vehicles

MDPI

Article

Strengthening Automotive Cybersecurity: A Comparative Analysis of ISO/SAE 21434-Compliant Automatic Collision Notification (ACN) Systems

Biagio Boi [1,†], Tarush Gupta [2,†], Marcelo Rinhel [3,†], Iuliana Jubea [4,†], Rahamatullah Khondoker [2,*], Christian Esposito [1] and Bruno Miguel Sousa [3]

[1] Department of Computer Science, University of Salerno, 84084 Fisciano, Italy; bboi@unisa.it (B.B.); esposito@unisa.it (C.E.)
[2] Department of Business Informatics, Faculty of Mathematics, Natural Science & Data Processing (MND), THM University of Applied Sciences, 61169 Friedberg, Germany; tarush.gupta@iem.thm.de
[3] Departamento de Engenharia Informática, University of Coimbra, Pinhal de Marrocos, 3030-290 Coimbra, Portugal; mfrinhel@student.dei.uc.pt (M.R.); bmsousa@dei.uc.pt (B.M.S.)
[4] Faculty of Automation and Computer Science, Politehnica University of Timișoara, 300223 Timisoara, Romania; iuliana.jubea@student.upt.ro
* Correspondence: rahamatullah.khondoker@mnd.thm.de
† These authors contributed equally to this work.

Abstract: The increasing usage of autonomous and automatic systems within the automotive industry is steering us towards a more interconnected world. This enhanced interconnectivity fosters a more streamlined driving experience, reduces costs, and provides timely driver assistance. The electric/electronic (EE) architectures of modern vehicles are inherently complex due to the multitude of components they encompass. Contemporary architectures reveal that these components converge at an electronic control unit (ECU) called the central gateway, which could potentially represent a single point of failure. While this central unit is typically adequately safeguarded, the same cannot be said for the connected components, which often remain vulnerable to cyber threats. The ISO/SAE 21434 standard paved the way for automotive cybersecurity and could be used in parallel with other standards such as ISO 26262 and ISO PAS 21488. automatic collision notification (ACN) is one of the most typical systems in a vehicle, and limited effort has been dedicated to identifying the most suitable architecture for this feature. This paper addresses the existing security and privacy gap of this feature by conducting a comparative analysis of security threats in two distinct ACN architectures. Notably, despite ACN architectures exhibiting inherent similarities, the primary distinction between the two architectures lies in their strategies for crash estimation and detection, followed by subsequent communication with emergency response teams. A rigorous security assessment was conducted using the ISO/SAE 21434 standard, employing the TARA and STRIDE methodologies through the Ansys medini analyze software. This analysis identified an average of 310 threats per architecture, including a significant number of high-level threats (11.8% and 15%, respectively), highlighting the importance of a comprehensive evaluation.

Keywords: automatic crash notification; internet of vehicles; ISO/SAE 21434; TARA

Citation: Boi, B.; Gupta, T.; Rinhel, M.; Jubea, I.; Khondoker, R.; Esposito, C.; Sousa, B.M. Strengthening Automotive Cybersecurity: A Comparative Analysis of ISO/SAE 21434-Compliant Automatic Collision Notification (ACN) Systems. *Vehicles* **2023**, *5*, 1760–1802. https://doi.org/10.3390/vehicles5040096

Academic Editor: Lihui Zhao

Received: 2 October 2023
Revised: 26 November 2023
Accepted: 1 December 2023
Published: 4 December 2023

1. Introduction

Smart Cities are integrating functionality like real-time vehicle management, anti-theft systems, and traffic management [1], which can reduce traffic congestion and improve the driving experience. For example, it is workable to optimize traffic flow, reduce congestion, and improve private and public transportation services by evaluating real-time data from sensors and cameras installed in strategic locations. Furthermore, smart cities can catalyze citizen empowerment and improve the engagement of public administrations with their citizens by delivering individualized services.

In recent years, the automotive industry has begun to examine sensors for enabling smart features within vehicles. Such integration paves the door for a more connected and safe driving experience. These functionalities leverage a myriad of sensors that are distributed in the city and in the cars enabling real-time collaboration thanks to emerging technologies like 5G, NB-IoT, WiFi, or long range (LoRa). This new era of smart communication evolved from classical internet of things (IoT), composed of a few devices, to a more complex system named internet of vehicles (IoV). Starting from 2019, many manufacturers have released cars equipped with smart systems. Considering the heterogeneous components currently existing, it is possible to distinguish five major approaches [2] to vehicle communication and connectivity: vehicle-to-vehicle (V2V), where vehicles communicate among each other; vehicle-to-infrastructure (V2I), characterized by vehicles that send and receive data from external gateways; vehicle-to-cloud (V2C), where vehicles directly send data to cloud services; vehicle-to-pedestrian (V2P), where vehicles communicate with the surrounding environment, such as pedestrians; and vehicle-to-everything (V2X), which can be a combination of the previously defined systems.

Among these systems, the most relevant ones are those related to the ACN systems, which, by leveraging many sensors and reliable communication, are able to save human lives. Road systems are becoming more congested due to the increasing number of cars that transit through them, potentially leading to crashes. The number of injuries from car crashes has increased over the last few years, as reported by Scanlon et al. [3], where traffic intersections are the most critical point. ACN systems have the ability to provide earlier notification of a vehicle crash enabling a faster and precise emergency response service (ERS) response by sending a notification with the crash location identification. Such systems are able to increase the probability of survival; as shown by Spicer et al. [4], advanced driver assistance system (ADAS) (a complementary system for ACN) are able to reduce crashes by 14%.

Many standards have been proposed by the International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE) to assess the quality and security of cars produced. Among them, ISO/SAE 21434 [5] attempts to redefine and give the original equipment manufacturer (OEM) and suppliers a complete standard for security and quality checks regarding cybersecurity. Costantino et al. [6] compared this new standard with the existing ones, highlighting the correlation with the others; showing the completeness of ISO/SAE 21434, which includes all the other protocols in a compact form. In particular, sections like information sharing and impact analysis are in common with ISO 26262-2 [7] making this new standard more complete.

The authors investigate the security and privacy of ACN systems in light of the growing complexity of embedded systems within cars. As previously said, these systems are the most important and need appropriate security. All the elements of a typical ACN will be taken into account as part of an analysis conducted following the ISO/SAE 21434 standardization. To better comprehend the components and their interactions, two architectures will be specifically contrasted. The analysis will adhere to the protocol exactly. The key contributions of the current paper are listed below:

1. **Comprehensive analysis of ACN architecture components**: We provide a detailed analysis of the fundamental components of a typical ACN architecture, elucidating the role and functionality of each device. This analysis provides a clear understanding of the ACN system's operation and the interdependencies between its components.
2. **Security evaluation of ACN architectures using ISO/SAE 21434**: We employ ISO/SAE 21434, a cybersecurity standard designed for automotive systems, to conduct a comprehensive security assessment of ACN architectures. This structured approach categorizes threats based on their severity and identifies potential vulnerabilities that could be exploited.
3. **In-depth analysis and countermeasures for high-risk ACN threats**: We explore the root causes and possible impacts of high-risk threats to ACN systems, enabling the

development of effective countermeasures. This detailed examination strengthens the security posture of ACN systems by mitigating the most critical threats.

To establish a clear and coherent manuscript, the document is structured into nine distinct sections:

- The second section delves into related work analogous to the current paper within the context of ACN and threat analysis in the automotive domain.
- The third section introduces the research methodology employed, highlighting the objective of the present work and the research question it seeks to address.
- The fourth section provides an overview of the features essential for the realization of a typical ACN architecture, accompanied by an analysis of selected architectures.
- The fifth section elaborates on the TARA methodology utilized for the security evaluation of the considered architectures.
- The sixth section presents a comparative analysis of the considered system architectures.
- The seventh section meticulously outlines a comprehensive threat analysis of both systems.
- The eighth section aims to engage in a discussion on potential security enhancements to the architectures under consideration. The impetus for this discussion stems from the necessity of providing a practical and tangible response to the threats identified in the seventh section.
- The ninth section concludes the research findings.

2. Related Work

Security requirements for a typical vehicle system can be summarized by the following properties: authenticity, availability, data integrity, and confidentiality [8]. These properties are able to enhance security while guaranteeing a high level of privacy, but unfortunately, they are not always taken into consideration with the same relevance. On one side, the European Commission (2009) discussed data protection considerations and suggested that positioning systems should remain inactive until an emergency incident occurs where vehicle tracking is prohibited [9]; however, the same cannot be said for non-European countries. In certain US advanced automatic collision notification (AACN) systems, the vehicle location and speed history are recorded before a crash. However, the extent to which this information can adversely affect drivers remains uncertain, leaving room for multiple interpretations. Although few studies have been conducted on the security analysis of ACN systems using the introduced protocol, the authors attempt to identify the primary security analysis methodologies used in other works within the automotive context in order to gather existing methodologies, architectures, and results.

2.1. Secure ACN Systems

Primary studies have investigated various aspects of general automotive systems, communication protocols, data encryption methods, and vulnerability assessments. Threat assessment is not limited to the network but also to the vehicle itself [8]; some given examples of authenticity attacks are the Sybil attack, falsified entity attack, replication attack, Global Navigation Satellite System (GNSS) spoofing and injection attack, and timing attack. The system investigated in [10] shows the existence of multiple components within a simple ACN system: a secure-access server that requires login credentials, and a mobile application running on the terminals. The server processes the gathered data and notifies the authorities with designated emergency contacts, while the application interacts with the user. Bonyar et al. [11] highlights the usage of event data recorder (EDR) for cybersecurity event reconstruction. As a general overview, the study provides an examination of the sensors integrated within emergency call (eCall) systems, including crash detection sensors, positional and velocity data systems, and communication methodologies. Additionally, the paper conducts a comparative analysis of existing eCall device solutions, considering factors such as their degree of autonomy, technical implementation, and the range of services they offer. A method for testing the security of vehicles based on threat modeling was proposed in [12]. In particular, it is performed manually by cybersecurity experts, and

the attack trees are created in a specific format. The penetration tests developed by the authors were based on the attack trees, with the primary goal of assessing the security of the system. These tests were designed to comprehensively check the vulnerabilities and potential weaknesses within the system. As part of this evaluation, each attack scenario was assigned both a privacy severity rating and an operational severity rating. These ratings served as quantitative measures to assess the potential impact and consequences of the identified attacks on both the privacy of the system's users and the operational integrity of the system itself. The authors of [13] introduced a highly effective security system tailored for mobile vehicles through the use of an short message service (SMS) alert system. This system stands out due to its integration of a microcontroller, setting it apart from other comparable systems. The components employed in this proposed approach are intricately linked with accident detection, storage of contact numbers, and SMS transmission. The safeguarding of vehicles revolves around the identification of accidents, executed by a vibration sensor. The notification of this detection is conveyed through SMS alerts to mobile devices via Global System for Mobile Communications (GSM). The enclosed embedded system, comprising these components, finds its place within the vehicle, serving as an accident detection mechanism. A study in this domain was conducted by the authors of [14]. They designed a system to analyze audio streams to detect road accidents. The underlying hypothesis posits that sound can be deconstructed into atomic audio units, much like words in a text. The appearance of specific audio units, termed "audio words", within a given time frame serves as a distinguishing factor for identifying specific sounds. Injury risk assessment is one of the major risks when considering the ACN system; an extensive analysis was conducted in [15], the studies goal was to assess the severity of crashes by utilizing information collected before the crash occurred. Additionally, the study aimed to uncover the underlying mechanism of impact response (IR) using appropriate interpretation techniques. The impulse–momentum theory was employed to introduce innovative mathematical formulations for several indicators of crash severity. These indicators encompassed metrics such as a change in velocity (delta V), energy equivalent speed (EES), crash momentum index (CMI), and crash severity index (CSI). A comprehensive dataset comprising 24,082 samples at the vehicle level was amalgamated, and six distinct IR models employed, each rooted in a different machine learning approach. The results of these predictive models highlighted that the indicators gathered before the crash (referred to as previous (pre)-crash indicators or pre-crash indicators (PCIs)) exerted more influence compared to the commonly used fundamental crash data. Remarkably, the integration of the PCIs led to an average accuracy enhancement of 14.35% across the six models.

2.2. Security Standard

A thorough examination of numerous articles on comparable systems reveals a noticeable absence of discussions or evaluations of ACN security according to standardization. While the literature offers a diverse range of approaches, the importance of standardization cannot be overlooked during system analysis. The ISO 26262 was one of the first standardization protocols within the automotive context. The document contains guidelines regarding the functional security of a vehicle intended for component malfunctions, which can cause damage to things or people [16]. Despite the fact that this protocol provides a relevant framework for assessing the reliability of components within an automotive system, the main focus does not take into account multiple external factors, which can lead to failure [17]. A more recent protocol is defined in ISO PAS 21448 [18], which is currently used for evaluating the safety of intended functionality (SOTIF), and this is usually combined with the previously described ISO 26262. A particularly relevant combination of these two protocols can be found within the context of automated [19,20] and autonomous [21,22] driving. This combination can give a complete overview and assess the complete security of both components and functionalities related to such components. As reported in Table 1, there are slight differences between ISO PAS 21448 and ISO 26262,

which can be considered as complementary to each other. Even though such synergistic protocols can assess the security of the entire system, these protocols do not consider the external environment.

Table 1. Key differences between ISO 26262, ISO PAS 21448, and ISO/SAE 21434.

Feature	ISO 26262	ISO PAS 21448	ISO/SAE 21434
Objective	Functional safety	Safety of intended functionality (SOTIF)	Cybersecurity
Application	All electrical and electronic systems in vehicles	Vehicle road systems requiring a SOTIF assessment	Electrical and electronic systems in vehicles connected to a network or the internet
Process	Development and verification of electrical and electronic systems	SOTIF management	Cybersecurity management
Phases	Hazard identification and assessment, control definition and implementation, verification and validation	Hazard identification and assessment, control definition and implementation	Risk identification and assessment, control definition and implementation, verification and validation
Results	Electrical and electronic systems in vehicles are designed and built to minimize the risk of malfunctions that could cause harm to people or properties	Vehicle road systems requiring a SOTIF assessment are designed and built to minimize the risk of malfunctions that could cause harm to people or properties due to reasonably foreseeable use by people	Electrical and electronic systems in vehicles connected to a network or the internet are designed and built to minimize the risk of cyberattacks

As is widely known, the environment plays a relevant role in attack modeling, and the entire cyber–physical system must be considered for a reliable threat assessment. The ISO/SAE 21434 was released with the goal of establishing standards for designing a secure system within the automotive context able to standardize the minimal security and privacy criteria [6]. A recent study [23] applied the ISO/SAE 21434 to a generic E/E architecture. This work attempted to mitigate the gap in the literature by creating a comparative image of the E/E architectures on a generalized level, highlighting the importance of ECUs in all possible automotive systems.

According to the analysis conducted in [23], the authors of the current paper want to assess security in a more detailed system, highlighting the potential of this protocol even for smaller systems. Given the sensitive nature of the data and the potential impact on individuals' safety and privacy, ensuring the cybersecurity of ACN systems is paramount. ACN systems collect and send data such as the location of the crash, driver information, and potentially health details. These data must be protected from unauthorized access, interception, or disclosure to maintain individuals' privacy.

3. Research Methodology

Considering the importance of ACN and its progressive adoption, many studies have proposed different approaches and architectures in the literature. Despite this huge number of studies, only a few exhibit a reliable structure and related security analysis, as discussed in Section 2, leaving room for myriad threats and vulnerabilities that can, in the worst case, cause a decrease in survival probability [4].

Meticulous work has been performed to determine the most appropriate research questions by taking into consideration ISO/SAE 21434. Motivations for the architecture selection are given in the following subsections, considering a huge number of features related to both communication and data analysis technologies put in place by the analyzed works.

3.1. Research Questions

In this subsection, research questions (RQs) are defined. Recalling that the aim of our work is to understand the main components used in typical ACN systems and to assess the security of these architectures, three questions have been formulated.

- **RQ1**: Which are the components used for creating a typical ACN system?
- **RQ2**: Which are the typical communication means used in the ACN system for connecting components?
- **RQ3**: Which are the external services used in the ACN system?

On the one hand, it seems that ACN systems involve only a few components; on the other hand, the possible combination makes room for a large number of threats. The authors of this paper strongly believe that the automotive industry is an incremental field where more systems are included in new vehicles.

3.2. Study Selection and Data Extraction

ACN systems are composed of many components that offer various technologies for detection, connection, and data processing. A study selection phase is needed to focus only on the most relevant and complete works that fit our requirements. This research was conducted using electronic databases such as Scopus and Google Scholar, including only documents from 2011 to 2023. In a primary analysis, 69 papers were selected for full-text reading. Among them, only 37 papers were considered suitable for the data extraction process. In the data extraction process, we focused on the proposed RQs, and for each of them, after a full-text read of the documents, we selected a group of features as suitable for the aim of our work:

- **Sensing layer**—mobile application, car application, GPS, camera.
- **Communication layer**—WiFi, Bluetooth, GPS, cellular, IoT.
- **Cloud layer**—cloud, ML model, ERS system.

These features are the most relevant for answering the proposed RQs and for finding the best ACN architecture.

3.3. Synthesis

As reported in Table 2, only a few works have considered the security concerns in the proposed work. White et al. [24] conducted an informal analysis of possible points of failure in a typical ACN system, highlighting the problems related to smartphone applications due to filters used for preventing false-positive detection. In [25], the authors performed an evaluation of the availability and performance of the proposed architecture; their results showed a reliable network, independently from the number of vehicles considered, but a decreasing performance when vehicle speed increased. The work analyzed in [26] confirmed the poor availability of full smartphone-based systems, where if the phone battery is dead, it is impossible to notify emergency services.

Taking a look at the other works, which do not exhibit any security evaluations, it is possible to notice that almost all the systems integrate GPS, which is one of the most important components in the ACN system, while many connections, such as cellular, Bluetooth (BT), and WiFi, can be applied depending on the architecture. Regarding the external services, only a few of them leverage the machine learning (ML) model, while ERS is included in the majority of works. The communication with the final user is usually implemented using a mobile or car application, leveraging infotainment systems.

Table 2. Features included in crash notification systems. The ✓ denotes the presence of a feature.

	Security	Mobile Application	Car Application	WiFi	Bluetooth	GPS	Cellular (4G, 5G)	Cloud	IoT	ML Model	ERS Call	Camera
[27]		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[28]			✓	✓		✓		✓	✓		✓	✓
[29]			✓				✓	✓	✓	✓		
[30]		✓	✓		✓	✓					✓	
[31]		✓				✓						
[32]				✓	✓	✓	✓		✓		✓	
[33]				✓	✓	✓		✓	✓		✓	
[34]		✓		✓	✓	✓		✓	✓			
[35]		✓	✓	✓	✓	✓	✓					
[36]								✓	✓		✓	
[37]		✓				✓					✓	
[38]						✓	✓					
[39]										✓	✓	
[40]				✓	✓	✓						
[41]		✓		✓	✓	✓	✓	✓	✓		✓	
[42]											✓	
[43]				✓		✓			✓			
[44]				✓			✓	✓	✓			
[45]							✓	✓		✓		
[46]							✓			✓		
[47]			✓			✓	✓				✓	
[48]						✓			✓			
[49]		✓							✓		✓	
[50]											✓	
[24]	✓	✓				✓	✓	✓			✓	✓
[25]	✓	✓	✓	✓		✓			✓	✓	✓	✓
[51]							✓				✓	
[52]									✓			
[15]										✓		
[53]		✓				✓						
[54]		✓				✓	✓			✓		
[55]		✓				✓	✓					
[56]		✓			✓	✓	✓				✓	
[57]			✓						✓	✓		
[26]	✓	✓			✓	✓	✓				✓	
[58]						✓	✓		✓			

Considering the intricate nature of these systems and the considerations made in some of these works, it appears evident that multiple methods must be employed for communication and sensing, and that these methods cannot be restricted to a single approach. While machine learning (ML) can play a crucial role, it is not the sole determinant of accurate detection, as demonstrated by the majority of studies. GPS, on the other hand, stands out as one of the most critical components, capable of significantly reducing the response time of emergency services. Despite the existence of several works advocating a similar reliable and comprehensive architecture, the authors chose to focus on the works of Chang et al. [27] and Khaliq et al. [28] due to the following considerations:

- The dissimilarity between these two architectures primarily lies in the diversity of connectivity options they offer. While one architecture presents a multitude of methods, the other exclusively relies on WiFi. Our focus centers on assessing the ramifications of employing a singular communication method in contrast to an architecture that incorporates a variety of means.
- While alternative architectures may exhibit similar disparities in connectivity, these two stand out as the exclusive implementations integrating a camera system alongside diverse connectivity. This amalgamation represents a novel direction in ACN systems, necessitating thorough consideration and mitigation of privacy concerns.
- A direct comparison of a non-ML-based system with an ML-based system can be achieved by examining these two architectures. This comparative endeavor is driven by the aspiration to contribute valuable insights into the comparative efficacy and performance characteristics of these divergent technological approaches.

Although there are some differences in communication means and some similarities in their architecture components, the possible attacks on components can vary considering the data flows adopted, as shown in the following sections. In what follows, we use the name of the first author to refer to them.

4. Feature Description

ACN is an advanced feature integrated into the majority of modern vehicles, aimed at bolstering safety and optimizing response efficiency in the event of a collision or accident. ACN systems use an array of sensors, cutting-edge communication methods, and algorithms to autonomously detect and send vital information about a crash to emergency services and relevant parties. The core goal is to reduce response times, potentially resulting in saved lives and reduced injuries. In the current section, we will introduce the components of a typical ACN system in order to have a clear picture before the discussion of the components used in the considered architectures.

4.1. Typical Components and Interactions

ACN systems typically combine a diverse range of sensors, encompassing accelerometers, gyroscopes, and in certain instances, sound, temperature, and pulse sensors. These instruments detect abrupt changes in the vehicle's dynamics, indicative of a collision or crash event. Depending on the approach proposed, a sophisticated crash detection algorithm is used, in some cases artificial intelligence can also be used in order to avoid false positives and to enhance the quality of the system. Key features and components integrated into ACN systems include:

1. **In-vehicle communication mechanisms:** Sensors typically communicate with ECUs using CAN-bus. Depending on circumstantial evidence and data collected from sensors, some additional modules can be activated to enhance the quality of the input. Upon identifying a possible crash, the ACN system activates communication modules within the vehicle, like cellular or satellite technology. These modules help the transmission of data to external entities.
2. **Efficient data transmission:** A standardized data package dispatched to a dedicated emergency response hub, manned by trained operators. This package commonly includes vital details such as the vehicle's precise location, impact severity, and in some instances, occupant information.
3. **Sophisticated crash detection algorithms**: Utilizing advanced algorithms, the sensor data are instantaneously assessed to determine if a crash has occurred. These algorithms weigh factors like the seriousness of impact, rapid deceleration, and the collision's nature to make an accurate evaluation.
4. **Central emergency response center:** The emergency response center receives the data package and promptly dispatches suitable emergency services—ranging from paramedics to law enforcement or fire personnel—to the scene of the accident. The

operators in the center can also communicate with the vehicle's occupants through an integrated communication system.

5. **User notification mechanisms:** Beyond notifying emergency services, some ACN systems may also inform the vehicle's manufacturer or a designated contact about the crash occurrence. This enables swift communication with concerned parties, including family members.
6. **Accelerated response:** ACN systems are designed to drastically diminish the time between a collision and the arrival of emergency services at the incident site. This holds critical importance in scenarios where immediate medical attention is needed.

4.2. Components and Interactions in Chang et al. [27] Architecture

In this subsection, components and interactions are summarized from [27].

1. **Sensor data collection:** The ECU receives data from various sensors such as sound, pulse, gyroscope, and accelerometer sensors. These sensors are responsible for gathering different types of data related to vehicle movement, environment, and user well-being.
2. **Threshold comparison:** The received sensor data are compared against predefined thresholds that are set within the ECU. If any of the sensor values cross their respective thresholds, it indicates a potential event of interest, such as a crash or accident.
3. **Sending data to cloud and deep learning platform:** If a sensor value crosses its threshold, the ECU sends the relevant sensor data to the cloud. These data are then forwarded to a deep learning platform for further analysis and decision-making.
4. **Deep learning model analysis:** The deep learning model processes the sensor data to determine whether a crash or accident has occurred. If the model detects that no crash has taken place, no further action is taken and the ECU continues monitoring the sensor data.
5. **Alert generation for user interaction:** If the deep learning model detects a crash or accident, an alert is generated and is displayed on the head unit of the car. The alert likely asks the users if they are alright or not.
6. **User response handling:** If the user responds to the alert and confirms they are okay, the ECU resumes monitoring the sensor data without taking any further action.
7. **No user response (assumed crash):** If the user does not respond to the alert, the ECU assumes a crash has occurred and proceeds with further actions.
8. **Sending data to TCU:** The ECU sends the sensor data, images captured by the camera, and location information fetched from GPS to the TCU.
9. **Data transmission to cloud:** The TCU sends all the collected data (sensor data, images, location) to the cloud.
10. **Emergency services dispatch:** The cloud processes the received data and informs the appropriate emergency services based on the severity and type of accident. This could include paramedics, law enforcement, or fire personnel.
11. **User-generated alarm:** If the user generates an alarm, indicating that they need help, the same sequence of steps are followed as in the case of crash detection.

In summary, as shown in Figure 1, this architecture involves the ECU continuously monitoring sensor data and making decisions based on the threshold comparison and the deep learning analysis. It ensures that appropriate actions are taken in response to potential crashes or accidents, and it leverages cloud and deep learning technologies to provide an efficient emergency response.

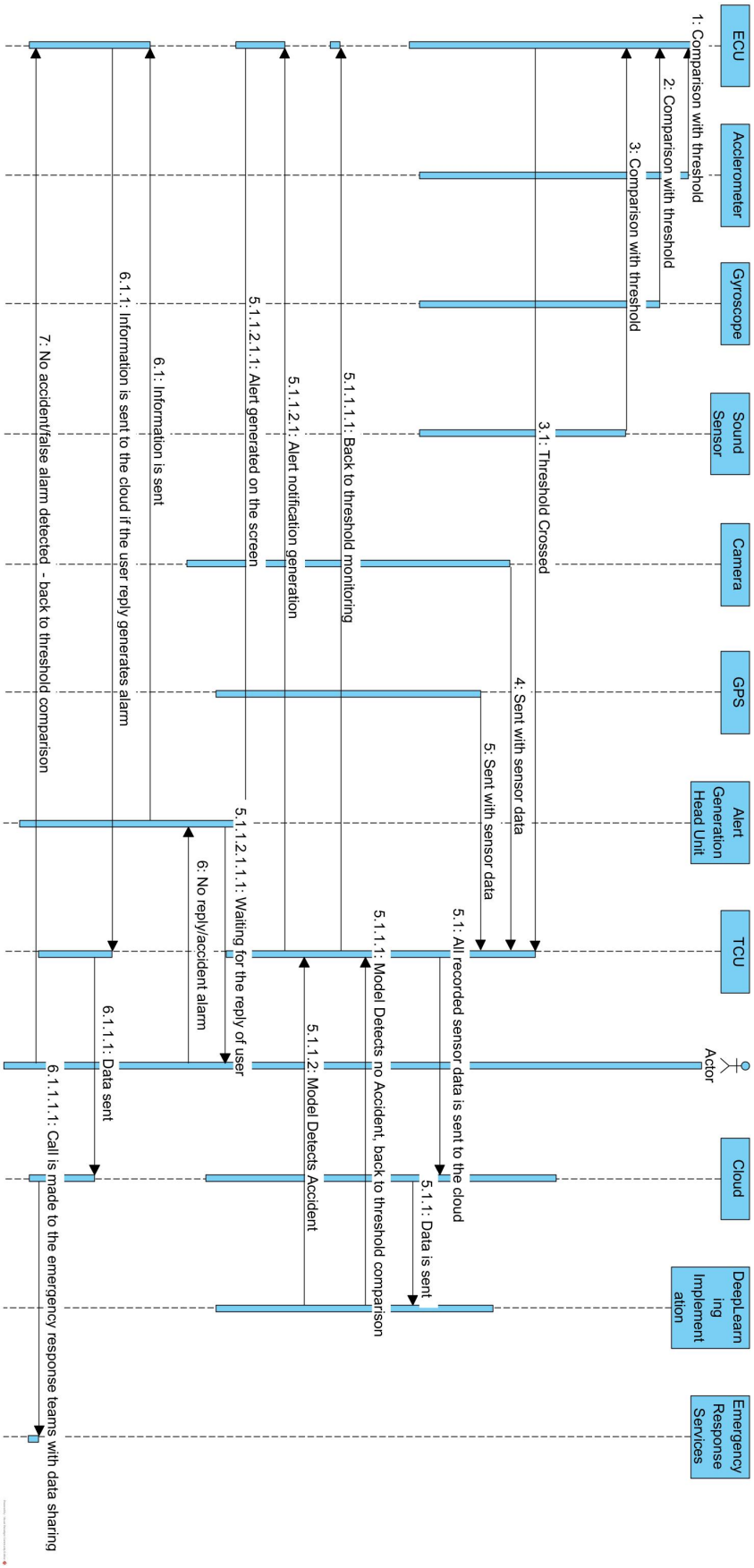

Figure 1. Sequence diagram of Chang et al. [27] architecture.

4.3. Components and Interactions of Khaliq et al. [28] Architecture

In this subsection, components and interactions are summarized from [28].

1. **ECU:** The ECU receives sensor data from various sensors (temperature, sound, pulse, gyroscope, accelerometer) placed within the car. Then, it compares the received sensor values with predefined thresholds. If any of the sensor values cross their respective thresholds, the ECU triggers an alert.
2. **Head unit:** The head unit receives alerts from the ECU when sensor values cross the thresholds. If a sensor reading is unusual, a message appears on the car's screen, asking if the occupants are okay.
3. **User interaction:** The user responds to the alert (either confirming they are okay or not responding).
4. **Crash detection:** If the user does not respond to the alert, the ECU interprets it as a crash. The ECU then activates the camera and GPS unit.
5. **Camera and GPS:** The camera captures visual data of the surroundings, while the GPS unit accurately determines the precise location of the vehicle.
6. **Telematics control unit (TCU):** The ECU sends the collected sensor data, images, and GPS location to the TCU. The TCU then aggregates and packages these data.
7. **Control room:** The TCU sends the combined data to the control room. Experts in the control room process and analyze the data.
8. **Emergency services dispatch:** Based on the analysis, appropriate emergency services (paramedics, law enforcement, fire personnel) are informed and dispatched to the accident scene.
9. **Cloud platform:** The crash data are securely saved in a cloud platform. This repository of crash data will be invaluable in refining the system, ensuring more effective responses in future accidents.

In summary, as shown in Figure 2, the architecture involves sensors within the car, an ECU for processing sensor data and generating alerts, a head unit for user interaction, a TCU for collecting and transmitting data, a control room for analysis and emergency service dispatch, and a cloud platform for data storage. This system aims to enhance safety by detecting and responding to potential accidents while also collecting data for future improvements.

4.4. Data Flow Diagrams of the Features

In Figures 3 and 4, data flow diagrams for both architectures are presented.

Despite them seeming to be very similar to each other, some crucial differences exist in the components and interactions, which are also highlighted in the data flow diagrams. In the Chang et al. architecture [27], the sensors (i.e., accelerometers, gyroscope, speed, microphone, and temperature sensors) continuously collect data, which are then transmitted via Bluetooth. These data are gathered and analyzed by the ECU. When a predefined threshold is reached, the ECU prompts the TCU to send the crash event data to the cloud. At this point, the system makes a request to the ML model in order to assess the presence of a false alarm. The deep learning method then conducts a detailed analysis of the crash event data to determine whether the event corresponds to an accident or not. Particularly, if the data coming from the accelerometer and gyroscope are too random and there is no correlation that demonstrates the existence of a crash, then the request is aborted. Instead, if the data suggest a crash, a notification is sent to the user, asking for confirmation, and an emergency alert is simultaneously sent to the emergency services. If the event does not qualify as an accident, the system reverts back to its initial state of monitoring the sensors.

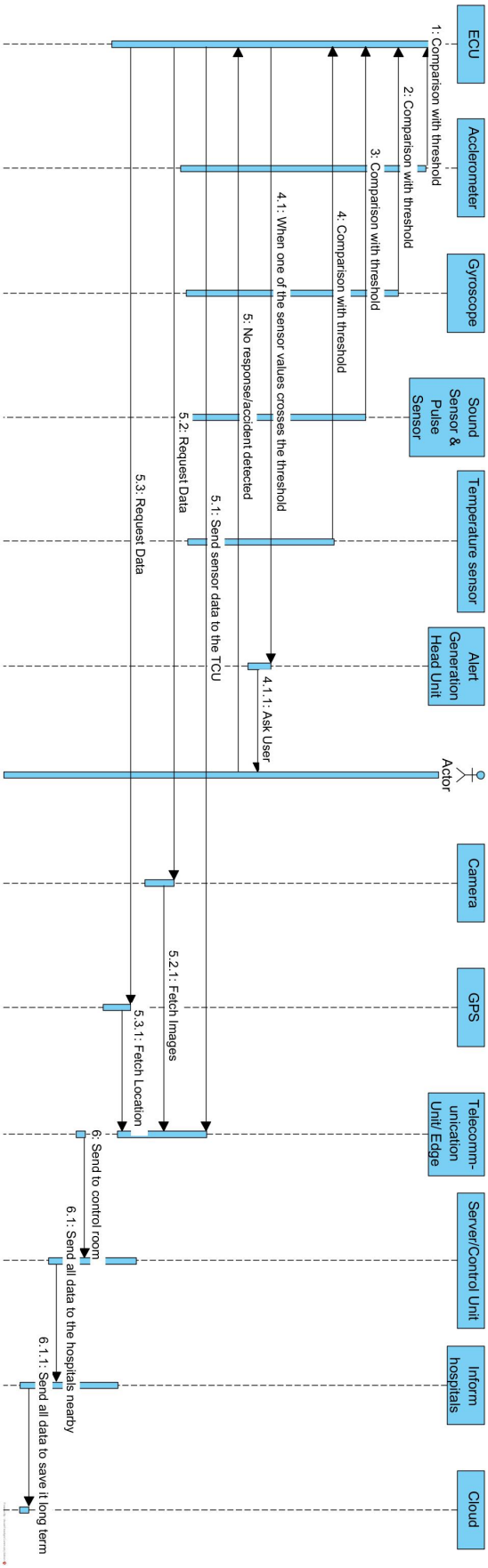

Figure 2. Sequence diagram of Khaliq et al. [28] architecture.

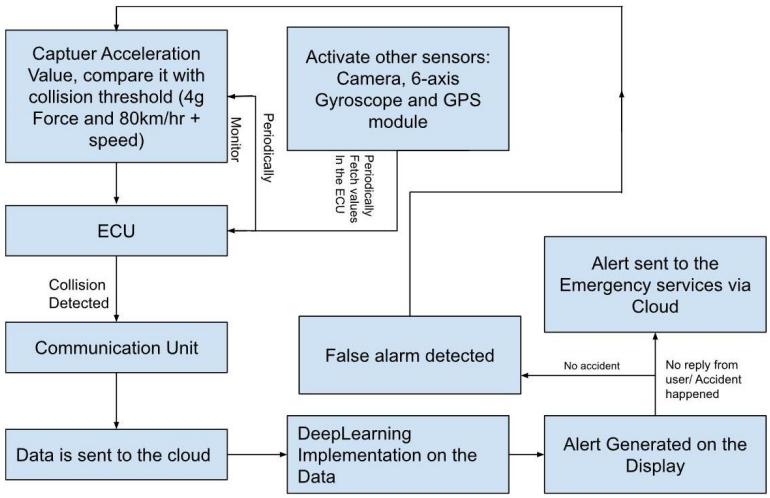

Figure 3. Data flow diagram of Chang et al. [27] architecture.

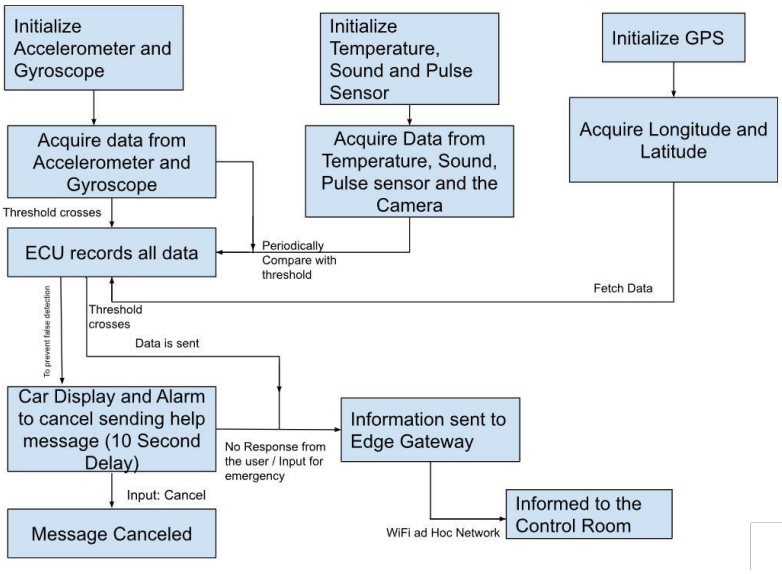

Figure 4. Data flow diagram of Khaliq et al. [28] architecture.

Differently from the Chang et al. [27] architecture, in the Khaliq et al. [28], there is no usage of an ML model. After initialization, the accelerometer and gyroscope sensors periodically gather data and compare them to a predefined threshold. If the data surpass this threshold, a collision event is reported. Similarly, the sound, temperature, and pulse sensors are continuously monitored. If any of these sensors' data also exceed the threshold, a collision event is reported. Additionally, a picture from the internal camera and the vehicle's location data acquired with the GPS are included in the report.

If the collected data do not exceed the threshold, a message is displayed to the driver along with an alarm. The driver can dismiss the message. If the driver is unable to dismiss it, the collision event report is sent to the edge gateway, which forwards it to the control room.

5. Threat Analysis and Risk Assessment (TARA)

The selected architecture underwent a TARA following the methodologies outlined in ISO/SAE 21434. This analysis was conducted from the perspective of potentially affected road users, with each TARA method being meticulously applied, as described in the subsequent subsections.

5.1. Asset Identification

An analysis was conducted on all components within the selected architectures to pinpoint those that, when compromised, would result in a damage scenario. We assigned the relevant cybersecurity properties for each component, port, or connection between two ports: confidentiality, integrity, and availability. Elements such as ECUs or sensors were additionally assigned authenticity, non-repudiability, and authorization.

5.2. Threat Scenario Identification

Threat scenarios were identified using the Medini Analyze 2023 R1 software, employing the spoofing; tampering; repudiation; information disclosure; denial of service; elevation of privilege (STRIDE) model as the foundational framework. This model correlates each cybersecurity property—authenticity, integrity, non-repudiability, confidentiality, availability, and authorization—with potential threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, respectively. Each identified threat scenario is characterized by a set of three elements: the specific asset under threat, the compromised cybersecurity property affecting the asset, and the underlying cause behind the compromise of said cybersecurity property. To define the cybersecurity properties pertinent to each asset, a manual process was followed. Subsequently, the software facilitated the extraction of the corresponding threat scenarios associated with these attributes.

5.3. Impact Rating

The evaluation of damage scenarios wrapped up a comprehensive assessment of their impact on road users. The consequences were divided into four distinct categories: safety (injuries or fatal injuries potentially suffered), financial (impact of the financial damage endured by the road user), operational (loss or impairment of vehicle function or core function), and privacy (sensitiveness of road user's information disclosed). For each damage scenario and each impact category, an impact rating was determined. The scale used for the ratings considered four levels of impact, ranked in descending order of severity: severe, major, moderate, and negligible.

5.4. Attack Path Analysis

The attack path analysis was executed for each threat scenario previously discovered. It delineated the routes that potential adversaries could traverse to exploit vulnerabilities. For each threat scenario, one or more distinct attack paths were identified, each providing details on the sequence of actions an attacker could attempt to navigate through the network of assets. To give an example, an attack path could be accessed through the WiFi module to the TCU, then reaching the gateway ECU to finally spoof the MEMS.

5.5. Attack Feasibility Rating

The attack feasibility rating can be executed adhering to one of the following three approaches: attack-potential-based, Common Vulnerability Scoring System (CVSS)-based, and attack-vector-based. The latter two require in-depth knowledge of all the elements, technologies, and actors involved as well as an advanced system architecture design unavailable at the time of the realization of this research, the attack-vector-based approach has been pursued. According to it, the attack feasibility rating should be determined based on evaluating the predominant attack vector of the attack path. The scale used for the ratings takes into account the contextual framework that underlies the potential exploitation of attack paths. The rating of attack feasibility escalates as the attacker's remoteness increases in relation to the targeted attack path. This assumption stems from the idea that obtaining physical access to an asset requires more effort as well as being less desirable for a potential attacker than accessing it through the network. Thus, the scale used is composed of the following levels: high, medium, low, and very low, respectively mapped to the following context criteria: network, adjacent, local, and physical. More details can be found in the ISO/SAE 21434 document.

5.6. Risk Value Determination

The analysis of risk values was achieved by applying a sequence of risk formulas that incorporate impact ratings and attack feasibility ratings before being determined. Initially, a translation of potential impact and attack feasibility ratings into corresponding scores was performed. Subsequently, for each distinct threat scenario, the average of all impact scores was computed and then multiplied by the feasibility score. The resultant risk scores were eventually subject to a transformation process, wherein they were calibrated into risk values based on a predefined mapping. The scale for risk values included the following values, ranked in descending order of danger: high, medium, low, very low. The impact factor was computed for each feature on the basis of four aspects: safety (S), financial (F), operational (O), and privacy (P). It is possible now to define an equation for computing the risk for each threat:

$$Risk = Avg(S + F + O + P) \times Feasibility \quad (1)$$

The value obtained from the equation can be converted to a risk level following Table 3.

Table 3. Table of risk value according to defined formula.

Risk Level	Min	Max
Very Low	0	200
Low	201	400
Medium	401	800
High	801	1600

Considering the context of our system, which is strictly related to human life, operational and safety impacts are the most important impact metrics. Anyway, considering the economic impact of the components involved and the data exchanged when these components are used, financial and privacy impacts are also relevant. For this reason, we decided to consider all the metrics with an equal impact on the risk.

Nevertheless, we choose to alter the natural distribution of risk level classes in line with Table H.8 defined in ISO/SAE 21434. We started by splitting half the maximum value ($40 \times 40 = 1600/2 = 800$) and assigning the highest part of this to high-level threats. For the remaining half, we performed another splitting ($800/2 = 400$), assigning the highest part to the medium-level threats and for the remaining part half and half to low- and very low level threats.

These operations are needed to have a good threat model, able to consider as high risk all the threats that can lead to possible harm to the driver.

5.7. Risk Treatment Decision

The array of potential decisions for risk treatment encompassed the following values: mitigation, avoidance, acceptance, and transfer. Yet, in practice, only mitigation and acceptance were implemented, with avoidance and transfer excluded from consideration. The notion of avoidance entailed relinquishing certain fundamental system features, which was deemed undesirable. But, transfer necessitated relying on external entities to assume risk management responsibilities, a prospect that had not been anticipated. The course of action was determined to involve the mitigation of threat scenarios categorized as high and medium, while accepting the low and very low scenarios. Each identified threat scenario slated for mitigation underwent the formulation of a distinct set of security measures and corresponding security requirements to reduce or nullify the associated risk.

6. Architectures Comparison

In the following section, the selected architectures will be compared. In the first two subsections, a short introduction is given, highlighting the main components; while in Sections 6.3 and 6.4 a comparison of the components and security is discussed.

6.1. Chang et al. [27] Architecture

The system proposed by Chang et al. [27] defines a system that can detect high-speed head-on collisions and accidents in the golden hour for survival—the emergency services can be contacted, and the survival probability of the affected people increases. As depicted in Figure 5, the proposed architecture in the paper uses various in-vehicle (I-V) networks including BT, Bluetooth low energy (BLE), WiFi, etc. These networks are connected using an in-vehicle infotainment telematics unit. The system is divided into three layers: sensing layer, networking layer, application layer (with deep learning model). The sensing layer is comprised of the sensors that are used to detect the accident, like a micro-electro-mechanical system (MEMS) sensor, Global Positioning System (GPS) module, and on-board diagnostics (OBD)-II bridge. The network layer consists of communication protocols like cellular, 3G/4G, BT, BLE, WiFi, universal asynchronous receiver/transmitter (UART), and ethernet. The application layer is the main layer responsible for the analysis of the accident and contacting emergency services. This layer also involves the deep learning model for assessing the situation, based on the cloud.

1. Sensing layer: This layer is defined as the layer responsible for the sensing of data values to detect the head-on collision in a vehicle. The sensing layer includes the six-axis gyroscope and MEMS sensor with an embedded accelerometer, OBD-II bridge, and GPS. A collision detection system is a continuous process. When a collision occurs, the window of the collision is 0.1 to 0.2 s, as per several reports. When a collision occurs, the data fetched from the above-mentioned sensors is sent to the network layer to further communicate it to the cloud for deep learning analysis.
2. Networking layer: Since the development and use of vehicular networks and infrastructure has increased in the past years to automate vehicles and services, there is a dedicated use of the Telemetrics platform in vehicles, which is the main basis for the communication here. The telematics unit uses in-vehicle infotainment (IVI) to update the mobile application. This system uses 3G/4G mobile networks for sending the data to the cloud from the network layer. Messages from the IVI system are directly transmitted to the user via this interface:
    (a) Driver information screen: The information is digitized and transmitted to the driver directly through the driving information screen of the IVI system.
    (b) Collision detection and alarm screen: The collision detection and alarm screen updates the driver of a car during the driving process. A camera is placed in the front of the vehicle and connected to the proposed IVI system to record real-time streaming images. The collision threshold is defined when the braking is at 4 g and the speed of the car is greater than 80 km/h, as per the Insurance Institute for Highway Safety (IIHS) report for a fatal accident. In such a case, the IVI system will record an image of the abnormal event and upload the relevant information to the cloud-based platform for further vehicle crash-event analysis.
3. Application layer: The IVI system utilizes 3G/4G mobile networks to send relevant data to a cloud server database. The recorded data in the cloud database is then utilized to create a data model that can recognize high-speed head-on collisions or accidents involving a single vehicle. In this research, the cloud-based information platform was built using web development tools like hypertext preprocessor (PHP) and Structured Query Language (SQL). This platform facilitates real-time notifications for incidents of high-speed head-on collisions or single-vehicle accidents.

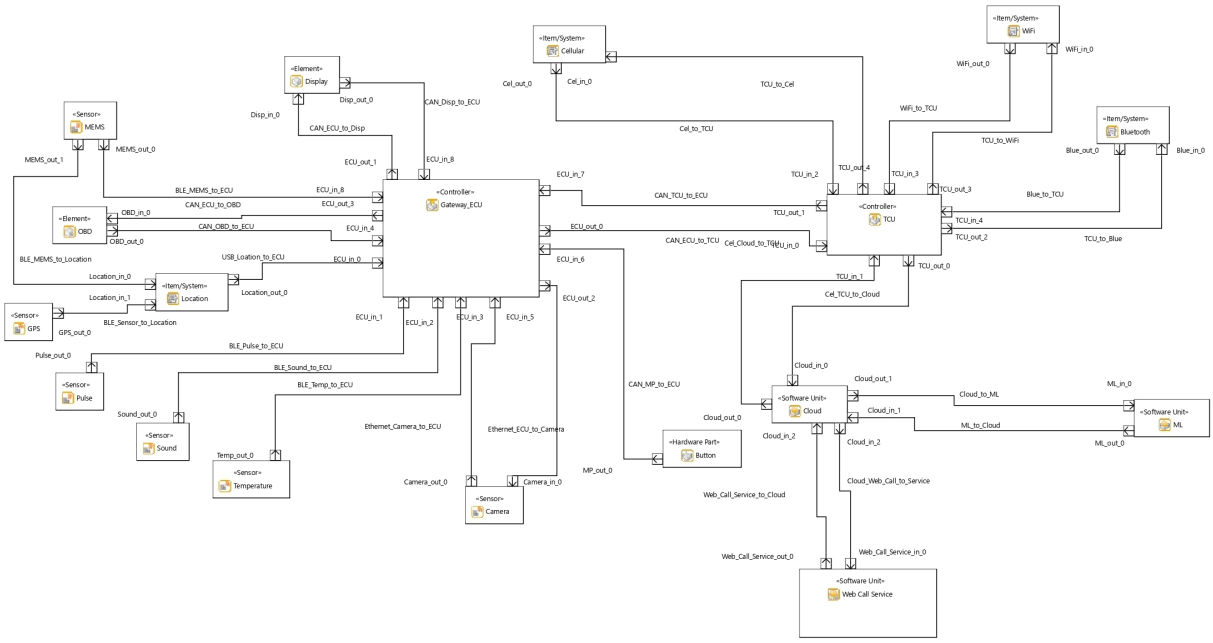

Figure 5. Chang et al. [27] architecture.

6.2. Khaliq et al. [28] Architecture

The architectural framework posited by Khaliq et al. [28] delineates a structured system designed to mitigate road hazards and enhance the likelihood of preserving lives in the event of road accident injuries. As illustrated in Figure 6, analogous to the antecedent architectural model, the system comprises a substantial array of devices and can be categorically compartmentalized into three principal layers:

1. On-board sensors: In order to detect accidents, the on-board sensors constantly track the acceleration and gyroscope data. In case of an accident, the crucial data like the date, time, location of the accident, age, gender, and even images is sent to the edge. This phase has two major features: automatic accident detection with emergency alert, and accident management. The architecture is deployed in the vehicle but also in the nearby control room with the edge gateway. The on-board unit (OBU), where all the sensors are deployed, is constantly active and monitoring the data. When an accident happens, the speed decreases drastically, which can be measured by the accelerometer. Rollovers can be detected by the change in orientation using the gyroscope. In this case information is directly sent to the control room with the information from other sensors. In case of a collision, all the sensors are taken into account. All sensors have pre-defined threshold values, against which the real-time sensor values are checked. If the threshold is crossed by any sensor, the vehicle generates an alert to check for a false alarm. If it is not a false alarm the data are sent to the edge node. Once the data are sent, a nearby hospital dispatches an ambulance with accident-specific first aid.
2. IoT gateway: This gateway handles collecting data in the edge node, refining it, and then sending the refined data to the nearby control room edge gateway to save the network bandwidth. The data are transferred via a vehicle ad hoc network, using a Institute of Electrical and Electronics Engineers (IEEE) 802.11n dongle. This node extracts useful data, stores associated pictures, and forwards the processed data. It also has the following features:
    (a) Face detection: This is used to identify the number of victims involved in the accident, and the state of the victims, using Open Source Computer Vision Library (OpenCV).
    (b) Data pre-processing: Whenever needed, the OBU monitors the sensor data. The data are sent to the edge node, where the data are processed closer to the network

i.e., in the control room. Then, the data are transmitted to the cloud for long-term storage. There are two benefits resulting from this: the non-useful information is cleaned beforehand to avoid reducing the network bandwidth, and it simplifies the data in the cloud for easier interpretation. The communication of the edge is achieved using transmission control protocol (TCP)/IP because of its connection-oriented nature and reliability.

3. Cloud platform: The central control unit accepts the accident alert notification to take action. It handles receiving data packets, storage, and visualization. We needed a testbed on which to test the implemented system. It required an infrastructure-as-a-service model as per the defined architecture. The web server application Apache was used to build a personal server on a Linux-based operating system. This cloud stores accident data and provides it to the authorities to implement road safety on the most insecure places in a road structure.

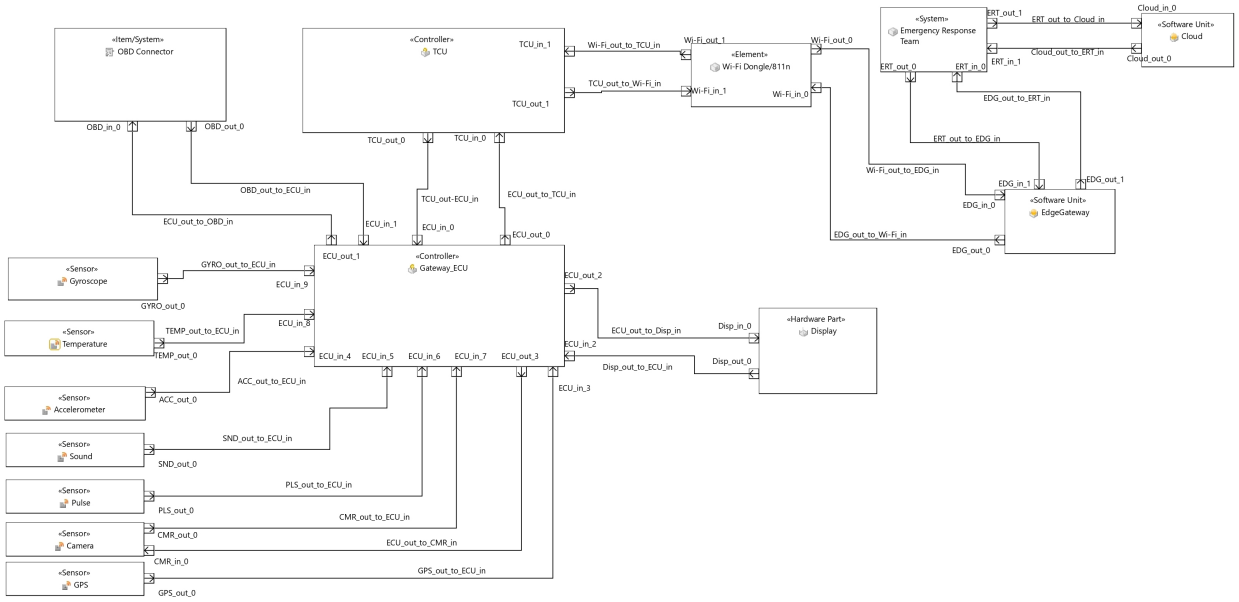

Figure 6. Khaliq et al. [28] architecture.

6.3. Components Comparison

The components of the two ACN architectures can be categorized into three distinct layers to facilitate a comprehensive understanding of their respective architectures.

1. **Sensing layer**: The sensors used in each of the systems are similar. As shown by Table 4, a difference exists between the two architectures. The Chang et al. [27] architecture utilizes fewer sensors but is based on a deep learning model where the user input is required to confirm the model prediction, while the second architecture [28] uses all the sensors mentioned above, and every time the values of these sensors cross the defined threshold, the user is asked to confirm the accident. The first model is based on artificial intelligence (AI) and automation prediction, while the second model is more manual and inaccurate as it will generate more alerts. In the first paper, the sensors are connected to the ECU using various communication technologies, e.g., Bluetooth, WiFi, universal serial bus (USB), CAN, ethernet, and BLE.
2. **Communication layer**: This layer is used to communicate with the vehicles and infrastructure outside the car. As reported in Table 5, the architecture proposed by Chang et al. [27] uses telematics with 3G/4G and cellular services to connect to the outside V2X. This layer also includes networking protocols like BLE, Bluetooth, ethernet, WiFi, and cellular to communicate with in-vehicle sensors and other parts. Bluetooth communicates with the sensors and ECU, ethernet with the camera and ECU, and the CAN bus with the display. On the other hand, the architecture proposed

by Khaliq et al. [28] uses this layer to create an ad hoc network dynamically to use V2X to transfer the data to the edge. There the data are refined, filtered, and cached, and face detection takes place to recognize the number of passengers and check the injuries. The communication layer then uses TCP to send the data to the cloud. A comparison of the network protocols used in the above papers is given below.

3. **Cloud layer**: This layer in both architectures is used to contact the emergency services when an accident is detected and confirmed with the user. In the first paper [27], this layer is used to install the deep learning model. It checks if the accident has taken place by analyzing the data provided by the sensors and other mounted devices, and then contacts the emergency services with all the vehicle data and the prediction from the model. The second paper [28] uses this unit to accept the accident alert notification to contact the emergency services. It handles receiving data packets, storage, and visualization, and shares the statistics with the authorities to implement accident countermeasures.

Table 4. Components detected in each architecture belonging to sensing layer.

Component	**[27]**	**[28]**
GPS	✓	✓
Accelerometer and gyroscope (6-axis sensor)	✓	✓
Camera	✓	✓
Sound	✓	✓
Temperature		✓
Pulse		✓
OBD-II redundancy	✓	

Table 5. Components detected in each architecture belonging to communication layer.

Communication Protocols	**[27]**	**[28]**
Cellular	✓	
3G/4G	✓	
Bluetooth	✓	
BLE	✓	
WiFi	✓	✓
WiFi dongle		✓
TCP		✓
CAN bus	✓	✓

6.4. Security Comparison

Each category within the STRIDE threat modeling framework encompasses a distinct set of components. Notably, a component that may constitute an entry point for an attack in one architectural design may not be considered critical in another. This variance stems from the inherent differences in the architectures themselves, as well as the specific context in which they are employed. It is possible to classify threats into four groups following the equation defined in (1) and Table 3. The greatest number of threats are classified as very low and medium, as reported in Figure 7, by following the attack vector approach. For very low threats, it is not needed to put in place any security mechanisms and we decided to accept them; for the medium-level threats, we applied mitigation to all threats, while more details are given in the next sections for the high-risk threats. Although most components

are shared from both architectures, such as GPS and ECU, some others are different. After the threats were created through the Ansys medini analyze software, the TARA method was applied.

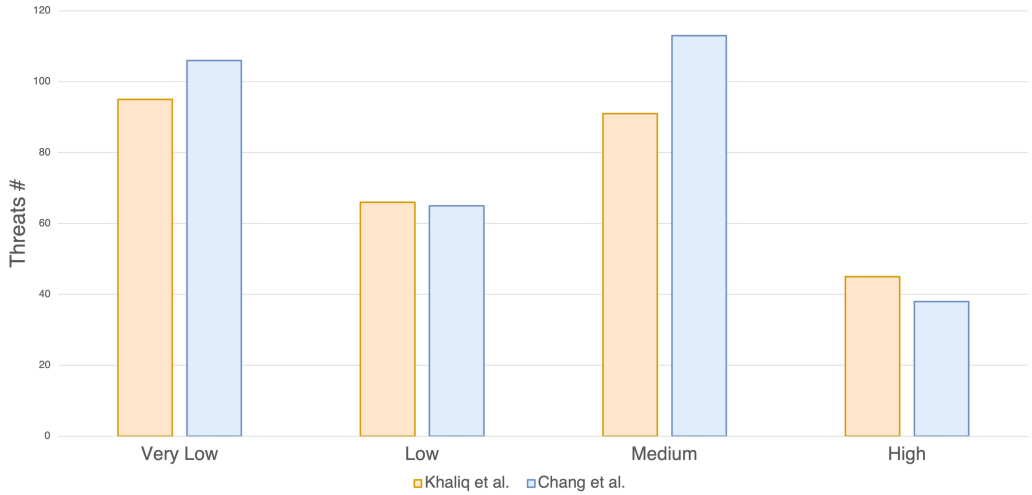

Figure 7. Number of threats detected using TARA, classified by risk level.

The software yielded a total of 297 threats for Chang et al. [27] and 322 threats for Khaliq et al. [28]. These threats were divided into six main types according to the STRIDE model: denial of service, information disclosure, repudiation, spoofing, elevation of privilege, and tampering.

6.4.1. Security Analysis of Chang et al. [27] Architecture

Table 6 shows the threats detected in the Chang et al. architecture, with the greatest number being very low or medium threats, according to the typical analysis.

Table 6. Security analysis of Chang et al. [27] architecture. The ratio of the number of current risk levels of that category to the total number of threats related to that category is given in parentheses.

Threat	Very Low	Low	Medium	High
Information Disclosure	31 (36.5%)	23 (27.1%)	37 (43.5%)	1 (1.2%)
Tampering	28 (32.9%)	16 (18.8%)	32 (37.6%)	13 (15.3%)
DoS	33 (38.4%)	18 (20.9%)	27 (31.4%)	15 (17.4%)
Repudiation	6 (40%)	3 (20%)	4 (26.7%)	3 (20%)
Spoofing	2 (13.3%)	3 (20%)	8 (53.3%)	3 (20%)
Elevation of Privilege	6 (40%)	1 (6.7%)	4 (26.7%)	4 (26.7%)

1. **Very Low Risk Threats:** This category represents the lowest possible level of threat to the component that it relates to, and through the application of TARA we concluded that 106 (33%) of all of the threats fitted into this level of risk.
   From the above statistical analysis, we can draw conclusions. The highest percentage of very low risk threats comes from elevation of privilege (40% of total elevation of privilege (EoP) threats), which corresponds to putting more authorization in sensors, which is not possible as most sensors are permanently configured and calibrated during manufacturing. The least come from spoofing (12.5%), as it is a major risk. Important assets can be spoofed to cause harm to the user. Other threats contribute almost one third to the very low risk category as those attacks on the assets would not cause trouble for the user.

2. **Low-Risk Threats:** This category represents a low level of threat to the component that it relates to. Through the application of TARA we concluded that 64 (19.9%) of all of the threats fitted into this level of risk. From the above analysis, it is clear that a low percentage of threats fall into this category, with the highest percentage of these being information disclosure threats (25%). Information disclosure of assets like temperature sensor, pulse sensor, and accelerometer data would not harm the user physically or cause failure of systems. The lowest percentage of low-risk threats is elevation of privilege threats, with only one threat (6.7%). There is no compromising event that an attacker can cause, only the control over the display can be obtained. The rest of the attacks contribute less than 20%.
3. **Medium-Risk Threats:** The threats presented here are the ones that are classified as medium risk, through the application of TARA. We concluded that 112 (34.9%) of all of the threats fitted into this level of risk.
   It is evident that information disclosure threats and spoofing contribute the most to the medium-risk threat category. When the information of some of the assets can be monitored by the attacker, harm could be done to the user. For example, the TCU or ECU can be attacked to check the communication within and outside the system or track all the car data that run through the ECU. Repudiation contributes the least to this category as repudiation of only a few selected components can cause damage to the user. For example, repudiation of GPS can occur, where the attacker can send wrong GPS information to the user as well as to the emergency services, which can be threatening. The rest of the threats also contribute a large amount to this category as they can cause critical damage depending on the attacked asset, e.g., DoS on the ECU can compromise all functions of the car, and tampering can give control to the attacker completely.
4. **High-Risk Threats:** This category represents the highest possible level of threat to the component that it relates to, and through our analysis, we concluded that 39 (12.1%) of all of the threats fitted into this level of risk. A dokeeper analysis will be given in the next section.

6.4.2. Security Analysis of Khaliq et al. [28] Architecture

Table 7 shows the threats detected in the Khaliq et al. [28] architecture, with the greatest number of them relying on very low or medium threats, according to the typical analysis.

Table 7. Security analysis of Khaliq et al. architecture. The ratio of the number of current risk levels of that category to the total number of threats related to that category is given in parentheses.

Threat	Very Low	Low	Medium	High
Information Disclosure	33 (38.8%)	15 (17.6%)	34 (40%)	3 (3.5%)
Tampering	24 (28.2%)	25 (29.4%)	21 (24.7%)	15 (17.6%)
DoS	26 (30.2.5%)	24 (27.9%)	21 (24.4%)	15 (17.4%)
Repudiation	5 (33.3%)	0 (0%)	5 (33.3%)	5 (33.3%)
Spoofing	4 (26.7%)	3 (20%)	6 (40%)	2 (13.3%)
Elevation of Privilege	4 (26.7%)	1 (6.7%)	5 (33.3%)	5 (33.3%)

1. **Very Low Risk Threats:** We concluded that 96 (31.9%) of all of the threats fitted into this level of risk. By looking at the percentage distribution of each type of threat within each risk category, it is noticeable how evenly they are all distributed. The lowest value is 26.7% and the highest is 37.5%, corresponding to spoofing and elevation of privilege, and information disclosure, respectively. The latter concerns privacy risks associated with violation of confidentiality, thus does not carry a high risk for the safety or operability of the ACN. Other threats such as tampering or denial of service,

whose risk is usually high, fall within this region because they are associated with non-critical components, for which the vehicle behavior is not compromised, like sound or pulse sensors. Lastly, for spoofing or elevation of privilege, these percentage values are once again associated with low-importance sensors, which will not impact the ACN considerably.

2. **Low-Risk Threats:** We conclude that the paper has 68 low-risk threats in total (22.6%). We noticed that there are no repudiation threats associated with a low risk level, with them being concentrated more on the medium and high levels. The same logic applies to the low level of spoofing and elevation of privilege threats. Although there are fifteen threats present, these represent only 17% of the total information disclosure threats. This is mainly because information disclosure of extremely sensitive private data falls under a higher level of risk. For example, when the information disclosed relates to the gyroscope, cloud, or accelerometer, it can relate to a low risk level as it does not allow attacker to interfere with the ACN functionality. About 27.3% of denial of service attacks are categorized as low risk level. This is mainly because certain components being out of commission by a denial of service does not directly affect the functioning of the overall ACN system, for example, the gyroscope, cloud, and OBD. Lastly, the highest percentage of overall threats present in the low level of risk are related to tampering. This is mainly because there are many components, whose tampering does not affect the overall functionality of the system, similarly to denial of service.
3. **Medium-Risk Threats:** Through the analysis we found that 92 (30.6%) of the threats belong to this category. It is important to note that for each type of threat the percentage of medium threats is near 25%, which means that at least a quarter of the threats are medium risk level. When we talk about the automotive scenario and ACN functionality it is more likely that all threats will not have a very high impact, but also not a low impact. So, the rest of the threats will be split among the others risk levels. Looking into each percentage, we see that denial of service is the lowest, which is expected because normally this threat will represent a high level of risk. Finally, spoofing has the highest percentage here. Within the context of ACN functionality, this threat usually has clearly a medium level of risk; as we have stated, the majority of these threats have a low severity level and a high feasibility level or vice-versa. The elements affected also correspond to some of the most important in the vehicle, but attacking them will most likely be quite infeasible or the earnings from it will not compensate for the effort; this is why most of these spoofing attacks are medium-level risk. Finally, spoofing has the highest percentage here, which again is not a surprise because this threat is something that cannot pose a high level of threat, but it cannot ignored too, so a medium level is a normal value for this.
4. **High-Risk Threats:** Through the application of TARA we concluded that 45 (15%) of all of the threats fitted into this level of risk, a deeper analysis is given in the next section.

7. Risk Analysis

In the current section, the risks detected using TARA are associated with the architectures described by Chang et al. [27] and by Khaliq et al. [28], as discussed. For each component, port, and communication channel, a description of high-level risk threats is given in conjunction with a possible countermeasure. This analysis, according to Section 5, was performed using the STRIDE threat model. Figure 8 depicts the detected threats referring to the STRIDE model. In the following subsections, one for each component, a risk analysis is discussed, together with possible countermeasures.

7.1. ECU

In both architectural frameworks, the ECUs represent tangible physical electronic components, often configured as systems-on-chips (SoCs). These components are inherently susceptible to a range of security threats since they become integral parts of printed circuit boards and are in charge of centralizing the data processing.

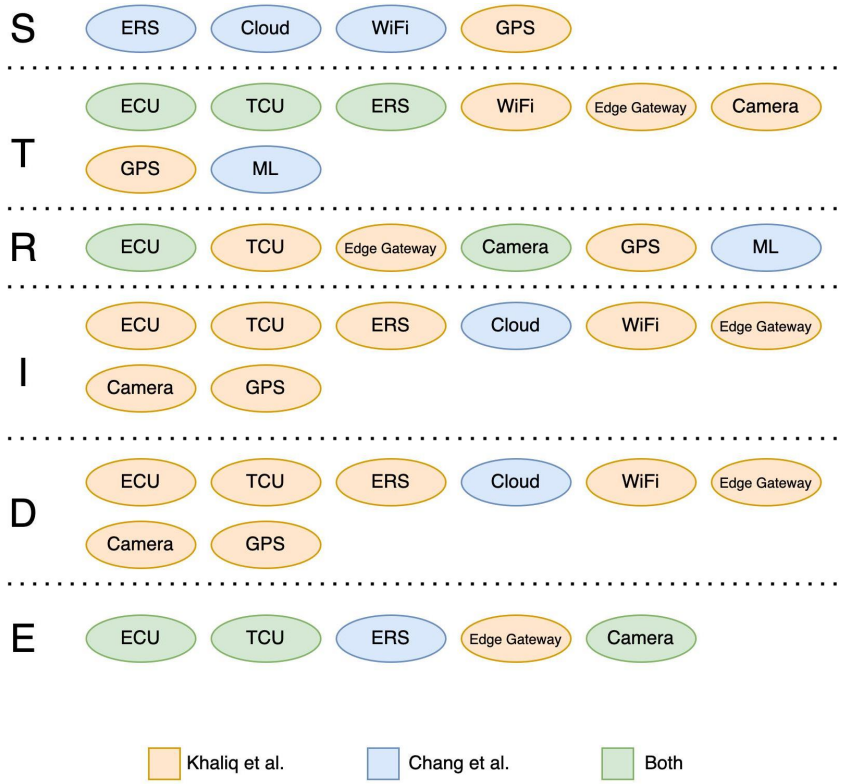

Figure 8. Detected threats in analyzed papers according to STRIDE threat model.

7.1.1. Tampering

1. **Component**
   Security risk: If unauthorized individuals gain access to the ECU and tamper with its functionality, they could intentionally trigger false crash notifications. This could lead to unnecessary deployment of emergency services, wasting resources, and causing confusion. In some cases, tampering with the ECU might be achieved by modifying the log files of the insurance about crashes. This can result in financial losses for insurance companies and increased premiums for users. Tampering with the ECU could also potentially compromise the privacy of the vehicle owner, as the attacker might collect data beyond crash-related information and expose sensitive personal data.
   Security measures: Encryption can be used to ensure that communication between the ECU and other components of the system is encrypted, making it difficult for unauthorized parties to intercept or manipulate data. Intrusion detection mechanisms can also be incorporated to detect and respond to attempts to tamper with the ECU. For instance, if unauthorized changes are detected, the system might disable itself or start security protocols.
2. **Ports**
   Security risk: If the ECU port is tampered with, the ACN system may not receive accurate crash data on time. This could result in delayed or no response from emergency services, putting the safety of the vehicle occupants at risk. In some cases, attackers might target the ECU port with the intention of disrupting the ACN

service. This could lead to a complete or partial service outage, leaving users without the safety features they rely on.
Security measures: Firewalls can be used to segment the network and restrict direct access to the ECU port. Hashes of sensor data can be computed and stored by the ECU. The ACN system can compare these hashes with the received data to detect any discrepancies that may indicate tampering. The ACN system can also digitally sign the data it sends to the ECU. This signature verifies the authenticity of the data and ensures that it has not been altered since being signed. Strong authentication mechanisms can also be used to ensure that only authorized personnel or systems can access the ECU port. This prevents unauthorized tampering attempts.

3. **Connections**
Security risk: The TCU is responsible for relaying critical information to emergency services. Tampering with the connection between the ECU and TCU can lead to delays or failures in transmitting crash data to these services, resulting in slower response times. Delays in emergency response can have severe consequences, particularly in situations where prompt assistance is crucial. Tampering with ECU connections to the TCU can also lead to service outages or system failures. These outages can result in the complete loss of ACN functionality, rendering the system incapable of providing any crash-related notifications.
Security measures: The secure on-board communication protocol (SecOC) protocol can implemented to establish secure communication channels between the ECU and other components, such as the TCU. During the initialization process, the SecOC protocol can also be utilized for secure bootstrapping to ensure that the ECU authenticates itself before data exchange begins.

7.1.2. Denial of Service (DoS)

1. **Ports and Connections**
Security risk: A DoS attack on the ECU would result in the complete shutdown of the entire automatic crash notification system. This is because it would become impossible to receive information from sensors that detect accidents and to communicate with the components responsible for triggering the alarm.
Security measure: By implementing a firewall and an intrusion detection system (IDS), it is possible to establish an effective defense against DoS attacks directed at the ECU within connected vehicles. The firewall filters incoming and outgoing traffic, allowing only legitimate communications while blocking suspicious or harmful ones. The IDS constantly monitors system activity to identify any unusual traffic patterns associated with a DoS attack. Upon detecting signs of overload or malicious traffic, the firewall can react promptly by blocking connections from malicious sources and initiating mitigation measures.

7.1.3. Elevation of Privilege

1. **Component**
Security risk: The (main) ECU is the main component in the vehicle's electronic control and is where all sensors and devices converge. As such, it is of high value for a potential malicious actor. The attack path is either physically to the CAN bus, locally via OBD-II, or via a vulnerable network interface to the TCU and then to the ECU. The access to the ECU provides read-only access to the information retrieved or sent by the ECU. An elevation-of-privilege attack towards the ECU allows the actor to change data, and damage other connected devices or the ECU itself. Some motivations for this attack range from clearing diagnostic trouble codes (DTCs), reconfiguring parameters, enabling paid-only features, or even damaging car electronics beyond repair (e.g., a ransomware attack).

Security measure: The standard security controls for mitigating this risk are through authentication, role-based control, the least privilege principle, or multi-factor authentication.

7.1.4. Repudiation

1. **Component**
   Security risk: The ECU could be compromised by a malicious attacker through the exploitation of the WiFi module and the TCU. In the absence of a reliable non-repudiation mechanism, any malicious activity performed on the ECU—and consequently affecting the entire vehicle—could be denied later on. Such a scenario has the potential to result in substantial operational and safety consequences for the entire system, ultimately undermining the effectiveness of critical features like the ACN.
   Security measure: Implementing digital signatures with asymmetric keys provided by reputable third parties stands out as a highly effective approach in guaranteeing non-repudiation. By adopting this method, the recipient of the message gains an accentuated sense of assurance, as it verifies the origin of the content to the intended source.

7.2. TCU

TCU assumes a pivotal role in both architectures, acting as the central hub for communication between the ACN and emergency services. Noteworthily, in the Chang et al. [27] architecture, the TCU extends its mandate to manage Bluetooth and WiFi, responsible for acquiring sensor data, making this component less vulnerable to attacks due to the redundancy introduced. On the contrary, the Khaliq et al. [28] architecture, despite entailing direct sensor communication with the engine control unit (ECU), does not exhibit redundancy, increasing the responsibility of the TCU and causing a more vulnerable component.

7.2.1. Tampering

1. **Ports and Communications**
   Security risk: The TCU is a controller that gathers and packages the GPS location, pictures, and sensor data from the ECU before sending them to outside services. Tampering assaults in the TCU have the power to alter the behavior of the device to the attacker's advantage. By changing the properties of the transmission route, communication attacks can be either physical or virtual. Ports for input and output must be secured against these attacks.
   Security measure: One common method for preventing tampering attacks is the usage of data integrity checks by leveraging cryptographic hash functions. The ECU can calculate a cryptographic hash of the collected data and send it to the TCU. Upon receiving the data, the TCU recalculates the hash using the same algorithm and compares it. If they match, it indicates that the data has not been tampered with during transmission, securing both the outgoing and incoming communications. A trusted platform module (TPM) can be used for speeding up the encryption and decryption process using hardware acceleration.

7.2.2. Denial of Service

1. **Component**
   Security risk: If unauthorized individuals are able to perform DoS on the TCU, the attacker will be able to block all the outgoing and incoming vehicle communication. Moreover, the in-vehicle functions communicate with each other using the networking protocols enabled by the TCU, making the entire communication system not available.
   Security measure: The communication between the TCU and external devices can be equipped with frequency-hopping spread spectrum (FHSS), which is a technique for hopping between random radio frequencies in a short amount of time. Such hopping in frequency is used to send and receive data on changing carriers that can help block

DoS packages. The usage of hardware- or software-based solutions can be applied as an alternative to FHSS. A typical solution for preventing DoS attacks is the use of firewall-based applications that aim at preventing flooding attacks by detecting malicious traffic.

7.2.3. Elevation of Privilege

1. **Component**
   Security risk: The TCU is the component in the car in charge of external communication, so in charge of V2X. The attack path is either physically to the CAN bus, locally via OBD-II, or via a vulnerable network interface to the TCU. The access to the TCU provides read-only access to the information retrieved or sent by the TCU as well as possible lateral movement to other ECUs. An elevation-of-privilege attack towards the TCU allows the actor to change data or damage other connected devices or the TCU itself. Some motivations for such an attack range from clearing DTCs, reconfiguring parameters, enabling paid-only features, allowing lateral movements, or even damaging car electronics beyond repair (e.g., a ransomware attack).
   Security measure: The standard security controls for mitigating this risk are through authentication, role-based control, the least privilege principle, or multi-factor authentication.

7.2.4. Information Disclosure

1. **Ports and Communications**
   Security risk: Threats to the telematics control unit (TCU) component's information leakage may result in privacy concerns over the collection of sensitive information such as photographs shot with a camera. The most well-known attack in this area is the so-called man in the middle (MITM), which is carried out by listening to wireless transmission while utilizing a promiscuous antenna. One of the main hazards of information leakage is the packets collected in combination with bad data encryption.
   Security measure: MITM attacks cannot be avoided directly since a wireless channel is always available and can be listened to at any time, but some techniques can be used for obfuscating the content that flows on channels. Data encryption can be applied using a symmetric-key approach like Advanced Encryption Standard (AES) or session-key-based communication can be established between nodes in order to securely exchange data over the channel.

7.2.5. Repudiation

1. **Component**
   Security risk: In the event of an ongoing MITM attack targeting the TCU communication, the absence of non-repudiation techniques becomes a critical concern. This vulnerability opens the door for the attacker to either steal sensitive data or inject falsified information into the system. In the latter scenario, the system would incorporate these data alongside legitimate inputs, eroding its reliability and undermining its intended functionality. Consequently, both the optimal operation of the vehicle and the safety of the driver could be compromised, especially in the event of a serious incident necessitating the activation of the ACN.
   Security measure: Among the most potent strategies to establish non-repudiation is the implementation of digital signatures utilizing asymmetric keys issued by trusted third parties. This approach instills confidence in the message recipient regarding the origin of the content, ensuring its authenticity. Also, in this case, TPM can be used to reduce the overhead introduced with digital signatures.

7.3. Emergency Response Service

In both architectural frameworks, the ERS is implemented as a cloud service, necessitating a shared set of considerations and concerns. The cloud-based nature of this component and its relevance for speeding up the arrival of the emergency services make the threat analysis for both architectures quite similar.

7.3.1. Tampering

1. **Component**
   Security risk: ERS tampering leads to a deliberate delay or obstruction of responses to emergencies, dissemination of inaccurate information leading to incorrect decisions, misallocation of resources, and compromise of operational efficiency. The attacker engages in activities such as manipulating data, modifying processes, or changing communication channels within the emergency response team, that is, compromising the integrity of the ERS system.
   Security measure: Measures like implementing strong access controls to limit who can interact with the system, user authentication and authorization mechanisms, database integrity verification using cryptographic hashes and digital signatures, system logging and auditing which records every database modification, and network segmentation to shrink the attack surface by isolating critical system components can be used.
2. **Ports and Communication**
   Security risk: Tampering with ERS ports introduces both safety and privacy risks. If ERS is not able to correctly receive data, it will not be able to help the driver when needed. Moreover, considering the connection to the internet of such a component, many checks must be performed in order to avoid possible port tampering.
   Security measure: Like in the case of component analysis, in this case, possible countermeasures relate to authentication and traffic control. Securing the entire communication can prevent port tampering and reduce the overall risk.

7.3.2. Denial of Service

1. **Component**
   Security risk: A DoS performed on the ERS could lead to a situation where the service becomes unavailable, potentially preventing critical crash notifications. This could be due to overwhelming traffic, malicious attacks, or technical failures.
   Security measure: It is possible to prevent DoS attacks through multiple mechanisms that can be applied directly to the server. By enforcing rate limits on incoming requests, it is possible to prevent excessive traffic from a single source. By applying anomaly detection mechanisms, the system can identify unusual traffic patterns that could indicate an attack. web application firewall (WAF): Employ a WAF to filter and block malicious traffic before it reaches the web service. content delivery network (CDN): Use a CDN to distribute traffic and absorb distributed denial of service (DDoS) attacks, improving availability. Redundancy and failover: Set up redundant servers in different geographical regions and implement failover mechanisms to maintain service in case of a failure.
2. **Ports**
   Security risk: DoS attacks on ports are high risk because they disrupt critical network services, causing downtime, data loss, and financial harm. Limited resources, collateral damage, reputation loss, and potential legal consequences make these attacks highly damaging.
   Security measures: Network-level protection: Firewalls—deploy firewalls to filter incoming traffic and block suspicious or excessive requests to the ports. Intrusion detection/prevention systems (IDS/IPS)—use IDS/IPS systems to detect and prevent unauthorized access or abnormal traffic patterns. access control list (ACL)—configure ACLs on network devices to allow only legitimate traffic to reach the ports. Encryption and

authentication: Encryption—use encryption (e.g., hypertext transfer protocol secure (HTTPS)) to secure communication between clients and the web service, preventing unauthorized access and tampering. Authentication—install strong authentication mechanisms to ensure that only authorized users can access the service.

7.3.3. Elevation of Privilege

1. **Component**
   Security risk: Considering the huge number of ports that are typically opened on a server and the multiple exploitation shown for performing privilege escalation this threat is particularly relevant since an attacker might be able to change the server configuration in order to deny access to the emergency services.
   Security measure: A typical countermeasure could be the IDS and firewall, both aiming at reducing the possible attacks. Moreover, considering that privilege escalation is usually associated with database systems, a simple denying port service could be enough.

7.3.4. Spoofing

1. **Component**
   Security risk: Unauthorized persons can manipulate ERS components to intentionally trigger false crash notifications. This can lead to unnecessary deployment of emergency services, wasting resources, and causing confusion.
   Security measure: A possible mitigation may based on appropriate authentication mechanisms for the cloud.

7.3.5. Information Disclosure

1. **Ports**
   Security risk: In the event of compromised communication between an autonomous vehicle and emergency services, the outcome can be ineffective, potentially culminating in accidents, harm, or even loss of life.
   Security measure: Enable the vehicle to communicate via multiple technologies, such as cellular networks, dedicated short-range communication (DSRC), and satellite links. This minimizes the likelihood of total communication breakdown.

7.4. Cloud

In both architectural models, this layer serves the purpose of connecting with emergency services upon detecting and confirming an accident with the user. The Chang et al. [27] architecture incorporates an ML model to verify accident occurrences and subsequently communicate with emergency services, making this component critical for both privacy and security. On the other side, Kahliq et al. [28] limit the usage of the cloud to receive accident alerts, manage data packets, storage, visualization, and collaborate with authorities by sharing statistical insights to implement effective accident countermeasures.

7.4.1. Denial of Service

1. **Ports and Communication**
   Security risk: The cloud has a high-level of risk because the access vector is the network (the attacker only needs network access), and also because the operational impact is high. For example, if a crash occurs and the port is not working, the cloud will not be notified and this can result in bad consequences for the passengers.
   Security measures: A solution for this would be rate-limiting. Implementing a mechanism to limit the rate for the cloud can mitigate the risk level for denial of service of the cloud.

7.4.2. Spoofing

1. **Component**
   Security risk: If someone is spoofing the cloud, they can obtain access to it by pretending

they are someone else. The attacker can obtain data about the road user from the cloud. In some cases this can result in obtaining the user's passwords and infotainment. The privacy of the road user will be highly affected. Also, the risk can be considered high because the attack vector is high, so the attacker can obtain access to the cloud via the internet.
Security measures: Authentication can be a good solution for this attack. By implementing an authentication mechanism for the cloud, other entities cannot gain unauthorized access to the cloud.

7.4.3. Information Disclosure

1. **Component**
Security risk: The cloud has a high-level privacy risk because the attacker can potentially access the road user's data from an access vector due to the always available resource on the network (the attacker only needs network access). Regarding financial losses, the company can suffer financial losses depending on the stolen information.
Security measures: It is possible to leverage asymmetric encryption to protect road users data by encrypting them using a user private key, which can be exchanged with the legitimate destination of the data, or using proxy re-encryption [59], which is a special type of encryption. Such a technique allows a proxy (hosted in the cloud in our use case) to transform ciphertexts from one key to another without the proxy being able to learn any information about the original message. The cloud should implement encryption protection so that attackers cannot easily obtain access to the data.

7.5. WiFi

For both architectural paradigms, the WiFi module interfaces with the TCU yet assumes nuanced roles. In the Chang et al. [27] model, its function involves data reception from sensors while in the Kahliq et al. [28] design, the WiFi module's distinctive role lies in direct communication with the edge gateway.

7.5.1. Tampering

1. **Communications**
An attacker can gain unauthorized access to the communication between the vehicle's WiFi module sending data to the TCU, and thus tamper with the messages. Exploitation of this vulnerability can lead to the compromise of the vehicle software. Altered data reaching the WiFi module could significantly affect the operations: vehicle systems, performance, and operational decisions. Tampering with data exchange could expose or manipulate sensitive information, violating user privacy and security.
Security measures: Measures that can be implemented are data integrity checks and proper penetration testing. For data integrity, checks can use cryptographic hashing or digital signatures in order to verify the integrity of the data during transmission.

7.5.2. Denial of Service (DoS)

1. **Communications**
Security risk: If the attacker possesses knowledge about the network where the communication between the ERS and the vehicle occurs, they can execute a DoS attack by sending multiple packets to the ERS. The ERS not being able to receive information about an accident could have a severe impact on the road users' safety. Also, the operation of the entire ACN system is compromised.
Security measures: To mitigate the risk of this attack, firewalls and access control lists should be implemented in order to restrict communication between devices on the network. They would only allow necessary traffic to and from the ERS system. Other possible measures are rate limiting, load balancing, and anomaly detection.

7.5.3. Spoofing

1. **Component**
   Security risk: If the information exchange is not properly protected, the attacker can gain access to WiFi and execute a spoofing attack by exploiting the Bluetooth interface and then gain access to the TCU and then to the WiFi module. Spoofing might allow the manipulation of certain features by an unauthorized user, leading to major safety complications. On the privacy side, the attacker could trick users into sharing personal information, which could be used for identity theft and fraudulent activities.
   Security measures: In order to mitigate this risk, the latest security protocol should be implemented, wireless protected access (WPA3), which provides stronger encryption and protection against brute force attacks.

7.6. Edge Gateway

In the Khaliq et al. [28] architecture, the edge gateway assumes a crucial role in ensuring the safety of both the driver and passengers. This integral component is responsible for receiving collision event reports, refining the pertinent data, and subsequently forwarding it to the control room. Conversely, in the Chang et al. [27] architecture, an edge gateway is absent, with the WiFi module directly collecting data from the sensors.

7.6.1. Tampering

1. **Component**
   Security risk: The risk associated with tampering with the edge gateway presents a threat with far-reaching implications. In this context, the edge gateway lacks a validation mechanism for incoming information, leaving it vulnerable to being tampered with by malicious actors. This vulnerability opens the door for attackers to manipulate the information before it reaches the edge gateway, enabling them to introduce erroneous data into the system. This lack of integrity checks introduces a severe risk, as the compromised information could potentially mislead emergency services, causing incorrect actions to be taken based on the tampered-with data.
   Security measures: To counter the risk of data tampering, implementing data integrity verification mechanisms is essential. Employing techniques like message authentication codes media access controls (MACs) or digital signatures can ensure that the information received by the edge gateway remains unaltered and originates from a trusted source.

7.6.2. Denial of Service (DoS)

1. **Component**
   Security risk: The risk of denial of service (DoS) of edge gateway poses a critical threat with potentially severe consequences. In this context, an attacker with access to the WiFi network and sufficient resources can orchestrate a DoS attack, effectively overwhelming the edge gateway. By exploiting vulnerabilities such as those leading to a SYN flood attack, the attacker can inundate the edge gateway with a barrage of malicious requests. This vulnerability could lead to a severe disruption of service, rendering the edge gateway incapable of processing legitimate emergency requests.
   Security measures: Employing DDoS mitigation solutions can help detect and mitigate such attacks in real time. These solutions analyze incoming traffic patterns and automatically filter out malicious traffic, ensuring that legitimate requests reach the edge gateway. For example, implementing traffic monitoring and anomaly detection systems to identify unusual spikes in traffic patterns that could be indicative of a DoS attack.

7.6.3. Information Disclosure

1. **Component**
   Security risk: The vulnerability of information disclosure of the edge gateway presents a significant high-risk scenario. In this context, the edge gateway lacks encryption for

the information it receives, rendering it susceptible to man-in-the-middle attacks. This exposes a critical weakness in the system's security architecture, allowing attackers to intercept and potentially steal sensitive data during transmission. The absence of encryption heightens the risk of unauthorized access, potentially compromising the integrity of the emergency communication process and the confidentiality of the transmitted information.
Security measures: To mitigate the risk of information disclosure, it is imperative to implement robust encryption mechanisms. Encrypting the information transmitted to the edge gateway ensures that even if intercepted, the data remains unreadable to unauthorized parties, safeguarding the confidentiality and integrity of the communication.

7.6.4. Elevation of Privilege

1. **Component**
Security risk: If the attacker finds vulnerabilities in the authentication, for example, using a brute force attack or social engineering, they may be able to find out the password of the admin account. This leads to them gaining high-level privileges to the edge gateway. This could lead to a severe safety impact, like dispatching a fake call or denying the service. In order to isolate and fix the consequences of the attack, a lot of resources are consumed. The whole system could be compromised, and the attacker could obtain access to sensitive data.
Security measures: In order to mitigate the attack risk, strong access controls should be implemented to limit who can access the edge gateway. The principle of least privilege is recommended, ensuring that users only have the permissions necessary for their tasks. Also, firewalls can be deployed to filter incoming and outgoing traffic, blocking unauthorized access attempts.

7.6.5. Repudiation

1. **Component**
Security risk: If the edge gateway has multiple legitimate accounts, the attacker might gain access to one of them and compromise the non-repudiation principle. This attack may compromise the whole system and also cause a major privacy impact, as important data can be stolen.
Security measures: For mitigation, comprehensive logging of all relevant activities should be enabled on the edge gateway. Also, a trusted execution environment can be used, as well as multiple-factor authentication.

7.7. Camera

The camera component ensures that the surroundings and details of the accident will be known to the emergency services. In both architectures, the data acquired from the camera is sent for further processing along with the sensor data, causing potential privacy issues. Given the Khaliq et al. [28] architecture usage of many components to process the camera data before uploading it to the cloud, such a system could lead to more attacks compared to the other architecture.

7.7.1. Tampering

1. **Component**
Security risk: Tampering with the camera itself in an ACN system compromises the accuracy of the crash data, potentially leading to inaccurate emergency response, delayed aid, and challenges in insurance claims processing. This endangers lives, undermines accountability, and hampers the system's overall effectiveness.
Security measures: Physical tamper-evident enclosures: Implementing tamper-evident enclosures for cameras can deter unauthorized access. These enclosures are designed to show clear signs of tampering if someone tries to open or manipulate the camera, alerting administrators to potential breaches.

2. **Ports**
   Security risk: Tampering with the port connecting the ACN camera compromises the integrity of the data transmission, potentially leading to delayed or disrupted crash notifications. This can result in delayed emergency responses and hinder accurate accident reporting.
   Security measures: Intrusion detection algorithms that monitor the connection status and data flow through the ports can be implemented. Any abnormal patterns or unauthorized access attempts trigger alerts, allowing administrators to take appropriate action.

7.7.2. Denial of Service

1. **Component**
   Security risk: Denial of service attacks targeting the camera can disrupt crash data collection and transmission, leading to delayed or missed crash notifications. This compromises the emergency response, hampers insurance claims processing, and undermines the overall effectiveness of the ACN system.
   Security measures: intrusion prevention systems (IPS) can be deployed to track network traffic and detect patterns indicative of DoS attacks. The system can automatically block or mitigate traffic from suspected attackers, ensuring the camera's availability and data integrity.
2. **Ports**
   Security risk: Denial of service attacks targeting the port connecting the ACN camera disrupt data transmission, leading to delayed crash notifications and compromised emergency response efforts.
   Security measures: The implementation of rate limiting on incoming connections to the port can prevent overload on the port with excessive requests and reduce the risk of DoS attacks causing disruptions in data transmission.

7.7.3. Elevation of Privilege

1. **Component**
   Security risk: Elevation-of-privilege targeting of ACN camera systems is a significant concern as it allows unauthorized access to gain higher-level control, potentially compromising the integrity of accident data and system operations. This can lead to falsified crash reports, delayed emergency responses, and hindered insurance claims processing, undermining the overall effectiveness of ACN systems.
   Security measures: To mitigate this threat, multi-factor authentication (MFA) can be used. Implementing MFA requires users to provide many forms of verification before accessing ACN camera controls. This could include a combination of something they know (password), something they have (security token), or something they are (biometric data). MFA strengthens access controls and prevents unauthorized users from gaining elevated privileges, enhancing the security of the ACN camera system.

7.7.4. Repudiation

1. **Component**
   Security risk: Repudiation threats against ACN camera systems are a critical concern as they enable malicious users to deny their involvement in recorded incidents, leading to legal and accountability issues. This jeopardizes the reliability of accident data, emergency response efforts, and insurance claims, undermining the trustworthiness of ACN systems.
   Security measure: Implementing digital signatures for all captured crash data and maintaining comprehensive audit logs can counter repudiation attempts. Digital signatures provide a unique and verifiable identifier for each piece of data, ensuring its authenticity and origin. Audit logs record all interactions and changes made to the system, creating a trail of evidence that can be used to confirm the legitimacy of the

actions taken. These measures collectively deter users from denying their involvement in modifying or deleting crash data.

7.8. GPS

GPS is a relevant component for understanding the location of a user when an accident happens and consequentially for enhancing the efficiency of ERS. Despite being a critical component in both architectures, Figure 8 shows that the Khaliq et al. [28] architecture is vulnerable to more threats due to the absence of communication redundancy and the low-level communication protocol used.

Repudiation

1. **Component**
   Security risk: A critical risk lies in the potential compromise of non-repudiation within the GPS component of the ACN system, with implications that extend far beyond mere data manipulation. This vulnerability threatens the accuracy and reliability of crash event notifications, potentially leading to delayed or inadequate emergency responses and legal complications.
   Security measures: To mitigate this, the integration of robust cryptographic signatures, secure time synchronization, and immutable logs, combined with the use of hardware security modules (HSMs) and secure time synchronization protocols, bolsters the accuracy and veracity of GPS data. Digital certificates and public key infrastructure (PKI) facilitate trusted sender authentication, while anomaly detection and IPS monitor data streams for irregularities. Implementing redundant GPS sensors, frequent auditing, real-time data validation, and secure cross-referencing aligns with the security enhancements proposed in the system's architecture. These measures collectively ensure data integrity, origin verification, and effective operation of the ACN system while preserving user safety and privacy.

7.9. Machine Learning

In the architectural framework proposed by Chang et al. [27], ML is used. It serves the purpose of augmenting the precision of crash predictions. Conversely, this component introduces vulnerability to potential adversarial actions, such as data tampering. Instances of tampering with the collected data have the potential to induce inaccurate responses from the model, consequently posing risks to the well-being of the driver. The other architecture does not consider any ML model, decreasing the accuracy but enhancing the security.

7.9.1. Tampering

1. **Component**
   Security risk: The ML component is placed at a remote location and carries out the execution of algorithms to determine the initiation of an emergency response. Tampering with this component can lead to incorrect prediction, which means that some possible emergencies are not correctly detected. Typical attacks consist of data poisoning and other attacks which lead to confusing the model.
   Security measures: Data validation must be put in place by regularly validating the data used for training.
2. **Ports**
   Security risk: An attacker can tamper with the connection between the ML and the cloud via network, thus making it a high risk level. The safety of the passengers can be highly affected. For instance, if a crash occurs, the ML program will not be able to communicate with the cloud. In this situation, there will be a big financial impact because if there is a false alarm, sending out the emergency services still costs a lot.
   Security measures: The communication between the ML and the cloud can be ensured through encryption. Communication between the cloud and ML units should implement encryption mechanisms to ensure that the communication remains secure and unaltered.

7.9.2. Repudiation

1. **Component**
   Security risk: The absence of non-repudiation may assist a malevolent attacker in obtaining data from an untrustworthy source. This could have significant safety implications in the event of an accident, as the systems notifying the ERS might not be accessible, potentially leading to serious or even fatal injuries. Even without considering the security repercussions for the road users, the operational ramifications are also noteworthy. This is due to the fact that the lack of ACN continues to signify a significant failure of a core feature.
   Security measures: To mitigate the absence of non-repudiation, digital signatures remain one of the most potent methods. Thus, the machine learning service should incorporate asymmetric encryption for every data piece transmitted or received.

7.10. Privacy Measures

The evolution of automobiles has led to the collection of an increasingly amount of information about every aspect of the driving experience, prompting manufacturers of such technologies to deal with a large amount of sensitive information. This, in turn, makes privacy a fundamental aspect of the process of creating new technologies of this kind. Considering the privacy flaws highlighted in the previous subsection, some countermeasures must be taken into consideration when developing a privacy-by-design system. Constant vehicle geolocation captures every detail of users' daily routines and movements, making it possible for third parties to exploit this information. Moreover, data collection and processing can unveil extra personal and sensitive information such as contacts stored or, if using the ACN system, even images captured inside the car. This underscores the critical need to implement privacy countermeasures to safeguard this information.

Privacy by default is increasing the proactivity at the beginning of the developing stage, considering privacy not anymore as a passive activity, to be taken care of when privacy issues are detected, but before they happen. Consideration of privacy at an earlier stage is able to enhance **transparency**, so there will be open and clear communication about data collection. The driver must be informed about the collected data and must be able to stop the collection whenever they believe it is not necessary anymore. Moreover, data produced by vehicle systems are usually used by multiple parties, **data minimization** can be put in place so that the collected data will limited to what is necessary for specific functionalities. Another interesting property to be considered, especially for the architecture defined by Chang et al. [27] is **data anonymization**; this is particularly relevant for ML models where personal data are used to feed models. Among other properties, it is necessary to recall **user consent**, so the permission will be explicit and informed, **purpose binding**, so the data will be only used for the purposes explicitly communicated to the user during consent, **data portability**, so the user has the right to access and retrieve their personal data, and **the right to be forgotten**, so the user's entitled to have their personal data erased.

General Data Protection Regulation (GDPR) in Europe defines the way in which these methods are applied. To assess the risks and prevent threats in a proactive way, a model like LINDDUN can be considered:

- **Linkability**: Apparently unrelated data can be linked together to identify a person or reveal sensitive information.
- **Identifiability**: An individual can be identified through a collection of data.
- **Non-repudiation**: The ability of an individual to deny an action or event they have undertaken.
- **Detectability**: Detecting that a user's personal data has been collected and used without their consent.
- **Disclosure of information**: Collected data are disclosed to unauthorized third parties.
- **Unawareness**: The user is unaware that specific data are being collected.

- **Non-compliance**: The organization does not conform to privacy policies and laws.

Numerous privacy preservation strategies can be implemented to lower risks at various levels in light of the mentioned designs and related threats:

1. **Differential privacy**: Ensures that the addition or removal of a single individual's data does not significantly impact the results of a data analysis. It allows for the collection of aggregate information while minimizing the risk of identifying individual contributors.
2. **Synthetic data**: Generating artificial data that retains statistical properties of the original dataset, but does not contain actual sensitive information. This helps in sharing information for analysis while maintaining privacy.
3. **Homomorphic encryption**: An encryption that allows computations to be performed on encrypted data without decrypting it first, preserving privacy during data processing.
4. **Zero-knowledge proofs**: Allows it to be proved that a statement is true, without revealing any specific information about the statement itself.
5. **Trusted execution environments**: Secure hardware-based environments that ensure the confidentiality and integrity of computations and data even in the presence of potentially compromised software.
6. **Secure multiparty computation**: Enabling multiple parties to perform joint computations on their private data without revealing the actual data to each other.
7. **Private set intersection**: A cryptographic technique that allows the intersection of their datasets to be determined without sharing the actual data contained within them.
8. **Federated learning**: A machine learning approach where models are trained across decentralized devices or servers, allowing data to remain local and reducing the need for centralized data sharing.

These privacy enhancing technologies contribute to preserving privacy while enabling data analysis and processing, promoting a balance between utility and individual data protection.

8. Suggested Improvements

The realm of architectural and security improvements that collectively form an intricate web of defense mechanisms against the spectrum of threats looming over the ACN system needs continuous improvements because of the continuous enlargement of the threat panorama.

8.1. Encryption, Authentication, and Access Control

The ubiquitous integration of technologies such as BLE, WiFi, LTE, and the emerging 6G is able to enhance the reliability of automotive systems, but on the other side, it leads to an expansion of the attack surface. This expansion, as demonstrated in the threat assessment phase, mandates a comprehensive approach to secure these communication channels, thereby fortifying the ACN system against a diverse range of potential breaches. A very relevant branch of the literature is mainly focused on securing physical layers on heterogeneous networks [60,61]. Continuing the discourse, major improvements in the reliability of the solutions analyzed may be the implementation of satellite communication leading to the research undergoing for the sixth generation of cellular networks [62]. While this technology augments communication coverage, it introduces the need for meticulous implementation of encryption and authentication protocols [63].

By bolstering the security of satellite-based data exchanges, the ACN system's resilience against adversarial exploitation is substantially elevated. The narrative then shifts towards the inseparable duo of the TCU and ECU. In both the analyzed architectures, we can identify them as two potential single points of failure, but as these two core components are crucial for the correct behavior of the module, some redundancy-based mechanisms and fail-safe protocols [64] need to be adopted. These safeguards ensure that even in the event of the TCU or ECU being compromised, the ACN system maintains its operational efficacy. An essential facet of fortifying the communication security of the ACN

system, and more generally of automotive systems, resides in meticulous evaluation and streamlined elimination of redundant or unused features, such as Bluetooth connectivity when not essential. This pragmatic approach directly addresses the expansion of the attack surface, a concern paramount in contemporary vehicular cybersecurity. By meticulously examining and selectively deactivating features that are extraneous to the ACN system's core functionality, the potential vectors for malicious intrusion are substantially curtailed. This undertaking not only reduces the system's vulnerability but also enhances operational efficiency and elevates resource allocation. Moreover, this judicious removal of unnecessary features aligns seamlessly with the principle of minimalistic design, fostering a leaner, more secure vehicular architecture. Amidst these solutions, TPMs, as depicted in Figure 9, and more particularly HSMs emerge as potent tools [65,66]. These specialized hardware devices provide a secure enclave for cryptographic operations, safeguarding sensitive cryptographic keys from potential compromise. While the introduction of HSMs needs a careful assessment of cost and potential performance implications, their integration aligns seamlessly with the ACN system's security imperatives. Tailored to address the diverse demands of the vehicular environment, HSMs can be optimally deployed across varying components based on their performance requirements and specific contexts. Low-performance HSMs find their niche within components like sensors, where resource constraints and real-time demands are of paramount concern. Designed for efficiency, these HSMs provide a lightweight cryptographic solution that ensures data integrity and privacy for these critical data collection nodes. These low-performance HSMs strike a balance between robust security and the exigencies of low-power sensors, safeguarding data even in the face of constrained resources. Transitioning to the TCU, the complexities of this central hub need a high-performance HSM. This level of HSM offers elevated processing power, capable of handling intricate cryptographic operations while maintaining real-time performance. As the link of data aggregation and communication, the TCU's high-performance HSM ensures secure data transmission without compromising the operational efficiency demanded by the ACN system's dynamic environment. Situating itself between these two extremes, the medium-performance HSM finds its role in various intermediate components. This tier balances cryptographic processing power with efficiency, catering to components that require more processing capability than sensors but less than the TCU, like the ECU. By offering a scalable solution, the medium-performance HSM serves as a versatile cryptographic guardian across a spectrum of ACN system elements. On the first analyzed architecture, a major vulnerability is the misuse of the OBD-II system. In particular, the usage of the OBD-II system, a system meant for diagnostic purposes, is used to retrieve data about the car speed. This misuse can considered as a vulnerability, highlighting its potential for misuse in extracting vehicle speed data. This revelation underscores the urgency of instituting stringent access controls and authentication mechanisms for OBD-II interfaces [67]. By erecting these digital ramparts, it is possible to ensure the veracity of data exchanged and defend against potential unauthorized incursions. Authentication and authorization mechanisms stand as crucial gatekeepers within the ACN system. Their absence exposes the system to the risk of unauthorized access, data manipulation, and even malicious attacks. The usage of HSM, as shown in the previous subsection, is not limited to efficient encryption. These modules are able to guarantee key management, which could be a resolution for the problem of authentication in the automotive context. Decentralized key management enhances security by removing the need for a centralized server. Authorization can be achieved through the usage of a distributed ledger, such as blockchain [68], or a more classical system based on certification [69].

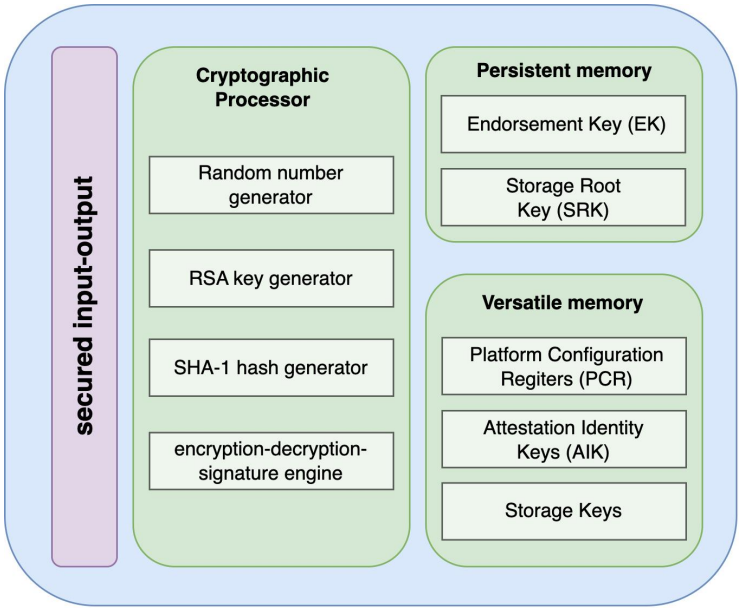

Figure 9. Trusted platform module (TPM) components.

8.2. Intrusion Detection System

Reinventing the security dynamics of the ACN system involves rethinking the approach to the traditional direct link between sensors and the ECU. To fortify this connection, the concept of zonal controllers equipped with filtering capabilities or IDS [70–72] emerges as a robust alternative. By sidestepping the direct linkage, potential vulnerabilities stemming from unfiltered data streams can thwarted. Zonal controllers act as vigilant gatekeepers, scrutinizing incoming data before transmitting it to the ECU, thus mitigating the risk of potentially malicious input and allowing for the definition of different security policies and controls for each zone, reducing the attack surface and enhancing overall security. Following this perspective, we can consider the incorporation of a controller area network (CAN) whitelist. This approach meticulously regulates communication access, repelling unauthorized entities and forming a proactive defense against intrusion attempts. It is through this measure that the foundation of security is established, ensuring the sanctity of data within the ACN system. Anyway, it is important to acknowledge that the implementation of zonal controllers introduces complexities in data management and latency. Another avenue to explore could involve decentralized processing, distributing some control functions across various vehicle components, potentially reducing the dependency on a single point of failure. The deployment of IDS further bolsters the security posture by actively monitoring data traffic for anomalous patterns that could indicate an incipient cyberattack. This architectural evolution not only heightens resilience but also amplifies the system's capacity to withstand intrusion attempts.

The dynamic landscape of modern cybersecurity offers a panoply of solutions tailored to the specific constraints of vehicular environments. Comprehensive cybersecurity solutions, ranging from privacy-preserving techniques like data pseudonymization and differential privacy to encryption both at rest and during transmission, can be artfully woven into the fabric of the ACN system's architecture. In summation, the principles of "privacy-by-design" and "security-by-default" emerge as cardinal tenets governing the cybersecurity paradigm of the ACN system [73]. This precept underscores the profound importance of integrating security considerations at the start of component development, thereby establishing a comprehensive foundation of protection against a dynamic array of cyber threats. Looking ahead, the transformative odyssey embarked upon by the ACN system serves as a poignant exemplar of the inextricable fusion between innovation and security. This trajectory charts a course toward a future where vehicular cybersecurity stands as an

intrinsic facet of technological progress, a vanguard of privacy preservation, user trust, and societal well-being.

9. Conclusions

This security analysis of an ACN system highlights the importance of robust cybersecurity measures within the automotive industry, particularly regarding functions within a car and the automatic notification system for crash incidents. As the automotive landscape rapidly evolves with the integration of advanced technologies, the potential benefits of such a system are undeniable: rapid and accurate crash detection, coupled with the immediate deployment of emergency response teams, holds the promise of saving countless lives. The interconnected nature of modern vehicles and their reliance on digital infrastructure make them susceptible to a number of cyber threats. Malicious actors could exploit vulnerabilities in the system to not only manipulate critical functions of the vehicle but also compromise the privacy and safety of vehicle occupants. To manage the cybersecurity risks, all product life-cycle phases must be covered: concept, development, production, operation, and maintenance. The usage of ISO/SAE 21434 provided a valuable tool for assessing the security of automotive architecture, paving the way for its usage on multiple systems, and possibly detecting all the risks of a given architecture. An average of 310 threats were detected using the TARA methodology in combination with ISO/SAE 21434, demonstrating its applicability also to individual architectures. Furthermore, the privacy concerns of an ACN system cannot be overlooked. As demonstrated by the study, personal data such as pictures of the user and continuous tracking using GPS can lead to critical threats from the information disclosure and snooping point of view. Handling personal data, including location and health information, demands a balance between emergency response efficacy and individual privacy. This balance requires transparent data usage policies, explicit user consent, and stringent access controls to prevent unauthorized use or abuse of sensitive information. Therefore, deeper analysis must be conducted on the following topics in order to improve and extend the current work:

1. **User privacy**: One of the first steps is to expand the scope of our analysis to consider how the system handles user data. This includes examining the practices for collecting, storing, and using data. It is important to look at how long data are retained and the potential for unauthorized access to these data. Decentralization solutions are expanding and can be provided by moving the data collected in the automotive context away from centralized servers, leveraging techniques related to user-centric data spaces.
2. **Ethical considerations**: It is not just about technology; there are ethical dimensions to securing the ACN system. This involves diving deep into the moral and societal consequences of our actions. We must consider the safety of users, their privacy rights, and our responsibility as system developers. Establishing ethical disclosure practices for vulnerabilities is critical to maintaining trust and transparency. Modifications to Equation (1) can be applied in order to add the ethical impact (EI) of the considered feature.
3. **Autonomous system and regulatory compliance**: We also need to ensure that our security measures align with legal and regulatory frameworks related to autonomous systems. This involves researching and understanding the specific rules and standards that apply to automated systems, which have always been characterized by privacy issues, such as in the case of GDPR. Compliance not only keeps us within the bounds of the law but also enhances security.
4. **Risk value determination**: The parameters considered in Equation (1) consider the same weight for all the impacts (safety, financial, operational and privacy), but in some cases this is not completely correct. For example, certain parameters can be

prioritized based on the application or business requirements, so that the equation can be modified as follows:

$$Risk = Avg(w_1S + w_2F + w_3O + w_4P) \times Feasibility \quad (2)$$

where $W = [w_1, w_2, w_3, w_4]$ is the vector containing the weight of each impact factor for the considered application. In such an approach, it is possible to give precise weight to each component of the risk value determination formula and conduct a more precise analysis. In addition, based on the requirements, impact (ethical as mentioned above) and feasibility analysis criteria can be added/updated.

By taking into consideration these points, it is possible to draw a complete picture of each system. An extension of ISO/SAE 21434 can be considered for including all these concerns, like in the case of financial risk assessment proposed in [74]. This comprehensive approach ensures that we protect user privacy, adhere to ethical principles, leverage advanced technology, meet legal requirements, and maintain continuous vigilance against evolving threats. Ultimately, the need for a more decentralized world that is able to preserve users' data paves the way for a user-centric automotive environment that prioritizes both cybersecurity and user safety.

Author Contributions: Conceptualization, T.G. and R.K.; data curation, M.R.; investigation, I.J.; methodology, T.G.; software, T.G.; supervision, C.E. and B.M.S.; validation, R.K.; writing—original draft, B.B., M.R. and I.J.; writing—review and editing, B.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research work was completed by the on-site participants of the 2nd version of Automotive Cybersecurity Academy (ACSA) (Weblink of ACSA 2023: https://www.autocybersec.ro/past-acsas/acsa-2023), 2023 which is funded by the European Commission as part of Erasmus+ Blended Intensive Program (BIP). Led by Prof. Dr. Rahamatullah Khondoker, Students, teachers, and researchers of the following universities and industries contributed in the BIP: University of Salerno in Italy, Technische Hochschule Mittelhessen in Germany, Politehnica University of Timișoara in Romania, University Politehnica of Bucharest in Romania, Hochschule Darmstadt in Germany, Technische Hochschule Ingolstadt in Germany, Continental Automotive Romania, CES Automotive in Germany, SAPAR in Germany, ARRK Europe Limited in Germany and HORIBA MIRA in United Kingdom. Appreciations to ANSYS and CADFEM Germany for providing us the free access of Ansys Medini Analyze. The work of 1st ACSA was published in MDPI journal [23].

Data Availability Statement: The data for the research area available at https://github.com/acsaeurope/acncomparison.

Acknowledgments: This work was performed in an Erasmus+ Blended Intensive Program (BIP) titled Automotive Cybersecurity Academy (ACSA) that was held in the University of Coimbra, Portugal, from 16 August 2023 to 30 August 2023. We would like to acknowledge all other contributors to this paper: Pranav Tetey, Aldo Claudini, Alexander Reusch, Antonio Cacciapuoti, Bathula Vamsi Krishna, Bighiu Tamara-Stefania, Andreea Dumitrescu, Krister Matteo Herban, Madalin Ostroveanu, Muhannad Umair Shakir, Tibor-David Olah, Emilio Schiavo, Sergio del Sorbo, Snehashis Nath, Somesh Teja Yerramsetty, Thevathas Mary Sutharshini, Ahsen Nur Karahan, Rui Pires, Pedro Afonso Ferreira Lopes Martins, João Carlos Borges Silva, Mário Guilherme de Almeida Martins Sequeira Lemos.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

AACN	advanced automatic collision notification
ACL	access control list
ACN	automatic collision notification
ADAS	advanced driver assistance system
AES	Advanced Encryption Standard
AI	artificial intelligence
BLE	Bluetooth low energy
BT	Bluetooth

CAN	controller area network
CDN	content delivery network
CMI	crash momentum index
CSI	crash severity index
CVSS	Common Vulnerability Scoring System
DDoS	distributed denial of service
DoS	denial of service
DSRC	dedicated short-range communication
DTC	diagnostic trouble code
GDPR	General Data Protection Regulation
eCall	emergency call
ECU	electronic control unit
EDR	event data recorder
EES	energy equivalent speed
EoP	elevation of privilege
ERS	emergency response service
FHSS	frequency-hopping spread spectrum
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSM	hardware security module
HTTPS	hypertext transfer protocol secure
I-V	in-vehicle
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IIHS	Insurance Institute for Highway Safety
IoT	internet of things
IoV	internet of vehicles
IPS	intrusion prevention systems
IR	impact response
ISO	International Organization for Standardization
IVI	in-vehicle infotainment
LoRa	long range
MAC	media access control
MEMS	micro-electro-mechanical system
MFA	multi-factor authentication
MITM	man in the middle
ML	machine learning
OBD	on-board diagnostics
OBU	on-board unit
OEM	original equipment manufacturer
OpenCV	Open Source Computer Vision Library
PCIs	pre-crash indicators
PHP	hypertext preprocessor
PKI	public key infrastructure
pre	previous
SAE	Society of Automotive Engineers
SecOC	secure on-board communication protocol
SMS	short message service
SQL	Structured Query Language
STRIDE	spoofing; tampering; repudiation; information disclosure; denial of service; elevation of privilege
TARA	threat analysis and risk assessment
TPM	trusted platform module
TCP	transmission control protocol
TCU	telematics control unit
UART	universal asynchronous receiver/transmitter
USB	universal serial bus
V2C	vehicle-to-cloud
V2I	vehicle-to-infrastructure
V2P	vehicle-to-pedestrian
V2V	vehicle-to-vehicle
V2X	vehicle-to-everything
WAF	web application firewall

References

1. Rahim, M.A.; Rahman, M.A.; Rahman, M.M.; Asyhari, A.T.; Bhuiyan, M.Z.A.; Ramasamy, D. Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Veh. Commun.* **2021**, *27*, 100285. [CrossRef]
2. Mahmood, Z. Connected vehicles in the IoV: Concepts, technologies and architectures. In *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–18.
3. Scanlon, J.M.; Sherony, R.; Gabler, H.C. Injury mitigation estimates for an intersection driver assistance system in straight crossing path crashes in the United States. *Traffic Inj. Prev.* **2017**, *18*, S9–S17. [CrossRef]
4. Spicer, R.; Vahabaghaie, A.; Bahouth, G.; Drees, L.; Martinez von Bülow, R.; Baur, P. Field effectiveness evaluation of advanced driver assistance systems. *Traffic Inj. Prev.* **2018**, *19*, S91–S95. [CrossRef] [PubMed]
5. *ISO/SAE 21434:2020*; Road Vehicles—Cybersecurity Engineering. International Organization for Standardization and Society of Automotive Engineers. Available online: https://www.iso.org/standard/71639.html (accessed on 1 October 2023).
6. Costantino, G.; De Vincenzi, M.; Matteucci, I. In-depth exploration of ISO/SAE 21434 and its correlations with existing standards. *IEEE Commun. Stand. Mag.* **2022**, *6*, 84–92. [CrossRef]
7. *ISO 26262:2018*; Road Vehicles—Functional Safety. International Organization for Standardization. Available online: https://www.iso.org/standard/68383.html (accessed on 1 October 2023).
8. Cui, J.; Liew, L.S.; Sabaliauskaite, G.; Zhou, F. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Netw.* **2019**, *90*, 101823. [CrossRef]
9. Ponte, G.; Ryan, G.A.; Anderson, R. Automatic Crash Notification. Tech. Report. Centre for Automotive Safety Research. 2013. Available online: https://casr.adelaide.edu.au/casrpubfile/1595/CASR124.pdf (accessed on 1 October 2023).
10. Khot, I.; Jadhav, M.; Desai, A.; Bangar, V. Go Safe: Android application for accident detection and notification. *Int. Res. J. Eng. Technol.* **2018**, *5*, 4118–4122.
11. Bonyár, A.; Géczy, A.; Krammer, O.; Sántha, H.; Illés, B.; Kámán, J.; Szalay, Z.; Hanák, P.; Harsányi, G. A review on current eCall systems for autonomous car accident detection. In Proceedings of the 2017 40th International Spring Seminar on Electronics Technology (ISSE), Sofia, Bulgaria, 10–14 May 2017; pp. 1–8. [CrossRef]
12. Cheah, M.; Shaikh, S.A.; Bryans, J.; Wooderson, P. Building an automotive security assurance case using systematic security evaluations. *Comput. Secur.* **2018**, *77*, 360–379. [CrossRef]
13. Tushara, D.B.; Vardhini, P.H. Wireless vehicle alert and collision prevention system design using Atmel microcontroller. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 2784–2787. [CrossRef]
14. Foggia, P.; Saggese, A.; Strisciuglio, N.; Vento, M.; Petkov, N. Car crashes detection by audio analysis in crowded roads. In Proceedings of the 2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Karlsruhe, Germany, 25–28 August 2015; pp. 1–6. [CrossRef]
15. Gu, C.; Xu, J.; Li, S.; Gao, C.; Ma, Y. Injury Risk Assessment and Interpretation for Roadway Crashes Based on Pre-Crash Indicators and Machine Learning Methods. *Appl. Sci.* **2023**, *13*, 6983. [CrossRef]
16. Tiusanen, R.; Malm, T.; Ronkainen, A. An overview of current safety requirements for autonomous machines—Review of standards. *Open Eng.* **2020**, *10*, 665–673. [CrossRef]
17. Debouk, R. Review of the Latest Developments in Automotive Safety Standardization for Driving Automation Systems. *J. Syst. Saf.* **2023**, *58*, 40–45. [CrossRef]
18. *ISO/PAS 21448:2019*; Road Vehicles—Safety of the Intended Functionality. Publicly Available Specification; International Organization for Standardization. Available online: https://www.iso.org/standard/70464.html (accessed on 1 October 2023).
19. Kirovskii, O.; Gorelov, V. Driver assistance systems: Analysis, tests and the safety case. ISO 26262 and ISO PAS 21448. In *Proceedings of the IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2019; Volume 534, p. 012019.
20. Kramer, B.; Neurohr, C.; Büker, M.; Böde, E.; Fränzle, M.; Damm, W. Identification and quantification of hazardous scenarios for automated driving. In *International Symposium on Model-Based Safety and Assessment*; Springer: Cham, Switzerland, 2020; pp. 163–178.
21. Madala, K.; Avalos-Gonzalez, C.; Krithivasan, G. Workflow between ISO 26262 and ISO 21448 standards for autonomous vehicles. *J. Syst. Saf.* **2021**, *57*, 34–42. [CrossRef]
22. Tabani, H.; Kosmidis, L.; Abella, J.; Cazorla, F.J.; Bernat, G. Assessing the adherence of an industrial autonomous driving framework to iso 26262 software guidelines. In Proceedings of the 56th Annual Design Automation Conference 2019, Las Vegas, NV, USA, 2–6 June 2019; pp. 1–6.
23. Tany, N.S.; Suresh, S.; Sinha, D.N.; Shinde, C.; Stolojescu-Crisan, C.; Khondoker, R. Cybersecurity Comparison of Brain-Based Automotive Electrical and Electronic Architectures. *Information* **2022**, *13*, 518. [CrossRef]
24. White, J.; Thompson, C.; Turner, H.; Dougherty, B.; Schmidt, D. WreckWatch: Automatic Traffic Accident Detection and Notification with Smartphones. *Mob. Netw. Appl.* **2011**, *16*, 285–303. [CrossRef]
25. Choi, H.Y.; Han, I.S.; Lee, J.W.; Shin, J.K. Development of ACNS in Korea. In Proceedings of the 22nd International Technical Conference on the Enhanced Safety of Vehicles (ESV) National Highway Traffic Safety Administration, Washington, DC, USA, 13–16 June 2011.
26. Topinkatti, A.; Yadav, D.; Kushwaha, V.S.; Kumari, A. Car accident detection system using GPS and GSM. *Int. J. Eng. Res. Gen. Sci.* **2015**, *3*, 1025–1033.

27. Chang, W.J.; Chen, L.B.; Su, K.Y. DeepCrash: A Deep Learning-Based Internet of Vehicles System for Head-On and Single-Vehicle Accident Detection With Emergency Notification. *IEEE Access* **2019**, *7*, 148163–148175. [CrossRef]
28. Khaliq, K.A.; Chughtai, O.; Shahwani, A.; Qayyum, A.; Pannek, J. Road accidents detection, data collection and data analysis using V2X communication and edge/cloud computing. *Electronics* **2019**, *8*, 896. [CrossRef]
29. Fogue, M.; Garrido, P.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. Using data mining and vehicular networks to estimate the severity of traffic accidents. In *Management Intelligent Systems: First International Symposium*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 37–46.
30. Hassan, A.; Abbas, M.S.; Asif, M.; Ahmad, M.B.; Tariq, M.Z. An Automatic Accident Detection System: A Hybrid Solution. In Proceedings of the 2019 4th International Conference on Information Systems Engineering (ICISE), Shanghai, China, 4–6 May 2019; pp. 53–57. ISSN 2643-7309. [CrossRef]
31. Sharma, H.; Reddy, R.K.; Karthik, A. S-CarCrash: Real-time crash detection analysis and emergency alert using smartphone. In Proceedings of the 2016 International Conference on Connected Vehicles and Expo (ICCVE), Seattle, WA, USA, 12–16 September 2016; pp. 36–42. [CrossRef]
32. Manoharan, R.; Balamurugan, G.; Rajmohan, B. Enhanced automated crash reporting system in vehicles based on SMS & MMS with Fish eye CAM camera. In Proceedings of the 2012 International Conference on Radar, Communication and Computing (ICRCC), Tiruvannamalai, India, 21–22 December 2012; pp. 307–311. [CrossRef]
33. Mohith, M.; Rahul, S.; Kumar, R. A Novel Internet of Things Assisted Car Accident Prevention and Alert System using an Intelligent Distance Measurement Sensor. In Proceedings of the 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 5–6 May 2023; pp. 1–6. [CrossRef]
34. Parmar, K.; Solanki, D.; Sangada, J.; Parekh, R. Accident Detection and Notification System Using AWS. In Proceedings of the 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 4–6 August 2021; pp. 1468–1476. [CrossRef]
35. Fernandes, B.; Alam, M.; Gomes, V.; Ferreira, J.; Oliveira, A. Automatic accident detection with multi-modal alert system implementation for ITS. *Veh. Commun.* **2016**, *3*, 1–11. [CrossRef]
36. Pal, C.; Hirayama, S.; Sangolla, N.; Manoharan, J.; Kulothungan, V. A new approach in improving traffic accident injury prediction accuracy. *Int. J. Automot. Eng.* **2017**, *8*, 179–185. [CrossRef]
37. Alwan, Z.; Alshaibani, H. Car Accident Detection and Notification System Using Smartphone. *Int. J. Comput. Sci. Mob. Comput.* **2015**, *4*, 620–635.
38. Bhavana, K.; Munappa, S.; Bhavani, K.D.; Deshmanth, P.; Swathi, A.; Vanga, S.R. Automatic Pothole and Humps on Roads Detection and Notification Alert. In Proceedings of the 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2–4 March 2023; pp. 1–6.
39. Miyoshi, T.; Koase, T.; Nishimoto, T.; Ishikawa, H. *Evaluation of Threshold Used by Advanced Automatic Collision Notification System For Dispatching Doctors to Accident Sites*; National Highway Traffic Safety Administration: Washington, DC, USA, 2019; pp. 1–12.
40. Outay, F.; Bargaoui, H.; Chemek, A.; Kamoun, F.; Yasar, A. The COVCRAV project: Architecture and design of a cooperative V2V crash avoidance system. *Procedia Comput. Sci.* **2019**, *160*, 473–478. [CrossRef]
41. Abdul Razak, S.F.; Suhaimi, F.A.; Yogarayan, S.; Abdullah, M.F.A. 2-Phase Crash Detection and Notification System. *J. Logist. Inform. Serv. Sci.* **2022**, *9*, 258–270.
42. Chen, L.; Englund, C. Every second counts: Integrating edge computing and service oriented architecture for automatic emergency management. *J. Adv. Transp.* **2018**, *2018*, 1–13. [CrossRef]
43. Manuja, M.; Kowshika, S.; Narmatha, S.; Theresa, G. IoT based automatic accident detection and rescue management in Vanet. *SSRG Int. J. Comput. Sci. Eng.* **2019**, *2*, 36–41.
44. Boehme, M.; Stang, M.; Muetsch, F.; Sax, E. Talkycars: A distributed software platform for cooperative perception. In Proceedings of the 2020 IEEE Intelligent Vehicles Symposium (IV). IEEE, Las Vegas, NV, USA, 19 October 2020–13 November 2020; pp. 701–707.
45. Ribeiro, B.; Nicolau, M.J.; Santos, A. Using Machine Learning on V2X Communications Data for VRU Collision Prediction. *Sensors* **2023**, *23*, 1260. [CrossRef] [PubMed]
46. Prathiba, S.B.; Raja, G.; Kumar, N. Intelligent cooperative collision avoidance at overtaking and lane changing maneuver in 6G-V2X communications. *IEEE Trans. Veh. Technol.* **2021**, *71*, 112–122. [CrossRef]
47. Iyoda, M.; Trisdale, T.; Sherony, R.; Mikat, D.; Rose, W. Event data recorder (EDR) developed by Toyota Motor Corporation. *SAE Int. J. Transp. Saf.* **2016**, *4*, 187–201. [CrossRef]
48. Sahil, M.Y.S.S.M.; Kumathekar, A.P.A.S.; Deshmukh, P.S. Vehicle Crash Alert System. *Int. J. Sci. Res. Eng. Trends* **2019**, *5*, 2269–2271.
49. Matuszczyk, G.; Åberg, R. Smartphone Based Automatic Incident Detection Algorithm and Crash Notification System for All-Terrain Vehicle Drivers. 2016; pp. 1–90. Available online: https://odr.chalmers.se/server/api/core/bitstreams/25193c95-c7b9-40dc-a2f6-daf2fa06b491/content (accessed on 1 October 2023).
50. Nassar, L.; Kamel, M.S.; Karray, F. VANET IR-CAS for Safety ACN: Information Retrieval Context Aware System for VANET Automatic Crash Notification Safety Application. *Int. J. Intell. Transp. Syst. Res.* **2016**, *14*, 127–138. [CrossRef]
51. Pareek, S.; Shanmughasundaram, R. Implementation of Broadcasting Protocol for Emergency Notification in Vehicular Ad hoc Network(VANET). In Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018; pp. 1032–1037. [CrossRef]

52. Kathiravan, M.; Reddy, M.P.K.; Malarvel, M.; Amrutha, A.; Reddy, P.H.; Kavitha, S. IoT-based Vehicle Surveillance and Crash Detection System. In Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 9–11 May 2022; pp. 1523–1529.
53. Mukerji, A.; Chakraborty, R.; Chatterjee, K.; Banerjee, S. Design, modeling and fabrication of an efficient car crash management system. *PREPARE@u® | Gen. Prepr. Serv.* **2019**, *1*. [CrossRef]
54. Blancou, J.; Almeida, J.; Fernandes, B.; Silva, L.; Alam, M.; Fonseca, J.; Ferreira, J. eCall++: An enhanced emergency call system for improved road safety. In Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016; pp. 1–8. [CrossRef]
55. Jose, S.K.; Mary, X.A.; Mathew, N. Arm 7 based accident alert and vehicle tracking system. *Int. J. Innov. Technol. Explor. Eng.* **2013**, *2*, 93–96.
56. Sammarco, M.; Detyniecki, M. Crashzam: Sound-based Car Crash Detection. In Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018), Funchal, Portugal, 16–18 March 2018; pp. 27–35.
57. Khaliq, K.A.; Qayyum, A.; Pannek, J. Prototype of automatic accident detection and management in vehicular environment using VANET and IoT. In Proceedings of the 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Malabe, Sri Lanka, 6–8 December 2017; pp. 1–7.
58. Razdan, R. *Unsettled Issues Regarding Autonomous Vehicles and Open-source Software*; Technical Report, SAE Technical Paper; SAE International: Warrendale, PA, USA, 2021.
59. Green, M.; Ateniese, G. Identity-based proxy re-encryption. In Proceedings of the Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, 5–8 June 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 288–306.
60. Kakkar, A. A survey on secure communication techniques for 5G wireless heterogeneous networks. *Inf. Fusion* **2020**, *62*, 89–109. [CrossRef]
61. Wang, D.; Bai, B.; Lei, K.; Zhao, W.; Yang, Y.; Han, Z. Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. *IEEE Access* **2019**, *7*, 54508–54521. [CrossRef]
62. Chen, S.; Sun, S.; Kang, S. System integration of terrestrial mobile communication and satellite communication—The trends, challenges and key technologies in B5G and 6G. *China Commun.* **2020**, *17*, 156–171. [CrossRef]
63. Liu, Y.; Ni, L.; Peng, M. A secure and efficient authentication protocol for satellite-terrestrial networks. *IEEE Internet Things J.* **2022**, *10*, 5810–5822. [CrossRef]
64. Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–39. [CrossRef]
65. Xie, Y.; Guo, Y.; Yang, S.; Zhou, J.; Chen, X. Security-related hardware cost optimization for CAN FD-based automotive cyber-physical systems. *Sensors* **2021**, *21*, 6807. [CrossRef] [PubMed]
66. Xie, Y.; Zhou, Y.; Xu, J.; Zhou, J.; Chen, X.; Xiao, F. Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges. *Softw. Pract. Exp.* **2021**, *51*, 2108–2127. [CrossRef]
67. Humayed, A. An Overview of Vehicle OBD-II Port Countermeasures. In *International Conference on Interactive Collaborative Robotics*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 256–266.
68. Ali, G.; ElAffendi, M.; Ahmad, N. BlockAuth: A blockchain-based framework for secure vehicle authentication and authorization. *PloS ONE* **2023**, *18*, e0291596. [CrossRef]
69. Krishnan, A.; Shyjila, P.; Kizhakethottam, J.J. Electronic-secure Vehicle Authorization Mechanism (e-SVAM). *Procedia Technol.* **2016**, *25*, 318–325. [CrossRef]
70. Lampe, B.; Meng, W. IDS for CAN: A practical intrusion detection system for CAN bus security. In Proceedings of the GLOBECOM 2022-2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 1782–1787.
71. Lokman, S.F.; Othman, A.T.; Abu-Bakar, M.H. Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–17. [CrossRef]
72. Islam, R.; Refat, R.U.D. Improving CAN bus security by assigning dynamic arbitration IDs. *J. Transp. Secur.* **2020**, *13*, 19–31. [CrossRef]
73. Liu, N.; Nikitas, A.; Parkinson, S. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transp. Res. Part Traffic Psychol. Behav.* **2020**, *75*, 66–86. [CrossRef]
74. Oberti, F.; Sanchez, E.; Savino, A.; Parisi, F.; Di Carlo, S. PSP Framework: A novel risk assessment method in compliance with ISO/SAE-21434. *arXiv* **2023**, arXiv:2305.05309.