IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 June 2022, accepted 24 July 2022, date of publication 4 August 2022, date of current version 11 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3196346

RESEARCH ARTICLE

Post-Accident Cyberattack Event Analysis for Connected and Automated Vehicles

MANSI GIRDHAR[1], (Graduate Student Member, IEEE),
YONGSIK YOU[2], (Graduate Student Member, IEEE), TAI-JIN SONG[2], (Member, IEEE),
SUBHADIP GHOSH[1], (Graduate Student Member, IEEE),
AND JUNHO HONG[1], (Member, IEEE)
[1]Department of Electrical and Computer Engineering, University of Michigan–Dearborn, Dearborn, MI 48128, USA
[2]Department of Urban Engineering, Chungbuk National University, Cheongju 28644, South Korea

Corresponding author: Tai-Jin Song (tj@chungbuk.ac.kr)

This work was supported by the Korea Institute of Policy Technology (KIPoT) Grant by the Korean Government through the Korean National Police Agency (KNPA), Development of a Data Extraction and Analysis System for Data Storage System (DSSAD), under Grant 092021D74000000.

ABSTRACT Smart mobility is an imperative facet of smart cities, and the transition of conventional automotive systems to connected and automated vehicles (CAVs) is envisioned as one of the emerging technologies on urban roads. The existing AV mobility environment is perhaps centered around road users and infrastructure, but it does not support future CAV implementation due to its proximity with distinct modules nested in the cyber layer. Therefore, this paper conceptualizes a more sustainable CAV-enabled mobility framework that accommodates all cyber-based entities. Further, the key to a thriving autonomous system relies on accurate decision making in real-time, but cyberattacks on these entities can disrupt decision-making capabilities, leading to complicated CAV accidents. Due to the incompetence of the existing accident investigation frameworks to comprehend and handle these accidents, this paper proposes a 5Ws and 1H-based investigation approach to deal with cyberattack-related accidents. Further, this paper develops STRIDE threat modeling to analyze potential threats endured by the cyber-physical system (CPS) of a CAV ecosystem. Also, a stochastic anomaly detection system is proposed to identify the anomalies, abnormal activities, and unusual operations of the automated driving system (ADS) functions during a crash analysis.

INDEX TERMS CAV-enabled transport mobility environment, cybersecurity, STRIDE threat modeling, accident investigation.

I. INTRODUCTION

The world is witnessing the fourth industrial revolution, which is largely driven by the convergence of increased connectivity and smart automation [1]. There have been several breakthrough innovations in the emerging disciplines, e.g., artificial intelligence (AI), internet of things (IoTs), fifth-generation wireless technologies, and fully autonomous vehicles (AVs). In order to automate processes, AI is replacing human capabilities with technology (e.g., industrial robots) to achieve significant performance improvements, reducing safety hazards [2].

CAVs are perceived as a revolutionary advancement that is associated with many potential benefits, e.g., reduced traffic congestion, improved road safety, and high degrees of transportation efficiency [3]. Also, the auto industry has now begun to transition away from conventional internal combustion engine-based vehicles (ICEVs) to electric vehicles (EVs) for better carbon emission benefits and to enable green mobility [4]. Notably, the connected and automated driving system (CADS) has been a focal point of extensive analysis among evolving technologies [5]. Therefore, in recent years, transportation engineers and researchers have performed comprehensive research to facilitate the development and integration of this transformative technology onto roadways.

Many business verticals or original equipment manufacturers (OEMs), e.g., General Motors (GM), Google's Waymo, Honda, Tesla, Toyota, and Uber, are spending billions on research and development of CAVs, although suffering

The associate editor coordinating the review of this manuscript and approving it for publication was Jjun Cheng.

serious setbacks [6]. Waymo [7], which shares a parent company with Google, became the first service provider to offer driverless taxi rides in the form of robo-taxi service to the public in Phoenix, Arizona in 2020.

In general, CAV is a safety-critical system consisting of a myriad of heterogeneous components, both cyber and physical, which pose serious security challenges [8]. It is very important to understand different environment dynamics to evaluate the CAV operating principle. Compared to the traditional automobile traffic system, which includes the physical interactions between its three core elements (i.e., automobile, driver, and road infrastructure), digital transformation enables the CAV system to establish these interactions via data and services. However, in the current era of autonomous driving, we are accelerating autonomous cooperative driving by equipping the CAV ecosystem with communication concepts (e.g., vehicle-to-everything (V2X)). AVs currently running on the roads are at SAE L2, and some manufacturers are also mass-producing L3 self-driving cars. For the current paper, the vehicles under consideration are assumed to be SAE L4. The Society of Automotive Engineers (SAE) J3016 clearly defines the degree of L4 vehicle as high driving automation, which does not require any human interaction in the vehicle's operation in the event of system failure when the automated driving features are engaged. Moreover, the realistic target for L4 CAV will most likely be on EVs, considering the global acceptance of carbon neutrality and accelerated pace of EV design and manufacturing amongst the OEMs. Hence, bi-directional interactions between the utility distribution grids, EVs, and charging infrastructure, e.g., EV chargers (EVCs)and EV charging stations (EVCSs), are critical areas to analyze [9]. It also includes crucial data exchange between the cooperative intelligent transport system (C-ITS) center and infrastructure behaviors that highly impact the performance of a CAV [10].

Besides the advantageous aspects of the revolutionary technology, e.g., energy savings, overall traffic flow efficiency, mobility for the disabled, and improvements in social cohesion, CAV offers safety-critical issues at the same time. AVs are becoming more pervasive with the continuous technology refinement, but safety is a significant deterrent factor toward their adoption. Contrary to the claims, CAVs currently have a higher rate of accidents than human-driven cars. On average, there are 9.1 AV car accidents per million miles driven, while the same rate is 4.1 crashes per million miles for regular motor vehicles [11]. Although the introduction of AVs has the effect of reducing traffic accidents caused by human factors, AVs are not safe from external threats [12]. The concept of autonomous driving revolves around a CAV's capabilities to understand its environment and respond to the dynamic events of the environment, which is designated as the vehicle's perception or situational awareness [13]. Since various data and AI drive the decision-making processes of a CAV, the system malfunctioning and cybersecurity have turned out to be the most critical aspects to determine safety and security. Cybersecurity variables and situations are alien to the CAV machine learning (ML) algorithms, so relying on physical and logical mechanisms may not suffice to achieve the goals of CADS. As a result, system failures and CAV accidents caused by a cyberattack could be deadly and may lead to casualties, loss of property, or even deaths.

Also, it is ambiguous how a CAV can cope with different situations and environments in the presence of several cybersecurity threats that might interrupt its functioning. Moreover, cyber-induced CAV crash investigation in such a complex urban environment becomes very tedious and challenging.

The key contributions of this paper are: (1) development of a connected mobility environment (e.g., vehicle, transportation, and power grid) for a CAV, (2) STRIDE threat modeling to analyze the cybersecurity events causing a CAV crash, along with the mitigation measures, (3) development of a post-accident investigation framework based on 5Ws and 1H models, and (4) proposition of a probability-based anomaly detection system during a CAV crash investigation. This paper also offers some parametric variations to differentiate the automated levels defined by the SAE, although it is not currently within the scope of the SAE J3016. This can be considered to be a pragmatic step forward in the AV industry.

The remaining parts of this paper are structured as follows:

Section II briefly summarizes some of the related works. Section III discusses the automation levels defined by SAE along with the distinguishing aspects of the automated levels. Section IV outlines the CPS of the proposed traffic mobility environment. Section V outlines the accident mechanisms induced by cyber incidents on various environmental entities. In addition, it presents existing threat modeling techniques in the automotive sector, with an extensive application of STRIDE to analyze different cybersecurity vulnerabilities as well as mitigation actions. Further, a digital forensic investigation framework based on 5Ws and 1H to find the causes and effects of a crash is discussed in Section VI. Section VII proposes an anomaly detection model to identify the abnormal behavior of an ADS function responsible for causing the crash. Section VIII analyzes the performance of the proposed frameworks by engaging some case studies of cyberattacks on EVCS and C-ITS technology. Finally, Section IX concludes the paper along with the limitations and recommendations for future work.

II. LITERATURE SURVEY

Although there has been some dedicated research done on different automobile mobility environments in the literature, there are huge gaps that have not been fully addressed for an intelligent CAV environment. There have been several digital architectures proposed in the past to model the mobility environment of a CAV. To substantiate, [14] introduces a typical dedicated short-range communication (DSRC)-based architecture of a connected vehicle (CV), which consists mainly of on-board units (OBUs), roadside units (RSUs), and a DSRC communication protocol. Reference [15] supports the Third Generation Partnership Project (3GPP) New Radio (NR) Release 16 sidelink as the building block of advanced V2X services, e.g., vehicles platooning, extended sensors, advanced driving, and remote driving. This infrastructure includes communication from vehicle-to-vehicle (V2V), pedestrian (V2P), RSU, and application server. However, in [13], a number of dynamics of the complex urban environments are visualized by exploiting either direct PC5 or indirect 5G/LTE-V/DSRC communication. Further, it provides details of road infrastructure and communication infrastructure for cooperative, connected, and automated mobility (CCAM). A model based on connected cars, automated driving, car sharing, and electrification as the primary components of the mobility environment is specified in [16]. The work proposed in [17] develops a conceptual framework that highlights the concept of shared and electric mobility in which the infrastructure, services, and data management centers are interconnected with the development of digital technology. An IoT-based architecture is explained in [18] that supports different wireless communication modes such as V2V, vehicle-to-infrastructure (V2I), V2P, and vehicle-to-sensor. Reference [19] proposes a cognitive advanced driver assistance system (ADAS) architecture for L4 autonomous-capable EVs that assimilates cloud, central ADAS management system, electrified powertrain, V2I, and V2V communication.

While all these architectures present a good high-level representation of the traffic environments, cyber components of the power grid and charging infrastructure are not explained as a part of the systems. The conventional AV driving environment does not include the necessary ingredients and asks for the upgrade of existing assets (e.g., network infrastructure, cloud infrastructure, and vehicles) to achieve the objectives of higher automation levels. Therefore, this paper envisions a novel and comprehensive mobility environment for a hyper-connected CAV that encompasses important primary entities. As a result, it correlates the security of a specific CAV system with the security of all the subsystems. For instance, any erroneous cyber interactions may lead to an unexpected situation with a huge impact (accident/crash) in a CAV environment. The intention of the proposal is not only to support the existing vehicle automation levels but also to gear the discussion toward the future L4 CAVs and above.

AV cybersecurity comprises both functional security and driving automation system (DAS) security. Although international standards ISO 26262, SAE J3061, and ISO 21434 provide guidelines for the functional safety and functional security of conventional road vehicles (on-board electrical and electronic systems), respectively [20], these standards are not created for AV-specific functionalities. For DAS safety, some recent standards, e.g., UL4600 [21] and SOTIF [22], have been developed. Although there are no AV-specific cybersecurity regulations yet, UNECE WP.29/vehicle cybersecurity regulation requires vehicle approval authority to ensure a holistic analysis encompassing ISO 26262-2018 (functional safety), ISO/PAS 21448 (SOTIF), and ISO/SAE 21434 (cybersecurity of E/E systems).

Further, cyberattack patterns on critical infrastructures, especially CAVs, are evolving and diversifying, indebted to the IoT paradigm, which has infused innumerable vulnerabilities. The perpetrators might use these existing vulnerabilities of the CAV ecosystem to compromise the system (jeopardizing its security). For instance, a CAV owner may lose the availability of the EV charging process due to a denial of service (DoS) attack. The severe implications incurred by the adversarial attacks have triggered a broad interest of white-hat hackers and researchers to address the cybersecurity aspects of the CAVs. Kaspersky Lab researchers exposed the software vulnerabilities of EVCSs that make them accessible to unauthorized hackers [23]. Furthermore, well-trained attackers could initiate instability problems in the power grid by compromising CAV security (e.g., shut off multiple high-power EV chargers). So, this paper elaborates the complex mechanism of a CAV accident that may be caused due to multiple trigger conditions in its ecosystem along with the application of threat modeling tools to identify different cyber threats.

Post-accident analysis refers to the object of the investigation team to identify the cyber factors responsible for the disengagement or crash. There have been earlier investigation tools, but they do not include the cybersecurity aspects. For example, as of February 9, 2022, the California AV collision report cites various causal factors for AV disengagement or collision, e.g., incorrect perception of a traffic signal, degrading localization, map discrepancy, reduced visibility due to occlusions, and other hardware health issues [24]. However, it does not refer to the cyber-related anomalies. Further, with an inclusion of cloud, grid, and charging infrastructure in the CAV environment, the probability that a CAV crash can be caused increases. There are multiple cybersecurity frameworks being developed for power grids, but they do not support either EVCSs or CAVs. Also, we have the iISO 12353-1 standard for conventional road vehicles and traffic accident analysis, but it does not cover CAVs [25]. So, post-collision investigation of CAVs may not be done with the existing frameworks or algorithms as they are unable to identify the cyber factors liable for causing an accident. As a result, there is a need to develop solutions that can be used by all relevant actors in an interconnected CAV environment. So, this paper lays out a digital forensic investigation model that law enforcement may use to reconstruct the crash scenarios in the highly complex CAV environment.

III. SAE VEHICLE AUTOMATION LEVELS

In 2014, SAE published the J3016 standard that classifies six levels of ADS, which was updated significantly in collaboration with the ISO in 2021 [26]. This standard is accepted by regulatory bodies like UNECE WP.29/GRVA [27], NHTSA, US DOT [28], and California DMV [24] as well as by the key players of AV standardization like ISO/PAS 21448-SOTIF [22], ISO 34501 [29], ISO 34502 [30], ISO 34503 [31], UL4600 [21], IAMTS, and ASAM [32] to create other standards, laws and guidelines for AVs. It is stated that the driving system is described by the word ''automation''. However, several complex terms such as ''Automation System'', ''Automated Driving'', and ''Driving Automation'' are used in SAE J3016 and presented differently such as ''Automated Driving System'' (NHTSA, 2016) and ''Autonomous Driving System'' [33]. Therefore, before developing the research process, this study intends to define ''autonomy'' and ''automation.'' The dictionary definition of ''automation'' is ''made to be written by a machine or computer in order to reduce the work done by humans'' (Cambridge Dictionary). ''Automated systems'' in vehicles cannot yet drive reliably and safely in all traffic scenarios and situations that occur on the road, and the driver does not need to monitor the system and driving environment but the driving ability of the automated systems. It states that when this is limited or when the system fails, the driver should take control of the vehicle [34], [35]. ''Autonomy'' is defined as ''having the power to be independent and make decisions for yourself'' (Cambridge Dictionary). In other words, an AI-based AV has the ability to recognize the surrounding environment and drive itself without human intervention [33], [36]. To simplify, an automated system cannot drive safely and steadily in all traffic scenarios and situations on the road. For example, when the road is blocked, it is difficult for an automated car to return to the normal driving state without driver intervention to search for another route. However, an AV can drive itself using AI technology without human input in all traffic scenarios and situations.

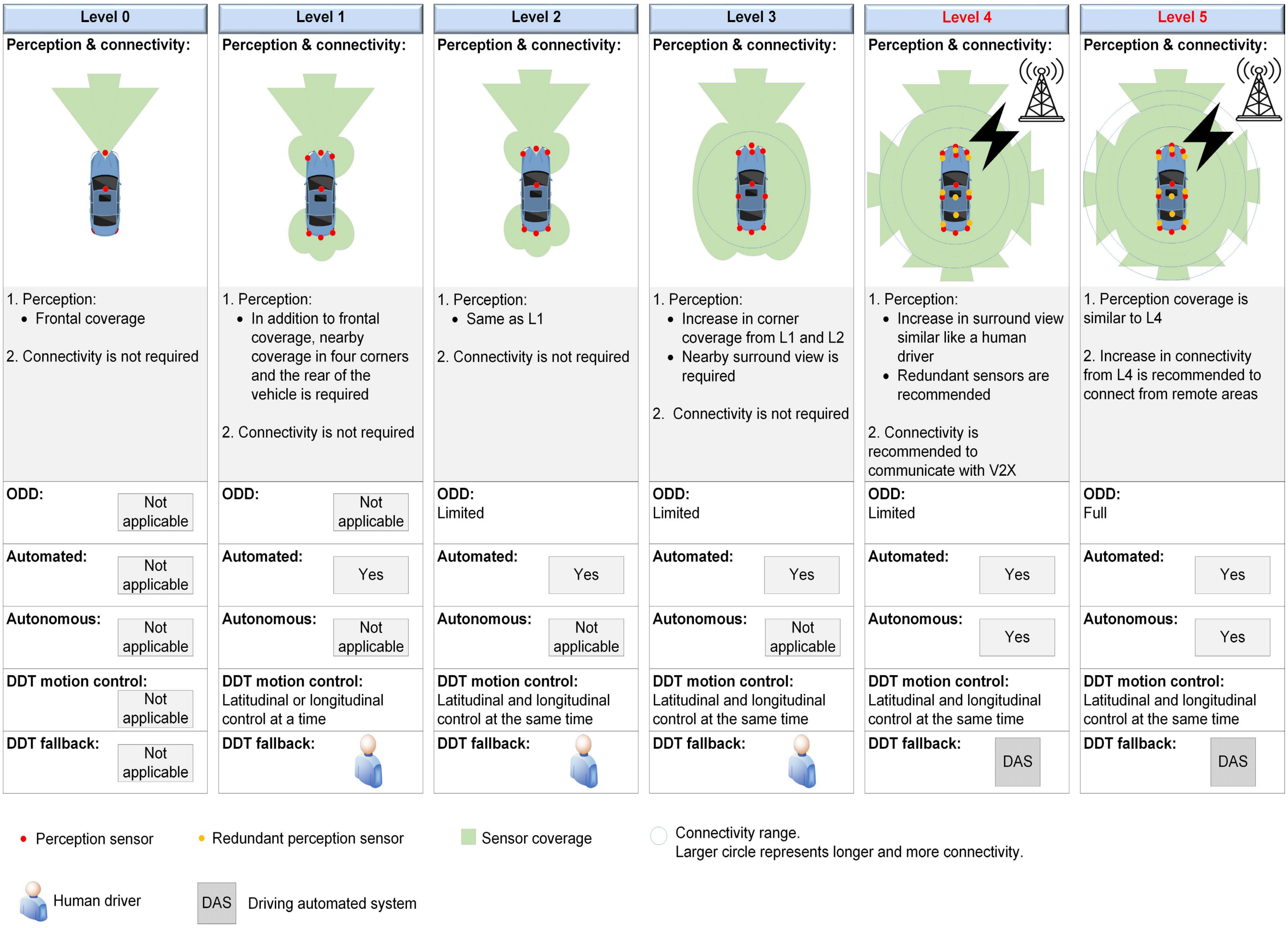
At a high level, the first three levels (L0, L1, and L2) of J3016 are excerpted as ''Driver Support Systems,'' while L3, L4, and L5 are exercised for actual ADS [37]. It is important to note that these automation levels do not classify the automation level of the whole vehicle but rather define the level of automation of a feature when it is engaged [37]. For example, a vehicle capable of traffic jam chauffeur as an L3 ADS feature will have a specific operational design domain (ODD) and relevant dynamic driving task (DDT) to perform the feature, whereas exiting from the highway can still be manually operated by a human driver without involving DAS. In Table 1, we have summarized six levels of driving automation along with the applicability and scope of the associated key terminologies used in J3016 to define them, e.g., ODD, DDT, DDT fallback, minimal risk condition (MRC) and a few more. As per our interpretation of J3016, ODD is arguably the most critical parameter, as other parameters are highly dependent on it. We also note that the definition of ODD in J3016 is very high level and does not give enough clarity on how ODD can be parameterized. To address this limitation, European standards have created a taxonomy document, PAS 1883 [38], which classifies ODD parameters into three main categories, (1) scenery, (2) environmental conditions, and (3) dynamic element, but this standard does not provide boundary conditions for each automated level. SAE has recently started an initiative to create J3259 for ODD taxonomy and definition, but this standard is not available for use yet. In our study, we have analyzed the ODD from a perception and connectivity perspective. As we have shown in Fig. 1, for perception coverage in L0, only frontal coverage is required, but in L1 and L2, coverage in the rear and four corners is required as well. Perception coverage for L3 should be augmented with a surround-view in the nearby zone of the vehicle, and for L4 and L5, the surround-view coverage needs to be extended like a human driver. Connectivity is recommended starting from L4 to communicate with V2X, and for L5, the connectivity range needs to be extended to communicate with V2X from remote areas. For DDT, in L3 and above, the expectation is to have complete and continuous DDT by the system, whereas in L1 and L2, it is limited to a sustained basis. DDT fallback and MRC are significant distinguishing factors between L3 and the levels above L3, as the driver is responsible for DDT fallback and MRC for L3 features, and MRC is not mandatory. In contrast, the system must handle the DDT fallback for L4 and L5.

A. DISTINGUISHING ASPECTS OF SAE AUTOMATION LEVELS

The primary objective of vehicle automation is to improve safety by eliminating or at least significantly reducing the accidents caused by human error. Hence, ADS must perform better than a human driver. J3016 divides the act of driving into three main categories, (1) strategic (trip planning), (2) tactical (motion planning), and (3) operational, which can be lateral (steering) and/or longitudinal (acceleration/deceleration) control. Tactical and operational efforts and object and event detection and response (OEDR) are sub-tasks of DDT in DASs, determined by feature and associated automation level. A typical automated architecture includes five main building blocks: perception, localization, sensor fusion, planning, and control subsystems. This architecture is composed of various components such as camera, radar, lidar, and ultrasonic sensors for perception; IMU and GPS sensors for localization; high-bandwidth in-vehicle communication, V2X connectivity, and a sophisticated AI/ML algorithm for sensor processing; and sensor fusion, scene creation, motion planning, a combination of real-time and high-computing energy-efficient processor, memory with more bandwidth and bus width and ample data storage. Furthermore, depending on the scope of ODD and DDT, these components may need to follow a higher category of specific standards such as ISO 26262 (functional safety) and ISO/PAS 21448 (safety of the intended functionality) to ensure safety-driven design. This means that a highly automated driving (L4) feature in which DAS is expected to operate independently in complex driving scenarios will require more capable and reliable hardware (sensors, processor, memory), V2X connectivity, faster as well as broader communication bandwidth, and a significant increase in lines of code and data storage as compared to conditional automation (L3) where the human driver can act as a complementary driver in complex driving condition. A typical safety-critical system like AV should also be capable of responding to failures in fail-operational, fail-safe, and fail-secure ways, which may need redundancy in some of the critical hardware

TABLE 1. Parametric variations of SAE J3016 automation level.

	SAE J3016 Automation Level					
Parameters	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Automation	None	Driver-assistance	Partial	Conditional	High	Full
ODD perception	Frontal coverage	Coverage in front, rear and four corners of the vehicle	Same as L1	Increase in corner coverage from L1, L2 Nearby surround view coverage	Increase in surround view like human driver is recommended	Similar to L4
ODD connectivity	Not required	Not required	Not required	Not required	Connectivity is recommended to communicate with V2X	Increase in connectivity from L4 to connect from remote areas
DDT scope of DAS	None	Longitudinal or lateral control at a time (sustained basis)	Longitudinal and lateral control at the same time (sustained basis)	Complete DDT (OEDR+ tactical+ operational)	Complete DDT (OEDR+ tactical+ operational)	Complete DDT (OEDR+tactical+ operational)
DDT fallback	Driver	Driver	Driver	Driver	DAS	DAS
Monitor DDT performance system failure	N/A	Driver	Driver	Driver	DAS	DAS
Monitor DAS performance	N/A	Driver	Driver	DAS	DAS	DAS
Minimal risk condition	N/A	N/A	N/A	Not mandatory, user decides final action	must	must
Failure mitigation	N/A	N/A	N/A	Recommended	Recommended	Recommended
Misuse or abuse	N/A	No significant evidence	Important	Important	N/A	N/A
Response to user request	N/A	N/A	N/A	Relinquish DDT upon request by DDT fallback-ready user	ADS may delay relinquishing DDT for performance or hazard prevention	ADS may delay relinquishing DDT for performance or hazard prevention
Standards regulations	ISO 26262 UNECE-WP.29	ISO 26262 ISO/ SAE 21434 UNECE WP.29	ISO 26262 ISO/ SAE 21434 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29
Functional system architecture	Distributed [39]	Domain-centric [39]	Domain-centric [39]	Domain-centric [39]	Centralized [39]	Centralized [39]
DDT sensors (#)	Radar (1) [40], [41], [42]	RADAR (1-3) SONAR (1-12) Camera (1-2) IMU (1) [40], [41], [42], [43]	RADAR (3-5) SONAR (up to 17) Camera (2-6) IMU (1) GNSS/GPS (1) [40], [41], [42], [43]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (>1) GNSS/GPS (>1) [40], [41], [42], [43], [44]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (>1) GNSS/GPS (>1) [40], [41], [42], [43], [44]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (>1) GNSS/GPS (>1) [40], [41], [42], [43], [44]
Connector bandwidth	1 MB [45]	1 GB [45]	1 GB [45]	6 GB - 12 GB [45]	6 GB - 12 GB [45]	6 GB - 12 GB [45]
Data generation (per day)	N/A	0.3 TB [46]	0.3 TB [46]	5 TB - 32 TB [44], [46], [47]	5 TB - 32 TB [44], [46], [47]	5 TB - 32 TB [44], [46], [47]
Data storage technology	SLC NAND e.MMC UFS [48]	SLC NAND e.MMC UFS [48]	SLC NAND e.MMC UFS [48]	e.MMC UFS Embedded SSD [48]	e.MMC UFS Embedded SSD [48]	e.MMC UFS Embedded SSD [48], [49]
Vehicle to cloud data (per hour)	N/A	10 GB	25 GB [50]	300 GB	400 GB	500 GB [50]
AI processor throughput (Trillion operations per second)	N/A	1	2 [51]	24 [51]	320 [51]	4000+ [51]
RAM bandwidth	500 MB/s [52]	60 GB/s [52]	60 GB/s [52]	512 - 1024 GB/s [52]	512 - 1024 GB/s [52]	1024 GB/s [52]
Lines of code	10 million [53]	100 millions [53]	100 million [53]	300 - 500 million [53]	300 - 500 million [53]	300 - 500 million [53]
AI compute energy (% total energy consumed in car)	N/A	1-4% [54]	1-4% [54]	13%-20% [55] [56]	40%	40%-50%



Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Perception & connectivity:	Perception & connectivity:	Perception & connectivity:	Perception & connectivity:	Perception & connectivity:	Perception & connectivity:
1. Perception: • Frontal coverage 2. Connectivity is not required	1. Perception: • In addition to frontal coverage, nearby coverage in four corners and the rear of the vehicle is required 2. Connectivity is not required	1. Perception: • Same as L1 2. Connectivity is not required	1. Perception: • Increase in corner coverage from L1 and L2 • Nearby surround view is required 2. Connectivity is not required	1. Perception: • Increase in surround view similar like a human driver • Redundant sensors are recommended 2. Connectivity is recommended to communicate with V2X	1. Perception coverage is similar to L4 2. Increase in connectivity from L4 is recommended to connect from remote areas
ODD: Not applicable	ODD: Not applicable	ODD: Limited	ODD: Limited	ODD: Limited	ODD: Full
Automated: Not applicable	Automated: Yes	Automated: Yes	Automated: Yes	Automated: Yes	Automated: Yes
Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Yes	Autonomous: Yes
DDT motion control: Not applicable	DDT motion control: Latitudinal or longitudinal control at a time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time
DDT fallback: Not applicable	DDT fallback: 👤	DDT fallback: 👤	DDT fallback: 👤	DDT fallback: DAS	DDT fallback: DAS

● Perception sensor
● Redundant perception sensor
🟩 Sensor coverage
○ Connectivity range.
Larger circle represents longer and more connectivity.
👤 Human driver
DAS Driving automated system

FIGURE 1. Comparison between SAE automation levels.

and software. In Table 1, a plausible comparison is captured for some of the systems requirements based on our understanding of variations in driving automation tasks at each level, technology trends, and observations from some of the key players in the industry. For example, DDT sensors for perception in L3 will be more numerous than in L1 and L2 to cover the surrounding view in addition to frontal, rear, and corner coverage. In L4 and L5, the surround-view sensors need a more extended range to cover the area like a human driver. Further, redundant perception and localization sensors and computing devices will be required for DDT in L4 and L5 to replace the human driver as a complementary driver and fallback element. The enormous amount of data generated from the sensors augmented by connectivity increases the demand for communication bandwidth and data storage in L3 and above, at least five times more than in L1 and L2. For computation needs, software lines of code and processor throughput can increase at a very high rate from each level to the next one, increasing the memory requirement 10 to 20 times more in L3 and above. Also, energy utilization and heat management should be done efficiently to maintain the optimal performance from this high-computing hardware. Some of the data reported from L3 test vehicles showed that 13 to 20 percent of the total energy consumed during the drive cycle was used by the computing devices in the car. If this trend is observed more persistently, we expect this power requirement to go beyond 40% or even 50% considering the complete DDT fallback responsibility in L4 and L5, as it may require double or triple redundancy in computing and control devices.

IV. A NOVEL CAV TRAFFIC MOBILITY ENVIRONMENT

As we experience a higher penetration of intelligent transportation systems (ITSs) [57], the demand to extend the perceptual boundaries of sensor-equipped vehicles (beyond the individual vehicle) is more pressing than ever. There have been widespread research and standardization efforts toward C-ITS communications to support applications ranging from fully AV operation and essential road safety support to traffic flow optimization and in-car delivery of infotainment services. To realize these goals, the coordination of several different entities and support for several modes of communication are necessary. Fig. 2 describes commonly identified forms of ITS communication, including V2V, V2I,

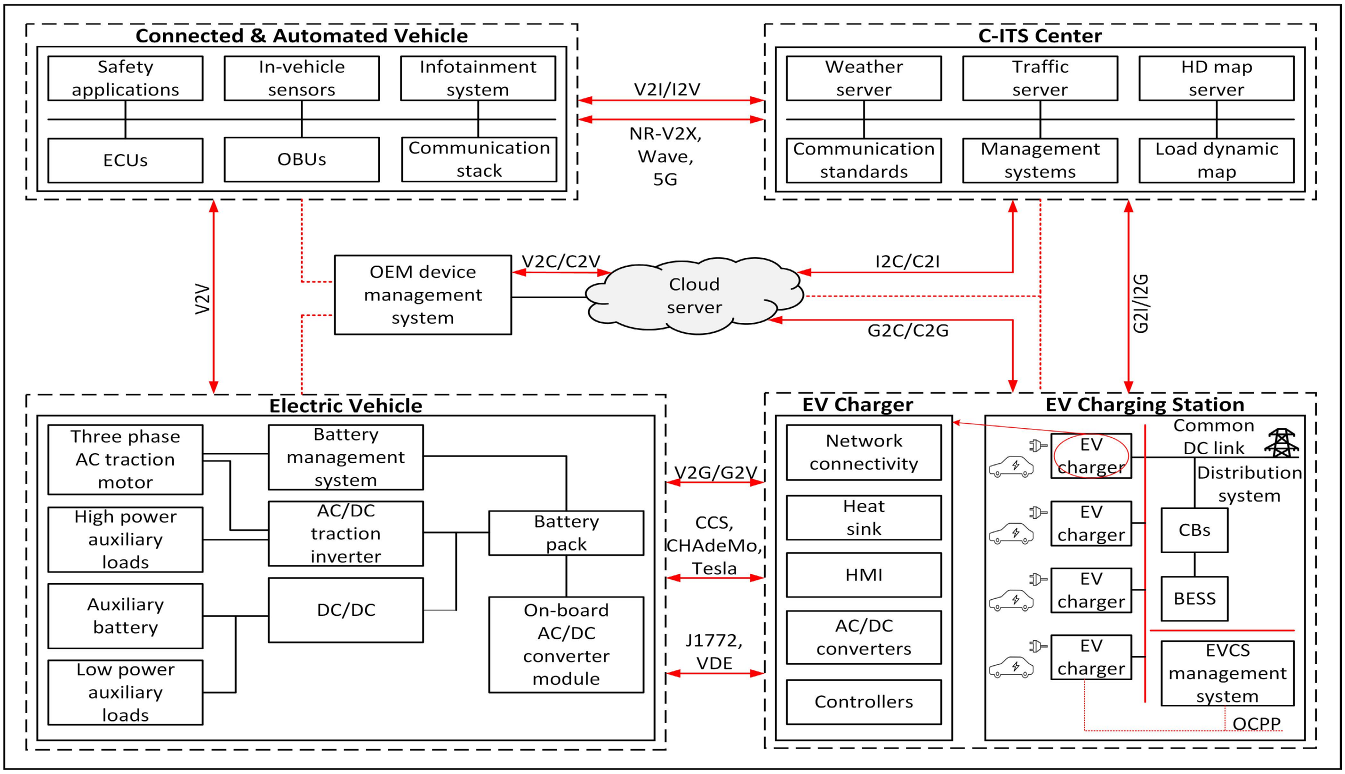


FIGURE 2. Proposed CAV traffic mobility environment.

vehicle-to-grid (V2G), and vehicle-to-cloud (V2C) communications, collectively referred to as V2X technology [58]. Autonomous driving technology is progressing most vigorously around the globe, and so is the mobility environment. However, due to the reservations and withholdings offered by multiple AV mobility environments in the literature, a novel CAV mobility environment is developed in this section that incorporates security at a holistic level. It implies that the proposed structure consolidates all the subsystems, e.g., CAV, EV, cloud server, C-ITS center, and the charging infrastructure as prominent facets of the traffic mobility environment to broaden the definition of V2X communication. Moreover, as shown in Fig. 2, the proposed environment overviews the CAV and its highly networked environment, which integrates leading-edge technologies, e.g., advanced wireless communications, intelligent traveler applications, on-board computer processing, advanced vehicle sensors, GPS navigation, smart infrastructure, C-ITS center, EV charging infrastructure, and power grid to enhance the state-of-the-art capabilities of the vehicles.

CVs and automated vehicles are two different technologies. A CV is equipped with several different communication technologies to communicate with the driver, other vehicles on the road, roadside infrastructure, and the cloud server [59]. However, in accordance with the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA), automated vehicles are characterized by some aspects of a safety-critical control function (e.g., steering, throttle, or braking) that operate without a driver's direct input [60]. In general, C-ITS is an advanced transport system where two or more ITS subsystems (personal, vehicle, roadside, and central) cooperate and provide an ITS application [10]. It uses mature ad-hoc short-range (e.g., ETSI ITS G5) and complementary wide-area communication technologies that allow AVs to communicate with other vehicles, traffic signals, internet gateways, roadside infrastructure, charging infrastructure, and other road users. DSRC, the longest-considered candidate for V2X, has been proposed as a mandated standard by the U.S. Department of Transportation (USDOT). Also, it is the subject of intensive standardization efforts by the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), and the Association of Radio Industries and Businesses (ARIB), among others. However, it is not expected that a single technology can support such a variety of typical V2X applications for a large number of CAVs in the near future. Another candidate access technology for V2X is the mobile cellular network, a proposition often referred to as Cellular V2X (C-V2X) [61]. Beyond these two major candidates for V2X communications, several other technologies, including Bluetooth, satellite radio, and visible light communications, have been considered for V2X applications. While each of these technologies has features that make it potentially promising, each also has some unavoidable limitations. An additional option is a heterogeneous network solution, combining the features of DSRC and LTE/5G to complement their respective benefits while ameliorating their drawbacks. Many studies have shown a significant improvement in performance when heterogeneous communication technology is used, but its limitations include standardization and high implementation costs. The wireless communication between the different actors and ITS stations and related functions are named cooperative V2X communication, which comprises V2V, V2I, V2C, and V2G communications. In a cooperative road traffic scenario, communication units such as ITS stations are implemented in vehicles and traffic infrastructure. These units exchange information via the cooperative V2X short-range ad-hoc network. The OBUs in the vehicles transmit data such as their position, speed, and driving direction. Additionally, they send out event-triggered messages about particular incidents, such as emergency braking, a vehicle defect, or a slippery road detected. The RSUs or equipment in the C-ITS infrastructure (traffic signal controller (TSC)) send data about, for example, signal phases of traffic lights, speed limits, or road work. Connected V2X analyzes the data received and warns the CAVs against dangers. For instance, when a sudden obstacle appears on the road, the roadside infrastructure (e.g., sensor) identifies it and transmits the information to its nearby CAV by infrastructure-to-vehicle (I2V) communication. The CAV relays this information to other CVs through V2V. Further, the C-ITS center provides the information necessary for sudden braking to the host vehicle, which alarms the emergency vehicle via V2V.

For a carbon-neutral future, the new era of travel is focused on fusing the three technologies (connected, automated, and electric) together, hence providing a higher quality of transportation and environmental sustainability. Thus, a battery-operated CAV is critical in successfully building an intelligent module for ITS in a smart city IoT application. In this CAV, the battery provides power to drive the vehicle's powertrain. Moreover, due to consideration of electrification of CAV, its connections to the power grid through EVCS and an EV charging adapter for charging its battery are also important. Hence, this section identifies the significant factors that make a new sustainable CAV mobility environment.

V. CYBER EVENT IDENTIFICATION FRAMEWORK

A. CYBERATTACK-INDUCED CAV ACCIDENT ANALYSIS

Due to a fundamental transition in the transport mobility environment, the new paradigm recognizes multiple entities as defined in Section III. This implies that there can be multiple risk factors responsible for targeting a CAV crash. Since existing CAVs drive while exchanging information using big data, cloud, V2X communication technology, and internal communication, they are vulnerable to various attacks such as physical attacks on hardware, e.g., electronic control devices, sensors, or actuators from the outside while driving and failures caused by firmware forgery or falsification, which can cause traffic accidents. Although the currently deployed safety standards do not explicitly address security, the security issues that arise in AVs are strongly allied with safety. In the aspect of automobiles, safety is one of the key issues in vehicle development, and in the development of automobile functions, functional safety aims to prevent risks due to hazards caused by E/E system malfunction (ISO 26262-1). Please note that this paper assumes that only cyberattacks are accountable for causing a battery-operated CAV crash. Fig. 3 presents a high-level overview of a CAV accident mechanism, which attempts to explain traffic accidents that may occur due to specific causes by using the mechanical model concept on the occurrence of vehicle accidents suggested by ISO 26262 and the failure chain presented in [62]. It shows the correlations between different cyber, physical, and logical elements and states how various key factors can aggravate the impacts of cyberattacks, thus resulting in a fatal accident. In this paper, prominent standards such as ISO 26262, ISO/PAS 21448, and ISO/SAE 21434 have been leveraged to develop some key terminologies.

Several endogenous or exogenous trigger conditions (intended or unintended) may cause safety and security failures, leading to a hazardous condition in one or more interconnected elements present in the CAV ecosystem. Trigger conditions may include either environmental, traffic, or geometric factors that impart a fault in an entity. Since cyberattacks are being considered, disparate vulnerabilities accompany each entity in the mobility environment that could be exploited by the attackers to compromise the safety and security of the system. The existence of vulnerable points facilitates a potential cyber threat or attack with an intent to cause unauthorized access, disruption, or damage, hence undermining the security aspects. Though integrating effective mitigation measures might reduce the damage from risks or hazards, failure of these mitigations may lead to a system fault. Fault refers to any physical defect or imperfection in some hardware or software component [63] or is defined as an abnormal condition that prompts the component failure. Error that arises due to a fault in accuracy is a discrepancy or deviation in the computation of measurements, perception, cognition, or decision-making. Another term called failure is a consequence of termination or malfunction of a component due to fault (ADS function failure, C-ITS failure, or electrification failure), which impacts the driving maneuver of the CAV. The following scenario can show an example. Due to a foggy environment (trigger condition), an incorrect perception of the lane markings is caused in the sensors (fault) in a CAV. This will lead to a control discrepancy (error), so an abnormal lane-departure function executes the lane change at an improper speed (failure), resulting in a collision with a vehicle in the target lane. Exposure is defined as an estimation of the likelihood that the CAV is in a particular operating situation when a hazard occurs. Also, it is considered a factor that modifies the severity of the trigger condition. In other words, it outlines the complex urban environment with numerous intersections, cross streets, or unsignaled crosswalks and vulnerable road users (VRUs). A hazard event is explicated as the direct implication of an accident that can occur when driving in a hazardous condition. However, there

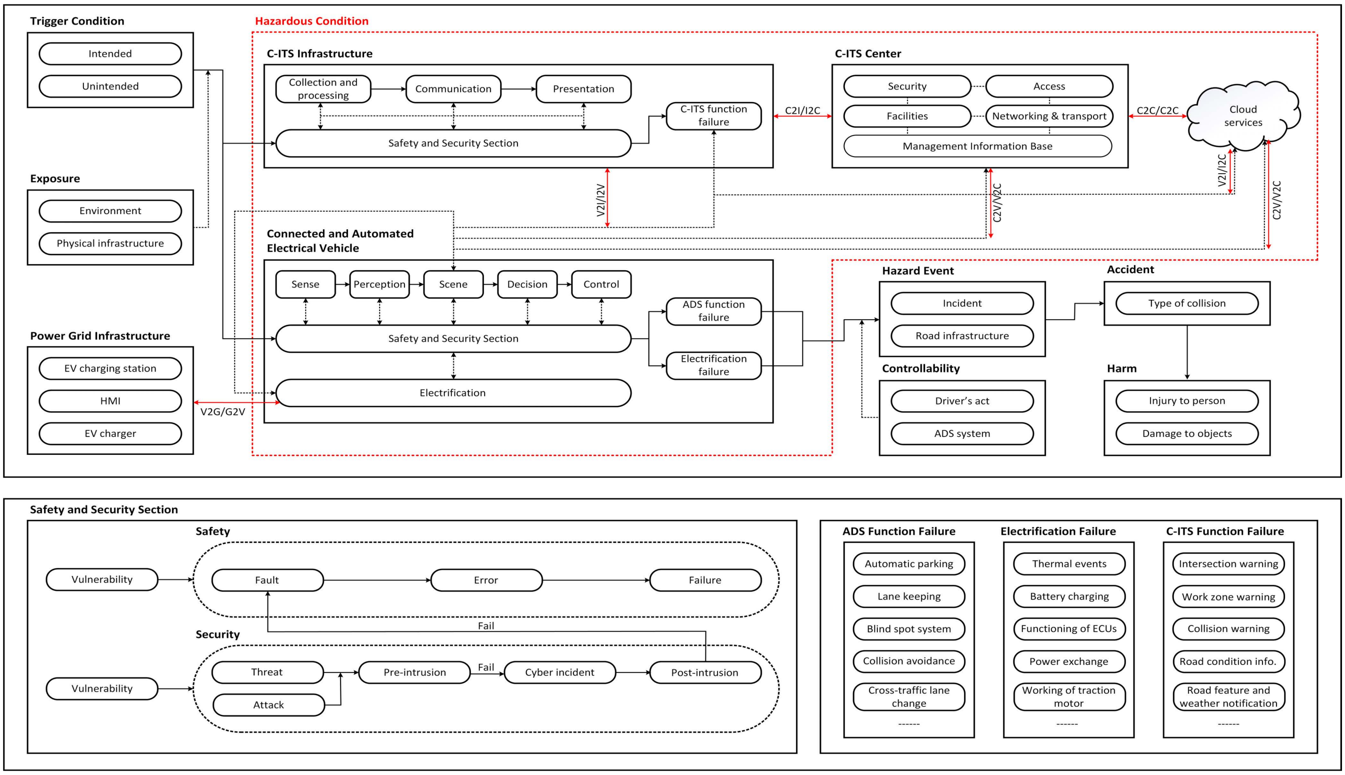


FIGURE 3. Proposed cyberattack induced CAV accident mechanism.

is a probability that the CAV returns to its normal driving behavior, provided the human driver or the ADS applies some control measures. Hence, controllability is an estimation of how easily the controlling factors can avert the hazard. For instance, the presence of a skilled and trained CAV operator might mitigate the effects of potential system failures and thus prevent an accident. Finally, harm is recognized as injury to the passengers, fatality, or environmental damage. Using this framework, cybersecurity events responsible for the CAV crash can be tracked to identify the responsibility of a specific candidate for the accident. Further, the existing accident analysis models are vehicle-centered, insufficient to validate a CAV crash induced by a cyber event.

Furthermore, a CAV crash in a multi-model environment can be mathematically formulated as,

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha_i \times \delta_j) \geq 1, \tag{1}$$

where,

$$\alpha_i = \begin{cases} 1 : \text{entity}(\mathrm{E}_i^k) \text{ undergoes a cyberattack} \\ 0 : \text{no cyberattack} \end{cases} \tag{2}$$

$$\delta_j = \begin{cases} 1 : \text{no controllability by the controlling factors } \mathrm{CF}_j^l \\ 0 : \text{successful controllability} \end{cases} \tag{3}$$

The symbols used in the above equations are defined as:

$\mathrm{E}_\mathrm{i}^\mathrm{k}$: ith component of the k entity or subsystem in the mobility environment, where $\mathrm{k} = \{\mathrm{C, I, P, A, O}\}$

C: C-ITS center

I: C-ITS infrastructure

P: power grid or charging infrastructure

A: CAV

O: cloud server

$\mathrm{CF}_\mathrm{j}^\mathrm{l}$: jth component of the controlling factor responsible for averting the accident, where $\mathrm{l} = \{\mathrm{H, S}\}$

H: human driver

S: ADS

B. STRIDE THREAT MODELING

With high penetration of computing hardware and software, sophisticated in-vehicle networks and poorly configured devices of an AV are at risk from physical attacks and vulnerable to cyberattacks. Unfortunately, the value proposition of multiple features (e.g., Wi-Fi hotspots, self-parking, communication with apps, over-the-air (OTA) software updates, and more) overshadowed the crucial role of integrating security. On account of this, a security breach could trigger malfunction or unexpected behavior of the vehicle, which may lead to damages, from the reputational to serious safety accidents. This problem becomes more challenging with CAVs due to increased connectivity with the externally connected modules (e.g., C-ITS infrastructure, cloud server, power grid, and

EVCS), which widens the attack-vector space. Therefore, it is crucial to identify existing vulnerabilities and potential cybersecurity threats in a highly convoluted mobility environment to design countermeasures to prevent malicious attacks. Several paradigms for attack, threat, and defense analysis lay the foundation for the work presented herein. A literature review has identified numerous threat-modeling methodologies, e.g., OCTAVE, EVITA, HEAVENS, PASTA, and LINDDUN. One of the most important methods, STRIDE, has been widely used to identify and analyze the threats in the IT industry [64]. Also, it is recommended for automotive information security in SAE J3061 regulations. While multiple threat-modeling frameworks exist, this paper elaborates on STRIDE's common framework. It is an iterative threat modeling tool that has been applied in many CPSs in the past. It is an efficient approach focused on cybersecurity, while others are highly complex with more focus on safety and risks [4].

A DFD is a graphical representation of the data flow and is composed of various entities, as exhibited in Fig. 4. It also incorporates a high-level overview of the connectivities and potential vulnerabilities within a CAV and its mobility environment. It is centered around identifying and mitigating potential cyber threats against each system entity. Fig. 4 is a STRIDE model that shows the existing threats to the CAV, C-ITS center, DC charger, EV, and grid-connected EVCS. Hence, the STRIDE model defines six different types of security threats, as described below:

1) **S**poofing: It is defined as masquerading as a legitimate source, process, or system entity by falsifying data. For example, a compromised C-ITS infrastructure (a road sign) emits carefully crafted signals to the CAV sensors, which could cause a ''Stop'' sign to be misread as a ''Speed limit'' sign. As a result, the sensors may interpret the spoofing signals the same way as the authentic signals and may accelerate the speed; this could cause a crash.
2) **T**ampering: It refers to an unauthorized alteration of legitimate information. It is also known as data corruption or false data injection (FDI). To exemplify, the threat actor tampers with the code of the TSC and changes the original instruction. As a result, the TSC sends modified scheduling, signal phases, and time-controlling signals to the traffic signal. When a CAV receives a tampered traffic signal, unpredictable consequences could occur.
3) **R**epudiation: It means denying or disowning a specific action executed in the system. For instance, a compromised EVCS may deny the charging commands to a battery-operated CAV, and thus it will be unable to continue the charging process. Instead, the infected EVC may transmit incorrect transmissions in the connected CAV, enabling the failure of ADS functions. This could cause undesirable CAV crashes.
4) **I**nformation disclosure: It is denoted as a data breach or unauthorized access to security-sensitive information. For instance, the communication between the ECUs is highly vulnerable to interception by a threat agent. Hence, the attacker can gain access to sensitive information during the data exchange, mimic a valid ECU, and use these details to compromise the processing and impair message traffic.
5) **D**enial of Service: Also called a flooding attack, it causes the disruption of timely access to network services for intended users due to an attacker's action to jam and overload the bus network by sending a continuous stream of malicious traffic. In the case of a C-ITS center, worm-infected computers may generate malicious traffic with a similar payload signature (i.e., same malicious program code to conduct infection) and flood the communication network of a traffic signal management system with malicious packets. As a result, there is a detrimental ripple effect caused by the functioning of traffic signals. This can cause a collision among CAVs at the intersection.
6) **E**levation of Privilege: It occurs when an attacker gets greater access to resources or data in the system than the legitimate user. For instance, if a threat actor gets crucial details of sensor data (firmware and user data), they might compromise data and disrupt the functions, change files or configurations, and other modifications according to their needs. This adversarial attack on sensors might manipulate the inputs to the ADS algorithms and cause accidents.

   The evolution of AVs from closed to open systems has effectuated new attack surfaces an attacker can potentially exploit due to possible external communication with other entities present in the extended environment. On that account, there is a need to examine all the entities for the feasibility of such attacks, which can cause a CAV crash.

C. POTENTIAL CYBERSECURITY MEASURES

Once vulnerabilities are identified in a CPS, cyber hardening is a predominant practice to avert cyberattacks on the system. Therefore, this section develops various mitigation strategies to address the pre-attack phase of cyber intrusion. During the pre-attack stage, risk assessment methodologies can be applied to protect different system devices that could be attacked by using potential avenues. For instance, in this paper, STRIDE is used for threat and vulnerability analysis in the early development cycle. Further, system hardening can be done to reduce the vulnerabilities in all the entities. In addition, the communication infrastructure of multiple servers, including cloud servers operating within a given environment, can be secured by establishing software-based intrusion detection and prevention systems (ID&PSs). Similarly, communication paths between different entities (e.g., between EVs and EVCS) can be strongly encrypted and authenticated. Moreover, proper configuration of a firewall, encryption of network traffic, and other techniques can play an essential role in securing the network. Further, to secure the contents of the database (DB) management system, DB hardening can

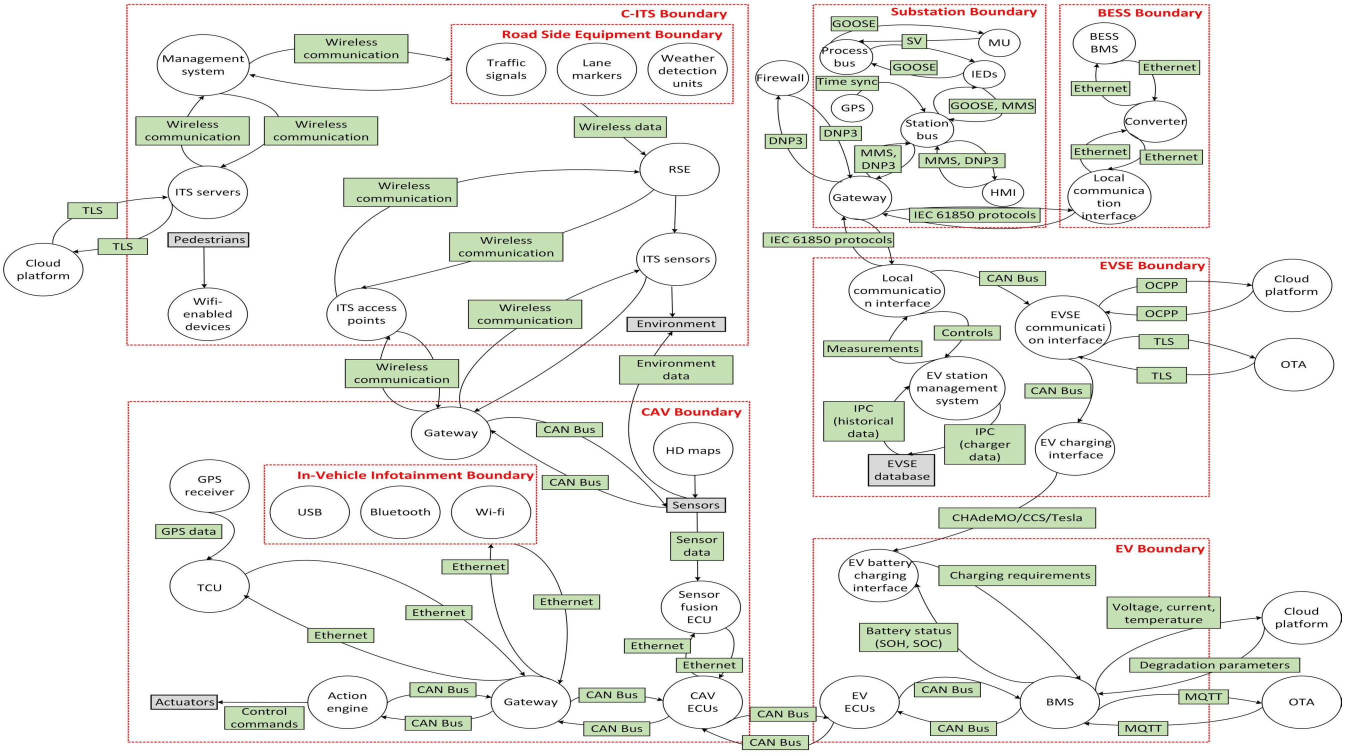


FIGURE 4. STRIDE model for threat analysis of a CAV and its environment.

be performed by regular patching and updating. In addition, vulnerability scanning prior to and post system installation of devices (e.g., EVC), multi-factor authentication, detection of abnormal activities using signature-based cryptography, and others can be used as mitigation techniques.

However, post-attack mitigation actions are performed to achieve cyber restoration. In other words, these measures are used to restore the attacked and damaged entity to its healthy state. So, by implementing digital forensics, a system engineer can identify the compromised equipment (e.g., EVC in case of a cyberattack on charging infrastructure), derive the source, and recover the compromised data to maintain a robust security system. Furthermore, the attacked system can be made more reliable and robust by disconnecting the compromised distribution feeder by tripping protection devices, e.g., circuit breakers (CBs), and/or disabling the compromised communication ports and substituting the compromised asset with a safer backup system that can be used until the original system resumes to its normal operations. Other protective measures may include updating the firmware/security updates or removing unauthorized software, etc., to resolve the issue during maintenance.

It should be noted that the objective of this paper is the development of a cybersecurity investigation framework for CAV crashes, not proposing mitigation actions for cyber intrusions.

VI. DIGITAL FORENSIC INVESTIGATION FRAMEWORK

Vehicle forensics has become an overriding attribute in a vehicle's design and operational life cycle [65]. Vehicles can undergo road accidents or play an instrumental role in committing a cybercrime with repercussions on safety and security (other than road traffic) and may subsequently be subject to a forensic investigation. Development of the CAV ecosystem due to digitization facilitates the potential stakeholders (including insurance claim investigators, law enforcement, criminalistic units, security-oriented institutions) for crash investigation (to determine the course of events), insurance claims (to decide the responsibility for an accident: human or system) and crime investigation (to deal with criminal activities and ensuring security at various levels). Fig. 5 highlights potential steps included in a forensic investigation of a CAV accident.

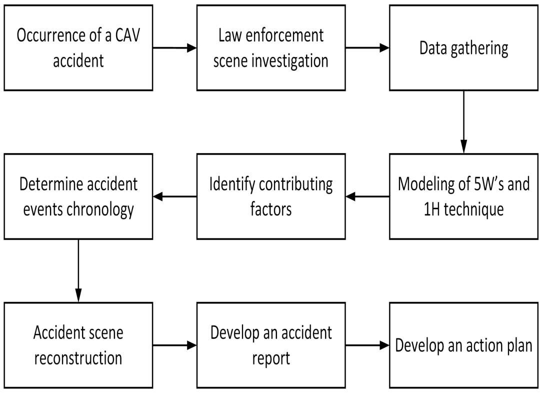

Occurrence of a CAV accident
Law enforcement scene investigation
Data gathering
Modeling of 5W's and 1H technique
Identify contributing factors
Determine accident events chronology
Accident scene reconstruction
Develop an accident report
Develop an action plan

FIGURE 5. Proposed cyber event identification framework.

The crash investigation starts on the scene with law enforcement. Law enforcement is often the first responders called to formalize an evaluation of a crash scene and report their findings based on first impressions. This includes accurately assessing crucial evidence and recreating complex accidents. Crash reconstruction is essentially reverse-engineering the elements of a scene to determine the factors contributing to a vehicle crash [66].

The contemporary technological advancement of the auto sector is collateral with the emergence of e-mobility and AVs. In an intelligent vehicle, ECUs that control the overall vehicle operations can be used to process and preserve digital data on the vehicle's activity and its occupants. Multiple electronic processes are being carried out in the vehicle, which involves processing in-vehicle communication (CAN, CAN FD, MOST, LIN, Ethernet, FlexRay) and communication with the external environment (traffic, road infrastructure). The integration of cloud computing further allows the exchange of real-time data from the devices installed in the vehicle (sensors, on-board computers, HD maps, etc.) and devices that are connected to the vehicle (mobile phones, tablets, computers of its occupants, etc.) with the cloud or remote data centers. For instance, Tesla, which is now striving toward making its own data center and AI training supercomputers, offers cloud computing services to its customers through a public cloud platform called Amazon Web Services (AWS). Consequently, a contemporary high-end CAV may contain hundreds of ECUs to store more than 150 million lines of source codes of programs and may generate over 30 GB of data for every hour of vehicle operation. Hence, every CAV produces an enormous volume of data or information, which can serve as digital evidence in forensics investigation and analysis. In addition, much greater vehicle automation, coupled with robust information support and telecommunications with all objects involved in driving and road logistics, including AI elements, can be used for forensic works in the future. Typical data sources of digital evidence may include [67]:

- CCTVs
- Black box or event data recorder (EDR)
- Data storage system for automated driving (DSSAD)
- Telematics and infotainment system
- eCALL units
- Key fobs
- Dash cams
- Cloud server

Data can be extracted from some mandatory sources to initiate the investigation; for instance, on-board EDRs can automatically read and record the vehicle kinematics 5 seconds before the accident and subsequently over the course of the entire event. Hence, it can be used to analyze (1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage or deployment status, and (5) post-crash data. However, there are some limitations of using EDR for CAV-involved collisions, as highlighted by [68]. So, SAE J3197 recommends the deployment of an ADS data logger or DSSAD in conjunction with EDR for a more comprehensive crash reconstruction. DSSAD, with a limited storage capability, provides for an extended period of 6 months valuable data gathered by ADS technologies, e.g., radar, camera, and ultrasonic. Parallel to these developments, many manufacturers are recording non-standardized accident data of vehicles. It is to be noted that much of the data is usually very untransparent to the accident analysts in this context, i.e., the manufacturers decide which data will be made available to the experts during an investigation. In addition, accidents can be reconstructed more accurately if the information is fed from other data sources and anonymous accident databases, which would be of enormous value to many stakeholders. Also, due to the reliance of modern CAVs on the cloud infrastructure and the diversity of configurations, accident investigation has become grueling for the investigators as it also involves assembling data from these resources. So, there is a need to design a sophisticated forensic model with a powerful digital forensic tool at the back end as an effective solution to overcome IoT-based criminal activities on CAVs.

Crash investigation has evolved over time. It incorporates state-of-the-art devices in data accumulation and crash reconstruction analysis to improve the reliability of field investigations and ensure the accuracy of the findings [69]. To exemplify, it has advanced from measuring tapes to photogrammetry, total station theodolite (TST), FARO Focus 3D laser scanner, crush analysis and simulation (CA&S), and vehicle mapping (VM).

With a conventional vehicle crash, after securing the crash scene and checking for injured parties, the initial examination of the scene encompasses gathering large amounts of pieces of evidence or information, including vehicle locations, roadway signage, signals, and roadway markings such as skids, slides, yaws, and gouges. Next, the investigators document the site conditions, examine vehicle damage characteristics, inspect mechanical and electrical systems, and gather hard evidence. Further, pertinent data, for instance, speed and direction of the vehicles, skid-mark lengths, line-of-sight, and road conditions, are analyzed to develop the facts of the case.

After the accident data extraction, also known as live data extraction, specific devices are seized, followed by lab analysis. Further, the investigation involves the proposed 5Ws and 1H model to identify the contributing factors (human errors, equipment failures, etc.).

The inclusion of CAVs within the existing system has precipitated new challenges for the investigation process as accidents can be associated with poorly maintained road markings or light reflections affecting the vehicle sensors and in-vehicle or external communication faults or compromised charging infrastructure. For instance, in California DMV reports, Waymo and Mercedes specifically cited weather as a disengagement cause, indicating the pivotal association between weather and AV performance.

Hence, in a more complex environment, it becomes important to analyze the crash sequence of events describing the CAV's interactions with other road users before, during, and after a collision in a temporal (time-space) manner.

TABLE 2. Proposed 5Ws and 1H-based digital forensic investigation of a CAV accident.

Parameter	Description	Dataset
Who	Attacker (ω)	ω = {ω1: hacker, ω2: spy, ω3: terrorist, ω4: vandal, ω5: raider}
	Victim (υ)	υ = {υ1: C-ITS center, υ2: C-ITS infrastructure, υ3: power grid or charging infrastructure, υ4: CAV, υ5: cloud server}
What	Target (µ)	µ = {µ1: control module, µ2: BMS, µ3: TSC, µ4: HD maps, µ5: sensors}
When	Date (λ)	λ = {λ1: month, λ2: date, λ3: year}, Format: (mm-dd-yyyy)
	Time (τ)	τ = {τ1: timezone , τ2: hours, τ3: minutes, τ4: seconds, τ5: milliseconds}, Format: (hh:mm:sec:msec)
Where	Attack path (σ)	σ = {σ1: OTA, σ2: software kickout, σ3: incorrect map coding}
Why	Hazardous behavior (β)	β = {β1: undesirable motion, β2: unintended brake, β3: wrong lane, β4: improper speed}
How	Attack method (η)	η = {η1: spoofing, η2: tampering, η3: repudiation, η4: denial of service, η5: jamming}

To elaborate, an investigator must understand whether the human driver or the system initiated the disengagement, AV maneuvers, errors, and faults responsible for failures terminating in an accident. As a result, an AV maneuver can be diagnosed by determining the maneuver at the time of the accident (which considers data corresponding to crash site, vehicle damage, or collision type), maneuver at 5 seconds before the crash (which considers data from CCTV, Dashcam, EDR), and maneuver at more than 5 seconds after the accident (which considers data from CCTV, Dashcam, or DSSAD). Also, other databases, e.g., cloud servers, and ecall units, can provide essential data. Further, the object of failure, which includes driving failure (flat tire), communication failure (forfeited signals), ADS function failure (incorrect behavior of ADS algorithms), and security failure (counterpoising firewalls), is also a subject of investigation. In the next step, the intent is to discern errors that cause corresponding faults. They can include driving errors, e.g., hardware irregularity leading to visibility fault, C-ITS service discrepancy causing data latency, etc.

This approach produces a holistic and extensive forensic analysis of a cyber incident, which decomposes the incident into its atomic stages and determines its causes and effects as the investigator infers the missing events from the hypothesis about the crash (due to cyberattack) and reconstructs the accident scene.

To properly document and evaluate the accident scene, the incident responder can apply the 5Ws and 1H to plan, report and present his findings in an investigation that covers the six primary questions as illustrated in Table 2. First, it shows 5Ws and 1H, defined as (i) **W**ho, stating the type of attacker and the CAV component under attack; (ii) **W**hat, stating the attack target or system failure (hardware or software); (iii) **W**hen, stating the accident date as well as a failure occurrence time; (iv) **W**here, stating accident place or attack path for each CAV function, communication; (v) **W**hy, stating the hazardous behavior or the trigger conditions responsible for such behavior; and (vi) **H**ow, stating the attack method used by the attacker to induce the CAV into a hazardous event or crash situation.

Whenever there is a cyber incident, the attacker (hacker, spy, terrorist, vandal, corporate raider, professional criminal) uses some tool (user command, script program, toolkit, distributed tool, data tap, information exchange) to perform an attack or malicious action by exploiting a vulnerability (design, implementation, configuration) of a target component (process, data, C-ITS network, charging infrastructure, communication), thereby causing an unauthorized result (increased access, information disclosure or corruption, denial of service, theft of resources) to meet their objectives (political gain, financial gain, damage). Hence, the investigation is paramount to determine the causes and take corrective steps to prevent future occurrences. So, the investigation team can employ this technique for collision investigation to identify the patterns of severe CAV crashes and deduce the causes of these accidents.

Please note that we may have more sophisticated attack tools, attacks, and attack methods in the system in the future. So, more components can be added to Table 2 depending upon the diversity of cyberattacks and the mobility environment.

Hence, the primary objective of the proposed work is how investigators can use the digital forensic model based on 5Ws and 1H to analyze the chronologically ordered events that happened in a CAV crash. Further, it will facilitate a direction for an investigation team, which can take necessary actions.

VII. ANOMALY DETECTION IN A CAV CRASH

CAVs rely on precise and accurate information exchange among different elements to follow a set of waypoints along a planned route in an urban traffic environment. However, this information exchange involves high non-linearities and is affected by many distortions and spurious propagation. So, any malfunction in this transmission can cause an accident. Consequently, to promote functional safety, a stochastic M-ary classification-based approach is presented to decipher the problem of anomaly detection during crash analysis in real-time road scenarios. This probabilistic model proposed in the paper determines the probabilities of driving maneuvers and identifies the abnormal behavior of the ADS function in a CAV crash. Further, it estimates collision probability and makes driving decisions based on spatially and temporally probabilistic descriptions among different layer components.

The networked structure model, as illustrated in Fig. 6, consists of five prime layers, which are elaborated below:

Urban roads are usually limited by specific features, e.g., curbs, road markings, vegetation areas, or other obstacles, including vehicles, buildings, trees, traffic lights, or traffic signs. These road attributes yield crucial information concerning the scene. Sensing interprets the scene with

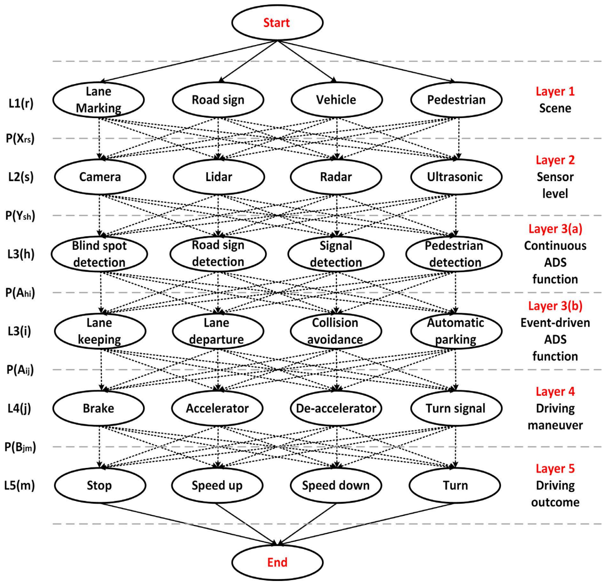


FIGURE 6. **Probability-based anomaly detection in a CAV accident.**

awareness and produces an environmental model. The ecological model includes the location of the moving obstacles, road limits, curbs, and barriers. The sensing is based on multiple sensors, active or passive. While active sensors (lidar and radar) can detect obstacles at long distances and under poor weather conditions, passive sensors (cameras and ultrasonic sensors) have the main advantage of being economical. Sensor fusion, which is a combined detection using multiple sensors, is also used to detect the road in the most challenging scenarios, thanks to the complementary features of each sensor.

Furthermore, CAVs are considered to integrate discrete ADS functions, e.g., continuous functions (road sign detection, traffic sign recognition, pedestrian detection) and event-driven functions (collision avoidance, automatic parking), and the visual information from the sensors is essential to run these applications. The last layer is driving outcomes dependent on the motion planning executed by the vehicular control modules, including the rules to merge into the traffic and manage driving behaviors in the coordinated driving environment. To exemplify, when the vehicle detects an obstacle (pedestrian), a sensor (lidar) mounted on the top of the CAV captures 3D images for the scene interpretation and transmits the measurements (e.g., distance, speed) to the pedestrian detection function, which is then required to detect the drivable area and make the corresponding decisions (“Stop” or “Turn”) through the control modules. Since the objects are controlled and connected through a network, any cyber-induced transmission delay or packet loss may cause an undesirable change of trajectory. Further, any deviation from the planned route of actions is assumed to cause a failure in the ADS function capability, leading to a fatal accident. Hence, this model allows the dynamically moving information to generate the mapping relationship between input images and output driving decisions and maneuvers.

Please note that this model is flexible to adapt to more components present in the urban environment at each layer.

Mathematically, this model can be formulated to differentiate the normal and abnormal behaviors such that:

Probability of occurrence of any abnormal event (E) due to incorrect transmissions of A_{ij} is,

$$\mathrm{P}(E) = \sum_{j=1}^{k} P(E \cap A_{ij}) = \sum_{j=1}^{k} P(E|A_{ij})P(A_{ij}). \tag{4}$$

In other words,

$$P(E|A_{ij}) = P(E|A_{11})P(A_{11}) + P(E|A_{12})P(A_{12}) + \ldots + P(E|A_{ij})P(A_{ij}), \tag{5}$$

where,

$$P(E|A_{11}) = P(B_{j2}|A_{11}) + P(B_{j3}|A_{11}) + \ldots + P(B_{jm}|A_{11}), \tag{6}$$

or

$$P(E|A_{11}) = \sum_{m=2}^{k} P(B_{jm}|A_{11}). \tag{7}$$

We can summarize the above equation as,

$$P(E|A_{ij}) = \sum_{m=1}^{k}\sum_{j=1}^{k} P(B_{jm}|A_{ij}), j \neq m. \tag{8}$$

By the application of Bayes theorem,

$$P(B_{j2}|A_{11}) = \frac{P(A_{11}|B_{j2})P(B_{j2})}{P(A_{11})}. \tag{9}$$

In general,

$$P(B_{jm}|A_{ij}) = \frac{P(A_{ij}|B_{jm})P(B_{jm})}{P(A_{ij})}, \quad j \neq m. \tag{10}$$

We have given some definitions to the symbols used in the above equations as,

P(A_{ij}) = Probability that the transmitted signal from the ADS function is A_{ij}

P(B_{jm}) = Probability that the received signal by the driving action layer is B_{jm}

P(B_{jm}|A_{ij}) = Probability that the received signal is B_{jm}, when the transmitted signal is A_i

P(E|A_{ij}) = Probability of an abnormal behavior when A_{ij} signal is transmitted from the ADS function

It is to be noted that all transmitted signals or messages (A_{ij}) are mutually exhaustive such that,

$$\sum_{j=1}^{k}\sum_{i=1}^{k} P(A_{ij}) = 1. \tag{11}$$

For the normal operation, j = m, and for error or abnormal behavior (E), j ≠ m.

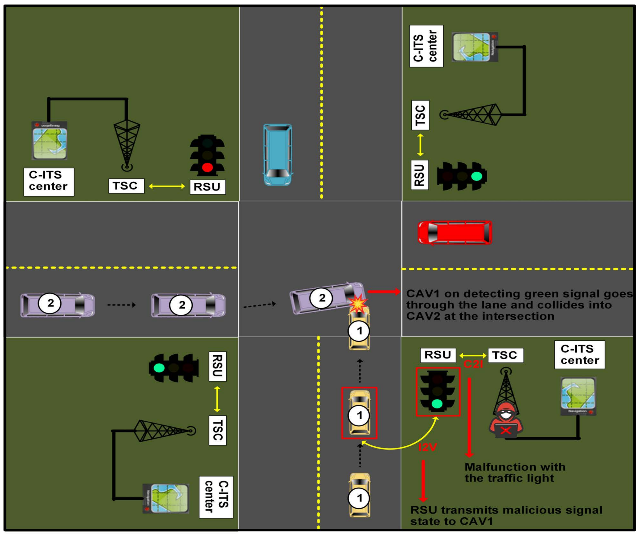

C-ITS center
TSC
RSU
C-ITS center
TSC
RSU
2
2
2
1
CAV1 on detecting green signal goes through the lane and collides into CAV2 at the intersection
RSU
TSC
C-ITS center
RSU
TSC
C2I
1
I2V
1
Malfunction with the traffic light
RSU transmits malicious signal state to CAV1
TSC
C-ITS center

FIGURE 7. CAV crash: application of C-ITS infrastructure cyberattack.

VIII. CASE STUDIES

We have presented here two hypothetical cyberattack scenarios causing a CAV road crash. 5Ws and 1H-based investigation is done to identify the contributing factors associated with the collision, and probability-based anomaly detection is directed toward identifying the abnormal activity corresponding to an ADS function.

A. ATTACK SCENARIO 1

An intended cyberattack event occurs in which an attacker exploits the vulnerability of lack of security consciousness of TSC and injects fake logic states and modified light timings to influence signal control decisions. Hence, it manipulates the traffic signal and renders it as "Green." As a result, RSU transmits the wrong signal state to CAV1. As a result, it disrupts the C-ITS application (e.g., traffic signal violations) and further impacts its vehicle detection algorithm. Due to this, CAV1 goes through the intersection and collides into CAV2 approaching from the left, and a collision is caused. Although the vehicle detection algorithm of CAV2 is running in good condition, due to the appearance of the "Green" signal, its speed is so high that it cannot avoid the situation, traverses the minimal stopping distance, and reaches the time of the collision. Therefore, it becomes too late in this situation to escape the crash, even though CAV2 has detected CAV1. Fig. 7 illustrates a CAV crash that is caused due to a cyberattack on the C-ITS infrastructure.

1) CAV CRASH INVESTIGATION

At the site of the CAV crash, the investigation team arrives and collects data from several sources, including cloud servers, CAV1, CAV2, and others, and formulates the data correlation. Then, based on conclusive evidence, reverse engineering is done, and the following analysis may be presented as shown in Table 3.

TABLE 3. 5Ws and 1H-based investigation for attack scenario 1.

Parameter	Description	Attack Scenario 1
Who	Attacker (ω)	ω: Hacker
	Victim (υ)	υ: C-ITS infrastructure
What	Attack target (μ)	μ: TSC
When	Date (λ)	λ1: 01, λ2: 22, λ3: 2022, Format: (01-22-2022)
	Time (τ)	τ1: EST, τ2: 04, τ3: 35, τ4: 40, τ5: 59, Format: (04:35:40:59)
Where	Attack path (σ)	σ: Manipulating the password and code of RSU controller
Why	Hazardous behavior (β)	β1: Non-detection of object, β2: hitting a car at intersection
How	Attack method (η)	η: Tampering

2) ANOMALY DETECTION

According to the proposed model, anomaly detection during the crash analysis for the given scenario can be done as illustrated in Fig. 8.

We have used synthetic signal transmission data between components of layer 4 and layer 5 to obtain the probability matrix given below,

The signal transmission probability matrix (T) is defined as,

$$\mathbf{T} = \begin{Bmatrix} 0.90 & 0.02 & 0.05 & 0.03 \\ 0.05 & 0.90 & 0.01 & 0.04 \\ 0.05 & 0.02 & 0.90 & 0.02 \\ 0.04 & 0.02 & 0.04 & 0.90 \end{Bmatrix}. \qquad (12)$$

In an ideal scenario (no cyberattack on the ADS functions), when the CAV sensors confront a "Green" traffic signal and a vehicle ahead at the intersection, the vehicle detection algorithm expects the car to decelerate and stop to avoid hitting the target vehicle. Therefore, based on probability, it sends the "Stop" control signal to the brake actuator to stop the car by 90%. However, the cyberattack perpetrates its vehicle detection algorithm, and it starts manifesting abnormal behaviors. As a result, even though the "Brake" control module has received the "Stop" control signal from the application, it denies it and transmits the unlikely signal, i.e., "Speed up," with a probability of 0.20, causing the acceleration of the CAV, which yields the host vehicle to an accident with the target vehicle. Hence, there is a non-adherence to the ideal path, which causes an accident.

B. ATTACK SCENARIO 2

An EVCS attacked by an adversary transmits wrong information over G2V communication to CAV1 (host vehicle), where the vehicle owner thinks that the battery is getting charged but the infected charging infrastructure attacks the ECUs of the vehicle. As a result, ECUs get corrupted during the charging process. Since ECUs control the car's sensors, the compromised ECUs send falsified messages to the sensors and cause them to misperceive their surroundings. Also, malicious data are sent to the ADS, which causes ADS function failure, such as non-detection of objects. There is a TSC

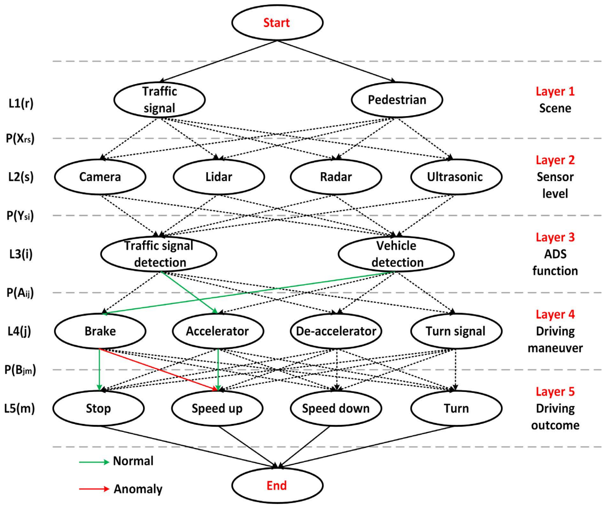


FIGURE 8. Probability-based abnormal behavior analysis of attack scenario 1.

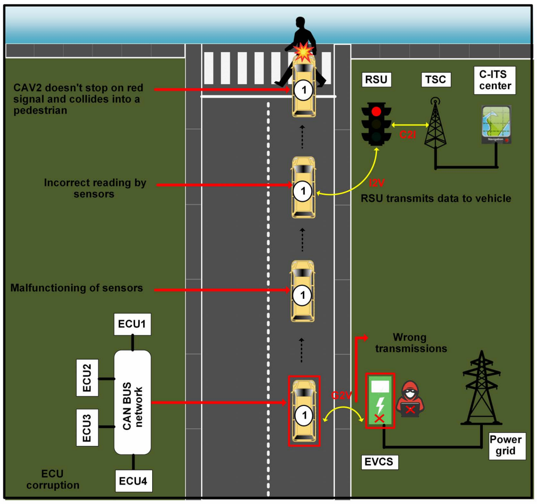

CAV2 doesn't stop on red signal and collides into a pedestrian
Incorrect reading by sensors
Malfunctioning of sensors
ECU1
ECU2
ECU3
CAN BUS network
ECU corruption
ECU4
1
RSU
TSC
C-ITS center
C2I
I2V
RSU transmits data to vehicle
Wrong transmissions
G2V
EVCS
Power grid

FIGURE 9. CAV crash: application of charging infrastructure cyberattack.

that transmits information on the signal phase to the RSU. The RSU broadcasts data to CAV1 via I2V communication. However, due to the sensors malfunctioning, CAV1 cannot detect the "Red" signal, and it does not stop. Further, ADS function failure causes non-detection of a pedestrian at the crosswalk, where it hits a pedestrian (VRU), and a collision is caused. Fig. 9 illustrates a CAV crash that is caused due to a cyberattack on the charging infrastructure.

1) CAV CRASH INVESTIGATION

Similar to case 1, the investigation is conducted at the crash site, and the following inferences may be drawn after data gathering as presented in Table 4.

2) ANOMALY DETECTION

According to this model, normal and abnormal behavior of the CAV can be distinguished as illustrated by Fig. 10. We have assumed the same synthetic dataset as defined by probability matrix (T).

In an ideal scenario (when there is no cyberattack), when the CAV sensors see a "Red" traffic signal and a pedestrian, the detection algorithms expect the vehicle to stop. Therefore, it sends the controlling commands to the brake actuator, which stops the car by 90%. However, due to the cyberattack, the ADS algorithms, i.e., traffic signal detection and pedestrian detection, get compromised and start exhibiting abnormal behaviors. As a result, even though the "Brake" control module has received the "Stop" control signal from the application, it transmits the falsified signal, e.g., "Speed up," with a probability of 0.20, causing the acceleration of the CAV, which renders the vehicle to an accident with the pedestrian. Therefore, the varying degree of conformity to the anticipated path contradicts the adopted course of actions, resulting in an anomaly.

TABLE 4. 5Ws and 1H-based investigation for attack scenario 2.

Parameter	Description	Attack Scenario 2
Who	Attacker (ω)	ω: Spy
	Victim (υ)	υ: Charging infrastructure (EVCS)
What	Attack target (μ)	μ: ECUs
When	Date (λ)	λ1: 03, λ2: 16, λ3: 2022, Format: (03-16-2022)
	Time (τ)	τ1: PST, τ2: 04, τ3: 35, τ4: 40, τ5: 59 τ5: 59, Format: (04:35:40:59)
Where	Attack path (σ)	σ: Charging process
Why	Hazardous behavior (β)	β1: Non-detection of pedestrian, β2: hitting a pedestrian at crosswalk
How	Attack method (η)	η: Spoofing

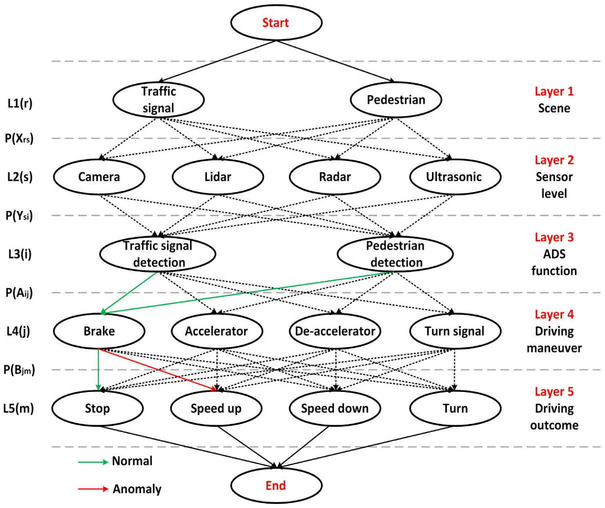


FIGURE 10. Probability-based abnormal behavior analysis of attack scenario 2.

IX. CONCLUSION

The modern mobility environment of a CAV, which is assumed to be a future L4 CAV, integrates the vehicle and the road infrastructure and other facilities. These include cloud servers, power grids, charging infrastructure, C-ITS center, etc. Hence, there are a lot of interactions involved among multiple entities, which drives the CAV ecosystem. However, the contributions from different cyber layer components come at the cost of cybersecurity issues. Due to complex CPSs associated with each of the entities, there are potential vulnerabilities that the threat agents can exploit to cause a CAV crash. Further, this paper applies STRIDE-based threat modeling to analyze and identify multiple potential threats endured by the CPSs engaged in the CAV ecosystem. By exploring the cyber processes behind the mobility environment and high-level ADS, we put forward a coordinated and balanced accident mechanism of a CAV and further review how a CAV accident can be caused by the inclusion of hostile communication from these entities. Moreover, analogous to the conventional vehicle accident investigation, the juxtaposition of multiple cyber elements enhances the complexity of the CAV accident, which renders the AV investigation very challenging. Therefore, a first-of-its-kind 5Ws and 1H-based digital investigation framework is designed, which identifies the cybersecurity events responsible for the functional failure or crash. In addition, we aim to provide a novel research concept and develop an effective probability-based anomaly detection to recognize the ADS function failure during a crash analysis. Further, case studies are presented to validate the proposed models, which show the accuracy and reliability of these frameworks. However, the investigation model has some limitations and boundaries since we do not have the real-time dataset to diagnose the attackers. For future work, using these frameworks, we can fabricate distinguishable cyberattack scenarios that can engender crashes in CAVs and investigate these crashes. Also, we can model these cyberattacks on CAVs by using any simulated platform for AVs to analyze their behavior. Besides, in a future mobility environment where L4 CAV driving relies completely on the ADS, we need to have a systematic investigation process for the diagnosis of the safety failures caused by external cyberattacks, faults caused by hardware or software malfunction, and unlearned edge case occurrences that lead to accidents. These frameworks for identifying a cyber event and investigating an accident can be used to diagnose the root causes of unexpected maneuvers of CAVs as a result of a cyber incident. Also, through this AV accident investigation process, we can calculate the ratio of negligence in the AV involved in an accident.

REFERENCES

[1] M. Fanoro, M. Božanić, and S. Sinha, "A review of 4IR/5IR enabling technologies and their linkage to manufacturing supply chain," *Technologies*, vol. 9, no. 4, p. 77, Oct. 2021.

[2] S. Khanam, S. Tanweer, and S. Khalid, "Artificial intelligence surpassing human intelligence: Factual or hoax," *Comput. J.*, vol. 64, no. 12, pp. 1832–1839, Dec. 2021.

[3] G. Thandavarayan, M. Sepulcre, and J. Gozalvez, "Cooperative perception for connected and automated vehicles: Evaluation and impact of congestion control," *IEEE Access*, vol. 8, pp. 197665–197683, 2020.

[4] M. Girdhar, J. Hong, H. Lee, and T.-J. Song, "Hidden Markov models based anomaly correlations for the cyber-physical security of EV charging stations," *IEEE Trans. Smart Grid*, early access, Oct. 21, 2021, doi: 10.1109/TSG.2021.3122106.

[5] Á. Takács, I. Rudas, D. Bösl, and T. Haidegger, "Highly automated vehicles and self-driving cars," *IEEE Robot. Autom. Mag.*, vol. 25, no. 4, pp. 106–112, Dec. 2018.

[6] S. Garg, M. Guizani, Y.-C. Liang, F. Granelli, N. Prasad, and R. R. V. Prasad, "Guest editorial special issue on intent-based networking for 5G-envisioned internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5009–5017, Aug. 2021.

[7] H. Alghodhaifi and S. Lakshmanan, "Autonomous vehicle evaluation: A comprehensive survey on modeling and simulation approaches," *IEEE Access*, vol. 9, pp. 151531–151566, 2021.

[8] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 1–20, Jul. 2021.

[9] L. Jiang, Y. Zhang, T. Li, X. Diao, and J. Zhang, "Analysis on charging safety and optimization of electric vehicles," in *Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC)*, Jun. 2020, pp. 2382–2385.

[10] S. Maaloul, H. Aniss, M. Kassab, and M. Berbineau, "Classification of C-ITS services in vehicular environments," *IEEE Access*, vol. 9, pp. 117868–117879, 2021.

[11] Z. Zhong, Y. Tang, Y. Zhou, V. Neves, Y. Liu, and B. Ray, "A survey on scenario-based testing for automated driving systems in high-fidelity simulation," 2021, *arXiv:2112.00964*.

[12] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transp. Telecommun. J.*, vol. 19, no. 4, pp. 325–334, Dec. 2018.

[13] M. A. Khan, "Intelligent environment enabling autonomous driving," *IEEE Access*, vol. 9, pp. 32997–33017, 2021.

[14] W. Xiong, S. He, and T. Z. Qiu, "Research on connected vehicle architecture based on DSRC technology," in *Proc. 4th Int. Conf. Transp. Inf. Saf. (ICTIS)*, Aug. 2017, pp. 530–534.

[15] J. Chen and J. Tan, "NR V2X: Technologies, performance, and standardization," in *Proc. 54th Asilomar Conf. Signals, Syst., Comput.*, Nov. 2020, pp. 1012–1016.

[16] H. Miyata, "Digital transformation of automobile and mobility service," in *Proc. Int. Conf. Field-Programmable Technol. (FPT)*, Dec. 2018, pp. 1–5.

[17] L. Butler, T. Yigitcanlar, and A. Paz, "How can smart mobility innovations alleviate transportation disadvantage? Assembling a conceptual framework through a systematic review," *Appl. Sci.*, vol. 10, no. 18, p. 6306, Sep. 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/18/6306

[18] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[19] K. P. Divakarla, A. Emadi, and S. Razavi, "A cognitive advanced driver assistance systems architecture for autonomous-capable electrified vehicles," *IEEE Trans. Transport. Electrific.*, vol. 5, no. 1, pp. 48–58, Mar. 2019.

[20] J. Cui, G. Sabaliauskaite, L. S. Liew, F. Zhou, and B. Zhang, "Collaborative analysis framework of safety and security for autonomous vehicles," *IEEE Access*, vol. 7, pp. 148672–148683, 2019.

[21] *Evaluation of Autonomous Products*, Standard UL4600, Underwriters Laboratories (UL) Standards, Geneva, CH, 2022.

[22] *Road Vehicles—Safety of the Intended Functionality*, Standard ISO/PAS 21448:2019, International Organization for Standardization, Geneva, CH, Jan. 2019.

[23] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[24] *California Autonomous Vehicle Regulations*, California Dept. Motor Vehicle, USA, Jun. 2020.

[25] *Road Vehicles—Traffic Accident Analysis*, Standard ISO 12353-1:2020, International Organization for Standardization, Geneva, CH, 2020.

[26] J. Shuttleworth, "SAE and iso refine the levels of driving automation," SAE News, SAE Int., USA, Tech. Rep., Jun. 4, 2021.

[27] *All You Need to Know About Automated Vehicles*, vol. 10, UNECE, Geneva, Switzerland, 2021.

[28] *Framework for Automated Driving System Safety*, NHTSA and USDOT, USA, Dec. 2020.

[29] *Road Vehicles—Terms and Definitions of Test Scenarios for Automated Driving Systems*, Standard ISO/DIS 34501, International Organization for Standardization, Geneva, CH, 2021.

[30] *Road Vehicles—Scenario-Based Safety Evaluation Framework for Automated Driving Systems*, Standard ISO/DIS 34502, International Organization for Standardization, Geneva, CH, 2021.

[31] *Road Vehicles—Taxonomy for Operational Design Domain for Automated Driving Systems*, Standard ISO/DIS 34503, International Organization for Standardization, Geneva, CH, 2021.

[32] *ASAM Publishes Concept for a New Autonomous Vehicle Safety Standard Enabling Testing for Road Readiness*, ASAM, Germany, Feb. 2022.

[33] K. Jo, J. Kim, D. Kim, C. Jang, and M. Sunwoo, ''Development of autonomous car—Part I: Distributed system architecture and development process,'' *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, pp. 7131–7140, Dec. 2014.

[34] M. L. Cunningham and M. A. Regan, ''Driver distraction and inattention in the realm of automated driving,'' *IET Intell. Transp. Syst.*, vol. 12, no. 6, pp. 407–413, Aug. 2018.

[35] O. Jarosch, H. Bellem, and K. Bengler, ''Effects of task-induced fatigue in prolonged conditional automated driving,'' *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 61, no. 7, pp. 1186–1199, Nov. 2019.

[36] H. Ning, R. Yin, A. Ullah, and F. Shi, ''A survey on hybrid human-artificial intelligence for autonomous driving,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6011–6026, Jul. 2022.

[37] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for on-Road Motor Vehicles*, Standard SAE j3016, SAE, Geneva, CH, Apr. 2021.

[38] C. Techblog, ''Understanding operational design domain to create informed safety in autonomous vehicles deployment,'' Tech Blog, Claytex, U.K., Jul. 23, 2021.

[39] *Timing in Autonomous Vehicles*, Srinivas Bangalore, India, Mar. 2019.

[40] *What are the Levels of Automated Driving?*, Aptiv Mobility Insider, Ireland, Nov. 2020.

[41] *Global Automotive Ultrasonic Sensors Market 2021–2026*, Mobility Foresights, India, 2021.

[42] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, ''Attacks on self-driving cars and their countermeasures: A survey,'' *IEEE Access*, vol. 8, pp. 207308–207342, 2020.

[43] *The Sensing Systems That Make Adas Work*, Ed Brown Sensor Technol., USA, Mar. 2021.

[44] C. Mellor, ''Autonomous vehicle data storage: We grill self-driving car experts about sensors, clouds and robo taxis,'' Tech News, Blocksandfiles, U.K., Feb. 3, 2020.

[45] *Automotive Connectivity Evolves to Meet Demands for Speed & Bandwidth*, Connection Supplier, USA, Nov. 2019.

[46] C. Mellor, ''Data storage estimates for intelligent vehicles vary widely,'' Tech News, Blocksandfiles, U.K., Jan. 17, 2020.

[47] S. Wright, ''Autonomous cars generate more than 300 TB of data per year,'' Tech Blog, Tuxera, Finland, Jul. 2, 2021.

[48] A. Madhok, ''Autonomous vehicles to boost memory requirement,'' Tech Mag. Article, Telematics Wire, India, Feb. 17, 2021.

[49] B. Popa, ''Next-gen cars will need 11tb of storage to handle the data we throw at them,'' Tech News, AutoEvol., USA, Nov. 6, 2020.

[50] M. Staff, ''High-speed data and connected cars,'' Tech Article, Wevolver, The Netherlands, May 21, 2021.

[51] M. Rafie, ''Edge ai computing advancements driving autonomous vehicle potential,'' Tech Forum Article, Global Semicond. Alliance, USA, Oct. 28, 2021.

[52] S. Evers, ''Cinco-play: Memory is that critical to autonomous driving,'' Tech Blog, Micron, USA, Nov. 1, 2017.

[53] A. World, ''Bosch: Did you know..facts and figures about electronics and software in vehicles,'' Tech News Article, Automot. World, U.K., Jul. 21, 2020.

[54] J. Mamala, M. Śmieja, and K. Prażnowski, ''Analysis of the total unit energy consumption of a car with a hybrid drive system in real operating conditions,'' *Energies*, vol. 14, no. 13, p. 3966, Jul. 2021.

[55] O. Mitchell, ''Self-driving cars have power consumption problems,'' Tech News Article, Robot Rep., USA, Feb. 26, 2018.

[56] N. Harris, ''Light is the key to long-range, fully autonomous EVS,'' Tech News Article, TechCrunch, USA, May 24, 2021.

[57] F. Zhu, Y. Lv, Y. Chen, X. Wang, and F. Wang, ''Parallel transportation systems: Toward IoT-enabled smart urban traffic control and management,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 10, pp. 4063–4071, Oct. 2020.

[58] F. A. Butt, J. N. Chattha, J. Ahmad, M. U. Zia, M. Rizwan, and I. H. Naqvi, ''On the integration of enabling wireless technologies and sensor fusion for next-generation connected and autonomous vehicles,'' *IEEE Access*, vol. 10, pp. 14643–14668, 2022.

[59] H. Wang, T. Liu, B. Kim, C.-W. Lin, S. Shiraishi, J. Xie, and Z. Han, ''Architectural design alternatives based on cloud/edge/fog computing for connected vehicles,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2349–2377, 4th Quart., 2020.

[60] B. C. Zanchin, R. Adamshuk, M. M. Santos, and K. S. Collazos, ''On the instrumentation and classification of autonomous cars,'' in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2631–2636.

[61] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, ''Evolution of V2X communication and integration of blockchain for security enhancements,'' *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020.

[62] M. Koschuch, W. Sebron, Z. Szalay, A. Torok, H. Tschiurtz, and I. Wahl, ''Safety & security in the context of autonomous driving,'' in *Proc. IEEE Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2019, pp. 1–7.

[63] E. Dubrova, *Fault-Tolerant Design*. New York, NY, USA: Springer, 2013.

[64] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, ''STRIDE-based threat modeling for cyber-physical systems,'' in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sep. 2017, pp. 1–6.

[65] M. Li, J. Weng, J.-N. Liu, X. Lin, and C. Obimbo, ''Toward vehicular digital forensics from decentralized trust: An accountable, privacy-preserving, and secure realization,'' *IEEE Internet Things J.*, vol. 9, no. 9, pp. 7009–7024, May 2021.

[66] D. Watson and A. Jones, *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*. Amsterdam, The Netherlands: Elsevier, 2013.

[67] D. Kopencova and R. Rak, ''Issues of vehicle digital forensics,'' in *Proc. 12th Int. Sci. Tech. Conf. Automot. Saf.*, Oct. 2020, pp. 1–6.

[68] M. Clamann, A. Khattak, and K. Clark, ''Advancing crash investigation with connected and automated vehicle data,'' Collaborative Sci. Center Road Saf., USA, Tech. Rep. CSCRS-R25.1, Jul. 2021.

[69] M. Brach, M. B. Raymond, and J. Mason, *Vehicle Accident Analysis and Reconstruction Methods*, 3rd ed. Warrendale, PA, USA: SAE, 2022.

MANSI GIRDHAR (Graduate Student Member, IEEE) received the B.Tech. and M.Tech. degrees in electronics and communication engineering from the Guru Nanak Dev Engineering College, India, in 2014 and 2017, respectively. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Michigan–Dearborn, USA. Her research interests include cybersecurity of power systems, electric vehicle charging stations (EVCSs), and connected and automated vehicles (CAVs).

YONGSIK YOU (Graduate Student Member, IEEE) received the B.E. degree in urban engineering from Chungbuk National University, Republic of Korea, in 2020, where he is currently pursuing the integrated master's and Ph.D. degree with the Department of Urban Environmental Energy Convergence. His research interests include transportation safety, traffic accident investigation, and connected and automated e-mobility environment.

TAI-JIN SONG (Member, IEEE) received the Ph.D. degree in civil, construction and environmental engineering from North Carolina State University, Raleigh, in 2016. His doctoral work was on the long-term congestion monitoring and analytics system in a large-scale network to support a connected automated vehicles systems. He is currently an Assistant Professor with the Department of Urban Engineering, Chungbuk National University. Prior to joining Chungbuk National University, he has worked as an Associate Research Fellow at The Korea Transport Institute for three years and conducted more than ten research projects for developing new green energy-based mobility systems (EVs) and a national transport big data platform, identifying insights from new sources of mobility big data in transportation field. His research interests include cybersecurity on connected automated vehicles under digital road infrastructure and multi-modal transportation systems, such as mobility as a service (MaaS). He serves in WG 19 ''Mobility Integration'' in ISO TC 204 (Intelligent Transport System).

SUBHADIP GHOSH (Graduate Student Member, IEEE) received the B.Tech. degree in computer science and engineering from the West Bengal University of Technology, India, in 2006, and the M.S. degree in electric-drive vehicle engineering from Wayne State University, MI, USA, in 2014. He is currently pursuing the Doctor of Engineering degree with the University of Michigan–Dearborn, USA. Since 2006, he has been working in systems and software development for automotive ECUs in body, EV, and ADAS domain. He has provided technical leadership in core product development, foundational architecture, and advanced feature design. He is an Automotive System-Software Engineer at Ford Motor Company, MI, USA. His research interest includes cybersecurity of autonomous and connected vehicles.

JUNHO HONG (Member, IEEE) received the Ph.D. degree in cybersecurity of substation automation system in electrical engineering from Washington State University, Pullman, in 2014. From 2014 to 2019, he has worked with ABB, where he provided technical project leadership and supports strategic corporate technology development/productization in the areas related to cyber-physical security for substation, power grids control and protection, renewable integration, and utility communications. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Michigan–Dearborn. He has been working on cybersecurity of energy delivery systems with the Department of Energy (DOE), as a Principal Investigator (PI) and a Co-PI in the areas of substation, microgrid, HVDC, FACTS, and high power EV charger. He serves in Cigre WG D2.50 ''Electric power utilities' cybersecurity for contingency operations.''