Cognitive Risk Assessment Models for Cybersecurity in Autonomous Vehicle Operations

By Dr. Siarhei Katsevich

Associate Professor of Computer Science, Belarusian State University of Informatics and Radioelectronics (BSUIR), Belarus

1. Introduction to Cognitive Risk Assessment in Cybersecurity

Many autonomous vehicle (AV) functions have already been defined and have demonstrated a positive potential impact if properly adapted, including platooning and cooperative adaptive cruise control (CACC) techniques [1]. Functional, reactive and object-oriented (FRaOOP) requirements, like primary safety (PS) and physical safety (PhS) and cyber safety (CS), have been taken into account in the cybersecurity literature, thus far excluding the characterization of human intelligence which is a key requirement as well. The current cybersecurity validation test benches combine the Reinforcement Learning approach to simulate an adversarial strategy for their implementation and a framework with the Fault Injection approach. Also, in the Authors' literature an automatic evaluation methodology for the test bench was investigated with the goal to assess countermeasure effectiveness. This paper enhances the research presented in the literature with a novel and innovative approach referred to as the cognitive cybersecurity framework, where the human intelligence characteristic has been introduced in the validation test bench. This approach allows the AV companies to evaluate the criticality of the residually exploitable cybersecurity weakness, thus improving the design-phase criticality mitigation and countermeasures ranking process by a V2I cognitive reticularity methodology.

The advent of connected, autonomous, and intelligent vehicles has revolutionized the automotive landscape and reshaped conventional paradigms for the development and testing of complex embedded system platforms [2]. Due to the exponentially increasing trend in the number of inter-vehicular communication networks and extent of public infrastructure integration, the level of cyber-physical engagement of these vehicles is extremely high—even comprising regular internet service provisioning for some advanced functionalities in which diverse strategic, safety-critical data are exchanged bilaterally [3]. This cyber-physical convergence of connected autonomous vehicles (CAVs) is trending toward development of the emerging paradigm of vehicular intelligent transportation systems (V-ITSs) in the transportation context. The vehicular security and privacy implications of cyber-physical systems have been recognized as one of the primary challenges for potential optimization, revolutionizing operational and safety-critical implications for these high-tech transportation systems.

1.1. Definition and Importance of Cognitive Risk Assessment

The large idea of this research is the "importance to push for collaborative "smart solutions" that could help to prevent, detect and respond in an automatic way without the need to stop the running systems or make manual reconfiguration, so that continue standard operation using the "untouched" autonomous or adaptive systems in face of the problems caused by the aggressor. Model is equipped with a collision learning network for determining the most significant events and parameters that make the system subject to cybersecurity attacks in the training session, and learning path search algorithm for both finding a subset of input and the most effective attack method of the parameter [4].

This article addresses the cognitive risk assessment in the context of cybersecurity in autonomous vehicle operations, aiming to propose a reasoning-oriented model for assessing the attack risk in the vehicle state prediction module [5]. In the period from 1980 to 2000, a range of probabilistic risk assessment models have been developed with the primary goal of better understanding and managing rare events in the risk-critical systems, especially for the safety-critical design domains (e.g., safety critical operations on airplanes) [6]. This area of research has since evolved dramatically focusing on managerial and legalistic element, making strides in international and national normative publications, which specifies the requirements and time driven processes for "evaluation for commercial systems, threat analysis" etc. International renowned actuarial norms like ISO/IEC 27001 fully incorporates the threats and vulnerabilities related elements, costing billions of dollars to loss and exposed to attacks, should only doubt this conventional approaches. One of the authentic example of such lost with respect to autonomous systems is cyber security was also estimated at 230 billion dollars.

1.2. Relevance to Cybersecurity in Autonomous Vehicles

It is only since the early 1990s that the previously largely ignored cybersecurity of in-vehicle components and automobile electronics has been given attention. The automotive industry plays a major role in the way that security risk is classically managed because risk assessment is integral to the ways that vehicle safety is approved and achieved. Cybersecurity risk is an important dimensional aspect of the vehicle safety landscape. No vehicle cybersecurity risks possessed were entertained by classic total vehicle conformance before automotive security threats became widely understood [6]. Furthermore, the paradigm fostering the ideal of self-learning systems is not only a set invitation to hacking but also a systemic normative training that in cyber-physical systems like autonomous vehicles proves dangerous when the system lies in a state of superintelligent moral incompetence within the risk factors for self-driving cars, completely independent of and ignorant about adverse ethical consequences.

Security and privacy concerns are paramount in the design and implementation of nine systems, especially in the context of AI solutions and IoT-based use cases such as autonomous vehicles (AVs). To address security threats and breaches, organizations need to have a defined risk assessment plan to mitigate security issues [4]. Security measures are particularly crucial in AVs, because once an attack is successful, the consequences could be severe, leading to injuries or fatalities or financial loss. Several security breach scenarios ranging from personal data theft to car accidents are familiar. As semi- and fully autonomous vehicles become more commonplace, cybersecurity becomes even more important. AVs depend on onboard computers to function, and if cyber threats such as hacking and malware become active security risks, the consequences can be significant. Existing risk assessment methods in cybersecurity risk management are not appropriate in the context of AVs because comprehensive understanding of how systems function is still evolving, and the methods do not recognize a navigation system in which humans are no longer necessary agents and cybersecurity systems should function as the guardians of a vehicle. Developments in risk-aware decision-making research could provide new avenues for navigation planning in the context of a first-stage risk assessment in AVs [7].

2. Fundamentals of Autonomous Vehicle Operations

By 2030, US$3.5 trillion will have been invested in connected, automated and autonomous vehicle (CAV) technologies. The positive impact of CAVs on society is undeniable and coming to fruition. Conversely, attacks against CAVs have become more frequent and disruptive, exhibiting a sixfold increase from just 2019 to 2020 [8]. In this paper, we attempt to fill the gap about formal, cognitive-based security risk assessment for cybersecurity in CAVs. This assessment will help to increase the operational reliability and security in CAVs for all stakeholders (public sector, governance institutions, and industries), ranging from automotive and ICT to system developers. The target model is to increase the perception level of CAVs by utilizing a cognitive architecture that emulates human-level perceptually-motivated risk assessment. The aim is to speed up the cyber risk assessment phase in the rapid development of cognitive approaches in the mature domains of anomaly detection and preventive security by enhancing the reliability, autonomy, and security of CAVs.

[7]To summarize, we first introduced the basic features of connected and automated vehicles (CAVs), classified the different types of cybersecurity attacks that an autonomous vehicle (AV) may encounter (Section 2). We then reviewed cybersecurity risk assessment controversies, research gaps, and emerging challenges, and covered most recent accomplishments. The remainder of the study is organized as follows. Section 3 presents the use of Cognitive CyRA as identified in the literature. We give a state of the art regarding security risk management approaches in Section 4. Section 5 presents how cognitive models are integrated into the CyRA approaches. We then develop our cognitive risk assessment model (Section 6). Finally, in Section 7, we present two case studies that validate our approach on an empirical scenario.

2.1. Overview of Autonomous Vehicle Technology

The significant advancement of technology that has led to the intuition of Industry 5.0 and the adaptive smart city concept-viz. 5G/6G has not completely developed yet. New technologies always look promising, but as the information evolves, cyber safety and privacy vulnerabilities must be ensured. A complete redesign of the existing security models is needed, in at least some IoT development efforts, which emphasize risk-correlated functional prioritization. Therefore, it is essential to unify the network security standard to ensure the acceptance of existing and future cybersecurity threats on resale of zero-day software and thus the protection of protection mechanisms and digital data confidence in automated driving vehicles.

Cyber–physical systems (CPSs) don't distinguish between the computing, networking, and physical parts. When attacked, the vehicle system becomes impaired, increasing the likelihood of accidents and creating data privacy threats. Connected and autonomous vehicles (CAVs), conceptually, are vehicles with self-driving functionality and having access to, and are using, connectivity for at least one of the operating purposes. For operational success, CAVs use emerging digital technologies such as Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain. In addition to construction, several physical safety and digital security measures are required.

2.2. Key Components and Systems

Studies need to be focused on i5G connection, communication policies, availability of quantum-based communication. Determining how electromagnetic risks can create potential health risks of distant and close living forms. One forming sitations are completely human vehicle relationship. The vehicle is not only the driver, mechatronic-based communication parts between the passenger and the vehicle, made by the defined risk components and margin values are exposed to spherical risks. These should also be prioritized for investigation [6, 15] [9]. These risks will change in proportion to machine intelligence and, like the connection and communication conditions, will be the determinative factors for the sustainability of the vehicle's life cycle. Therefore, for driverless vehicles, cyber-crime should be designed by focusing only on all of the high-level machines, together with students and public institutions with regulatory positions. The general element of the study explains that Cybersecurity risks in the actuator types in logic or in the transfer wave motor used in the endurance of the Analbot RedVehicle, the vehicle zone of the Z-transporter and the in-vehicle center. It is emphasized that it consists of that stopping and malfunctioning states may occur more than in the normal stopping case, and that the occurrence of the latter stopping and halting cases affects the error of passenger travel and jeopardizes road safety. Do it on the machine based Bits have given a decision in showing when they are the own car adverse, a parking point signal and also the obstacle on the road for 100 ms. When internal and external communication is approved through a service provider, in order to enhance the active system as much as possible for the multiplication of the toxic connection point by internal and external producing rules, usually risks that have never been mentioned much are then expressed. This method of providing instant information and implementation of the environmental service creates curative steps to be taken against potentially emerging cyber problems.

Like any other vehicle, a vehicle brain consists of several key components that are interconnected with numerous systems, which form the control surfaces, the communication systems, an the overall glide path of its operation on the roads (Maduna, Težak & Mrdović, 2019). Its body (like chassis and engine) is the one that will cover the most risks (engineer, 2020). However, the brains of future vehicles are recommended to have all the necessary components needed for cybersecurity, even more than the amount of components needed for the brains of today's vehicles (Sukhandeh, 2015). In the future, the volume of cyber parts will be about twenty to one hundred times larger than combustion engine related parts. Then, it would significantly reduce the risks related to cybersecurity concentrated on the vehicle. Addressable risk factors of physical cyber security is composed of a multitude of risks. The programmer and vehicle industries themselves; critical infrastructures that can be focused on by targeted cyber attacks; Terabyte data that experts can analyze for service improvement, marketing, and customer satisfaction have to be on the road together.

3. Cybersecurity Threats in Autonomous Vehicles

Constant developments in technologies have led to challenging vehicles from standalone developments to communication-enabled vehicles, drastically transforming the security goals, design principles and guidelines from disruptive security strategies to integrated automobile AV cybersecurity platforms. When a vehicle is driven by AI, protecting the privacy and ensuring user authentication becomes more paramount. Security theories and practices are bridged with new aims and elements toward building a secure stage of autonomous vehicles. Theoretical literature, requiring to be validated as a form of proof of concept and field investigated, is the basis for design and development of cybersecurity schemes of autonomous vehicle (AV) technologies [10]. As witnessed in the literature, however, there are not many continuous effort shedding light on the refuting grammatical biases of protecting autonomous vehicle privacy and user recognition. This paper attributed a typology to the seminal researches obtaining narratives on topics of protecting user datasets and sources of AVs by entitling the research as user privacy, and user recognition in the recognition of reviewed AutoML researches and their categories.

A number of cybersecurity threats are of growing concern in the autonomous vehicles. The vulnerabilities lead to motley adverse effects in a direct and indirect manner, e.g., messing with drivability and safety of AVs, breaking authentication protocols and hijacking their devices and stealing their personal and sensitive data [11]. The auto industry lacks well-formulated and well-implemented standards and operational strategies for ensuring and ascertaining the security of autonomous vehicles against cyberattacks. In this context, this chapter explores security breaches in autonomous vehicle (AV) systems and CAN systems. The controllers and in-vehicle hardware and software are connected through a built-in network called the Controller Area Network (CAN), and the controllers are also interconnected through the internet [12]. Thus, all data and commands use CAN as a medium of communication, making it a critical resourceful asset for the connected services in AVs. The author also proposes a security framework for AVs and CAN-based in- vehicle systems and how to find the danger of those vulnerabilities.

3.1. Types of Cybersecurity Threats

There is a need to develop a method to ensure transparency for any attack that potentially takes place in the vehicular network. However, in the context of interconnected and unconnected autonomous systems, it becomes increasingly difficult to design such decryption and verifiable decision-making algorithms. This difficulty exists in the cognitive risk assessment model; therefore, understanding different types of cyber threats and their objectives is the first step in the prevention, mitigation, and transfer of strategic cyber risks. If such an epic failure is intertwined with economic, environmental, military, intelligence, and political issues—global and national impacts could be easily contemplated. The real-world example of such catastrophic realization is the Zero-day attack of the STUXNET worm which caused more than 1000 gas centrifuges to get out of service causing big losses and protraction in the time left for Iran to have a bomb. SSA agents injected synchrophasor measurement data from four compromised Phasor Measurement Units (PMUs) to ten target supervisory control and data acquisition (SCADA) devices, and were never detected by any means for an average of 10/424 out of 110 times. Fundamental hurdles that have made it harder to identify advanced persistent threat attacks. Participating in the working groups, contributing to journals and conferences, and being part of standardization processes helps to reduce and manage global challenges and to promote societal wellbeing [8].

Road vehicle manufacturers have started producing advanced driver assistance systems, and it is estimated that autonomous vehicles will be commercially available in the near future. The utility of an autonomous vehicle is not limited to the transportation of humans but spans a wide range of activities including: labor and logistics, the military, intelligent transport, remote sensing, railroads, agricultural work, earth observation, air transport, radio astronomy, and mining. Such vehicles can navigate in urban and off-road environments and respond to complex events in these environments without direct human intervention. Key challenges of autonomous vehicle operation in off-road environments are that the perception of surroundings could be compromised due to stochastic (rain, snow, etc.) and human-made phenomena (smoke, etc.) and that the communication with the main operator or base could not be established at all times. Communication can be lost or jammed by bad actors, the environment may block signals to reach the main operator, and the time it takes for information to travel back and forth commands the system to take decisions autonomously. Moreover, in the case of mission critical operations, the system should be robust against various cyber threats such as: DoS attacks, de-synchronization attacks, sensor attacks, deception attacks, replay attacks, man-in-the-middle attacks, and malicious actor attacks that are designed to disable or to command the system. These cryptographic schemes have been shown not to be failure-free. In actual, because crypto vulnerabilities were exploited, numerous critical inter and non-interconnected road vehicle networks were misused or put out of service for different periods of time [13] [2].

3.2. Vulnerabilities in Autonomous Vehicle Systems

[11] The literature review reveals an extensive list of attacks including the Longitudinal Control Malfunction, the Latitudinal Control Malfunction, Shadow Attack, GPS Spoofing Attack, Rub Rate Malfunction, DA Injection, ESC Failure, Adaptive Cruise Control Failure, Automatic Parking System Failure, Hardware Insecurity Attack, Sensors Poisoning Bypass, Synthetic Image, Full Sensor Jamming, Hardware Toxic Data Attack, Stealthy Poisoning Modification, Cloaked Control Injection, Stealthy Fault Injection, and Optimization Challenge. The review also points out that these attacks can be Partitioned in three categories: Attacks through the Vehicle, Attacks through the Infrastructure, and Attacks through the Network. The review further discusses applications of Intrusion Detection Systems to address the latter category. The review fmed the inadequacy of previous negotiations method and hence pmpose a privacy preserving Federation Learning Negotiation (FLN) scheme which

not only mutes privacy issue but also provide better communication efficiency. The paper concludes witl i a comparison of different methods in18 Sectlon 5.[4] Abstract: This paper studies long-range electron–molecule interaction involving Rydberg states which possess well-defined molecular character. Dai et al. [H. Dai, C. Shi, X. Ren, Phys. Rev. Research 3 (4) (2021) 043101] have recently proposed a mixed Rydberg-Chrinsiek wave packet (MRCWP) scheme to accurately solve the time-dependent two-body Schrdinger equation mediated by the polar-catastrophic interaction potentials. We apply this method to further study the qualitative and quantitative electronic structures of the polar-catastrophic molecular orbital. We investigate two major types of states formed within the Rydberg manifold, the Rydberg mixed states and the Rydberg vibrational states. Both types of states require the MRCWP approach to exactly simulate their two-electron time-evolution properties. The consideration of the long-range interaction enables this model to obtain a series of molecular spectra of observed Rydberg molecules and prepare for further Rydberg-molecule studies through the polarization catastrophe model.

4. Theoretical Frameworks for Cognitive Risk Assessment

In contrast to TVRA, Carnegie Mellon University's systematic OCTAVE (Operationally Critical ThreatAsset, and Vulnerability Evaluation) curve is focused on structural systemic failure in the functioning of the system under analysis [14]. Criticality is introduced to bridge internal weaknesses with external threats. Contrary to the TVRA model, its evaluation is extended to cover weak points and assets, followed by grading them and directing the processes based on the degree of system importance. In addition, reflective evaluations further contributes to the model's accuracy. Conversely, TVRA does not have either a directed assessment process or an internal adversary perspective.

The most appropriate risk analysis methodology for the inter-relationship between passengertransport and autonomous vehicles is TVRA (ThreatVulnerabilityRiskAssessment) . This model is founded upon the integration of the following five dimensions: origin, mechanism, target, impact, and likelihood. Given the complexity of the autonomous vehicle system, the TVRA model can interpret the risk associated with each vehicle dimension, derived from the related threat. Most significantly, TVRA introduces the notion of TVRA with respect to autonomous transport as "TVRA-AV model." Accordingly, the crisis perspective guides the risk associated with the autonomous vehicle system.

4.1. Human Factors in Cybersecurity Risk Assessment

We review human involvement within the context of vehicle cyber hazard and put up a probabilistic hierarchical decision-making framework that predicts and isolates human-enacted hazards through the use of a Generative Adversarial Network (GAN)-based behavior model monitoring system. Moreover, we discuss the intermittently risk-averse character of cyber defense operations, which autonomously switch into heightened level of safety in the case of anomalies that demand additional protection [15]. For that level of heightened level of safety, the offered models can allow the hacker to stay under the radar of cybersecurity risk management, because, as long as no severe, malicious action is executed by the attacker, he is codified as a regular passenger.

Several studies have confirmed that human interaction with an autonomous vehicle (AV) upsets the firewall-like stance on cyber security. The addition of users, in several cases, introduces weaknesses which, if exploited, can directly impact system safety. In recent literature, several authors have planned a range of algorithms that aim at infiltration of in-vehicle networks under command of a cyber attacker [13]. However, another critical risk is also posed by crew members, pedestrians, passengers and people outside the vehicle, who may unexpectedly change their expected behavior and pose an unjustified threat to vehicle safety, no matter what command only the base (i.e., the AV) excretes. It is thus imperative that human factors are included in the cybersecurity risk assessment for autonomous vehicles.

4.2. Cognitive Bias and Decision Making

One of the initial and cornerstones for the development of automated vehicles and eventually highly autonomous or driverless vehicles is effective real-time perception, sensor information interpretation, and risk assessment and decision-making models able to help decision-making within large uncertainty in benign and adversarial traffic environment conditions [6]. It should be kept in mind that the vast majority of these systems serve AI systems that have been trained and validated for benign operational domains. This fact, however, does not imply that the system can make exactly the correct decision and perceived the traffic environment exactly and in due time. While there can be all kinds of benign risk sources that AI systems cann ot account for, a critical group of risk factors stems from the decisions the agent systems (automated vehicles (AVs) included) make and execute autonomously or semi-automatically, subject to a sequence of information perceptions, and infrequent sensor infrastructural updates due to strategic and not the real-time operational condition of the traffic scenario.

To unfold the DRAFC model in practical autonomous vehicle operations, this section first introduces several decision-making and decision-support models in the domain of cyber-physical infrastructure systems. Multiple AI and ML models in the mobility and energy sectors have been deployed to enable more efficient decision-making strategies through enhanced system awareness. Furthermore, the existing research work in cyber risk assessment and transferrable research and business strategies regarding cybersecurity operations have yet to be noticed by incumbent scientific literatures and will also be discussed in this section [16].

5. Existing Risk Assessment Models in Cybersecurity

[17]Risk assessment methods and models have been widely applied in various fields. In terms of cybersecurity of vehicular networks, risk assessment has been applied to evaluate the security of safety-critical systems in autonomous vehicles, including various specific vehicle systems. However, it is further observed that traditional safety risk assessment content in AVOSs appears incomplete regarding cybersecurity considerations. Most models investigated focus on unsafe driving conditions caused by hardware or software failures, as well as unsafe driving conditions caused by mixed hardware-software failure conditions. However, the cybersecurity environment of autonomous vehicles is also closely related to the safety risks related to configuration data and traffic network attacks, as shown in cyber-physical threats.[18] In an emergency situation, the performance of the second layers of vehicle systems (redundant systems) is of importance with respect to vehicle and occupant safety. In addition, the control loop of these vehicle systems should be revised to achieve a kind of autonomous mode that requires higher security levels. In the safety-critical domain, the trade-off needs to be highlighted versus vehicle performance and security readiness versus efficiency. Consequently, it is highlighted that (full) autonomous systems should also take into account the cybersecurity during their operation in varying environmental conditions. However, an inefficient vehicle management, varying environmental conditions and cybersecurity field in SAE Levels 0 to 4 vehicle operation can result in a highly increasing risk, not only for vehicle performance over time, but also for the appearance and result of attacks on hardware-dependent vehicle systems.

5.1. Overview of Current Models

Traditionally, cybersecurity vulnerabilities in VANET include attacks on VANET backbone cyber–physical systems such as traffic control systems, collision avoidance systems, networked guarants, and many others. The centralized authority in VANET contains huge network of possible vulnerabilities that could easily be compromised or disabled by an adversary. Over the last decade, with the development of connected and autonomous vehicles (CAVs) and global standard ETSI V2X, VANET has become part of V2V communication, and it is known as C-ITS standard. While C-ITS and ITS have been considered as a secure communication medium and are resistant to PDoS attack, previous research has shown that C-ITS can still trigger the underlying coordinated physical behaviors between infl us–out vehicles [19]. On a whole, existing solutions do not offer sufficient security guarantees for V2V systems, especially in the presence of mobile attackers (e.g., vehicles participating in attacks operate within the VANET network). Additionally, solutions based on signing certificates and roadside units are not suitable for V2V communication systems, they also cannot prevent the attacks due to large size of the VANET network. As per the proposed solution the simulator analytical outcomes progress to create and employ a robust and resilient platoon control strategy (RRCS) for overcoming the cyber–physical limitations and achieving the overall simulation objectives. Mobile attackers from the vehicle network cannot be identified and mitigate the attacks in VANET communication models. Hence other studies explored the integration of network defence systems such as “firewalls” in the communication landscape for neighbouring vehicles [14].

Different organizations employ various security risk management methods such as "Operationally Critical Threat, Asset, and Vulnerability Evaluation" (OCTAVE), the "National Institute of Standards and Technology Cybersecurity Framework" (NIST CSF), and MEdhode Harmonisée d'Analyse des Risques (MEHARI), depending on their preferences and the nature of the problem. The OCTAVE method incorporates risk assessment and management in a single framework, and pivots on a self-directed approach and organization-wide participation [4]. The NIST CSF method is adopted in this study as a basis for establishing a common cybersecurity lexicon and uniform criteria that will guide developing a standard-based cybersecurity assessment framework suitable for cybersecurity assurance in smart transportation systems. In Vehicular Ad-hoc Networks (VANET), safety applications rely on cooperative communication protocols V2V and V2I networks. However, increased connectivity within autonomous vehicles poses significant cybersecurity risks. The three main domains of attack vectors/models include personal devices of vehicle occupants, conflicts between electronic maps and sensors, and security/privacy risks for the vehicle occupants. On a whole, roadside infrastructures are more secure.

5.2. Strengths and Limitations

The Cybersecurity Maturity Model Certification (CMMC), established by the Department of Defense (DoD), expands on the NIST Cybersecurity Framework (CSF) to increase awareness and compliance with cybersecurity measures at all levels of contracting and supplier chains. Individual aspects and requirements are included within multiple processes of a cybersecurity risk management system and must be considered when defining a holistic approach to security. In addition to creating more precise protection mechanisms, this holistic view is recommended by the authors to target risk assessments more directly. This suitability can also be transferred to the systems field1, as it can have increasingly serious consequences for the failure of individual components. In their approach, an ISO/IEC 27001 framework1, as well as the relevant standards established in this context, are considered to include a full risk analysis in conjunction with standard scenarios usually handled in cyber security environments in their assessment. While these lists are intended to provide an initial overview of open issues covered in relevant literature, the authors recommend developing comprehensive and detailed analyses that are tailored to fit individual use case domains further on.

Standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and others guide security risk management, but methods and terminologies differ [14]. Organizations use different methods, e.g. OCTAVE, NIST Cybersecurity Framework, and MEHARI with the domain model for Information Systems Security Risk Management (ISSRM) being one of the most popular approaches. In the field of autonomous vehicle security, most research focuses on in-vehicle components, V2V and V2I communication, and potential attack vectors. According to their research, emphasis is often on individual areas of security such as a specific component that can be attacked or new security methods such as machine learning, yet there is less focus on a holistic vulnerability and threat analysis. They suggest further research in this area to develop a comprehensive list of vulnerabilities and threats, which should lead to appropriate protection mechanisms.

6. Proposed Cognitive Risk Assessment Model for Autonomous Vehicles

In this chapter, an end-to-end aim to develop the cognitive risk assessment layers of an autonomous vehicle that is environmentally friendly, traffic participant-agnostic, and capable of assessing the possible risks within the entire transportation system is proposed [7]. In the first layer, the objects in the scene are detected, the main object in the environment is selected according to the vehicle's so-called at the command and the control, communication area network of this object is analyzed. In the second layer, risk profiles that are constitutive of the risk records including the road-teammate characteristics, random demands and selected object's instant pose and acceleration values are formed. In the last layer, the possible causative variables are from the data set of 52 variables that includes selected team-mate's pose, speed, acceleration, guidance, acceleration, pitch, and roll on the main axis are discriminated [20]. After candidate input variables are generally characterized, the cognitive decision-aided deterministic, deterministic model that is valid at 0.000 level in the correlation relationships between outputs (risks) and inputs with an accuracy of 80% was set up during the literature survey. The possible inputs (localization, virtuosity, etc.) that should be put into the database as development in autonomous vehicle technologies are also proposed in the study.

Autonomous vehicles (AVs) may cause risky interactions with the external environment having unknown entities into consideration. Besides these, the malfunctioning of road-side units (RSUs), false information flows in vehicular ad-hoc network (VANET) and the security breach incidents may cause possible risks and material damages in vehicle operations [1]. The most important issue for autonomous vehicles then becomes how vehicles can assess the risky situations and environments and how vehicles can determine the causative events in their decisions. In burning clown-car example, for instance, one paint was forgotten to be painted on the image and signal in the image acknowledgment stage for a fraudulent intention in decision-making. Vanishing the red color caused a different decision from autonomous vehicle because it could not detect the painted with the color red in the legitimate image on the road.

6.1. Components and Methodology

Given the considerations previously made, it is evident that a structured approach to guarantee safety and resilience against all the possible threats present in a complete and dependable ARD (ASDRC) is necessary [14]. Data are extracted from existing resources and interviews with prestigious experts from a wide range of different domains in order to refine the results and to make the method structurally as complete as possible. Finally, cyber-physical dependencies and possible fatal events are described within a suitable ε-DICT in order to complete the complete ASDRC's very wide and multifaceted risk assessment condition space.

Autonomous vehicles are seen as the next frontier in intelligent transportation systems [3]. One of the most important aspects of offloading the driving task to such vehicles is how these machines can guarantee safety, resilience, and adaptability when faced with risky situations, considering that human intervention will not be possible or will be minimized in some (or many) scenarios [7]. Risk assessment methodology is fundamental for achieving the desired behavior and functional safety of the system; therefore, it is fundamental to use correct methods and tools to assess the risk of these vehicles. Several methodologies can be found in the literature that are capable of providing different qualitative or semi-quantitative risk assessments starting from qualitative descriptions of assets and threats. Some authors have then looked at more specific IoT devices or cyber physical systems, with a particular focus on autonomous vehicles. In these cases no clear trend can be followed, with presented methodologies focusing on very different facets of the self-driving vehicles.

6.2. Integration with Existing Security Measures

The methods described above, however, do not directly apply to fully autonomous systems for quite a few reasons. The first issue is that the risk assessment process is completely static, and it defines how the system should be architected against the expected threats according to the AAA coarse-grained model. In Fully Autonomous Systems, the vehicular risk assessment process has to evolve at runtime because a potential attacker can always find new ways to cause failures that the designers cannot anticipate [6]. The second issue with the AAA architecture is that it does not consider the risk associated with detected attacks. This is problematic because the risk assessment process should be used to evaluate the risk associated with detected attacks during runtime, to see if the systems still meets the acceptable level of risk or not. This process is completely missing in a static vehicular risk assessment process. The third issue with the AAA architecture is that it does not enable the va to take instantaneous decisions in the face of cybersecurity attacks, which is increasingly crucial as the time-to-collision decreases between fully autonomous vehicles in fully autonomous settings. It is thus necessary to define the complete process for performing security risk assessment for fully autonomous systems [18].

Standards like ISO/IEC 27001 and NIST guide security risk management, but their methods and terminologies vary [14].Organizations widely use different security risk management methods such as OCTAVE, NIST Cybersecurity Framework, MEHARI, and so on.According to ISO 27001, risk is defined as the expected frequency of occurrence of a particular threat causing a particular type of vulnerability. According to NIST, the process includes assessing vulnerability, risk, impact, and mitigation cost. In all the models, the first step is "risk assessment".

7. Case Studies and Practical Applications

Real and virtual-world impact of these cyber-attacks demonstrated in practical case study experiences. Assessing the security risks in V2X communication, different realistic data attacks and their subcategories are explored. Remote miscommercial attack, encouraging the roadside infrastructure to send dangerous data to prompt both a brake and an action by providing deception, and a variety of replay attacks, resulting in impacts on motion control of autonomous vehicles have been shown as representative attacks [7].

Vehicle security has emerged as an urgent research problem to address industry and regulatory challenges in the upcoming era of interconnected autonomous vehicles. This has led to considerable investigation into in-vehicle security, vehicle-to-vehicle and vehicle-to-infrastructure simulation, and potential attack vectors that may be used against these surfaces. Therefore, vehicles equipped with modern wireless communication technologies face several tens of attack vectors from multiple layers of the stack of protocols characterized by their different inherent vulnerabilities. Emerging from significant structural information system (IS) characteristics, information security dynamics have not been addressed.

Regardless of vehicle connectivity, physical surveillance, intentional deviation, and wireless hacking have been discussed. In, a model-based risk assessment approach is also designed, and the security properties that are violated in several attack scenarios are presented. The feasibility of these attacks is experimentally verified. Information security dynamics emerging from significant structural characteristics of information systems are addressed [14]. The paper focuses on the different security implications in the context of autonomous vehicles. A comprehensive taxonomy of autonomous vehicle (AV) attacks and defenses is proposed to assist in autonomous vehicle system architecture development. Information security (IS) aspects of passenger-vehicle interaction. Remote misuse, engineering mode misuses, intervention, and system hacking attacks have been identified as potential attack categories. Architecture for the identification of diverse attack vectors with various mitigating countermeasures in practice to be more secured.

In automotive security research, the focus is on different security implications in the context of autonomous vehicles. Various attack vectors are addressed and potential countermeasures are proposed. A comprehensive taxonomy of autonomous vehicle (AV) attacks and defenses is proposed to assist in system architecture development [4].

7.1. Real-World Examples of Cybersecurity Incidents in Autonomous Vehicles

The safety of an autonomous driving system depends not only on sensor measurements themselves, but also on their knowledge about the system. Following Schnjai's point of view, Xum highlighted main technical strengths and further possible weaknesses due to side-supplies/threats. Table 2.1 provides some concrete examples of corresponding challenges in AVs. As discussed here, the security of in-vehicle component communications is an increasingly popular topic in the literature [14]. In one of these studies, a large investigation was conducted to detect vulnerability of Xxxxxxxxxxxx's vehicle system to benign and malicious traffic. Three attack scenarios and their wide range of impacts were discussed.

Security and privacy of autonomous vehicles can be compromised due to weaknesses in the communication channel or the falsification of data from cloud services' manufacturers [21]. Examples of real-world incidents illustrate the wide spectrum of possible adverse outcomes including remote hijacking of a Tesla Model S, automatic piloting by an attacker, compromising the Cyberknife radiotherapy machine and nearly causing a ransomware attack on a hospital, and activating false bases for military mobile devices using GPS signal spoofing [13]. The task of securing an AV is very challenging and its objective is to ensure trusted behavior of each unit by protecting it against unauthorized access and malicious activities, including intrusion and data manipulation.

7.2. Application of Cognitive Risk Assessment Models

Additionally, future work will investigate the modelling and management of environmental factors including climate, rain, wind speed, wind displacements, construction work, and human behavioural dynamics. The intention is to uncover dynamic and possibly dangerous interactions between human behaviour and physical infrastructure, as well as between individual driving style and vehicle safety systems. This study refers to a multidisciplinary approach that stresses vehicle safety as an emergent property and transportation system safety as a sociotechnical system. The proposed research is expected to make significant contributions to the state-of-the art in AI-enabled vehicular autonomy by introducing human-like cognitive mechanisms that can overcome diverse deficits of traditional Controller-Lyapunov AI systems.

[22]In order to use the cognitive risk assessment models [Reactive Risk Assessor (ReRA) and Cyber Resilience Assessor (CRA)] in the context of autonomous vehicle cybersecurity, we must identify the relevant situational variables in the context of AV operation, and determine if existing models are sufficient to characterize the reliability of various interconnecting factors for cognitive/risk of malevolent attacks on AV systems. If not then we must develop new models that overcome such limitations. Any usage of the tools other than as a benchmark should incorporate dynamic intrinsic factors such as material wear, erosion and fatigue, in ReRA and Cyber Resilience Assessor (CRA) that are designed to emulate cognitive dimensions based on MERIT dataset. It is also necessary to determine if there are other relevant models such as, Labyrinth of Complex Systems (LoCS) to model the socio-technical system vulnerability that would complement AV Cyber Resilience Assessor [Ref:.

8. Future Directions and Emerging Technologies

[13] The major concepts presented are foundational and mostly drawn from the area of program behavior analysis and anomaly detection, which to date have been instrumental in developing personalized models for each vehicle by exploiting DoS techniques through our novel sensor fusion procedure. As a natural path forward, this work lends itself to several important modifications. An interesting area for future work is the area of the attack-tolerant estimation problems from a statistical learning perspective. Here, we make the subtle distinction between detecting an attack—perhaps by analyzing measurements and observed data—and later separating the effect of the attack from the estimation or control law design.[1] A natural way to extend the current attack-tolerant navigation framework is to develop multiple models of the process noise of the vehicle dynamics that correspond to different operating modes. Such a context-aware, multi-model, strategy is likely to tolerate large, short-

term attacks by quickly shifting to the correct operating mode. Event-triggered control strategy that is coupled with the navigation and sensor fusion as a part of the control law and estimation design is of significant interest and importance in mitigating unexpected network attacks on the system. Fully self adapts to these new concepts.

8.1. Trends in Autonomous Vehicle Security

Fully autonomous vehicles, combining fully dynamic bespoke control algorithms, lidar, visual cameras, bone detection and localizations systems, and 5G remote operations will form the next phase of the project. Which must necessarily include AI/ML-based defences against adversarial interference/attacks to local control systems, electronic communication busses, and 5G communications and backend systems [23]. Understanding the ways in which AI/ML poses new threats and novel forensic and protective mechanisms is essential—a good introduction and collective chapter defining adversarial AI is used. The proliferation of AI in areas that touch personal and national security—facial recognition, secure payments, home security, traffic management, and health diagnosis e.g. COVID-19 mortality assessment is provided in an active AI era with significant positive and negative impacts.

The significant rise in connected and autonomous vehicles (CAVs) on our roads has inevitably necessitated a rise in research and development surrounding securing these vehicles against adversarial action. With the end of the SAE automation levels in 2018, and the promise of more sophisticated vehicles by 2030 in mind, it is evident that researchers will need to develop improved methods to defend them against adversarial activity [24]. Although cybersecurity is a requirement of any internet-equipped component in the modern era, the ability to attack CAVs opens up the potential rewards to adversaries: effective attacks can result in real physical harm to drivers, passengers, and pedestrians, and can also have significant economic and public-relations consequences for the companies involved [8]. Incorporated in these worries are concerns mutual to all digital systems, including attacks aimed at damaging faith in the vehicles—of course, if either a vehicle's parent company's reputation, or the concept of CAVs' ability to improve our lives, is compromised, there is potential for lasting harm.

8.2. Innovations in Cognitive Risk Assessment

The advancement of technology implies an increasing level of functionality of the AI agent diminishing the risk applied to uncertain states [18]. In order to design comfortable and reliable attacking patterns, the AI ensures the execution of the attacks at the optimal time. The result of the dependent development of AI and security mechanisms is that the attackers would also deploy various AIs for the cyber and physical attacks against autonomous vehicles in the future. In the background of § 8.1, Fig. 2 is created with findings of the works highlighted in § 8.1. From Fig. 2, AI technologies and modeling various attacks, exploits and vulnerabilities, the focus is increasingly vast in the last five years compared to the previous one. The number of all studied works also shows an increasing trend.

Risk management is about taking the risks one can afford and avoiding the ones that cannot. Risk management strategies effectively eliminate cybersecurity vulnerabilities [3]. It is different from risk elimination, which ensures that the risk is permanently removed so that it no longer constitutes any threat to security. Further, the configuration of cybersecurity tools eliminates the risks associated with the security of autonomous vehicles, but, eventually transforming the vehicle into a Data-over-Cyber-Physical-System (DoCPS) [2]. Technically, the DoCPS is a M2M-physical process controlled and supervised by a cloud-communicative platform that communicates via Internet with the vehicle's IoT sensors/ coordinators integrating real-time processing and decision making functions.

9. Conclusion

The proposed Cyber Air Manipulator Architecture (CAMA) is supposed to improve CAW's security ceilings so that the Authorized People (AP) can confidently rely on its Service Level Agreements within the expected risk ranges. Moreover, the metrics are expected to cover two main aspects: block tolerable dimensions' weights (isk metrics weights) and the different threats' multi-anticipators (multi-anticipatory metaphors won in and out the Risk1). The weight λi of each block has been evaluated by having an average opinion of nep longitude, inclination, and angle (with the horizontal direction) to measure from the semantic origin of the threat team being evaluated to the restraining chessboard of the Multi-Porte d'Austerlitz (Multi-Condemner's Psychological Development HowIs)'. The proposed drone has reliably treated to be capable of tracking the flying object ordinarily from an arbitrary initial position and velocity. The proposed controller has optimally minimized the chaser's control effort to safely capture the target drone by the least-possible fuel consumption [1].

Normally, the concept of a "trustworthy sensor" refers to its trustworthiness. However, trustworthy sensors with respect to the desired system variables in the context of cybersecurity refer to the sensor's freedom from cyberattacks that modify the sensor's outputs or that are launched to impact the performance of the downstream modules and strategies. It is noted that having manually designed constraints and interacting with CARMF layers and level are leading factors of CARMF acceptability in real-world scenarios. Given the owing complexity and the infinitely many possible adversarial attacks, the unbounded risks are computed for the chosen model types and examples. As the integrated AARs (online risk assessments) present strong relationships with the selected abstracted AARs and as the abstracted AAR sparsify the involved risks, CARMFs function under limited computations and communication resources and effectively prescribe strategies for addressing (tackling) the yielded safety and security issues of CPSs [7].

10. References

1. [1] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
2. [2] A. Dinesh Kumar, K. Naga Renu Chebrolu, V. R, and S. KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities," 2018. [PDF]
3. [3] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
4. [4] H. Rivera-Rodriguez and R. Jauregui, "On the electrostatic interactions involving long-range Rydberg molecules," 2021. [PDF]
5. [5] Y. Guan, H. Liao, Z. Li, G. Zhang et al., "World Models for Autonomous Driving: An Initial Survey," 2024. [PDF]
6. [6] Y. Mei, "First-order coherent quantum Zeno dynamics and its appearance in tight-binding chains," 2023. [PDF]
7. [7] K. Mokhtari and A. R. Wagner, "Don't Get Yourself into Trouble! Risk-aware Decision-Making for Autonomous Vehicles," 2021. [PDF]
8. [8] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov
9. [9] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]

10. [10] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
11. [11] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov
12. [12] T. H. H. Aldhyani and H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," 2022. ncbi.nlm.nih.gov
13. [13] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
14. Tatineni, Sumanth. "Cloud-Based Business Continuity and Disaster Recovery Strategies." *International Research Journal of Modernization in Engineering, Technology, and Science*5.11 (2023): 1389-1397.
15. Vemori, Vamsi. "From Tactile Buttons to Digital Orchestration: A Paradigm Shift in Vehicle Control with Smartphone Integration and Smart UI–Unveiling Cybersecurity Vulnerabilities and Fortifying Autonomous Vehicles with Adaptive Learning Intrusion Detection Systems." *African Journal of Artificial Intelligence and Sustainable Development*3.1 (2023): 54-91.
16. Shaik, Mahammad, Leeladhar Gudala, and Ashok Kumar Reddy Sadhu. "Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive Authentication." *Australian Journal of Machine Learning Research & Applications* 3.2 (2023): 1-31.
17. Tatineni, Sumanth. "Security and Compliance in Parallel Computing Cloud Services." *International Journal of Science and Research (IJSR)* 12.10 (2023): 972-1977.
18. [18] E. Ochoa, N. Gracias, K. Istenič, J. Bosch et al., "Collision Detection and Avoidance for Underwater Vehicles Using Omnidirectional Vision †," 2022. ncbi.nlm.nih.gov
19. [19] T. Wang, M. Tu, H. Lyu, Y. Li et al., "Impact Evaluation of Cyberattacks on Connected and Automated Vehicles in Mixed Traffic Flow and Its Resilient and Robust Control Strategy," 2022. ncbi.nlm.nih.gov
20. [20] M. Strickland, G. Fainekos, and H. Ben Amor, "Deep Predictive Models for Collision Risk Assessment in Autonomous Driving," 2017. [PDF]

21. [21] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
22. [22] V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti et al., "Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users," 2018. ncbi.nlm.nih.gov
23. [23] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019. [PDF]
24. [24] R. Singh Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," 2022. ncbi.nlm.nih.gov