Dynamic Risk Assessment for Cybersecurity in Autonomous Vehicle Operations

By Dr. Yan Zhang

Professor of Data Science, Fudan University, China

1. Introduction to Autonomous Vehicles

Autonomous vehicles use various technologies to compute trajectories, detect potential threats, and avoid accidents without much driver intervention [1]. AVs use several sensors to monitor the vehicle's environment by scanning several details like the road and driving surfaces, and to detect pedestrians, vehicles, and road obstacles using radar and camera technologies. The AVs can use sensor fusion data to predict potential collision events and help the driver avoid accidents by using potential hazards. Taking road safety from different AV levels as a practical study, this project focuses on developing a complex real-time risk assessment for intervening at level-2 AVs. Hybrid state (between human control and sensor automation) between "human-in the loop" and "automation-in-the-loop", can recognize future or current risks. Although AVs have huge potentials of saving numerous lives and their social adoption is non-stoppable, they may be also affected by various kinds of hazards—stochastic or accidental road users and potential attacks. Breaking into AV control systems, hackers may cause synthetic accidents causing the robots to interfere with safety even if these "black box" state transitions are not directly possible. These types of hacking engagement require applying more standard cybersecurity models to recognize potential hazards. The primary standard that many countries are trying to adhere to is ISO€211. However, security cannot be ensured by following the required rules, physically incapable of communicating with the control hardware, validation engineers, or AI designers only. An architectural module, based on the cybersecurity risk-management model used by Bosch in operation, can fill the gap by measuring how much an ISO 21,194-by-compliant system provides security in practice. This model involves all kinds of perpetrators, professional and non-professional adversaries, autonomous and supervised attacks, such as jamming, spoofing, and penetrating through the communication networks between the car and infrastructure [2]. In general, cybersecurity attacks related to autonomous vehicles and their operations are formed by the

break of three phases. The first one occurs when attackers gain access to the target autonomous vehicle using over-the-air interfaces or physical ports. The second phase may start with reprogramming of electronic control units, like in the case of invalidating or changing the nominal management command set. The third is with a forged-or sniffed malicious traffic that is going outside from the system using diagnostic ports or wireless interfaces. As a whole result, bypassing the internal security gateways, adversaries remain under-the-radar for the advanced defense information systems [3]. With the help of the generally accepted guidelines about cybersecurity (citations), a broad cybersecurity risk assessment methodology will be presented with the proper PPDR for autonomous traffic.

1.1. Definition and Types of Autonomous Vehicles

[4] [5]Vehicle has become an indispensable part of modern life, providing prosperity, convenience, and efficiency. With technological advances, autonomous driving is the way transportation is heading. Increasingly more states and nations are recognizing autonomous vehicles (AVs) into road traffic. However, with growing literature, the augmented technical threat, hidden dangers of the adoption of AVs are being highlighted. The computer-based nature of AVs makes them vulnerable to cyber-attacks, while their soft integration into everyday society demands an evaluation of human factors. Researchers in the human factors area usually focus on AV influence on the behaviors, emotions and perceptions of drivers, and interaction between AV and human drivers[ref: 2f91accc-fc26-4f0a-b6a5-015cdfe7b43a, d2afffaa-3566-469e-8789-6daf7f8d662e]. The path toward autonomous vehicles (AVs) spans from vehicles equipped with advanced driver assistance (ADAS) systems through AVs with a driver to fullautonomy systems. Realizing an automated system generally promises not only safety improvements, but also reliability. Risk of crash frequently absent in human-driven vehicle. In an uncontrolled event, starting from managing influences on sensor output to prevent unwanted AV operation, ADAS aims to mimic human behavior to ascertain hazardous and potentially hazardous driving situations. The CYBERMOBIL project focalize on AVs as they are perceived by modern transport standards: particularly in the context of all possible road hazards including cyberattacks. However, this publication specifies AVs in the most general term without differentation where appropriate. II.1.1. Definition and Types of Autonomous Vehicles In research and in practice, autonomous vehicles often cluster in three broad categories: non-connected and non-cooperative; non-connected but cooperative vehicular traffic and heavily connected vehicle-to-everything (V2X) scenario. Such a category

of AVs are both connected and cooperative. These environmental objects include not only other AVs, but also objects representing traffic consequences. An optimizing scenario is achieved by coordinated actions of all environmental objects and represents the possibility of optimal driving. When choosing a design of an ADAS or AV, knowing its types throughout its entire lifecycle (R&D-implementation-use-maintenance) is crucial. Knowing its types facilitates contact with such concerns as accident risk assessment, safe testing strategies and their validation, and forecasting behavior of AV as well as other objects. Similarly, when discussing participant-behavioral aspects of autonomous vehicles, e.g. interactions between human drivers and AVs, knowledge about AV degree of autonomy is useful.

1.2. Evolution and Current State of Autonomous Vehicle Technology

Current research aims to achieve a wide range of key objectives. These focus on numerous functional aspects to meet the practical and high-level requirement of autonomous vehicles. Thinking aloud, adaptive user interfaces and Human-Machine Interfaces (HMIs) need well considered interfaces that give users improved legacy support and enable users to interact with the vehicles smoothly and efficiently. It is important to increase attention to driver needs for providing better experiences, reduce social complexity and remove issues and challenges through support. Security in terms of safety, privacy, data collection and overall vehicle function must also be addressed and improved and solves through optimization, dynamic vehicle functioning and performance, improved environmental perception. Accordingly, new methods and strategies to learn from data must be a focus of research: In other words, adopting improved machine learning and deep learning methodologies to enable better functionality for adaptation, relationship discovery, algorithmic performance and sentiment analysis with increasing levels of intelligence.

The market for commercially available player systems that are capable of performing Level 2 partial automation is growing rapidly [6]. These systems can assist drivers in controlling the vehicle but still need driver's intervention and supervision to operate in all conditions, as they're not capable enough to replace drivers in some specific scenarios [7]. Meanwhile, ongoing research [8] and development efforts are focusing more and more on steps toward fully-automated vehicles—those that are capable of operating without human intervention and in all scenarios. Here, fully autonomous vehicles are capable of self-operation in all scenarios without human intervention (i.e. are capable of handling all traffic and exceptions

without human driver intervention). In addition, automakers have laid out plans to release Level 3 and 4 highly automated vehicles in the near future.

2. Importance of Cybersecurity in Autonomous Vehicles

An AV is a complex robot that works in interaction with its environment and maintains its functional safety based on sophisticated and intertwined cybersecurity and functional safety mechanisms like robustness, fault tolerance and resiliency. The aim of the functional safety and cybersecurity functions are to make the system operational with 'a valid' state information. Functional Safety Standards ISO 26262/IEC 61508 are trying to make the system safe not versatile. More specifically, there is a gap concerning the evaluation of the severity of the possible attacks in the system safety. The safety vantage point of view is insufficient to automatically or manually validate an attack instance. What's more, ensuring the security of highly autonomous vehicles is largely non-deterministic and complex due to their long-term dynamics and multimodal nature, and decision-making processes are not cycle-based. Consequently, the problem of security assessment focuses on defining a software solution to build a cybersecurity envelope around an AV in a dynamic manner.

[9], [10] Autonomous Vehicles (AVs) are driven either partially or fully autonomously by one or more embedded controllers. They are equipped with various hardware and software components and connected to the web and other transportation systems. The functionality of these systems causes a set of cybersecurity risks that makes them different from traditional vehicles. Severe vulnerabilities can be developed to set an attack point in the autonomous system, not in the non-autonomous system [11]. We define three types of known possible attacks on AVs: vehicle, infrastructure and network cyber-attacks. In the case of a vehicle attack, a variety of attack vectors can be used to hack the system, ranging from local-hardware attacks to more sophisticated cyber-physical manipulation. Thus, protecting an AV against different types of possible attacks (Adversarial Example, backdoor, denials of service that might degrade or destroy the system's safety constraints) is crucial.

2.1. Vulnerabilities and Threats in Autonomous Vehicle Systems

Even if the computation of software risks is partially specifiable, computation costs would make them inappropriate when response time is critical issues (for example, when an autonomous system undergoes a cybersecurity attack). In the same way, dynamic risk

evaluation in general implies switching from a predefined list of possible events to continuous data analysis [12]. It implies the computation of the probability of different situations and the evaluation of their effects when performed inside of a machine-learning autonomous vehicle. This kind of process takes the form of the continuous extraction of knowledge from data and the evaluation of the risks of different situations. The possibilities here are numerous. Anomalies can be the results of many causes like system malfunctioning, human error, or, cybersecurity attacks. These situations wouldn't necessarily have been previously considered or foreseen. The dynamic evaluation of vulnerabilities and threats must, therefore, have a large latitude for addressing different acts, different types of operations, and different levels of trust in the vehicle's different components.

Evaluating the cybersecurity risks of fully autonomous systems is still a relatively new area [10]. In the case of autonomous vehicle systems, the process for assessing risks surrounding situations detected within these sophisticated systems would be based mainly on the attempt to include all possible unwanted situations in the design phase. Nonetheless, there are numerous problems with this approach. Future autonomous systems will have to cope with unforeseen and unexpected situations during their operations. They may face environmental and cybersecurity threats that differ from those considered in the design. In the case of autonomous systems, static and deprecated safety assessments won't function. Autonomous systems require safety mechanisms capable of instantaneously analyzing data and autonomously reacting to it [9].

3. Fundamentals of Risk Assessment

Cyber-security leaders have realised that advances in autonomous systems can be realised only by incorporating the cutting-edge technology and applying the best security practices in designing the systems. In this special issue, recent advances in computer systems, artificial intelligence (AI) and tactical autonomy are presented for cyber threats in autonomous systems. There is growing response to security pressures in advanced vehicles with fully autonomous and partially autonomous capabilities enabled by city-level, public and semi-abstract V2X. Which remains a significant distinction as the predominantly one-sided vehicle focus emphasis decreases. The identification of the autonomous vehicle risks in the design process must be identified without which an operational safety guarantee is present only with

reasonable confidence, reduced risk, and it can be taken into the passive protection system lifecycle design in [7].

Threat modeling of cyber-security has been conducted by multiple independent research groups. Threat model developers increasingly recognize the importance of an accurate, consistent and comprehensive risk assessment to ultimately meet the safety and security requirements for autonomous vehicle operations. Therefore, a methodology that builds on the existing frameworks and considers situational risks for the operation of a given autonomous vehicle that capture potentially unique vulnerabilities in challenging scenarios is being introduced in [ref: 80046a9d- e000-4c5e-a223-712cf6f394c7. The model fundamentally aims to increase system safety by considering these risks. The effectiveness of the proposed method, in identifying potential strong techniques improvements, is demonstrated by showing how an autonomous vehicle controller can be super upgraded with regards to meeting functional and security requirements in [12].

3.1. Definition and Concept of Risk Assessment

[13] Decades of automotive innovation have rapidly disrupted smart cities, and are moving the sector closer and closer to the robotization of urban areas so people and goods can move easily[,] 24 h a day and without human intervention. With all of the positive changes happening in city structures, the structure of managing urban areas and how to control this robotization have to adapt as a consequence. As the boundaries of city infrastructures change over time, new error scenarios and hazards are showing up in cities we never imagined possible, transforming the whole concept of hazard identification. Dynamic Design Safety Assessment (DDSA) is a new way of dealing with the hazardous scenarios constantly generated in our cities, such as the ones caused by modern automotive fleets moving in a smart city. This new asset, DDSA designed to complement classic Design Brake Performance Techniques (DBPT), studies strategies that are able to identify dangerous scenarios by working with constantly updated maps and logs of historical performance during real-time operation.[3] Since there are no sensor and/or modelling specifications that vary depending on hotel assumptions on the extension of city structures for the current and future years, the point of the present study is to elaborate, by using the brake performance (BP) as an example, an innovative concept on how, rather than meeting accumulated odds—e.g., 1×10^−7 event/year—autonomous vehicle (AV) and cooperative automated vehicle (CAV) systems

can perform error-free travel in (optimal, degrees 1&2) hazardous contexts even though it has never received information on that specific context. Instead of the classic target (that accumulated odds are below one mark), we still keep the classic target/way-to-proceed for the reaction time to be used to solve the above-mentioned problem. A general simulation process is proposed that permits a CAV to build up in real time (through validation of times needed to carry out specific tasks in similar contexts) speed- and time-dependent maps of excessive risk performance, Eigen safety speed (ESS), in accident-to-be scenarios, including the identification of speeds that guarantee "NESAC".

3.2. Types of Risk Assessment Models

In line with other authors, to date, no risk assessment framework is specialized for this context involving interactions between vehicles, passengers and the road infrastructure in an autonomous vehicle system. Traditional risk assessment is not dynamic and surely does not depend on any specific attribute or feature of the paced driving, nor is it designed to address unsafe scenarios initiated by threats or vulnerabilities in powerful cyber-physical systems ([7]). What is reported in Table 2 can confirm that both human-driver oriented and autonomous car scenarios could undergo some risky patterns. However, while recurrent and not rare, we highlighted the direct association of risky events and the PIR (pattern of interest) only in the second case. And we matched the PIRs with respective CVSS (Common Vulnerability Scoring System) scores, obtained from the NIST national vulnerability database (NVD), to distinguish between them. For these reasons, within our future work, we will extend the current security system of interest to integrate new functionalities and developer new related technologies able to assess the side effect of these risky pattered also with respect to the cyber-security perspective, quantifying which and how security vulnerabilities can deteriorate PIR events signalling them as risky.

The conventional way of dealing with risks involves an initial phase of identifying possible unsafe scenarios associated with the system of interest, followed by a phase of severity assessment. However, in dynamic contexts, risk assessment should perform a more continuous and monitored analysis, triggered, for example, by temporary changes or irregular working states of the risk-carrying system ([13]). In this respect, although two more sophisticated and more reactive subclasses of RAs have been defined, i.e., Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA), they are all characterized by the initial

division of a system into an ACZ and an FCZ. This division is static and made on the basis of physical knowledge of the system at an analyzing time point, at which the system is fully operative. It is clear that these techniques turn out to be inadequate or very limited in the context of cyber-physical systems, because the assumption that the FCZ coincides with the set of all subsets of ACZ variables that could take a certain observed value, given the other variables are fixed, is not satisfied ([14]). A risk assessment process able to deal with non-monotonic rate with metriciness, able to deal with dynamic situations, and to integrate knowledge about failures and dangerous states collected during the system operational life is required. Only through this is it possible to truly abrogate the logic "something did not work, it is likely that some cyber-attack is ongoing".

4. Dynamic Risk Assessment in Cybersecurity

Previous research emphasizes the need to address cybersecurity and safety risks in tandem and the challenges in practically implementing dynamic assurance or runtime-certification mechanisms. Although there are approaches that adapt safety monitors at runtime to verify that safety properties are satisfied, those approaches could detect unsafe inputs or scenarios after they occurred and are challenging to extend or adapt to evolving cyber and environmental risks. In contrast, the ReSonAte work introduces a novel technique that continuously estimates dynamic safety risk at runtime and provides a strong correlation with eventual vehicular collisions. Using safety monitors and system information available at runtime, ReSonAte estimates vehicular collision probabilities directly from the measured system and monitor's data traces.

Dynamic risk assessment is crucial when discussing the security of autonomous vehicles as there is always the possibility of an attacker targeting the vehicle's cybersecurity system . A cybersecurity solution for autonomous vehicle operations should perform a continuous computational observation and evaluation process and aim to predict the outcome of autonomous vehicle operations related to cyber risks and exhibit efficient reasoning ability [15]. Dynamic risk assessment techniques can be quite useful for mitigating unforeseen situations and managing the operation of a system in abnormal situations [16].

4.1. Need for Dynamic Risk Assessment in Cybersecurity

Most (if not all) of the security design assumption that are taken for granted in traditional information and operation technology (IO&T) are unapplicable in AV environment whose security posture will be much more dynamic than fixed trust domains. The shift towards autonomous or self-driving vehicles brings to fore a likely need for the roadways to become a more secure environment for vehicles to freely operate in. Findings in this work show the abstract concept of "trust" no longer encompasses the complexity of security and protection that is now required in modern day automotive technology. Through various definitions the term trust as has been explored and other terms like zero trust, blockchain and safe data will now be considered as core redefined terms to define secure self-driving vehicles' technological space.

[9] [17]The application of artificial intelligence (AI) in vehicles has the potential to make them smarter, safer, and more efficient. Advances in AI technology combined with evolving transportation requirements are leading to the development of autonomous vehicles (AVs). In addition to the great promise that AI and automation brings, there are host of concerns, the most obvious of which are security threats. Vehicles with AI-based systems are seen as the 'convergence' of IT -Industrial Technology coupled with consumer electronics systems which are generally known to be unsecure.

5. Key Components of Dynamic Risk Assessment

Cybersecurity that is effective for autonomous vehicle operations needs to be dynamic and comprehensive, especially since technology that is readily available today is continued to be supported in the future. While there is an effort to test the effectiveness of the cybersecurity in vehicles, this effort is not extended to assess the day-to-day changes in the risk levels, which is the difference between the attack likelihoods and the system's cybersecurity threshold. Such a deficiency leads to the significance of ensuring the drive experience is always secured which is also identified as a major dynamic risk of AVs cybersecurity issues. While utilizing new mitigations and defenses can reduce the attack likelihood, the likelihood can also increase due to the new threats. As a result, the investigation and development of DRAs are required to provide dynamic and just-in-time decisions for real-time driving in autonomous vehicles [5]. DRAs should use systems engineering to assess the risks in AVs' real-time driving and enforce the required responses. The development of DRAs in AVs should utilize systems engineering as it is traditionally applied to other industries, such as hardware, critical infrastructure, and

software, however the variants in threats, vulnerabilities, and risk levels in cybersecurity qualities like secrecy, integrity, and availability makes static and deterministic measurements impractical. The individual safety, particular environmental conditions, and route requirements must be covered to reflect the real-time risk and adapt to the environment with nominal cognitive load on the operators. Further, AVs are technology-oriented systems, so besides the safety and cybersecurity risk, their acquisition, maintenance, operation, management, and disposal should be governed by valuable practical applications [17].

5.1. Real-time Data Collection and Analysis

The autonomous vehicle responds to unknown, uncertain, and dynamic conditions in real-time. In order to respond to dynamic threats, the autonomous vehicle can calculate a dynamic risk level at each moment and adjusts decision-making criteria and eventually driving behavior. The real-time DRA architecture can be designed with right components and modules, enable vehicle to recognize the threat level of visited and unvisited areas for suggesting optimal action, and continue monitoring of those selected roads, optimize the hazard function of each path to allow reducing the vehicle speed as much as is necessary [3].

This part will clarify the real-time data need and collection, the real-time analysis architecture, and methodology presented in the previous sections. As introduced in Section 3, the autonomous vehicle performs real-time data collection and environment scanning activities by using sensors; including radar, camera, LiDAR, GNSS, IMU, odometer, and ultrasound. The Open Platform for Automated Simulation (OPAL-RT), HIL Platform which is capable to test the Electric Vehicle, Automated Vehicle, and Critical Embedded Systems simultaneously with the same Hardware-In-the-Loop (HIL) simulation, using high-precision trajectory generation and vehicle models. It enables real-time testing of controller and rule/algorithm being design to the vehicle. The Map shows road traffic parameters such as traffic flow, vehicle flow, and vehicle type for autonomous vehicles [17].

6. Challenges and Limitations of Dynamic Risk Assessment

In the AV domain, security of AV algorithms and techniques is a major concern. This problem is further exacerbated by the use of AI based techniques for enhancing AV functionalities. As it is well known, autonomous driving is inherently complex task, involving a multitude of safety hazards. Safety critical ACC units in an AV are susceptible to attacks that involve cyber-

physical interactions. This includes sensor spoofing attacks, feature injection and data tampering attacks, in which the attacker can inject arbitrary data inputs into the ACC by crafting signals and subsequently perturbs the initial configuration and mimics states from the compromised sensor. This would result in targeted (or stealth) attacks leading to critical car behaviors able to trigger safety hazards. This includes straightforward crashes or deceiving navigation dynamics that violate safety standards, like lane departure, USC, etc, for which state-of-the-art collision avoidance systems and airbags could not perform their services. Moreover, issues associated with transition between human driver and autopilot and even reached an agreement of going against authority. There are currently also concerns of system contamination including the possibility of coded malware from pirated software, system bugs and moreover platform for threat actor behavior (relay attacks), etc, from physical wireless connections [17].

In recent years, the investment in advanced information and communication technology (ICT) have gradually penetrated into the automobile industry. One of the many applications born in this context is autonomous vehicles (AVs). AVs, or simply autonomous cars, are anticipated to revolutionize individual and public transportation, having significant impacts in traffic efficiency, public safety, local economies, and overall quality of life. For instance, it is estimated that autonomous cars will bring benefits of approximately $3.2 trillion in social value by the year 2050. With these prospects, major car manufacturers and tech giants worldwide are heavily investing in R&D in the AV domain. However, like the case with any technological innovation, BI functionalities are coupled with numerous challenges. Unlike human vehicles, autonomous vehicles do not possess intelligence, consciousness and awareness by themselves. This makes the BYs considerably vulnerable to various security threats. It is thus imperative that potential security threats are studied in detail, and strategies to counter them are proposed. This is particularly important in case of passenger safety sensitive applications, such as collaborative mode traffic systems, urban aerial vehicle networks, etc. In this paper, we focus on the security of AVs and their vulnerability to various adversarial exploits. Specifically, we consider the problem of ensuring safety and security in an interconnected urban AV transportation scenario employing CAVs [18]. The above theme falls under the larger by of cyber-physical systems (CPS) security research, which today is a world leader in cyber security.

6.1. Data Privacy and Ethics Concerns

Today, self-driving vehicles like AVs are at a stage where beyond state-of-the-art manoeuvres like obstacle avoidance, lateral adjustments e.g. parking are increasingly carried out by an intelligent vehicle. Moreover, as S-DP-DRAS is a modular system, supplementing different functionalities, our results guide how similar manoeuvres will become autonomous under future vehicular scenarios [11]. Ethical dilemmas in autonomous vehicles are on the rise, especially in extreme traffic situations where the vehicle is necessitated to execute very challenging ethical choices. To comply with the norms of different societies, to address these dilemmas and to render autonomous systems more transparent and effective, standardization, legalization and the existence of policies are imperative. The efficient use of AI-based decision-making software in self-driving cars raises concerns pertaining to utilitarian ethics and the need for a respective legal, standardized and compliant system. Moreover, ethical issues connected with fairness, non-discrimination, justice, and hidden costs should be considered by the automotive industry [19].

Developments in the autonomous vehicle (AV) domain have been happening very swiftly in recent years. Manoeuvres like parking are increasingly being autonomous. A novel, modular risk assessment system − the Dynamic Risk Assessment System (DRAS) for Parking (Sequence) scenaRios (S-DP-DRAS) is described [3]. In comparison to other relevant research for guiding DRAS design in a seamless fashion, the distinct technological positioning of S-DP-DRAS is asserted in this article.

7. Case Studies and Applications

In the first chapter, we discuss the results of the automated framework for performing (dynamic) risk analysis (including TA) for different combinations of capabilities and risks relevant to different systems. For this purpose, in the second chapter, the authors present the details of a risk assessment method, which is capable of identifying the probability and consequences of cybersecurity attacks in the SCADA systems where no intrusion detection system and might be enforced. In the third chapter, the authors introduce a new method to automate the deployment of intrusion detection or prevention systems for SCADA systems by thoroughly assessing the probability and consequence of cyber threats and network availability cost. Finally, we extend this framework for IoT facilities with real-time capabilities in the fourth chapter. Defense strategies in real time can be selected and optimized by our ecosystem from components ranging from trustworthiness of the agents to post-positive

reporting. Moreover, we identify the top-most difficult factors associated with risk analysis and specify some promising new directions to adapt the presented system in these cases.

This chapter covers the discussions and application of different methods presented in this book. For the implemented methods in the book, conducting various experiments is not practical for all of them. Hence, for those methods, several experiments are conducted to just show the correctness of two main proposed scenarios. For the presented cybersecurity methods in this book, we can roughly divide them into three sections [12], [17].

In this section, we present various use cases and applications, which are solved using the methods and systems introduced in this book. To the best of the authors' knowledge, all of the proposed use cases and applications are original and most of them have never been presented in a conference or journal before. Each use case is explained in detail starting from the introduction, the methods and problem-solving approach, experiments and obtained results, and/or discussion if applicable [...] [20].

7.1. Examples of Dynamic Risk Assessment Implementation in Autonomous Vehicle Operations

A reliable AV and connected vehicle, as defined in the intelligent transportation system (ITS) features, must have a sustainable strategy to protect itself from cybersecurity incidents, and the vehicle and system must continuously assess risks for effective operational risk management. When cybersecurity attacks and incidents are detected during real-time AV operation, immediately controlling the detected vulnerabilities and evaluating the resulting risk and potential damage help AVs act as secure and protective systems against cybersecurity threats. Accordingly, a dynamic and real-time protective approach is necessary to determine whether a cybersecurity attack can harm the system, decide possible countermeasures, and execute them. During AV operation, the risk assessment process by the AV system, based on used cutting-edge techniques, determines the cybersecurity attack effect and possible damage on the AV, and the best countermeasures according to different AV use cases. These methods significantly impact risk assessment during known and unknown cybersecurity incidents. This document discusses the recent evolutions of AV security and the limitations of the reactive threat reduction system. The contribution herein corroborates the recent development of a novel security solution designed to provide proactive threat reduction features. [3]

Assessment of incidents within the sphere of autonomous vehicles (AVs) has captivated the research community, and many scholars have dedicated their time to developing methods and techniques that will integrate risk assessment during incidents. This approach includes the risk analysis of detected attacks by the AVs during operations. In recent attempts to counteract vehicle attacks and network intrusions, several frameworks and methodologies for the detection and response of detected cybersecurity attacks in AV systems have been proposed. Autonomous intrusion response systems (AIRS) aim to provide automatic responses to detected attacks, and they can be separated into predictive and FL-based response systems. AIRS can also be divided into two types: [20] [10] signature-based invasion reaction system (SIRS) and pattern- or behavior-based identification. From detected signals and anomalies, a pattern-based intrusion detection system develops corresponding responses and eliminates intrusions by reference. Predictive intrusion rebound systems can be classified according to the response use case as on-board vehicle software, communication networks, and vehicle-to-vehicle and vehicle-to-everything infrastructures. The defensive measure can also be grouped based on its energy consumption and performance overhead, which should be carefully considered for protective reactions in AV operations conducted.

8. Future Trends and Research Directions

With technological advances in vehicle automation, the paradigm of determining the cybersecurity readiness of a vehicle by considering traditional security features has shown to be insufficient. Universal software defined radio (SDR) vulnerability is a common vulnerability category found in autonomous vehicles. Privacy and security challenges are also faced in autonomous outdoor drone systems. Some other challenges include in-depth misperception/resilient defense systems, and credible and expressive dynamic risk representation in the abstract situation. As an emerging domain in the cybersecurity in autonomous driving technology, a significant amount of research regarding this area is still lacking. Future trends and research directions include the new communication methods to prevent the widely deployed monitoring methods like zero-interaction quantum radar; situational driver detection, situation-aware threat classification; privacy-preserving reinforcement learning-related risk assessment; and cyber insurance coupled Q-table enabled regulation of quantized risk. Additionally, security challenges must be addressed in the field of Connected Autonomous Vehicles (CAV) technology. Owing to close proximity, the wireless communication between vehicles will provide an unprecedented attack area for

attackers. Criminals will attempt to modify the vehicles' data and communication packets according to the protocol's characteristics to launch information-based attacks. Autonomy and intelligence of autonomous vehicle operations will facilitate significant changes to countless fields. As a result of these key benefits, autonomous driving and applications based on autonomous vehicle operations are receiving increasing attention. The next section details six levels of autonomous driving that describe the operational conditions in sequential order: traditional manual driving, conditional driving assistance, partial automated driving, fully automated driving, conditional self-driving, and highly automated self-driving.

[12] [4] [6]This paper focuses on real-time cybersecurity risk evaluation in autonomous vehicles. As dynamic risk assessment methods designed specifically for autonomous ground vehicles or other autonomous systems have not yet been developed, the methods in the cybersecurity field of general scenarios, especially in traditional network scenario, should be referenced and then narrowed down to the specific context of the autonomous ground vehicles. Therefore, there are some inherent limitations with the methods, such as some methods not focusing on the risk assessment high-dimensional state space stochastically changing with physically dynamic elements. In addition, the look-ahead operation behaviors factoring into the risk assessment decreasing the efficiency, but obviously promoting the effectiveness.

8.1. Emerging Technologies for Enhanced Dynamic Risk Assessment

Risk assessment techniques designed for autonomous vehicles are beginning to be developed and form the foundation for new regulatory regimes. For autonomous underwater vehicles (AUVs), the most common method to avoid collisions with terrain or static obstacles is to use a mobility-optimization framework that sets AUVs to avoid potential collisions a priori, while for dynamic obstacles two main obstacles are to be navigated around as late as possible. DRA encodes rapidly-changing context, like lane changes, that may lead to changes in risks. An untimely path change request results in a miss-of-service scenario leading to a crash. However, a risk engine designed to sense the impact of the context in the risk assessment cannot address all of the context scenarios such as eventual lane-move of other road users. Thus, the use of external perception is required to offer reliability to perform advanced risk assessment. Finally, it is noted multiple vehicles with coordination provide a richer stream of

data to the DRA process. Wireless communication may be employed to share the predictions of these vehicles to improve the awareness of the others [21].

As a new domain, cybersecurity risks in autonomous vehicle operations have attracted considerable attention recently. Because of the numerous onboard sensors and external vehicle-to-everything communication that these vehicles are equipped with, there exists an immense attack surface that could potentially be exploited by adversaries to affect vehicle safety [9]. The primary threat to the passenger safety in the imminent AV environment is expected to be from a collision, which may occur due to complex causes including cyberattacks, mechanical defects or environmental issues. The immediate economic and human safety impacts have motivated the automotive industry to maintain substantial efforts to mitigate the collision risks. Proactive measures are employed, typically through the use of preventative safety standards but many cyberattacks and also unexpected collisions cannot be predicted. Consequently, in the emerging dynamic risk assessment (DRA) field, the collision risk prediction task is attracting research attention in autonomous vehicle operations [17].

9. Conclusion

As a part of an overall approach, this paper focuses on the problem of ensuring cybersecurity in the context of autonomous driving, which consists of a number of elements of the system's flexibility. This flexibility helps to effectively adapt AV actions to the current properties and behavior, as well as to assess the effects of threat activity, which may take place in the form of fraud attempts or other forms of "cyber" attack possibilities. The assumptions of the analysis presented in the paper put emphasis on the complexity of the problem tackled, and take into account the variety of sources of threats, one of which is the possibility of the activation of so-called "insider threats." A specific aim consists of the development of scenarios leading to the effectiveness and efficiency of performance measurements, together with the necessary management of business continuity in critical conditions [22].

The use of autonomous systems in critical infrastructures is now becoming more extensive, which includes the automotive field. The utilization of these systems is intended to accompany the growing demand for many prospective changes concerning the development of advanced mobility system solutions. Myriad functionality possibilities provided by them contribute to the realization of these platforms. The rapidly increasing number of them on the

global market causes the arising need for investigating various problems. The Disaster Driving, called the case of exceptional situations, is one of these arising problems. The aim of the article is to present and evaluate the continuity risk impact on the effectiveness and efficiency of activities in the range of robotization of complexes with ground autonomous vehicles, called AGVs [17].

10. References

1. [1] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
2. [2] H. Rivera-Rodriguez and R. Jauregui, "On the electrostatic interactions involving long-range Rydberg molecules," 2021. [PDF]
3. [3] P. Natalia Cañas, M. García, N. Aranjuelo, M. Nieto et al., "Dynamic Risk Assessment Methodology with an LDM-based System for Parking Scenarios," 2024. [PDF]
4. [4] V. V. Dixit, S. Chand, and D. J. Nair, "Autonomous Vehicles: Disengagements, Accidents and Reaction Times," 2016. ncbi.nlm.nih.gov
5. Tatineni, Sumanth. "Deep Learning for Natural Language Processing in Low-Resource Languages." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 11.5 (2020): 1301-1311.
6. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.
7. Mahammad Shaik. "Reimagining Digital Identity: A Comparative Analysis of Advanced Identity Access Management (IAM) Frameworks Leveraging Blockchain Technology for Enhanced Security, Decentralized Authentication, and Trust-Centric Ecosystems". Distributed Learning and Broad Applications in Scientific Research, vol. 4, June 2018, pp. 1-22, https://dlabi.org/index.php/journal/article/view/2.
8. Tatineni, Sumanth. "Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 11.1 (2020): 8-15.

9. [9] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
10. [10] Y. Mei, "First-order coherent quantum Zeno dynamics and its appearance in tight-binding chains," 2023. [PDF]
11. [11] 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]
12. [12] 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
13. [13] M. Hamad and S. Steinhorst, "Security Challenges in Autonomous Systems Design," 2023. [PDF]
14. [14] D. Iberraken and L. Adouane, "Safety of autonomous vehicles: A survey on Model-based vs. AI-based approaches," 2023. [PDF]
15. [15] C. Hartsell, S. Ramakrishna, A. Dubey, D. Stojcsics et al., "ReSonAte: A Runtime Risk Assessment Framework for Autonomous Systems," 2021. [PDF]
16. [16] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
17. [17] A. Jafar Md Muzahid, S. Fauzi Kamarulzaman, M. Arafatur Rahman, S. Akbar Murad et al., "Multiple vehicle cooperation and collision avoidance in automated vehicles: survey and an AI-enabled conceptual framework," 2023. ncbi.nlm.nih.gov
18. [18] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
19. [19] L. Luxmi Dhirani, N. Mukhtiar, B. Shankar Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," 2023. ncbi.nlm.nih.gov
20. [20] M. Hamad, A. Finkenzeller, M. Kühr, A. Roberts et al., "REACT: Autonomous Intrusion Response System for Intelligent Vehicles," 2024. [PDF]
21. [21] 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
22. [22] D. H. Lee, C. M. Kim, H. S. Song, Y. H. Lee et al., "Simulation-Based Cybersecurity Testing and Evaluation Method for Connected Car V2X Application Using Virtual Machine," 2023. ncbi.nlm.nih.gov