Risk-Based Decision Support Systems for Cybersecurity in Autonomous Vehicle Operations

By Dr. Vincent Wong

Associate Professor of Computer Science, Hong Kong University of Science and Technology (HKUST)

1. Introduction

The Spatiotemporal Innovation Center at George Mason University is developing an autonomous airspace management concept, creating a new level of symbiotic analysis and decision-making that fuses high-frequency answer-rich data (command and control) with real-time low-frequency query-rich data. State-of-the-art safety-of-life functions use one model to control the vehicle and a different model to monitor the vehicle, without significant sharing of information between the two models, leading to sub-optimal performance. Our approach supports risk-based decision support systems to optimize vehicle operations by constructing executable queries that guide information retrieval from a network of capabilities that maximize mission benefit within resource constraints, enabling smart sharing of information and coordination for risk-aware intelligent data.

Autonomous vehicle (AV) operation generates and uses large volumes of data in real time to ensure safe operations. Wireless data transfer rates are constrained by the airwaves' available frequencies, transmission bandwidth, and transmission power, and the amount of useful information that can be transmitted in a unit of time. This spatial confinement creates gaps in real-time data transfer capabilities and available bandwidth, requiring automated algorithms to constrain AV operation to low-latency feedback communication to carry out safety-of-life functions, preventing accidents or ensuring the AV can carry out its primary functions, avoiding potential negative impacts. Consequently, many of the required analyses and decisions must be carried out on or by the AV, remotely or both. These design choices must meet industry practice standards.

1.1. Background and Significance

Despite the groundbreaking progress of AV driving technology, the growth in autonomous driving has introduced numerous security concerns at the scales of data, system, and enterprise. Prosecutions, such as the adversarial attacks and the data spoofing, against sensors and data streams may manipulate the model-interpretation process, N-tuple programming on the power consumption estimation, and public opinion towards AV safety, and subsequently deteriorate the performance of AVs in driving tasks. Large-scale attacks on AV data infrastructures may lead to severe consequences, including widespread traffic congestions, difficulties for authorities in understanding real traffic situations, and the reduced reliability in enterprise models and enterprise cyber securities. Regulatory standards and compliance evaluation criteria addressing potential cyber threats for AV driving remain underdeveloped. Proper responses to and recovery actions after attacks on AV data security and AV cybersecurity are also underdeveloped. Therefore, there is an urgent need for the development of a risk assessment framework that can estimate business impacts occurring when cybersecurity threats arise on AV data infrastructures, provide governmental authorities and AV enterprise with useful decision support for proactive and reactive cyber risk management practices, and promote the public interest in developing common security standards for AVs to operate in a shopping center. The theory and practice of capturing business impacts caused by cybersecurity threats on innovation of AV data infrastructures are understudied.

Advent of various advanced technologies such as connected and autonomous vehicles, Internet of Things (IoTs), shared-mobility, and big-data has been fostering unprecedented innovations in transportation systems. Because of these innovations, increasingly, the traditional way of owning a vehicle has been shifting to utilizing mobility services, and the role of autonomous driving technology becomes a key factor in ensuring a driver-less comfortable and reliable transportation service. With the development of autonomous vehicles (AVs) and related technologies, the society has been expecting that these AVs will be a widespread means of transportation that provides the elderly and people with disabilities with new mobility and also ensure that driving is no longer a challenging duty. The speedy development of AVs is largely attributed to the numerous real-time data provided by a large number of sensors equipped in an AV, the continuously improved driving models, and also the advances in artificial intelligence (AI) and data infrastructures. In particular, real-time

sensor data and data infrastructures have been extensively utilized in surveillance and security management practices.

1.2. Research Objectives and Scope

There are two major contexts of research that will be addressed by researchers in this project. The first research aim is to investigate the maximum survivable fault patterns (related to Cyber-Attacks) that incorrigibly lead to an undesirable level of consequence (risk) of autonomous vehicle operations, in which steer, throttle, and brake commands will be frequently required by the control algorithm module. The second research context supports development of a risk-based scheme of a prototype decision support system (DSS) for on-road operations of autonomous vehicles using the dynamic extension of Trajectory-Driven Risk-based conceptual design method that represents the extension to the modeling and design of systems with significant complex interactions such as vehicle driving risks factors, in conjunction with control system response affecting risk management for the dynamic nature of vehicle operations.

The focus of this research is to develop and integrate a novel risk assessment model using the non-deterministic probability (ND-P) model for on-board decision support system for autonomous vehicle control technology for cybersecurity of autonomous vehicles. The planned technology realization and integration approach will involve an adapted version of a vehicle control and mission planning algorithm that is well defined for acceptable vehicle control and safety while driving under nominal operating conditions. This research will involve a full integration of the ND-P model (for performing risk assessment) and the vehicle control algorithm, so a new framework will be developed for a prototype on-board decision support system involving assessment of residual risk during on-road operations of a vehicle.

2. Autonomous Vehicle Technology Overview

In this conception, humans are responsible for all driving activities, which basically corresponds to a level 0 automation vehicle. To increase the automation level in vehicles, many challenges need to be addressed. On one hand, the technological limitations for full automation are the major hurdle that separates the realization of fully autonomous vehicles. On the other hand, entrenched issues related to human-user trust in AV adoption and use still

remain to be attuned. Alongside the technological challenges with autonomous technology deployment, there are social and ethical issues.

In recent years, the automotive industry has made significant technological advancements that have allowed for the introduction of autonomous vehicles (also known as AVs) on the market. The Society of Automotive Engineers (SAE) has defined different automation levels, ranging from 0 to 5. A level 0 vehicle is one in which the human operator is fully responsible for driving, while a level 5 vehicle is fully automated and can perform all driving tasks in every condition that a human driver could perform. Currently, the actual autonomous technology is available at the SA level 2 in commercial vehicles. In these vehicles, the driver is expected to take full responsibility for the driving tasks unless the autonomy technology requests engagement into the planned driving route. The driver must be ready to take over driving tasks when the autonomy mode requests it. The autonomous vehicle then supervises some driving functions while providing the driver with a safe driving experience.

2.1. Levels of Automation

To differentiate the above levels of automation, NHTSA provided the regulatory definition of fully autonomous vehicles, which refers to no need for human control. In other words, all levels given by NHTSA had to include driver control of the vehicle because no design is capable of recognizing and responding to the whole range of driving tasks. However, in higher levels of automation, a safety assessment of the vehicle design must consider what role the vehicle occupant should play during the operational design domain (ODD).

Level 5, or full automation, refers to no human intervention in various driving conditions.

In level 4, high automation, the system is capable of performing all driving tasks under certain conditions without human intervention. The human can rely on the system to respond appropriately to any exceptions.

In level 3, conditional automation, the system can perform all driving tasks under certain conditions, with the expectation that control will shift back to the human in order to intervene as necessary.

In level 2, partial automation, the system is capable of steering, accelerating, and decelerating under limited conditions, while the human driver monitors the environment.

Level 1, or driver assistance, refers to the system supporting either steering, acceleration, or deceleration under the guidance of the human driver.

Level 0, or no automation, refers to the human performing all driving tasks.

In 2018, SAE International provided levels of driving automation for on-road vehicles. The six levels are as follows:

2.2. Key Components and Functions

Kim et al. investigate different decision support approaches and propose a comprehensive RBDSS design. Their approach highlights important key building blocks the RBDSS should include, and details prominent features that RBDSS should possess. The proposal leads to providing decision support for managers who require managerial control and still be proactive and improve operations.

Rubin et al. categorize available RBDSS options in multiple areas including the use of case competency, proactive guidance on further actions, and the knowledge Diffusion Data Server for expert feedback.

Gautam et al. argue the need for a "strong" DSS, integrate the DSS with multiple kinds of utilities such as optimization techniques in conjunction with other functionalities such as weather forecasting, visualization, spatial analysis, and autonomous decision making.

First, Thai and Dzombak identify a set of elements that should be embedded in a good DSS. They differentiate DSS with either "strong" or "weak", distinguished by the DSS complexity and complexity of the problems solved by the DSS.

After examining prevailing DSS and CDA types, the key building blocks and elements that should be embedded in an excellent risk-based DSS type that is imperative in autonomous vehicle operations are gathered. The key components of good RBDSS cover various technologies, embed an interdisciplinary approach, and should possess several explicit functions according to the requirements and tasks that a RBDSS targeting autonomous vehicles should accomplish.

3. Cybersecurity Threat Landscape

In addition to issues related to traditional computer attacks, the security risk is expanded manifold because drivers, passengers, and the autonomous control system perceive, learn, predict, and respond to the dynamic and uncertain environment in which it is located. As a result, the changes and updates of the characteristics of internal and external structures also reflect changes and updates of potential harm. These new potential harm have triggered and accelerated the construction of a new organization, test center, and other feasible studies. The ripple effect produced by the characteristics of the autopilot system should be explored and controlled precisely by the adversary. At the hardware level, lack of formal verification, software control issues, partial to complete driving motion sensor errors and external input security risks, lack of artificial intelligence security mechanisms and system bug vulnerabilities, application layer in vehicle-to-vehicle (V2V) and vehicle-to-Infrastructure (V2I) communication, cloud servers, root and enterprise servers, etc. The accessibility of the server can all lead to serious system defects. With the massive banding and integration of the Internet of things (IOT) and the vehicular ad-hoc network (VANET) in Smart Cities, the increase in autonomous vehicles connected to 5G and the excellent development of vehicle to surroundings data and information exchange, the security flaws embedded in autonomous vehicles must be addressed and tested comprehensively. These security holes may be exploited by malicious users or damaged individuals who intentionally target, endanger, monitor, hijack, or control a specific car and person. The danger, negative social impact, and various levels of autonomous control system infrastructure all stimulate extensive research and study to achieve the right balance between the safety protection and useful data environment with stability.

Regarding autonomous vehicles (AVs), the multimodal, multifunctional, highly connected, and complex system structure results in a large number of components that are susceptible to the expansion of new cybersecurity vulnerabilities. As a complex machine that integrates artificial intelligence, wireless communication, control algorithms, databases, computing platforms, etc., the reliability of the software and hardware as a whole determines the performance of the vehicle. Opportunities for cyber attacks also increase significantly. In a system that promotes safe responses in advance and real-time, there are a lot of information exchange and network interconnection related to data analysis and timely feedback. The well-known activities in this interaction model may involve data collection, communication, database, control, and other technical contents. The point is that the more connections and

complex algorithms involved, the more vulnerable a system is susceptible to various types of cyber attacks that may occur. Information disclosure, tampering of data, operational control, fire theft, and DoS attack strategies can alter the normal, effectively degraded performance and non-performance operation of an autonomous vehicle to manipulate terrain and safety vulnerabilities.

3.1. Cybersecurity Vulnerabilities in Autonomous Vehicles

3.1. Types of Cybersecurity Threats in Autonomous Vehicles

New types of threats related to cyber-physical system-based autonomous vehicles can lead to specific, disruptive, and destructive behavior discovered by cutting-edge means. The main security challenges consist of sensor spoofing and hacking, actuator hacking and fault injection, and wireless communication. In order to identify any extra functionality or changes to a component, a strict inventory of all functional elements has to be managed. Incoming supply chain integrity inspection helps to ensure secure component procurement. Developing obfuscator techniques and proposing redundant hardware for creating a defense mechanism for sensor and actuator exposed information networks is necessary for securing deployed assets. The hardware-in-loop testbed is leveraged for evaluating trust-unique compound strategies. These results help in reporting the limitations when securing critical information and thus create trust-oriented feedbacks.

According to Valenkamp et al., cybersecurity solutions must address confidentiality, allow limited or controlled access, and offer safety guarantees. In autonomous vehicles, it is important to secure sensitive information, and protection is necessary against various types of threats. Botnet attacks can cause severe damage through DDoS attacks, which can block emergency vehicle access to roads. This is an example of a service interruption to which a vehicle might be subjected. Additionally, intimate technologies, such as V2X communication, routing-related, and user profile data privacy threats may be present. Most attacks are difficult to mitigate and can also lead to conventional vehicle crashes due to malfunctions of vehicle safety-related systems such as brakes and airbags. These risks highlight the importance of the integration of a robust cyber-risk assessment policy. A risk management and assessment instrument combines the basic elements of cyber-risk assessment. The policy supports decision-makers who are responsible for formulating and implementing risk management policy.

3.2. Vulnerabilities in Autonomous Vehicle Systems

To respond to these threats, we propose to create the Security/Certainty Tests of Autonomous Vehicle Operations, a design objective for the probability of detection, resilience, response, and recovery that reflects that the TaaS provider fails to compete with traditional autonomous vehicle designs and business models unless the passenger has a chance to dutifully avail the vehicle from cyber-intrusion. The considered cost of the intrusion to each autonomous vehicle is up to a billion dollars, and if such intrusion does not promptly attract a systemic security-criminal intervention that contains and arrests the interested parties - to the discretion of the responding law enforcement command and according to the direction received from leadership for escalation - there is at least a possibility that the criminals can endanger personal safety: the data security-designated driver among passengers reports a suspected malfunction in a valuable environment, such as the presence of a concealed intruder in an unknown area, that is disconjointly discovered or derived from otherwise relatively unreliable data sources; the designated driver failed to remove responsibility in response to command and control audit, or the error in depth inconsistency in the estimated safety-patch in the vehicle's fault resolution model equals or exceeds the magnitude of the maximum deep-fault lateral separation heading uncertainty.

This said, we believe that the main motivation for agents willing to invest resources in cyber-intrusion in autonomous vehicles includes national security, ideology, or coercion - to instill fear and create physical and panic-related financial damages. These actors create destructive intentions by exploiting normal vehicle operational scenarios and minute-by-minute corridors to direct to the target a vehicle that appears as a low security risk to detection. Destructive intentions differ from motives in cyber-crime, but the possible modes of attack are the same.

There are several ways that a cyber-intruder can force a NHTSA level 3, 4, or 5 autonomous vehicle system to behave maliciously from inside or outside the vehicle. This modality of interfering with a commercially produced vehicle in daylight, driving at legal speeds, in existing traffic, and constrained to following the road infrastructure and traffic rules, opens a potential for large-scale disruption of land transportation infrastructure. Most frequently, intruders will consider tampering with or hijacking the autonomous vehicle to extract financial gains: by ransom-based denial-of-service intrusions, by masquerading undetected as a cooperating vehicle to provide fake measurements from the physical environment and

the driving history of the vehicle's users to create detailed simulations, with which an advanced persistent threat can perform a physical intrusion that appears nominally innocuous or unrelated to the preliminary activities and that appears as close as possible to the target vehicle in the system state trajectory during execution of the intrusion, to replace the genuine sensors with a cryptic adversary's sensors, which may bribe the supply chain, by creating a stealthy exfiltration channel out of the vehicle for zero days, by disrupting or conducting denial-of-service attacks on elevated communication infrastructure deployed in anticipation of increasing the efficiency of autonomous vehicles, by gaining insider financial gains through data acquisition and changes in driving history, or by creating anti-competitive conditions through disruption of services offered.

4. Risk Management Frameworks

The SEI developed the TARA, a structured approach to understand the potential technical and operational impact of the loss of trust in AVs and the mission. The approach helps identify the trustworthiness pertaining to the mission-specific objectives. The NIST framework, published as a result of the Presidential Executive Order 13636, provided a flexible and repeatable risk management process based on protection, detection, and response capabilities. This enables stakeholders to decide how to manage cybersecurity risks considering organizational contexts. The Cybersecurity Framework provides a cost-effective and scalable way to help organizations manage cybersecurity risks. The framework may be used to assess and improve the cybersecurity management processes. It is organized into three parts: framework core, framework profile, and framework implementation tiers. The framework core is the set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It links business terminology to technical capability. The framework profile is developed by aligning organizations' business requirements and risk tolerance against the framework core to achieve business objectives. It is used to determine opportunities for beefing up the framework implementation process. Finally, the framework implementation tiers provide additional context required to manage cybersecurity risks. This includes risk management practices and used resources, as well as available interfaces for coordination, cooperation, and collaboration.

Several frameworks consider the complete life cycle of a system, while others have a narrow focus, such as on the development or the operation of systems. NIST-IR 7434 defined a risk

management framework for an information system. This framework includes a risk management process consisting of six steps: prepare for assessment, prepare for security control assessment, conduct security control assessment, develop findings, recommendations, and lessons learned, conduct only of security control, and information system acceptance. Several industry and academia frameworks and standards have been developed to manage risks associated with cybersecurity. In the following paragraphs, several of these frameworks and standards are concisely described.

4.1. ISO/SAE 21434 Standard

On the contrary, vehicle cybersecurity standards have considerable importance from the viewpoint of law and regulations and contribute to the robust development of automated driving functions. The ISO/SAE 21434 standard was developed for the cybersecurity of road vehicles with respect to safety and is currently available. In this thesis, we will use ISO/SAE 21434, established for giving cybersecurity guidelines for road vehicles with advanced driving assistance systems, for autonomous vehicle AD security. Upon approval of ISO/SAE 21434, it is expected that it will be adapted to related standards. It is envisaged by the developers that ISO/SAE 21434 will be built in sync with the related standard ISO26262, so that ISO26262 would complement ISO/SAE 21434 on significant safety aspects while ISO/SAE 21434 would cover significant security aspects on vehicles.

Cybersecurity in autonomous vehicles is a safety-critical issue. Autonomous vehicles exist in a complex ecosystem from idea inception to the end of life, making cybersecurity essential for every phase of building, deploying, and decommissioning autonomous vehicles. In addition, modern vehicles are part of a connected transportation system and hence complex and open systems, where attackers can easily explore new paths of attack. Although different standards for securing systems exist (e.g., American NIST800-53, International ISO/SAE 21434), no standard exists solely related to cybersecurity issues for advanced autonomous vehicle driving systems.

4.2. NIST Cybersecurity Framework

The main objective of the NICE Framework is to assist government organizations with identifying the most critical cybersecurity workforce skills needed to protect government information and systems. It should also be considered by international organizations as well

as having an international workforce and responsibilities for nation-state cybersecurity against cybercrime and cyber warfare that pose a threat to the state. An understanding of the foundation concepts, principles, methods, and approach available and recommended by NIST should lead to the successful application of recognized threats and offered risk formulas in order to be in compliance with existing national cyber risk governance charters and cybersecurity principles.

The NICE Working Group, under the National Initiative for Cybersecurity Education (NICE), plays an important role in this initiative. The initiative produced their first version of a NICE Cybersecurity Workforce Framework in 2017 for roles and responsibilities of cybersecurity talent in the workforce. NIST also recommends the NICE Framework reference in conjunction with existing or future national cybersecurity centers and points to the specific crosswalk to the NICE Framework to assist organizations in utilizing their approved tool to address challenges associated with cybersecurity vulnerability risk. The NICE Cybersecurity Workforce Framework identifies various work roles and tasks required for cybersecurity work, which is applicable as wider cybersecurity knowledge for all involved in a project, including third-party suppliers of systems and services, to consider potential cybersecurity risks in their work products. NIST continues to lead a national effort to ensure that this framework is adopted by the current and future national cybersecurity workforce.

5. Decision Support Systems in Cybersecurity

Decision Support Systems (DSSs) are human-centered computer systems, which facilitate the process of knowledge-intensive decisions and have been extensively utilized in various domains. Designing DSSs for cybersecurity in autonomous vehicle operations plays a significant role in the implementation of appropriate countermeasures once detected security issues by Optical Computer Vision. The essential characteristics of the Decision Support Systems in cybersecurity for the autonomous vehicle could be defined as (1) Data-oriented: DSSs in cybersecurity require direct access to relevant data; (2) Event-driven: DSSs should monitor real-time events such as access, usage, and attack to raise alerts for decision-makers; (3) Risk-based: In cybersecurity management, decisions are, in general, made before or after the occurrence of the security event. The Risk-Based Decision Support System (RBDSS) for cybersecurity is a type of DSS that is intended to be used from the perspective of anticipating the occurrence of the event. The RBDSS serves two primary functions: (1) extraction of security

information to support the decision-makers and (2) supporting the computational modeling (i.e. data inference) of the environment. These functions accordingly can be used to support the event prediction associated with security. An RBDSS would provide knowledge management and problem-solving capabilities to analyze the impact, probability, and utility of the various potential actions for various security issues. Web-based system (available through web browser) provides 24/7 access to data, information, and knowledge, and external parties can quickly be consulted. Based on this, the company could stay up-to-date regarding the cybersecurity threat and the occurrence of security events. Moreover, an RBDSS offers different functionalities to communicate with the enterprise that is depicted graphically.

5.1. Definition and Functionality

The presented approach is capable of successively fitting a complex engineering model to the incomplete and partial input-output training data, and then utilize the resulting ROM within BO to optimize the solution, a process that significantly reduces the computational time. To entrap the solution, the ROM is used together with a Differential Evolution (DE) optimizer, which gives a rough guess and a probability to allow the EGO algorithm to explore those areas that are more likely to host the global minimum. Such advanced RDSS reduce risks tied to the safety and security of autonomous vehicles, while identifying a set of security layers contributing to the targeted Resilience Upkeep Capacity (RUC) and costs. The obtained solutions are employed in the prediction of a subject transportation system's expected performance for a set of security layers by utilizing the Composite Security Rating. Such advanced RDSSs are able to identify security enabling measures/stakeholders that should dominate a network of interconnected autonomous vehicles.

This chapter has proposed a Cybersecurity Agile Risk Reduction Engine (CARRE), consisting of efficient forward modeling and optimal decision-making techniques capable of solving complex risk-informed decision-making challenges under severe uncertainty. This is achieved by employing quick and efficient Reduced Order Models (ROMs) powered by Novelty-Based Adaptive Sampling (NAS) methods that operate seamlessly with the Sequential Quadratic Program (SQP) and the Efficient Global Optimization (EGO) groups of ROM-based Bayesian Optimization (BO) algorithms. These techniques are implemented within the CARRE Framework which uses NAS to populate an initial training set, learns a ROM that can be queried in vaster domain, and starts iteratively gathering the most informative points.

The emergence of autonomous and cooperative transportation platforms has unveiled the need for efficient Risk-Based Decision Support Systems (RDSS) able to evaluate the effectiveness of different cybersecurity strategies in order to maintain safety-critical transportation systems' optimal levels of safety. RDSSs refer specifically to decision support systems that are tailored to conduct risk evaluation of potential security-critical flaws tied to the use of enabling and autonomous vehicle technologies.

5.2. Types of Decision Support Systems

The decision logical component can be an alarm, a detector, an event predictor, a broader forecasting monitor, a finite state machine, a policy, a program, or a protocol. It could also be an action or directive for coordinated control that changes the current state at execution or in the future. Some decision support system components are related from the perspective of shared data and resource needs. They may or may not be physically separate entities, even though they are logically distinct. In particular, the layout and capabilities of decision support systems and physical control systems can vary greatly. With regard to cybersecurity and decision infotronics, two aspects are additionally important. The allocation of decision functionality to different on-board physical entities has a bearing on overall system reliability and cybersecurity.

Not all autonomous system decision support systems are the same or have the same requirements. The importance and timeliness of information quality can be different within the overall systems in an autonomous architecture. The physical element, a decision support system, can be of a different nature as well. The decision support system can range in functionality, performance, system integration, and infrastructure, and may include interactions with humans.

6. Integration of Risk Management and Decision Support Systems

For instance, the Auto-ISAC verses propose that the business analyses and influences legislative and governmental actions, and band of businesses to provide a safe and immune vehicle internet experience and report to strengthen significant trouble spots and enhance the risk governance and management actions and processes. The Alliance for Automotive Innovation, a business involved in decisions and standards, also made a few suggestions from their participation.

The task of certifying cybersecurity for connected automated vehicles (CAVs) has spawned a private market with specialists taking part at the legislative level, judicial branch, and workplace ethics across all the legal platform levels. Manufacturers and industry alliances and standards agencies in the area have released materials. They describe and construct measures, existent or potentially proposed, and different assessments that the reserving organizations coexist.

The context of Autonomous Vehicles (AVs) involves a range of laws that are being discussed, proposed, and enacted to handle management and data protection as new mobility and automation characteristics of the internet. The nature of legal drivers for cybersecurity and privacy for AVs has been researched by scholars. In judging the banks, the roles of laws and guidelines, traffic supervision services, and the tasks in which these entities are engaged appear to influence the function of different industries to find avenues in L3 and L4 Automation.

Decisions facing cybersecurity personnel reflect culture, policy, law, regulation, and analysis, which involve executing features and treatments in order to manage risk and maintain trust. As a result, cybersecurity is often a process of decision-making in which professionals take a wide range of methodologies that arise from the policies to risk areas they are engaged in.

6.1. Benefits and Challenges

There are many different approaches in how the data format of a vehicle might determine this reason, but the claims also need to be validated. If local DSS suggest different risks for a vehicle behavior, they should be provided out-of-band methods to interact and converge on a consistent, evidence-found solution using optimized and complementary autonomy pipeline programming interfaces designed to operate in untrusted environments. Often the results of validation of decision aid is not communicated outside of the system that uses it. Researching this space we validate our decision aids and decision support system to be part of the training data of the systems. This supports the improvement of the decision support system by updating their output with improved de-biasing and discrimination performance.

A challenge in using risk-based DSS for cybersecurity is understanding the real trustworthiness of offered risk assessments and recommendations. For autonomous systems, it is not enough to drive the system or lanes or behave in such a way that other autonomous

systems can trust it. Both the content, scope, depth, and most importantly autonomous DSS must work consistently and provide options as an experienced AI that manages associated risks. The main goal of intelligent techniques should be to provide sufficient evidence for faulty behavior in vehicle control processes that would convince evaluating systems that the risk values reported by the DSS are justified. These determinations require a well-structured data format to be broadcast to external systems in ways for feedback to be sent to the DSS to potentially provide more information for claimed risk values.

6.2. Case Studies

The collected telemetry measurements for each completed ground vehicle path-follower test simulating two different behavioral models contained driving pressures that reflect the real-world roadway following conditions associated with the upcoming roadway path-segments. The analysis results indicate that jungle-based response functions help the autonomous vehicle operate using less pressure on the drive-by-wire interface so that the vehicle follows an inefficiently smooth speed profile operation. The case studies also show the passenger detectable hard curved path-following tests compared results between the observed test vehicle operations and the road recognized test vehicle operations for a range of decision speeds-vision horizon choices.

The case studies for the vehicle testing simulations developed in this research used four different planning under uncertainty (PuU) operational strategies for the responsive navigation system of the autonomous ground vehicle. Dynamic programming was used to generate the decision functions and update the vehicle's trajectory to minimize energy consumption while considering roadway curvature radius properties, stoppage, or both. The results for both roadway observed path-following and harder than observed path-following indicate that the average power consumed during test vehicle operation was reduced by more than 26 percent. The vehicle testing results show that the responsive navigation architecture can improve the vehicle's fuel efficiency and still satisfy passenger comfort needs. The results for the vehicle path planning simulations compared the safety, mobility, and environmental risk cost trade-offs that four PuU behavioral decision functions can achieve based on the roadway officials' available real-time data quality.

7. Future Trends and Research Directions

Research is expected to contribute to both secure and resilient operations by addressing the realistic requirements of AI/ADS stakeholders for the CAVAS network with the public value of increasing societal trustworthiness. Interface toward real-world AI/ADS and RB-DSS (both C2C and C2X) users must be create risk balance cases derived from exemplar and threat CAVAS stakeholders. Develop use cases of CAVAS T/A with AI/ADS that have interest for RB-DSS ML end users. Assist CAVAS risk planning for typical AI/ADS stakeholders considering a suitable unit of analyses. Work toward development of city and countrywide data availability for AI/ADS in CAVAS. Promote traceable, explainable, and auditable T/A of AI/ADS and provide a legally informative defined category of defined trust-based (or threat credible) defined AI/ADS stakeholders. Align data in used CAVAS services with the legal definitions and societal expectations by updating the system and enabling transparent a reference platform for 'transparent sensory-driven cyber assurance of AI systems'.

The following subsections delineate a selection of future trends and research directions which are anticipated to be of key importance concerning both secure and resilient autonomous vehicle (AV) control operations and services. The authors recommend that an interconnected risk-based decision support system (RB-DSS) software framework featuring machine learning (RB-DSS-ML) algorithms is developed to support these important tasks. It is concluded that RB-DSS-ML systems for cybersecurity in autonomous vehicle operations will need to be developed with extensive attention to benefit realizations and increasing societal trust from desired applications and that regional data availability, diverse integration of use cases and supporting technologies for a taxonomy of legal definitions.

7.1. Emerging Technologies

Topic entities must account for cybersecurity risk when considering taking products to the market. Using cyber as a feature generates societal and infrastructure dependency that could be easily highlighted and exploited due to a breach in the landscape. The more self-driving vehicles, the greater the requirement for risk assessment to take an active role in respect of cybersecurity. The future of cyber in transportation holds possibilities for being autonomous, in private drones, long haul truck convoys. Cybersecurity is a critical issue in the above-mentioned and can provide both enormous benefits and be a path for exploitation of security concerns. High-risk transportation problems, such as truck convoys, can use autonomous technology to improve safety, increase passenger mobility, and save fuel by allowing the

convoys to run closer together, creating fuel economy savings. In a state-of-the-art scenario, the supply chain would extend from "the site" to the furthest destination, offering the opportunity to schedule "just in time" deliveries.

In recent years, new advanced technologies have emerged. The future of cybersecurity will demand that vehicles be connected to entities such as city infrastructures, making transportation more effective, efficient, and safer. Technology already available, just like the rest of cyber, must tread carefully and embrace good practices when running in environments of a dangerous nature and level of threats. Entities that bridge sensors to the outside world must have cyber practices that manage risk. Technologies of cyber, like centralized and decentralized firewalls, could be used, and even intrusion detections. Using technology to transport people from point of origin to destination will have a great impact on the modern world. These autonomous vehicles will introduce mobility, data, connectivity, and automation to roadways, with a potential impact on private lives, national economy, and legal implications, repercussions, and consequences to personal safety.

7.2. Regulatory Landscape

While state regulations allow for flexibility regarding deployment requirements to foster innovation, it inadvertently permits an unstable set of safety regulations among the various states. In 2016, NHTSA provided guidance by releasing the Federal Automated Vehicles Policy, which was recently updated in 2020. This document introduces four important regulations that may affect the development and deployment of autonomous vehicles: getting exemption authority, a framework for safe testing of High and Higher Automated Driving Systems (ADS), dealing with complex design elements, and identifying crash mitigation factors.

Starting in 2018, state activity on autonomous vehicles began to increase. The increased activity was aimed specifically at fostering the development of the technology. As of 2019, only a few states have tried to tackle cybersecurity issues for autonomous vehicle operations. The state legislatures of Tennessee, Ohio, and Michigan have each passed statutes addressing cybersecurity risk management. The methods prescribed by these statutes require a cybersecurity plan to incorporate identifying and reducing risks, ensuring risk management activities are conducted by support personnel, and establishing a process for regular autonomous vehicle system security validation. The Michigan statute requires a cybersecurity

plan that complies with National Institute of Standards and Technology (NIST) Special Publication 800-53 and/or NIST Special Publication 800-171.

Autonomous vehicle testing and deployment within the United States may have federal, state, and local agencies with jurisdictional interests. NHTSA is the primary federal agency responsible for regulating the safety aspects of autonomous vehicle testing and deployment. The overall regulatory landscape for autonomous vehicles is intricate and unique from that associated with traditional vehicles driven by humans. Approaching challenges such as the need to develop cybersecurity regulatory measures in an age where software updates occur remotely creates additional complexity.

8. Conclusion and Recommendations

In this paper, we focused on the cybersecurity data processing and the sullying logic of AV. The AV cybersecurity data processing technology consists of four elements: data fusion, high-level Joint Hypothesis Testing (JHT) and low-level data association, recursive evaluation with different weights, and situational strength evaluation. The sullying data processing technique constructs the Cyber Attack Situation Awareness Models (CASA) for distinguishing whether the process and sensor system have been sullied. The experiment results have shown the validity and feasibility of the suggested technique, and the matching test with other fault diagnostic and cybersecurity detection technologies has shown unique features such as accuracy, tolerance, and cyber modeling. With our suggested research, AV may provide a guarantee of cyber autonomy for both its own protection and attacks against the enemy, while letting maneuver consistency adapt to the unpredictable environment, context, or opponent.

With the extensive digital content, sophisticated sensor technology, and large amount of data, modern transportation systems have been transforming into intelligent, connected, and automated driving (AD), or so-called autonomous vehicles (AV). AV technology depends on high-level automation and is considered the future of transportation. However, the autonomy and open system of AV may increase some cybersecurity risks. Unresolved cybersecurity risks may seriously affect public trust in AVs, restrict companies' incentive to produce new technology, and might even lead to public safety and national security risks. Human factors and accidental incidents associated with human factors cannot be totally avoided, and the design limit with unauthorized access and use of computer technology is imperceptible, which has a direct impact on the long-held principle of separation between autonomy and

security function, which was regarded as an important philosophy for the safety of certified aviation operation.

8.1. Summary of Key Findings

We present a verified implementation of a DSS function that assesses vehicle state and monitors vehicle and system operations in order to measure and interpret the vehicle's interaction with and time to resolve risky situations. If desired, the DSS can call the vehicle's autonomous control system into action in situations where interactions within present normal vehicle capability are failing to resolve a developing vehicular risk. In summary, the DSS uses information provided by a set of sensors and vehicle controls, knowledge of the vehicle's current state, and knowledge of the risk of transportation mode in order to offer an operational check and resolution capability that responds to developing risk. It does so by asking the vehicle operator to take action, requesting that the driver/passenger give control over to the vehicle's autonomous control system, or by taking whichever of no action or distributing an advisory the on-board system deems most appropriate and following up with human-directed management of system interactions in the case of a vehicle warning, advisory, or alert.

We present a comparative evaluation of our risk-based decision support systems (DSS), implemented as part of an autonomous ground vehicle innovation project known as the Ann Arbor Autonomous Vehicle Initiative (AAVI). AAVI develops not only the vehicle platform, but also the operational policies, procedures, and supporting infrastructure which form the capability that makes the innovative technical advance useful as early as possible. The DSS assesses vehicle risk, policy compliance, and other factors drawing on a variety of sources and uses in-vehicle alerts and the vehicle's basic capability for autonomous operation to direct the human towards appropriate interventions when they are needed. We leverage our experiences with the DSS and vehicle development in order to clarify the higher-level requirements for a more robust implementation and suggest approaches that we have found useful for meeting these objectives.

8.2. Practical Implications

First, it becomes extremely important not to underestimate the complexity of integrating risk management and decision analysis in the context of the cyber supply chain. Underpinning the

development, adoption, and partnerships responsible for creating supply chain value. Rather, a commitment to proactive risk management more effectively incorporates supply chain system consideration into contemporaneous business decision-making. Surely, the temporal and spatial size of cyber risk now weighs heavily on the shoulders of decision-makers from multiple functional areas who daily engage the cyber supply chain both when directly managing cybersecurity in-house and for any partner they inform, especially in those strategic locations where national security relies on the system's effective operations. Rather, there is a need to assess and fill capability gaps in decision-making for investing guidance that more effectively balances proactive investment in cyber risk management with competition from countervailing interests.

In effect, four recommendations are presented in this paper for the development of risk-based decision support systems for cybersecurity in autonomous vehicle operations. Before these recommendations are discussed, a few practical notes are highlighted concerning the application of RBDSS to proactive risk assessment of intelligent and autonomous cyber-physical systems. Then, the paper suggests that future work needs to further investigate the reputational and behavioral adjustments, or lack thereof, of decision-makers regarding the trustworthiness of an RBDSS-based estimate in what could be considered a potential no-action bias effect. It is a basic assumption in RBDSS that cyber risk analysis results should be integrated into and help inform real-world decision-making, but no research to our knowledge has critically assessed the trustworthiness and credibility of the risk estimates generated by RBDSS.

9. References

1. L. Guan, Z. Yan, S. Wang, K. Lu, and M. Xie, "A Risk Evaluation Method for Cybersecurity of Autonomous Vehicles," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, pp. 380-387.

2. L. Sun, W. Liu, and G. Yan, "A Survey on Cybersecurity of Autonomous Vehicles," 2019 IEEE International Conference on Big Data, Cloud Computing, Data Science & Engineering (BCD), 2019, pp. 194-198.

3. A. K. Saha, A. K. Roy, and S. Ruj, "A Game-Theoretic Approach for Cybersecurity in Autonomous Vehicles," 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6.

4. Y. Ren, W. Shi, S. Yu, and Z. Li, "Cybersecurity for Autonomous Vehicles: A Survey," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760-776, Feb. 2019.

5. Y. Cao, W. Shi, S. Yu, and Z. Li, "A Survey of Cybersecurity in Connected and Automated Vehicles," 2018 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), 2018, pp. 100-106.

6. J. Ma, X. Liu, and W. Shi, "Cybersecurity for Autonomous Vehicles: Status, Challenges, and Future Directions," 2020 IEEE Intelligent Transportation Systems Conference (ITSC), 2020, pp. 1-6.

7. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.

8. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

9. 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.

10. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.

11. M. S. Ali, M. A. Hossain, M. M. Hassan, and S. U. Amin, "Cybersecurity Vulnerabilities and Solutions in Autonomous Vehicles: A Survey," 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2018, pp. 1-4.

12. K. Zhang, X. He, J. Li, and C. Jiang, "A Review on Cybersecurity of Autonomous Vehicles," 2018 IEEE International Conference on Intelligent Transportation Systems (ITSC), 2018, pp. 216-221.

13. C. Shen, J. M. Sharif, and K. G. Shin, "Security in Vehicular Ad-Hoc Networks," in IEEE Wireless Communications, vol. 13, no. 5, pp. 5-11, October 2006.

14. W. J. Phillips and H. L. Owen, "Autonomous Vehicle Cybersecurity: A Systematic Review," 2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 2020, pp. 1-8.

15. D. N. Islam, M. A. Razzaque, M. Hassan, and S. U. Amin, "Cybersecurity Challenges in Autonomous Vehicle Networks: A Systematic Review," 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019, pp. 1-6.

16. K. R. Kancherla, S. Ruj, and A. Nayak, "A Survey on Cybersecurity Challenges and Solutions in Vehicular Cloud Computing," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1453-1458.

17. M. B. Siddique, A. Hossain, and S. U. Amin, "A Comprehensive Survey on the Security and Privacy Issues of IoT-Enabled Autonomous Vehicles," 2019 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2019, pp. 1-4.

18. N. Kumar, S. Das, and M. Z. A. Bhuiyan, "A Review of Cybersecurity Threats and Defenses in Vehicular Ad Hoc Networks (VANETs)," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1480-1495, March 2021.

19. M. S. Ali, M. A. Hossain, M. M. Hassan, and S. U. Amin, "Cybersecurity Threats and Solutions in IoT-Enabled Autonomous Vehicles: A Comprehensive Review," 2018 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), 2018, pp. 1-8.

20. Y. Zhang, Y. Zhang, and S. Wang, "A Survey of Cybersecurity in Autonomous Vehicles," 2020 IEEE International Conference on Information Technology, Networking, Electronic and Automation Control (ITNEC), 2020, pp. 1401-1406.

21. M. A. Hossain, M. S. Ali, and S. U. Amin, "A Review on Cybersecurity Threats and Solutions in Vehicular Ad Hoc Networks," 2019 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2019, pp. 1-4.

22. A. K. Saha, A. K. Roy, and S. Ruj, "A Survey on Cybersecurity Challenges and Solutions in Autonomous Vehicles," 2018 IEEE International Conference on Smart Computing and Communication (SmartCom), 2018, pp. 1-7.

23. A. K. Saha, A. K. Roy, and S. Ruj, "A Comprehensive Survey on Cybersecurity in Autonomous Vehicles," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1-5.