchange. To prevent accidents, communication speed, bandwidth, data transfer capability, coverage, and reliability are essential. However, communication networks can also serve as platforms for harmful interventions, such as cyberattacks. Therefore, they must be resilient against cyberattacks [2], [14].

In autonomous intersections, communication is carried out over dedicated networks [15]. The technologies used may include Dedicated short-range communications (DSRC) or Cellular V2X (C-V2X) communication. The protocols implemented in each country may vary [16], [17]. While communication standards may vary regionally, these differences have a negligible impact on safety and reliability.

D. Security and cybersecurity in autonomous systems

Recently, the automotive industry has been experiencing significant changes, driven by the rapid development of electronics, mechatronics, and smart devices, which are increasingly being integrated into vehicles. In addition to traditional vehicles, autonomous vehicles have been introduced. These systems could enhance safety and security; however, they may also be more vulnerable to harmful interventions [18], [19].

Safety Integrity Levels (SIL) [20] serve as a baseline for autonomous safety systems. Each level defines the degree of risk. The higher the integrity level, the greater the impact and the higher the probability of failure. SIL are depicted in Fig. 1.

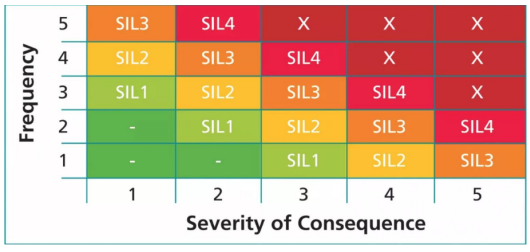

Fig. 1. SIL Levels [20]

Cybersecurity protects systems from detrimental actions, data leaks, and unauthorized network access. In the context of autonomous intersections, manipulation of either self-driving vehicles or the RSU's software could lead to serious accidents [21], [22]. To ensure safe operation, autonomous systems must be equipped with robust cybersecurity measures.

III. COMPONENTS OF CENTRALIZED AUTONOMOUS INTERSECTIONS

To properly assess safety and security in autonomous intersections, it is crucial to break down the system into smaller subsystems and components (see Fig. 2). Then, using FMEA, the potential consequences of a component malfunction are analyzed. This analysis helps identify critical components in the system and determine where redundancies or fallback mechanisms are needed.

This analysis is conducted at the system level, meaning that both the components of autonomous vehicles and the intersection are assessed.

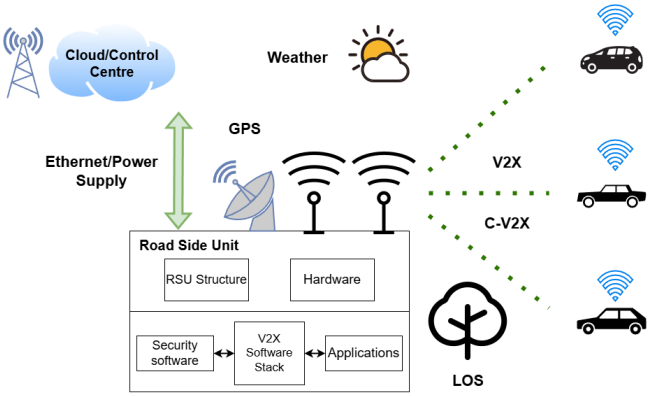

Fig. 2. Components of autonomous intersections

A. Autonomous vehicle components

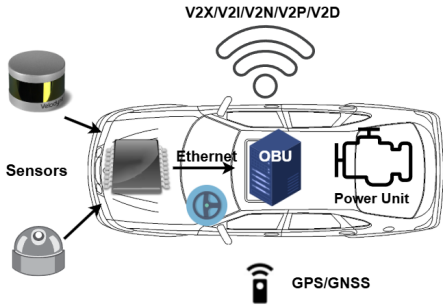

Fig. 3. Components of autonomous vehicles

To ensure the safety of transportation, self-driving vehicles must be equipped with systems that can accurately perceive their surroundings. Perception systems primarily consist of five subsystems (see Fig. 3): Light Detection And Ranging (LiDAR), RAdio Detection And Ranging (radar), cameras, ultrasonic sensors, and a positioning system. These systems help the vehicle maintain its desired trajectory and reduce the likelihood of accidents [23], [24]. Beyond perception, self-driving cars, like traditional vehicles, have drivetrain, steering, and braking systems, along with corresponding sensors (e.g., speed sensors), actuators (e.g., steering servo motors), and control systems such as Electronic Stability Program (ESP) and Anti-lock Braking System (ABS) , which are most likely integrated into a central self-driving Electronic Control

Unit (ECU). These systems must remain secure to ensure proper vehicle motion.

Most importantly, autonomous vehicles have an OBU. This system includes both hardware and software components for communication, can store data, and has access to wired and wireless networks. When a self-driving vehicle approaches an intersection, the OBU can send and receive messages from the intersection's RSU.

B. RSU, Intersection components

The main component of autonomous intersections is the RSU [25]–[27]. An RSU is a stationary communication device typically installed along roads or at intersections. It facilitates wireless communication between vehicles (Vehicle-to-Vehicle (V2V)), infrastructure (V2I), and other network components. The RSU also has a built-in positioning system that can calculate the speed and distance of approaching vehicles. Its security system protects the intersection from cyberattacks and other threats. Traffic lights may still be present in centralized intersections; however, they are not necessarily required, as alternative solutions can be used instead.

Road markings play an important role in perception, and the road surface should be considered in the context of physical failures. Additionally, the geographical location of the intersection can be a significant factor, as a flat, deserted area may differ from an urban environment in its effects on perception and communication. Intersections may also be equipped with surveillance cameras, which can be used for external observation and monitoring.

C. External factors as components

The Line of Sight (LOS) phenomenon can cause problems due to infrastructure characteristics or other factors, as the communication channel may be blocked, leading to dangerous situations. Lastly, weather also plays a role in our analysis, as it can contribute to failures or accidents either directly (e.g., slippery roads) or indirectly by accelerating the wear and tear of components.

IV. FAILURE MODE AND EFFECT ANALYSIS (FMEA)

A. FMEA method

We used the FMEA method [28]–[30] to analyze the impacts of component failures in an autonomous centralized intersection. This method focuses on identifying potential failure modes and causes while also proposing mitigation and prevention strategies. The aim of this research is to identify possible failures, pinpoint the most critical ones, and propose preliminary solutions. A comprehensive resolution of all potential issues is beyond the scope of this paper. This study employs the FMEA method due to its capability to analyze the system at the component level. This approach is advantageous in identifying potential weak points during the design of autonomous intersections. The proposed method offers valuable insights as early as the planning phase.

The main element of the FMEA method is a structured table in which failures, their causes, consequences, prevention and mitigation strategies, and risk factors are identified. The risk factor (R) is calculated based on three values: probability (P), severity (S), and detectability (D). Each value is classified on a scale of 1 to 3. These values are derived from theoretical analysis, as there are no statistical data or precise probabilities available for each component. Therefore, validation is necessary.

From the risk factors for each component, a theoretical conclusion can be drawn and validated through simulations. It is important to note that the FMEA method analyzes only single failures at a time and does not consider cases where multiple failures occur simultaneously [22].

B. Possible failures of RSU components

The RSU can be broken down into the following components (Table I):

- Physical structure
- Ethernet communication
- Power supply
- Antennas
- Positioning system (Global Navigation Satellite System (GNSS))
- Security hardware and software
- V2X communication module

The physical structure may be damaged due to cracking, corrosion, or fire incidents, which can result from weather conditions, temperature changes, or collisions. Damage to the structure can lead to failures in other internal components. Physical damage can be prevented with protective casings, stronger structural materials, and cooling-heating systems. Ethernet connects the RSU to the network and typically provides power through Power over Ethernet (PoE). One of the main failures is cable rupture, which can cause power outages. Cable failures can be prevented by using durable cable materials and proper system design. A power supply failure can lead to the loss of other critical components and may be caused by physical damage, fire, or grid outages. This issue can be mitigated with a backup battery system. Antennas may break off due to extreme weather conditions or collisions. Most RSUs have multiple antennas, allowing another antenna to take over the functions of a damaged one. The positioning system may fail due to power blackouts, coverage issues, or physical damage. It is crucial for the RSU to determine the exact positions of approaching vehicles to establish the order of crossing [31]. Optical distance-measuring sensors can be installed to mitigate GNSS failures.

The security system plays a critical role in preventing attackers from manipulating broadcasted messages or data. Additionally, the physical components should be protected against mechanical failures and vandalism.

C. Possible failures of autonomous vehicle components

Autonomous vehicles consist of various components, each posing potential failure risks (see Table II). The components assessed are:

- V2X communication modules
- Perception system
- Positioning system
- Power unit, brake system and steering
- ECUs
- Antennas
- Safety system
- Wired and wireless connection

Several factors can lead to communication failures. Antennas may break off for the same reasons as those on the RSU, or unwanted shielding may occur. Without the ability to communicate, vehicles would be unable to cross the intersection, as right-of-way instructions could not be received, nor could acknowledgments be transmitted. Such failures must be mitigated through fallback mechanisms, such as intervention by the vehicle user.

Failures in the drive, brake, and steering systems are primarily due to mechanical or electrical issues. These failures can alter the vehicle's trajectory, potentially causing accidents. Therefore, maintenance and fault detection are crucial.

Cybersecurity in self-driving vehicles is also critical. Data must not be manipulated, as harmful interventions could cause vehicles to deviate from their planned trajectories or send false information to the RSU, leading to serious accidents [32].

D. Possible failures due to external factors

In addition to the RSU and vehicles, other external factors can also be considered components, as listed in Table III. In these cases, no intersection components fail; however, external factors can disrupt traffic flow. For example, infrastructure failures - such as road damage, intended or unintended closures, or severe weather conditions - can negatively impact traffic. Additionally, congestion can be an issue if the intersection is unable to handle the volume of incoming vehicles [33].

V. VALIDATION OF FMEA ANALYSIS IN VEINS SIMULATOR

A. V2X simulation environment with Veins and OMNeT++

During the FMEA, numerous components were analyzed for possible failures, and risk values were determined, leading to a theoretical conclusion. However, since these results are only theoretical, it is essential to validate them in a simulated environment. For this task, three key scenarios were identified and analyzed through simulation.

The chosen simulation framework is based on the co-simulation of the traffic simulator Simulation of Urban MObility (SUMO) [34] and the event-based communication network simulator OMNeT++ [35], orchestrated by Veins [36], [37]. Communication is defined via the Traffic Control Interface (TraCI).

For this research, a symmetric, four legged intersection without predefined priority rules was modeled in SUMO for analysis. Each leg of the intersection was 100 meters long. There were no traffic lights; only the RSU determined the order of crossing. Each vehicle could proceed to any edge.

B. Analyzed scenarios

This section presents the three simulated scenarios. In each scenario, the RSU is positioned at the center of the intersection and is responsible for determining the order of crossing. This is managed by an algorithm that grants permission to cross to the closest approaching vehicle. The next vehicle can only receive permission once the previous vehicle has left the intersection. Messages are exchanged between the RSU and the vehicle's OBU using the WAVE Short Message (WSM) [38] format. These scenarios primarily focus on communication-based simulations and serve as general models for analyzing different failure types and operational modes within autonomous communication methodologies.

1) Scenario 1: RSU failure: In the first scenario, the failure of the RSU was analyzed. In this case, the RSU fails at a random time. After the failure, it can no longer send or receive messages. As a result, approaching vehicles are unable to obtain permission to cross the intersection. This leads to traffic congestion, with lane occupancy continuously increasing, as shown in Fig. 4.

To handle this failure, the theoretical FMEA suggested that the intersection should revert to a mode where it no longer functions autonomously. It is advantageous for approaching vehicles to know in advance whether the intersection contains an RSU. If the intersection has an RSU but vehicles are unable to communicate with it, the system should fall back to decentralized mode or default to a basic priority-to-the-right rule. This approach helps manage traffic congestion and allows vehicles to continue their journey.

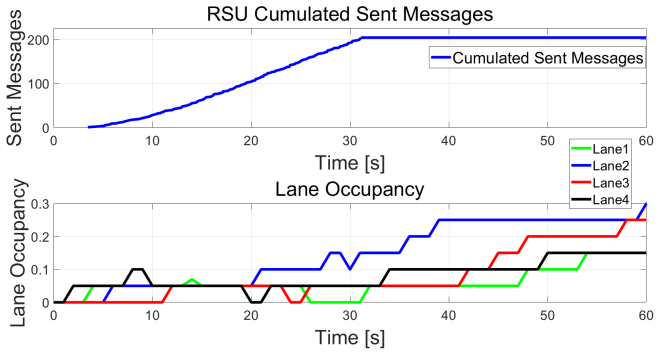

Fig. 4. Transmitted messages and lane occupancy in the event of an RSU failure

2) Scenario 2: Failure of autonomous vehicle communication: In the second scenario, the communication module of a randomly chosen vehicle fails, meaning the vehicle cannot receive messages from the RSU. Since the vehicle closest to the intersection is authorized to pass, when the vehicle with the failure approaches, it does not receive the message. This leads to congestion, and as shown in Fig. 5, lane occupancy increases.

This scenario could be managed by a watchdog timer, which monitors whether any vehicle has crossed the inter-

section. If the timer expires, permission could be granted to the next vehicle. Another option is to close the lane where the faulty vehicle is located while keeping the other lanes open.

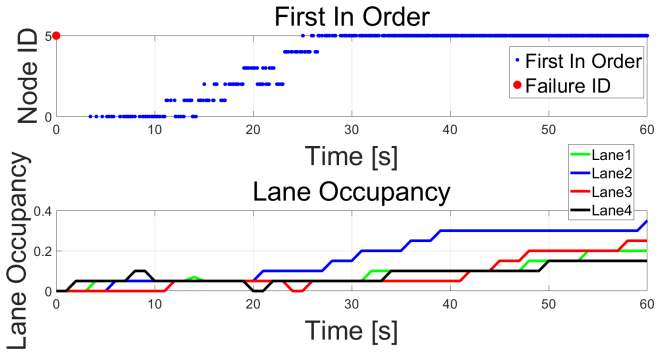

Fig. 5. Permitted vehicle ID and lane occupancy in the event of a vehicle communication module failure

3) Scenario 3: Failure of the GNSS module: In the third scenario, a randomly chosen vehicle's GNSS module sends incorrect values to the RSU. In this case, the lateral coordinate was offset by 40 meters. This incorrect value caused the RSU to perceive the vehicle as being closer to the intersection than it actually was. As a result, the RSU granted permission earlier than the vehicle's actual arrival at the intersection.

The algorithm includes a point-of-no-return function to prevent vehicles from stopping just before entering the intersection after they have already been approved. In the analyzed scenario, the faulty vehicle was already in the conflict zone when the RSU granted permission to a different vehicle, as shown in Fig. 6.

This case is particularly dangerous from a cybersecurity perspective, as the coordinates and transmitted messages could be manipulated. To mitigate this issue, the system could be extended with additional sensors to gather distance data for redundancy. An algorithm could also compare the transmitted and measured coordinates. If the two values differ significantly, the RSU should withhold permission to cross.

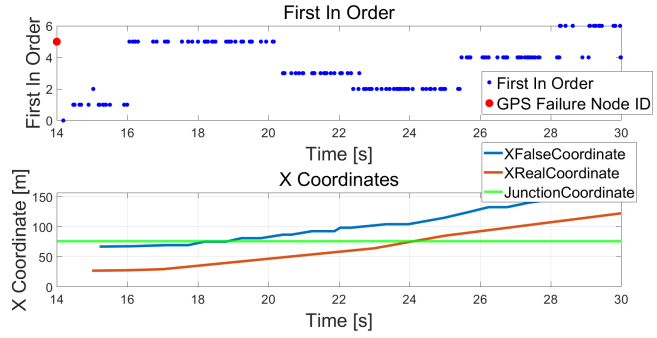

Fig. 6. Permitted vehicle ID, false and original X coordinates in the event of GNSS malfunction

VI. CONCLUSIONS

In this research, we demonstrated the use of the FMEA method to assess the safety and security of autonomous intersections, particularly four-way centralized intersections with autonomous vehicles. This method provided a comprehensive overview of the components and their significance. Theoretically, we identified the most critical components and areas. However, since many values were only theoretical, validation was necessary. We validated certain component results using the Veins framework.

In conclusion, communication between autonomous systems is crucial for safety and security. The primary goal is to maximize the SIL. Without proper communication, the intersection loses its autonomous functionality. Robust cybersecurity systems are essential to prevent harmful manipulation. For communication devices, a reliable power supply and durable physical design are critical. Additionally, proper monitoring and maintenance are essential. The FMEA method has certain limitations: it focuses solely on single failures and modes, and does not account for simultaneous failures across multiple components. However, the likelihood of multiple failures occurring simultaneously is relatively low. One advantage of FMEA is its ability to provide a more detailed analysis by examining each component individually. In contrast, methods such as Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) may overlook several failure modes associated with specific components. As future work, the intersection could be analyzed using the Systems-Theoretic Accident Model and Process (STAMP) method [39], which views the system as a hierarchy of control structures rather than just a collection of individual components.

ACKNOWLEDGEMENT

The research was supported by the European Union within the framework of the National Laboratory for Autonomous Systems (RRF-2.3.1-21-2022-00002).

REFERENCES

[1] D. Kurt, "AIM: Autonomous Intersection Management," *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2008)*, p. 2, 2008.

[2] A. C. Regan and R. Chen, "Vehicular ad hoc networks," in *Vehicular Communications and Networks*, pp. 29–35, Elsevier, 2015.

[3] C. Yaibok, P. Suwanno, T. Pornbunyanon, C. Kanjanakul, P. Luathep, and A. Fukuda, "Improving urban intersection safety insights from simulation analysis," vol. 48, no. 4, pp. 523–536.

[4] H. Pei, J. Zhang, Y. Zhang, X. Pei, S. Feng, and L. Li, "Fault-Tolerant Cooperative Driving at Signal-Free Intersections," *IEEE Transactions on Intelligent Vehicles*, vol. 8, pp. 121–134, Jan. 2023.

[5] D. Kurt and S. Peter, "Mitigating Catastrophic Failure at Intersections of Autonomous Vehicles," *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems*, p. 4, 2008.

[6] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 3–15, January 2011.

[7] J. J. Haas and Y.-C. Hu, "Communication requirements for crash avoidance," in *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, (Chicago Illinois USA), pp. 1–10, ACM, Sept. 2010.

Component	Pot. Failure Mode	Potential Causes	Potential Failure Effect	Possible prevention	Action Recomm.	P	S	D	R
Physical structure	Physical damage, rupture, corrosion.	Harsh weather, physical contact.	RSU failure: switch to decentralized mode.	Strong materials, protection, cooling system.	Physical repair.	3	2	1	6
Ethernet	Ethernet cable rupture.	Extreme weather, physical contact.	Losing connection to central system.	Strong cable usage, proper casing.	Phisycal repair.	2	2	2	8
Wired connection to the grid	Central blackouts, error on the supplier's side.	Extreme weather, cable rupture.	RSU failure may cause malfunction in vehicle communication.	Wider coverage area.	Designing systems that are capable of visual signals.	2	2	2	8
Power Supply	Power supply unit failure, physical contact.	Blackouts, overheating, impact damage, fire, cable rupture.	RSU failure: switch to decentralized mode, vehicles self-coordinate crossing.	Battery system, cooling system.	Hiring physical repair specialists for emergency scenarios.	3	3	1	9
Antennas	Damage, breaking down, shielding.	Extreme weather, collisions, external shielding.	Signal loss, all antennas down: decentralized mode.	Stronger physical structure, more antennas.	Working antennas take over tasks.	1	2	1	2
GNSS	Hardware failure, power outings, false positioning.	Satellite failure, shielding, damage, extreme weather.	Order determined by message order.	Wider coverage area, stronger mechanical structure.	Distance measuring unit built in to the RSU.	1	1	2	2
Security hardware	Power outings, electronical, mechanical failure.	Physical damage, loss of power supply for components.	Unprotected components may cause RSU failure.	Stronger physical structure, protection.	Switch to safety mode.	2	2	1	4
Security software	Disabling the security software for software attack.	Unauthorized interference, cyberattack, hacking.	The order and permissions may be manipulated.	Cybersecurity based approach in software developement.	Switch to safety mode.	2	3	2	12
Emergency alert unit	False or no emergency messages.	Power outings, Denial-of-Service (DOS), cyberattack.	RSU detects an emergency situation, traffic stops	Software development for correct detection.	Restart from an external location.	1	2	2	4
V2X Communication	Physical failure, communication loss, shielding, signal loss.	Power outages, extreme weather, shielding, rupture, new buildings.	Switching to decentralized mode.	Stronger structure, communication failure detection feature.	Removing or detecting of shielding objects in the intersection.	2	3	2	12

TABLE I

RISK FACTORS OF THE RSU

Component	Potential Failure Mode	Potential Causes	Pot. Failure Effect	Potential Prevention	Action Recomm.	P	S	D	R
V2X Communication	Shielding, antenna rupture, loss of communication.	Extreme weather, accident, material fatigue.	Signal loss, user intervention required.	Installing more communication components for redundancy.	Control should be given to the user.	2	3	2	12
Perception modules	LiDAR, radar, camera failure, false perception	Physical damage, blind spots, damaged lens, shielding.	Perception and positioning via GNSS, RSU, and vehicle collaboration.	More sensors to prevent blind spots and failures.	Detection of hard-to-see objects, module development.	1	1	2	2
GNSS	False positioning, loss of position data.	Blackout, satellite loss, mechanical damage.	Vehicles continue routes via RSU communication.	More sensors, wider coverage area.	Requesting location data from the RSU.	1	1	2	2
Power Unit	Failure of the components of the Power Unit.	Engine failure, fuel loss, battery issue, throttle malfunction.	Vehicle stops in conflict zone: sends message to RSU, stopping traffic flow.	Hybrid vehicles, no permission below certain fuel level, maintenance.	In an emergency, the vehicle sends its status to infrastructure.	2	3	1	6
Brake System	Failure of the brakes.	Brake pedal failure, pressure loss, disc failure.	The vehicle leaves its trajectory, the flow of traffic stops for safety reasons.	Maintenance, installing sensors for monitoring the brake system.	Emergency case: sending messages to RSU and other vehicles.	2	3	1	6
Steering System	Steering system, servo failure.	Incident, puncture, servo engine failure, axle break.	Leaving trajectory. During emergency, information given to the RSU, traffic stops.	More sensors to monitor the steering system, proper maintenance.	Emergency case: the vehicle sends message to the RSU and other vehicles.	2	3	1	6
ECU	Physical damage, power outings.	Contact, accident, ruptures, blackouts.	Component malfunction, user intervention.	Proper maintenance, optimalization.	User invention and control.	3	3	1	9
Antennas	Rupture of antennas, shielding.	Extreme weather, accident, physical contact, shielding.	Signal loss, all antennas down: switch to perception	Maintenance, stronger structural materials for antennas.	Working antennas take over tasks.	2	2	1	4
Security System	False functioning.	Cyberattack, physical damage to the hardware.	Cyberattack may manipulate vehicle behavior: accidents.	Software developement.	Switching to safety mode in case of a detected cyberattack.	2	3	2	12
Wireless comm.	Loss of communication, shielding.	Blackouts, physical damage, loss of signal	Communication loss, user intervention.	System which detects communication failure.	Visual signals, vehicle user intervention.	2	2	2	8
Ethernet	Ethernet cable rupture.	Electronic failure, overheating, blackouts.	Usage of controller area network (CAN).	Strong cable materials, proper protection.	Alternative communication modules.	1	2	1	2

TABLE II

RISK FACTORS OF THE VEHICLE

Component	Pot. Failure Mode	Potential Causes	Potential Failure Effect	Potential Prevention	Action Recomm.	P	S	D	R
Infrastructure	The intersection becomes unusable.	Road blockage, accident, physical damage, extreme weather conditions	The traffic stops at the intersection.	Proper maintenance and monitoring of the road.	Fixing of the road fault or other failures,	2	2	1	4
Congestion	Intersection and the RSU is congested.	Increased traffic, more interest in the area, tourism	Crossing efficiency decrease, lane occupancy increase.	Changing intersection type, increasing the number of lanes	The RSU or the OBU navigates the vehicles to another route.	2	2	1	4

TABLE III

RISK FACTORS OF EXTERNAL COMPONENTS

[8] M. Choi, A. Rubenecia, and H. H. Choi, "Reservation-based Autonomous Intersection Management Considering Vehicle Failures in the Intersection," in *2020 International Conference on Information Networking (ICOIN)*, (Barcelona, Spain), pp. 654–659, IEEE, Jan. 2020.

[9] M. Pourmehrab, L. Elefteriadou, and S. Ranka, "Smart intersection control algorithms for automated vehicles," in *2017 Tenth International Conference on Contemporary Computing (IC3)*, pp. 1–6. ISSN: 2572-6129.

[10] R. Zhao, K. Wang, Y. Li, Y. Fan, F. Gao, and Z. Gao, "Centralized cooperative control for autonomous vehicles at unsignalized all-directional intersections: A multi-agent projection-based constrained policy optimization approach," vol. 267, p. 126153.

[11] Y. Kong and Y. Ma, "Connected and automated vehicles: A cooperative eco-driving strategy for heterogeneous vehicle platoon among multiple signalized intersections," *IFAC-PapersOnLine*, vol. 58, no. 29, pp. 272–277, 2024. 7th IFAC Conference on Engine and Powertrain Control, Simulation and Modeling E-COSM 2024.

[12] L. Chai, X. Liu, W. ShangGuan, J. Wang, and B. Cai, "Parallel spatiotemporal slot-based heterogeneous vehicle hybrid coordinating method at intersections under intelligent network environment," *Physica A: Statistical Mechanics and its Applications*, vol. 628, p. 129126, 2023.

[13] F. Hart, M. Saraoglu, A. Morozov, and K. Janschek, "Fail-safe Priority-based Approach for Autonomous Intersection Management," *IFAC-PapersOnLine*, vol. 52, no. 8, pp. 233–238, 2019.

[14] C. Wietfeld and C. Ide, "Vehicle-to-infrastructure communications," in *Vehicular Communications and Networks*, pp. 3–28, Elsevier, 2015.

[15] H. Guan, Q. Bai, and Q. Meng, "A decentralized signal-free intersection control framework for connected and autonomous vehicles," pp. 1–1.

[16] A. Chekkouri, A. Ezzouhairi, and S. Pierre, "Connected vehicles in an intelligent transport system," in *Vehicular Communications and Networks*, pp. 193–221, Elsevier, 2015.

[17] H. J. Lak, A. Gholamhosseinian, and J. Seitz, "Distributed Vehicular Communication Protocols for Autonomous Intersection Management," *Procedia Computer Science*, vol. 201, pp. 150–157, 2022.

[18] S. Kim and R. Shrestha, "Introduction to Automotive Cybersecurity," in *Automotive Cyber Security*, pp. 1–13, Singapore: Springer Singapore, 2020.

[19] W. Wu, S. Chen, M. Xiong, and L. Xing, "Enhancing intersection safety in autonomous traffic: A grid-based approach with risk quantification," vol. 200, p. 107559.

[20] G. Automation and F. Solutions, "Beginner's guide to sil levels," 2019. Accessed: 2025-01-25.

[21] S. Hecker, D. Dai, and L. Van Gool, "Failure Prediction for Autonomous Driving," May 2018. arXiv:1805.01811 [cs].

[22] L. Langer, A. Bonitz, C. Schmittner, and S. Ruehrup, "Automated Right of Way for Emergency Vehicles in C-ITS: An Analysis of Cyber-Security Risks," in *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops* (A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, and P. Ferreira, eds.), vol. 12235, pp. 148–160, Cham: Springer International Publishing, 2020. Series Title: Lecture Notes in Computer Science.

[23] Bényei, G. Vida, K. Pintér, Z. Szalay, and G. Ágoston, "Evaluation of Highway-pilot Function Based on FMEA Safety Analysis," *Periodica Polytechnica Transportation Engineering*, vol. 48, pp. 253–259, Sept. 2019.

[24] A. Mihály, V. T. Vu, T. T. Do, K. D. Thinh, N. V. Vinh, and P. Gáspár, "Linear parameter varying and reinforcement learning approaches for trajectory tracking controller of autonomous vehicles," *Periodica Polytechnica Transportation Engineering*, vol. 53, no. 1, p. 94–102, 2025.

[25] B. Aslam, F. Amjad, and C. C. Zou, "Optimal roadside units placement in urban areas for vehicular networks," in *2012 IEEE Symposium on Computers and Communications (ISCC)*, pp. 000423–000429, 2012.

[26] J. Barrachina, P. Garrido, M. Fogue, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Road Side Unit Deployment: A Density-Based Approach," *IEEE Intelligent Transportation Systems Magazine*, vol. 5, no. 3, pp. 30–39, 2013.

[27] A. Guerna, S. Bitam, and C. T. Calafate, "Roadside Unit Deployment in Internet of Vehicles Systems: A Survey," *Sensors*, vol. 22, p. 3190, Jan. 2022. Number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

[28] D. S. Kapil and S. Shobhit, "Failure Mode and Effect Analysis (FMEA) Implementation: A Literature Review," *Journal of Advance Research in Aeronautics and Space Science*, vol. 5, no. 1,2, pp. 1–17, 2018.

[29] J. Yang, M. Ward, and J. Akhtar, "The Development of Safety Cases for an Autonomous Vehicle: A Comparative Study on Different Methods," pp. 2017–01–2010, Sept. 2017.

[30] A. Segismundo and P. Augusto Cauchick Miguel, "Failure mode and effects analysis (FMEA) in the context of risk management in new product development: A case study in an automotive company," *International Journal of Quality & Reliability Management*, vol. 25, pp. 899–912, Oct. 2008.

[31] A. A. Hassan and H. A. Rakha, "A Fully-Distributed Heuristic Algorithm for Control of Autonomous Vehicle Movements at Isolated Intersections," *International Journal of Transportation Science and Technology*, vol. 3, pp. 297–309, Dec. 2014.

[32] C. L. González, J. L. Zapotecatl, C. Gershenson, J. M. Alberola, and V. Julian, "A robustness approach to the distributed management of traffic intersections," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 4501–4512, Nov. 2020.

[33] E. Steinmetz, R. Hult, G. R. De Campos, M. Wildemeersch, P. Falcone, and H. Wymeersch, "Communication analysis for centralized intersection crossing coordination," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, (Barcelona, Spain), pp. 813–818, IEEE, Aug. 2014.

[34] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *The 21st IEEE International Conference on Intelligent Transportation Systems*, IEEE, 2018.

[35] A. Varga, "OMNeT++," in *Modeling and tools for network simulation*, pp. 35–59, Springer, 2010.

[36] C. Sommer and F. Dressler, "Veins: The open source vehicular network simulation framework," 2011. Accessed: 2025-01-25.

[37] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 3–15, January 2011.

[38] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Networking Services," 2016.

[39] Y. Zhang, C. Dong, W. Guo, J. Dai, and Z. Zhao, "Systems theoretic accident model and process (STAMP): A literature review," vol. 152, p. 105596.