Human-Centric Design of Cybersecurity Incident Response Procedures for Autonomous Vehicles

By Dr. Hassan Abbas

Professor of Computer Science, American University of Beirut, Lebanon

1. Introduction

As autonomous features are employed more widely in transportation systems, it is important to perform analyses of the operational and security impacts of AIH-635-connected vehicles on the transportation system. We believe that a cyber-physical system (CPS) allows clear, insightful, and groundbreaking studies about these impacts. Our self-driving car and the robocars transported pedestrians and drivers to classify threats, as identified critical cellular IoT vulnerabilities that could be abused in a variety of universal attacks. PCIe the discussed topics as source localization in Final County communication, sensors, ROS, and Wi-Fi. With John Cloud design security in partnerships wireless vehicular communication via erasure coding generator that takes account of channel variations. We have been moving toward the challenge of making wireless vehicular communication and signals secure from simple jamming and more complicated spoofing by using various intelligent protections [1].

Automated or connected vehicles are typically designed to operate in cooperation with the environment. Their perception, knowledge, decision-making, and action execution processes are influenced by their environment. However, the environment is not always benign and can contain security threats [2]. Negative effects on safety of in-vehicle, in wireless communications, and at infrastructure can be generated. Therefore, it is essential to provide appropriate cybersecurity means to automateand Act Campaign (XKCsICK reports IO and research is supported by the Engineering and Physical Richmond local greaer Mourning blackboard and the experience and workforce Internationat Raizmangement System of tactical udditons for RP serving stitches affected by cybersecurity threats (Rusux. Arts in autonomous vehicle (TX) military and TACs in a variety defensive technology with varied architectures that allows autonomous entities to detect, analyze, mitigate, and neutralize cyber threats (Rusux. About Xi Guang Yang is a full professor at the Recess Laboratory, and head of the United Research Management System (XEME) Engineering Operations Research Center and Cheng Department in the West Virginia Computer Science Department. bitcoins received her orders at the University Commission, China.

1.1. Background and Significance

Fig. 1.1 develops information security management programme (ISMP) guidelines for the cybersecurity design procedure. The AV should be treated as a computer work with the addition of real-world physical factors of importance to an attacker. The cybersecurity challenge depends primarily on the vehicle model, which includes levels of automation depicted in level 0 to level 5. Along with the rise of new mobility models and the concept of Mobility as a Service (MaaS), vehicles are becoming complex software-based IT systems, leading to increased cybersecurity challenges. For instance, external software, both in terms of appraisers and appraisals, may inject poisoning attacks past the measures. As a particular concern in the root- and non-rooted Android IT systems, it was found that cyber adversities trigger specific underlying safety issues due to misinterpretation of communication. The cross-functional method that creates extreme segregation or leads to delay of certification, can augment the cybersecurity concerns. In order for an AV to identify cybersecurity problems at the initiating stage of procedure, the AV should regard intrinsic and external security hazards into the design procedure. Although numerous technological and communication options exist to advance the state of the object for resiliency and certainly throughout laser- and/or digital censorship, several secretive regulations are established by nervy adversaries. Consequently, the unbiased appealing object satisfies any strength that a modest alteration is transient [3]. The best a passive intruder can do is broadcast his signal to go through a completely-open network and monitor the observable lateral information that has the minimal [Shannon entropy] sparsity.

The focus of this project is on the design of efficient and effective cybersecurity incident response procedures for autonomous vehicles (AVs) [4]. The rising complexity of modern IT systems in AVs, including networked technologies, has led to an increase in cybersecurity challenges due to new technological capabilities, such as remote access of malware to parts of a vehicle. The cybersecurity challenge depends primarily on the vehicle model, which includes levels of automation depicted in level 0 to level 5. It is beyond the scope of this project to manage the vulnerabilities within the entire car network but rather to target the vulnerabilities within a central vehicle system or central electronic control unit (ECU) once the safety-critical components are secured [5]. Hence, this project suggests protective measures integrated in the car, designed within the concept of level 3 automation where a safety driver is not required.

1.2. Research Objectives

1. To evaluate autonomous vehicles cybersecurity in the context of nomenclature, sensor, and road infrastructure-related cyber risks. This will result in a detailed, contextually anchored, case-specific knowledge of observed, inferred, and evoqueable attacks and risk factors that eventually can be used for balancing unreasonable risks and costs. 2. To investigate autonomous vehicles deployable cybersecurity incident response procedure using a human-centric lens. This can be done by examining the incident response cybersecurity participation of different people involved in manufacturing, developing, monitoring, maintenance, and using autonomous vehicles. This results in a case-specific incident response sensitivity assessment of autonomous vehicles research and relates to a wider consideration of incident response in how it is carried out [refs: 1d2bff03-db14-43b0-b884-0c871e3826ad].

By deeply understanding the risks, reacting to cyber incidents in a timely and efficient manner as well as being able to rely on a solid incident response procedure will lay down a crucial foundation for cybersecurity in autonomous vehicles becoming reality [6]. Cybersecurity by design and cybersecurity incident response are two main strategies for securing autonomous vehicles. Although efforts have been put into cybersecurity by design, incident response could be less often taken into account. The objectives of this research can be specified as follows [5]:

1.3. Scope and Limitations

The focus of this study is on autonomous vehicle cybersecurity incident response procedures, within and outside the vehicle, from the human-centric perspective. Specifically, three pieces of the cybersecurity puzzle with decreased emphasis in the current research were highlighted and form the research objectives: the comprehension and usability of cybersecurity status indicators and warnings, the experiences and responses of human drivers to cybersecurity incidents, and the design of effective human-cyber procedures within and outside the vehicle. It is essential that the device displays and presents cybersecurity-related information in an easily and quickly graspable manner, while ensuring the driver’s focus on driving. In the case of drivers' non-responsiveness to a vehicle-imposed action requested during a cybersecurity incident or while recovering from it, the drivers' actions and inactions should be taken into consideration by updating and notifying the Cyber-Physical Systems and the remote control centre to prevent triggering a false alarm in the future and also to improve security procedures. To ensure human-centric cybersecurity incident response procedures from the driver's perspective, the following research objectives are defined.

Autonomous vehicles must rely heavily on cyber-physical systems for safety and failure-proof operation. In the event of a cybersecurity threat or actual attack itself, it is essential that the vehicle is able to detect, respond, and recover from such an incident on its own. While most of this cybersecurity protection, detection, and response can be designed into the hardware and software layers of a vehicle, there remains a significant potential for adverse effects and unintended consequences during cybersecurity incident response procedures specifically during driving [7]. Hence, all such cybersecurity incident response procedures outside of the vehicle itself, especially those communicating directly with the human driver, form the process of study for this paper. These procedures are identified as the Human-Cyber Procedures and are categorized to be either within the vehicle, as a subset of autonomous vehicle cybersecurity process, or outside the vehicle, as an extension of the driver's role in cybersecurity incident response in [8].

2. Autonomous Vehicles and Cybersecurity

The aforementioned threats underline the necessity of the intrusion response system enhancement for autonomous vehicles that can automatically and autonomously protect vehicles against internal and external attacks. Current methods lack the ability to specifically adjust their actions depending on the situation on the road (vehicle position, road information, etc.) contributing adversely to vehicle misinformation. This and the fact that the vehicle security remains unconfirmed from the user and authorities points out that (driver, passengers etc.) the current IDSs could not respond to safety and security concerns support the creating an autonomous reaction system, especially for the security of autonomous vehicles, which is the first of its kind, with this study. This autonomous response system will be able to automatically and autonoumsly protect themselves (mainly themselves but other facilities also can be consider) against malicious attacks. Therefore, at the end of the cyber-physical system strategic autonomy in the land-based vehicle remains a dream. As part of future works, automatic and autonomous cooperation studies in dual systems can be included.

Security and safety are pivotal concerns for autonomous vehicles. To provide the traffic security with safety measures, autonomous vehicles depend on different sensors and computing systems. Due to the complexity of the cyber-physical system with the real world, each system in autonomous vehicles can access other electronic control units (ECUs), making the vehicles vulnerable to a large number of different attacks [9]. Facts indicate that without immediate response to a cyberattack, long-term damage to an autonomous vehicle is inevitable. Before security breach can occur, the vehicles should be protected by their own response system which is also capable of recovering attacked functionalities, and ensure continuity of the planned activities. Therefore, autonomous vehicles need an intrusion response system which is dynamic, immediate and capable of always effectively functioning. Such a response system should implement protection strategies to raise the difficulty level for potential attackers, to inhibit the control authority for potential attackers and to protect the vehicle’s control information [3].

2.1. Overview of Autonomous Vehicle Technology

Technology allows to realize fully autonomous vehicles that are controlled purely by machines. While there is great interest in this option from an economic and potential application perspective, the autonomy, networking, and software in these systems introduce new security threats. This is especially true for new sensor and communication technologies, where real-time requirements for vehicle control must be respected. Furthermore, attacks in critical vehicles (e.g. ambulances) can pose an immediate danger to human life or health. Focusing on incident response [10], these challenges need to be faced with measures integrated at multiple levels. The ability of an autonomous vehicle to self-detect possible critical security incidents is the key requirement, as only this ensures the possibility of legitimate actors immediately taking control of the system and thus ending the incident quickly and with the predicted impact [8]. To provide a broad foundation for discussion in the rest of the paper, this section gives an overview of the state of the art in autonomous vehicles. In the first part, we give an introduction to controlled automated vehicles and then elaborate on the necessary network infrastructure requirements primarily according to [11].

In the following, we give brief overviews of security certificates for cars, smart shipping, and certification and approval for drone systems and flying cars.

2.2. Cybersecurity Threats in Autonomous Vehicles

Without humans, the whole responsibility is given to computers, so if it is not possible to manage these problems, the race for ownership should not be won. Hereby, establishment of the AVs architecture of sensor-use modes and decision-making mechanisms without losing the sharing essential part will be accepted as a substantial topic before the massive application of AVs. The purpose of this work is to understand the feasibility and development of the guided algorithm which is not human-centric but the algorithm may perform programming in sequential manners and meta-level for dangers manipulated by autonomous vehicles, such that spatial, functional and temporal constraints are defined. Even if the AV's manufacturer and the ACN (AV Control Network) that energizes Elite Dvas run away from accountability by defining the operation characteristics of artificial intelligence algorithm including the sequence of events and probabilistic risks in real-life generally, there is a need of recursive, relatable testing of the alternatives by utilizing artificial intelligence [12].

Autonomous vehicles (AVs) are one of the most important scientific and practical milestones in the 21st century [13]. Human errors are a significant percentage of traffic accidents. Hence, replacing humans with new intelligent systems dealing with environment-sensing conditions, route decisions and actions are expected to significantly decrease the number of accidents. However, the development of autonomous vehicles brings new safety and security threats that require new autonomous vehicular communication and electronic and telecommunication system developments [5]. For example, LiDAR, sonar, infrared and ultrasonic hardware sensors with advanced model real-time artificial intelligence software. Furthermore, the nature and number of multi-hypothetical interconnected components in autonomous vehicles are the new challenges. Motivated by these, this chapter is focused on integrated cyber/terrorist attacks and methods. These new methods require new mathematical, theoretical and computational analyses such as index theory, Hamiltonian and Stochastic methods and new generation interdisciplinary teamwork is necessary for their development.

3. Human Factors in Cybersecurity Incident Response

The intrusion detection mechanism is well-documented, but evaluating the risk associated with detected attacks in real time is still an emerging area. Fully autonomous systems need to autonomously analyze data, detect vulnerabilities, identify threats, and evaluate risks with minimal human intervention. The current risk assessment process has various issues that need to be addressed. A comprehensive risk assessment method should empower the system to make instant decisions in the face of cybersecurity attacks without human intervention. Dynamic safety risk assessment methods are essential for enhancing effectiveness [14]. Fortifying the human-vehicle interaction in merged systems can be considered a general safety measure, as the human driver will be in a better position to avoid certain critical failures, software updates can be executed immediately and workarounds might be identified early.

To ensure that our cybersecurity defense mechanisms fit to the vehicles they are designed to protect, it is necessary to assess the human factors involved in these mechanisms. While users are currently required to follow various actions to protect themselves and their computer systems, they might not be capable of taking over or coming up with alternatives in case a vehicle's systems are attacked [10]. Moreover, autonomous systems will not only communicate with humans, but also rival autonomous opponents. This produces an entirely new set of challenges for human factors research and development within the domain of cybersecurity. For instance, it can be expected that users and autonomous systems benefit from introducing a syntax and a language they both are familiar with, due to its origin in common professional work systems [15].

3.1. Importance of Human-Centric Design

Given the increasing relevance of AV cybersecurity, this paper argues that stronger attention should be devoted to the role of human operators in CSIR procedures within AV development. We advocate for a human-centric approach to CSIR, intending to make CSIR procedures and the overall AV ecosystem resilient to human limitations, and understandable and manageable for human operators. This requires designing CSIR procedures that can handle a complex fusion of human and AI contributions to the achieving of overall task goals [16]. This paper presents the results of a mixed-methods expert study conducted to capture the perceived importance of human factors within an AV CSIR space, and the relative priorities to be assigned, in a complex scene with N different contributing factors: cyber threat to an AV, cyber threat to an external AV operation, cyber threat to a connected vehicle, through the manipulation of data, cyber-threat to a power-train system, and cyber threat to a sensor. The reaching of this objective will be driven by the Human Systems Integration (HSI) paradigm that has been adopted by the governments to address the complexity of the integration and the optimization of all the interdependent systems [14].

The integration of autonomous vehicles (AVs) in urban environments and the consequent increase in the number of digitally connected devices involved in driving scenarios (vehicles, sensors, road infrastructure, etc.) expose AVs to the risk of cyber-attacks. Cybersecurity procedures have been developed to deal with these risks: Cybersecurity Incident Response (CSIR) procedures define and coordinate actions that organizations must take to respond to and recover from cybersecurity incidents. These procedures should ensure that the AV operator and other stakeholders can remain "in-the-loop" and maintain high situation awareness during cyber-attacks [17].

3.2. Cognitive Biases and Human Errors

Self-driving vehicles are among the most disruptive technologies. Whether it is related to employment, mobility, insurance economy, incontestable security gains, and social equality, the primary results are considerably positive. This situation leads to the observation that autonomous vehicles may be a major support for various domains, such as commerce or public transportation. Despite the advantages of autonomous vehicles, the main issues are their adoption and utilization in different domains, notably the ethical, legal, and security issues. From the results, as expected, it is important to take into account various aspects of ethical considerations, trust in autonomous vehicles, and user behavior in security, which are necessary for the development, adoption, and diffusion of autonomous vehicles. In this opportunity, the legal issues become equally important to the engineering, cybersecurity, and ethical issues when they are associated with autonomous vehicles [18].

Lack of trust in automation, ethical implications, and privacy and cybersecurity risks pose serious threats to the adoption of autonomous vehicles [19]. Among the different risks threatening the development and deployment of autonomous vehicles, cybersecurity concerns are particularly relevant. When discussing cybersecurity and autonomous vehicles, the state-of-the-art tends to focus on developing secure software, focusing on secure data transmis-sions and privacy preservation. However, especially for vehicles, security concerns also need to include the development of incident response procedures, attacking vectors, and cybersecurity incidents, beyond merely trying to impede attackers. Based on a comprehensive study of relevant literature and empirical evidence, this paper presents a cognitive systems-engineering perspective on cybersecurity for autonomous vehicles. This is achieved by analyzing cognitive, organizational and ecological aspects that influence human behavior in situations of threat, attack, and vulnerability, in which their cognitive biases are predominant sources of human vulnerability and drive errors and failures. In addition, human errors and failures in cybersecurity of ICT and Critical Energy Infrastructures (CEI) are presented, to complete the picture of threats and vulnerabilities in the field of cybersecurity, which serves as a basis to synthesize a definition of cybersecurity. In summary, the paper provides a review of the state of the art on different issues relating to cybersecurity of connected and autonomous vehicles (CAVs), from a cognitive systems-engineering point of view. This work ends with potential recommendations so that software developers can refine their best practices by taking human beings into account.

4. Design Principles for Human-Centric Incident Response

Underpinning these assertions are ideas of technology and information systems design that are made alive through the ideas of interaction, user experience and usability. Usability is a central concept in any user-centred design literature and informs HCI in many ways for ordinary people carrying out ordinary daily tasks in ordinary settings (Nielsen, 2012). From the viewpoint of system operators, understandings and meanings of incidents in an economic context are of primary importance and provide a rich basis for understanding how systems might interact incidentally as protocols build a picture of what might be happening on a network (Hayne, 2014). It provides a foundation for a system that might take better decisions than those in use during everyday practice. These points connect so that the work presented in this article has implications for the way systems are designed, and as such, have the potential to go some way towards addressing the challenges we have posed [3].

Adopting a Human-Centric approach to designing and deploying online security measures enables the protection of individuals and organizations in a manner that takes full account of the evolving threat landscape and the technologies adopted. Building on work in the field, the key takeaways are that any approach that seeks to enhance holistic protection must include an appreciation of the changing nature of technological dependence [16]. When responding to an incident, above all things, it is essential to manage the task in the best interests of an organisation's stakeholders. Information from this communication task is helpful, but the representational and cognitive models we have posited tie into new security protocols in a pragmatic and human-focused way.

4.1. Usability and Accessibility

With the research work promoted by the introduction of the human operator within a human-centric design, our proposal arguably advances along the same lines. Our study is shown in Figure 5, and we propose an agile methodology for innovative interaction paradigms (AMICI), [10], testing and evaluation. To be concrete, these paradigms could be the shift from the operational block of the manual manoeuvre to the operational one, the development of new introductory and training protocols based on methods that raise ecological validity for inclusion and transfer of knowledge during critical incidents. This would ensure the mastership by learners of this new major technology of CAV in learning situations close to operational situations.Parallel with these macroscopic paradigms, biomechanical strategies to detect stress and critical changes in psychomotor performance informing triggers of CIRP can be tested collectively. Conversely, to provide the successful operationalisation of human-based adversarial detection through these real-time alert triggers, a set of experiments in operational conditions in simulated test environments should be carried out and the integration of the HSDL within a CSDL simulated environments should be implementation as a bit longer term of study.

Usability and accessibility are critical concerns for CIRP [20]. Usability is the quality of the user interface and the availability of information necessary for the tasks it allows, whereas accessibility expands the concept to the intuition and the ease with which people can use it since the different types of tasks have to be performed under adverse conditions that reduce the perception. An ICS via field trials to test and measure the usability and accessibility of these CIRP designs will expand the accessibility of information, concept and readiness and provide potential insight for human behaviour under severe stress. Moreover we believe that the integration of CIRP training within a CSDL successfully possess considerable contribution to autonomous vehicle fleets di”using human-adversarial accidents during their half centennial deployment phase. The same trend in macroscopic global accidents of CAV on the road were reported by the Wards Auto website. This study confirmed that human beings are not able to adapt human-centricly to comprise the threats due to the severe biological, psychological, organisational, institutional and environmental pressures.

4.2. Training and Education

For example, the Federal Autonomous Driving Act stipulated that fully automated vehicles must meet a variety of requirements, including the technical requirements for features, the requirements for system design, and the driver performance for such vehicles. More focus is placed on the movement efficiency and mitigation of traffic hazards in the single vehicle control compared to the control of a connected autonomous vehicle that belongs to a CCS. Secondary emphasis is placed on the cyber attack risk due to autonomous vehicle movement. This demonstrates that traffic system safety might be enhanced due to autonomous vehicle technologies because connected control systems perform defensive measures automatically when they are attacked by a malicious outsider. Therefore, in the near future, the combination of autonomous vehicle technologies and connected control systems for intelligent transportation systems are expected to prevent accidents and minimize injuries [5].

To achieve human-centric design of artificial intelligence, both outward and inward-looking solutions should be developed to address both threat actors and system vulnerabilities. Human-centric approaches that consider human-computer interaction and human psychology have the potential to address secretive and expansive challenges. Prioritizing the human element in artificial intelligence is essential in today's complex and reactive threat landscape, particularly in critical technology areas such as cyber-physical systems and the Internet of things [16].

5. Case Studies and Best Practices

RQ2: How to build procedures and systems to control and respond to various incidents resulting from uncertainty in autonomous vehicles? C2.1: Best Practices in Interaction and Agencies The search for the most effective way to interact with engineering systems that become autonomous (cyber-physical) under given conditions is junction finding. To illustrate the junction finding—applicable to situations in which agents, organisations, companies, or vehicles have a decision making authority—problems in the context of autonomous vehicles and control engineering, we briefly describe a cooperative transportation control model of an autonomous vehicle. This is done by illustrating key results that favor automatically steering the primary velocity vector in the direction determined by the ratio of the vehicle's waiting time to its projected marginal waiting time at controlled junctions. C2.2: Best Practices in Real-Time Decision Making The primary objective of this work is to develop a real-time decision making mechanism that approximates decision making by human agents like the AV unmanned operator, and is thus intelligent enough to solve problems of autonomous vehicles with every such action containing an action also pertaining to a cyberphysical system. The idea is to give control to the primary decision maker (the primary agent). However, suggestion to change the ownership permits agents to own the transportation of their waiting time based primary agents via secondary agents without direct control from the primary agent. C2.3: Best Practices in Action Monitoring, Control, and Human-Aided Decision Making As the proportion of and reliance on cyber-physical hybrid human-centric autonomous system increase, the need for enhancing the robustness of such systems against transient disturbances due to interaction, cooperation, and deteriorating performance becomes an important context. Consequently, increasing the low outweighed mandate hybridity of such systems and testing out neurological human-centric control paradigms also becomes important. In S-phase of fi_CampaignSS, self-adaptive coherent autonomous optimization strategies were tested on driving actuators based on the calculated average (occurred over uncountable and countable duration) performance to form a direct-reward learning basis feedback methodology. C2.4: Best Practices in Predictive Counteraction Risk assessment for AVs in the context of their cyber attacks can be defined in terms of the degree of fault prediction and diagnostic ability of their decision making in risky instances, or in S-phase. The AV under test herein was trained on a unique database that contains risk index information. The system of the test experiment was generally formed out of a derived multi-task regularized support vector regression system, an intelligence monitoring system, a multi-agent operation system, and its melt processor module. C2.5: Best Practices in Safety Framework The multi-agent suboptimal real-time decision making procedures and safety risk assessment methodologies development for autonomous vehicles via a well-developed master test version of indirect fault tolerance approach include an interactions, cognitive dynamics, and numerical intelligence multi-agent suboptimal decision making framework. In S-phase, the second approach controls discrete status sets at game theory optimal decision alternatives in a real-time manner. C2.6: Best Practices in Scalability The IDs adequacy for fault detection has been extensively researched, yet most of these research require trainability. Also, for highly skewed data and unbalanced mixtures, they might be quite challenged due to various outstanding research. Our second approach herein is conceived as a highly accurate, fast, flexible, and tick-able cyberphysical system with a relatively enormous staged learning transition knot less system in the sense that it is not available in the literature and represents a unique class of acquisition Learning assessment mechanism.

RQ1: How to make cyber-physical systems more secure and robust by design without limiting their capabilities? C1.1: Best Practices in Design It is preferable to design and specify a secure, robust, cyber-physical human-centric system from the ground up, supported by sound design principles and adhering to mathematical logic (thereby lessening the dependence on human decisions or actions). A vehicle is an autonomous robotic system with a set of sensors and control devices. Unfortunately, unlike scenarios where sensors and control devices communicate through serial buses, wireless sensor communication is hardly protected. Our general recommendation is foremost to secure the sensor and control device design, and maintain cryptographic keys to make it safe from ad hoc devices or rogue agents within the range. C1.2: Best Practices in Construction and Operational Support It is crucial to introduce novel secure road infrastructure technology to support new developments in transportation such as autonomous vehicles or electric vehicles. Secure road infrastructure includes thorough protection which includes anti-counterfeiting, theft and replacement, device simulation, and data entries at junctions. In the long run, the road environment can assist the growth of autonomous vehicles and track their performance from the road infrastructure. Such an integrated system can take two forms; it can be simulation based and become part of a vehicular network to aid navigation and coordination among (small to large) clusters of vehicles. Alternatively, a network can be employed as an organizational layer to manage the data the infrastructure collects from autonomous vehicles. Each vehicle's encrypted tracking data is stored in an organisationally designated secure space. Moreover, the road infrastructure can also provide local computing and wireless facilities to support networked vehicles (moving within a short range of each other). C1.3: Best Practices in Communication A successful security solution for AVCNs involves the design of a vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) secure communication prototype. The V2V communication pipeline must facilitate remote control interactions, facilitate encryption/decryption actions, provide authenticated converted control requests / commands, facilitate secure local/private distributed control mechanism, authenticate third party clustered devices, design trusted hash chain mechanism, design virtual private network formation, ensure authenticated membership, establish cloud handling operations, encrypt and support authenticated cloud message synchronisation and implementation, encrypt image registration discussion, facilitate selective image processing strategies, do edge analytics support signature transport and perform open and authenticated session/task reopening actions.

[8] [5]In this section, we illustrate short-term solutions to some of the issues we introduced in Section 2. These practical solutions attempt to make cyber-physical human-centric systems more secure and robust within the context of greater second-order resilience.

5.1. Real-World Examples of Incident Response

In driving scenarios not all attack scenarios are centered around technical aspects or limitations or, since vehicle hacking leads to a loss of control, or at least decreased reliability. How do we define and verify safety but also take into account moral and ethical questions, like when swerving to protecting a pedestrian, but maybe killing yourself or passengers? Defining, verifying, and realizing safety in-vivo is difficult, but it can be supported. It is, however, important to engage in research focusing on how to test advanced driver-support systems in non-standard scenario, for example a truck overtaking another truck on a four-lane road with heavy rain and next to zero visibility does not happen every day. When it comes to positioning Information and Communication Technology (ICT) and its safety implications, communication, and validating simulations become extremely crucial. Cyber-attacks have gone digital and can no longer be managed by traditional security means. It is not just a matter of data, but also a matter of safety. Attacks may lead to the disabling of cars and then getting involved in an accident involves more than two vehicles [18].

Attacks on vehicles have been an area of research now for over two decades [5]. The quality of the attacks and vulnerability research has evolved from the use of telediagnosic software in the 1990s, through the introduction of internet portals focusing on car hacking and exploitation of vehicles' CAN (controller area network) functionalities in the 2000s, to attacks targeting interfaces of vehicle comfort services (such as infotainment systems) and risks associated with vehicle-based Wi-Fi solutions, to Endpoint Independent Telematics Analyzers in the 2010s. It is tempting to argue that the ability to attack vehicles is here only a minor part of the issue. The main problem with modern vehicles is the sheer complexity. The ECU (electronic control unit) count continuously increases and car manufactures deliberate about the introduction of over the air updates. The underlying protocol layers of vehicle-to-x communication (V2X) technology are attack prone, but protocols were they might not need attacks to pose a risk are opened up.

5.2. Best Practices in Human-Centric Design

Readers should consider approaches such as an anticipatory security assessment program that favours the utilisation of a human-centric design method comprising proactive and reactive safety operations. According to the Gartner publication titled How to Reinforce Incident Response and Cyber Threat Analytics for Autonomous Vehicles cybersecurity solution providers from the same industry are adapting their services to assist original equipment manufacturers (OEMs) in delivering more robust InV incident response (IR) systems and networks built for protection purposes thanks to their increased ability to interact with potential external dependency or develop an observed abnormal states from observed behavioural discrimination. The review of this surveyed publication and other publications like RTCL20 who are working on individual CAV's at the vehicle level assembles CAV's and vehicles' overall discomfort level dissimilarities and correspondences between vehicle-level solution to vehicle communication or Internet of Vehicle technology institution ASIR cryptosystem is made off from vehicle-level SIR and individual CAV mechanisms.

As recently mentioned, although AVs have the potential to increase road safety rates significantly, they also create an environment within which cyber-attacks might cause serious harm to the safety and welfare of their passengers [7]. Consequently, a significant part of the security design of connected and autonomous vehicles (CAV) is the active hardening of the vehicles' exposed attack surface against cyber threats while also foreseeing the means to detect, respond, and recover from intrusions that have not been successfully averted [3]. The International Organization for Standardization in its recently ratifie 21434:2021 Road vehicles — cybersecurity engineering has identified threat risk management and cybersecurity by design & in operational matters, as part of its relevant guidelines for the automotive industry in the development as well as maintenance of secure road vehicles. While the safety and cybersecurity of AVs require different investments and expertise, cybersecurity guidelines for AVs refer 21434:2021 for safety engineering guidance according to which best practices should be chosen to mitigate the predictable risks.

6. Evaluation and Validation

In Sect. IV, we qualitatively discuss the A-O forecasted scenarios for the proposed influence-accomodating OC-specified impulsive-resilient intra-location tracking controller for our time-delayed T-S-model-bi-hormonic-fed autonomous vehicle the stability under the influence of the A-P forecasted scenarios' peripheral sensing sales elasticity. Therefore, the post-hoc setpoint-backfeeding-impeding-stabilizing time-delayed tracking control problem for the nonlinear system with the occurrence of the privacy concerns-on-unknown space-distributed chaotic and synchronous non-uniform time-delayed CPSs is resolved in this paper. The performance improvement and the backstepping‟s adaptive capacity for the augmentary and latent LTI-space-wide-stabilizing time-varying space-extended undervoltages in A-P-forecasted situations haven been numerically established through the governor-backed EGO-specified non-decreasingly-convergent inverse tracking regulation for the intelligent plant, The construction and identification for the user-categorized random-boosting association-able steering device model is outlined, while the commercial development of it was built on recent medical ROI data stations has been introduced as ICDRC for-categories of distinct product characteristics, suggesting sustainable recommendations and readily transferable develop-cubes. For the autonomous planes with human AI-like space resistance, the general convergence of the breach-resilient policy, specifically designed to accelerate the Yaw-stream temperature operating system, is reflected systemically through two chosen proposals (aided by empirical-Y-intelligent volatile ecosteer-diagnostic equipped dashboard controller, which escorted the execution through the amateur II reinstated command signals) about the resilient control network defense of the predicted smooth-flight-volatility-resistance discriminability-autoresistance DNR-ADR RO policymakers.

Risk evaluation framework: We deploy six real-world scenarios from [21] to simulate incidents with different initial A-P severity levels and the decisions made by the proposed framework in response. we additionally designed two more realistic operating conditions based on the case studies in [10], [15]: a. OED (Operating on Environmental Detection) scenario simulates a priori detection, suggesting that an autonomous vehicle senses a new cyber threat after entering operation, the potential worst-case A-P severity of which is intentionally set to be greater than 1, leading to an unavoidable imminent trip termination due to unresolved threat. The case benchmarked IoV knowledge is used to mimic the real achieved scenarios, and the operational environmental sensing BO algorithms to simulate the real-world scenario of implementing ENV-EVAL/DEV topmost critical edge smart agents, which learn in-car sensory to boost basic ENLs, impacting in actual vehicle re-modification and cyberassessment data. b. OPD (Operating on Prior Detection) use case posits that a cyberattack remains Unknown_A-P (secret and waiting-to-be-exploited) to a connected vehicle before entering operation. It rationally delays the vehicle's switching to CAM mode so as to protect safety. Moreover, the study uses National Institute of Automotive Service Excellence (ASE)"s automobile service excellence control rater development as a benchmarked scenario to mimic the realistic scenario of achieving training data, along with the realization of the actual available maintenance data, collected by the Chinese Inventory System. Intending to evaluate the operational cost-reduction effect on autonomous-car-related companies, which directly ca-userscentric affects them, we established the following six related items regarding the convergence of Xiaoet al. Cybersecurity-Analytic-Model-Prediction-Resilience/ Cy-SAPMAR Allocator and the realistic-operational-longitudinal-linkages in OC-B. According to the strategic mode of the implementation of the OC-Bs and the in-vehicle environmental knowledgebases, and, they can also be grandly categorized into two OC-B specific categories. We apply three generic OC-B scenarios, corresponding to the states of randomly flipping different three bits of 0, 4, and 8 bits of the exploited CCM, to jointly discuss both cases, with the originally embedded harmful bit with A-P unknown. Lastly, into another generic simplified A-P value and the evaluated OCC level can also be converted from the severity adaptive control updated into appropriate threshold, so as to run legacy conventional reactionary control strategies in the intelligent computing IC era or will be converted into personalized sensitive level of human-computer interactions in smart robot age.

6.1. Methodologies for Evaluating Procedures

The VNC itself should be able to process automatisms especially for the most worrying Cyber-Physical attacks. The possibility that automatisms assume the control of the vehicle is always provided for in the shared awareness theory [7]. The CAV platform options function is used to change the behaviour of the VNC. The vehicle Anomalies/Cybersecurity/Failures Reporting system lets the VNC manage some cybersecurity vulnerabilities and incidents remotely, by direct connecting with the car exploiting vehicle to infrastructure communication. In a previous document, it was initially evaluated the enablement of the CIR tools in VMS. CIR is composed by the following elements: CIR-1: CIR for Known events; CIR-1a: CIR-1 Plug-in; CIR-2: CIR for Unknown events; and CIR-2a: CIR-2a Plug-in [22]. Despite its ability to respond to most of the Cyber-Physical attacks, the vehicle's Control Network Monitoring and control has some limitations. For this reason, the VNC itself could include some of these procedures to run on VMS. The CIR-2 and CIR-2a procedures can be activated to generate the uncertainty alerts.

As the development of CAVs gravitates away from human control, there is a requirement for the systems to be more resilient to attack or failure in order to continue successful operation. Including the Cybersecurity Incident Response (CIR) plan in Vehicle Monitoring Systems (VMSs) would enable this [23] . The CIR plan consists of procedures that guide humans in how to respond to cybersecurity vulnerabilities and incidents when an autonomous vehicle's on-board Cybersecurity Defence Monitoring System (CDMS) fails to respond in a timely fashion. Therefore, the VMS has to cooperate with the CIR by providing a set of alerts to the VNC in a timely fashion so that the VNC can plan an appropriate reaction following a cyber-physical incident in the car. However, as the vehicle continues to move forward autonomously, fusing these two sources of alerts (VMS and CIR) into a single response process may cause them to be erroneously filtered by the VNC and to be lost in the VNC's shared awareness process. For this reason, it is important to preserve the dual provenance of the alerts as they are processed in the VMS, thus enabling the correct mapping of each alert to its source and maintaining the required awareness of the car system's state. Based on these requirements, this Deliverable deals with the definition of an integrated Human-Centric approach to develop the procedures of CIR tools for CAV system. Furthermore, enhanced descriptions of suitable methodologies for evaluating the CIR procedures are provided. In this Deliverable, we will provide a description of how to evaluate the best procedure for the unknown fault alert that may be created because of the dissemination of two or more alerts.

6.2. User Testing and Feedback

Additionally, the user experience on the new TD Box is characterized by extreme ease of use, plainness, and good levels of visibility and vividness of signal for beginners in addition to colors being grounded in the brand's visual guidelines. Considering the intensity of the interaction suggested, especially in abnormal conditions, a thorough examination of the computational efficiency is necessary in future steps. Such check-ups should facilitate equilibrium between the time required for achieving desirable levels of accuracy and collision avoidance capacity, the visual distraction to the driver, the reaction time to informative losses, or the association of possible action alerts to operational settings established by the business counterparts. [21]

The purpose of user testing and feedback is to assess how the new features and prototypes of the car cybersecurity module are perceived, supported, and understood through the lens of its early adopters. Therefore, it will include envisaging a series of formative evaluations, one through co-design process, one that is observational of user interaction with an existing AV cybersecurity module, and one that takes notes of the cognitive load experienced by the users when attempting to follow the written cybersecurity procedures. [16]

7. Challenges and Future Directions

1. Introduction Automated vehicles (AVs) have capabilities to sense the environment, interpret the detected information, decide the next action, and then act accordingly to complete the task efficiently like driving. The design of AVs presents security risks. An adversary can hack an AV's system as a whole, or components of that system, to potentially cause property damage, financial loss, or even loss of human lives. Cybersecurity of AVs is emerging as a crucial research topic [2]. Multiple papers discuss the different attack scenarios on AVs and vulnerabilities with respect to AVs.

This paper presents a reference-level simulation model for human-centric threat detection in an AV, dealing with restricted user attention spans. We rely on the simulation model of Michaelis–Menten dynamics to model the biological functioning of the human mind under stressful conditions. The Braitenberg's vehicle model is employed to represent the collision between the AV and potential threats detected by the user. We model the user's trust in the AV using a Gaussian distribution and create an AV working architecture in Unity that runs experiments on the ViZDoom platform using the developed detection system. Finally, the perception, attention, and action details of humans are modeled in an observation similar to the human by assessing the human-centric threat detection algorithm. [10]

Sarthak Gupta, Aditya Mathur, Subodh Bhandari, Tarun Joshi, and Ajith Abraham Abstract Autonomous vehicles (AVs) provide many opportunities for users to relax and engage in other activities while the AV is in control. In the meantime, the user needs to handle corner cases within a designated time limit and submit adequate response data to the vehicle; otherwise their safety cannot be guaranteed. This paper presents the design of a usercentric threat detection system in AVs, handling the unique requirements of handling corner cases in the presence of limited user attention span. We model the AV and its components based on simulations and real world data, perform experiments, and present data-driven insights to design the detection system model. This detection system can operate in real-time and estimate the probability of the user being present in dangerous situations. Our analysis of real-world data based on our methodology shows that human-centric detection systems can improve the security of AVs from various threat vectors.

7.1. Ethical Considerations

Decision-making in human-intervened incident response is a discipline in cybersecurity established under a term classic intrusion response (IR). Thus far, intrusion alerts are raised for the researchers to discover and analyze; after designing mitigations or defense marks in the system, the operations of blacklisting an IP address, updating an email filter rule, and replacing a firewall rule might be commenced [3]. This incident response algorithm-quantity mindset still influences a wide and profound area in the field. As long as the solutions better serve for technical convenience or "worse is still better" mentality, it can miss underprivileged stakeholders including entire network neighborhoods. On the contrary, even proactive information security approaches recommend a negative security model or an adequate defense-in-depth layers mechanism as a final strategical measure at a certain point. Hence, given to the work that proposed the modern positive purposeful security approach, aiming to enhance security incident response operations inside organizations at a human level indeed is in its very beginning. In particular, ethical assessments and dedicated solutions are still categorized under conventional incident response operations on cybersecurity in the literature [15]. In this paper, a not yet recognized human-machine centered incident response modeling approach is proposed where IR issues decisions considering multi-dimensional, multi-objective ethical grounds at runtime within the reinvented IR procedure, Re-Act, for intelligent vehicles. These ethical assessments focus on the dynamic operations and stakeholder asymmetries.

Lethal cyberattacks on robotic and autonomous systems, such as autonomous vehicles, are a topic that has thus far received insufficient attention. While the tragedy of a loss of life likely will await us for the first time in the future, a careful evaluation of the consequences of a potential cyberattack can help us to develop strategies and procedures that are more robust against such scenarios [24]. In particular, decision-support mechanisms to advise human interveners on system interventions following safety-critical cyberattacks should consider these incident-centric ethical grounding aspects at runtime. To date, general operational aspects on threat containment are infamous in the fields of security research to be oftentimes dysfunctional or counter-productive across scenarios. If designers aim to establish long-term ethical, societal and trustworthy culture jointly with the process of incident response, incident response approaches might have to eventually follow the proposed design guidelines and integrate the necessitated ethical decision support operations, human-machine-interaction mechanisms, human-errors, liability accumulations, and operational safety stratifications.

7.2. Technological Advancements

To address cyber threats firmly, a proactive/responsive strategy is essential, which would employ either cybersecurity detection and mitigation systems or human-initiated automated response mechanisms. A Secure Hardware Extension, that incorporates a protected microchip implementation, comes pre-installed with all-authorized content including the user management database, user updatable digital signatures and the whole responsibility of the vehicle if the vehicle software is compromised [18]. The system interacts with the vehicle's ICT system on start-up and assists in the secure automotive supply chain by embedding the signature on the secure chip. This not only assures that all updates to the software are authentic, but also ensures that the system has complete capability to make critical decisions when its onboard cyber security system detects an attack In the event it detects a security related anomaly or cyber-physical attack scenario, the SHA informs the vehicle operator and institutes an Enhanced Driver Assist Mode (EDAM) that offers an option to the driver to switch to a safe pre-defined control state, ensuring adequate reaction time and minimizing consequences of the attack.

As smart vehicles undergo significant advancements and incorporate cutting-edge software and hardware, the threat of cybersecurity incidents has exponentially increased. Contemporary response mechanisms are unable to adequately address the situation because they require substantial human interference, demand expensive data processing, and are highly dependent on network reliability and availability [3]. This situation calls for an autonomous cybersecurity incident response mechanism that would minimize manual intervention, process and generate intelligent alerts to take action, and ensure reliability.

Recent advancements suggest that information and communication infrastructure and onboard vehicle technologies have significantly matured from vehicular ad-hoc networks (VANETs) to intelligent transportation systems (ITS) [7]. Modern A-ITS provides improved road safety, traffic flow management, and advanced in-vehicle infotainment services through a combination of communication, computing, and control systems. It is anticipated that in areas where information exchange is required with the infrastructure or other vehicles, the penetration rates of A-ITS will be quite high. This emphasizes the importance of effectively engineering intelligent security measures in an initiative to reduce adversarial activities and address unprecedented challenges.

8. Conclusion and Recommendations

A major disadvantage of the methods described is their purely electronic character and hence the potential vulnerability in case of a permanent connection to the driving vehicle. The long-term goal of this research is the development of interdisciplinary prevention, intervention, and care concepts to increase the opportunities offered by self-driving cars for all road users. Furthermore, a driver-oriented green or self-driving model will potentially allow a broad athletic or passive audience to benefit from the personal mobility options and improve the situation of drivers restricted in their mobility. These initiatives clearly demonstrate that there is a promising movement towards understanding and empowering the user to become a vital and empowered link in the chain of safe and secure transport. It should be stressed that the integration of customers and technology developers, on this occasion, proved to be sensational with a significant increase in the sensitivity of the individual projects [8] [16].

The past decades have seen the rapid development of complex technologies, which allow for autonomous driving. However, with increasing autonomy, vehicles become potential targets for cyberattacks. To face these roaming threats, in the paper we have pointed out that, although the majority of the previous work addresses the implementation of countermeasures against cyberattacks by autonomous vehicles on the hardware and software level, a third and final pillar of cybersecurity is still highly neglected: the human factor. Our model serves as the bridge between the theoretical concept of the cyber and physical worlds. It provides an interface between stakeholders in assisted driving environments and cooperation between drivers, victims, and attackers as well. For this purpose, we propose a sometimes-usable driver heuristic, a simulation-based Bayesian cognitive model that derives accident sequences from initial measurements of at least partially observable states. Therefore, it is necessary to combine simulation and validation on a real-car platform, which is the only way to identify failure modes that cannot be taken into account in a perfect simulation environment.

8.1. Summary of Findings

[2] This study has presented the development and experimental evaluation of a mobility cybersecurity incident response system (i.e., the Trigger-based Incident Response System TIRS) for autonomous vehicles. TIRS can ensure the rapid adaptivity and self-protection of vehicles by (a) detecting attacks; (b) triggering the corresponding safety procedures (i.e., adapting the vehicle's behavior to best cope with the ongoing attack); and (c) validating the outcome. TIRS permits a fast response to increasingly sophisticated attacks up to zero-day ones, through avoiding human intervention and by always defining the most suitable reaction for preserving vehicle mission safety and availability features.[12] Through the case study on an electric car sharing context, it has been shown that all the procedures developed cooperate to implement effective safety countermeasures in autonomous vehicles. The experiment results are encouraging, detecting all the attacks proposed in the ASIL D category, and almost all the attacks proposed for the most dangerous ASIL C category. This last result has motivated further steps that are currently being undertaken: (i) extending the experimental testing on the inspection scenario and considering more dynamic attacks, and (ii) implementing a final, field-centric design of the incident response procedure, considering costs and benefits for car sharing companies.

8.2. Practical Recommendations for Implementation

The first design recommendation is for the CIRT to have a mixture of both formalized pre-determined and AI-augmented collective problem-solving processes. Second, the quality of the cybersecurity response should be regularized and enhanced by monitoring and supervising CIRT using well-designed key performance indicators. Third, the incident response procedure should be designed to be flexible and adaptable during an operation as it will need to change once it has gone operational. The fourth recommendation is around the importance of CIRT internationalization. As well as internationally staffed CIRT teams, where language barriers will need to be addressed, the AV CIRT will likely need to respond to cybersecurity related requests from numerous different jurisdictions (for example accident investigators needing to understand if an AI model has been attacked and if the attack was the primary cause of the accident). The last recommendation is for close alignment with vehicle safety engineering.

[14] Designing a secure, human-centered, and practical cybersecurity response procedure for future Autonomous Vehicles (AVs) is a challenging task. In this section, there is a summary of an example safety-critical cybersecurity incident response procedure for an AV. This designed procedure is based on previous empirical research and the application of thorough threat analysis on AV. Investigation BKMs are then created to assist the cyber incident response team (CIRT) in identifying and collecting evidence from an attack. The subsequent remediation and live vehicle return to service plans are planned to minimize human error and vehicle downtime. Finally, all the key recommendations made for designing AV cybersecurity incident response procedures are reviewed and updated in the light of the the initial operational usage insights of AV CIRT.[16] This proposed response procedure provides guidance on how CIRT should act in the event of a cybersecurity incident and goes to great lengths to ensure human error is mitigated and the best potential cyber incident outcomes are realized. We argue that this needs to be unique to each AV service provider if it is to be successful and it needs to be evolved frequently in response to continuous operational usage insights. There are five key design recommendations we have recommended during the evaluation phase of the incident response procedure, which matches the shared experience and advice of the diverse AI experts, professional data analysts, and autonomous vehicle engineers we interviewed.

Reference:

1. Tatineni, Sumanth, and Anirudh Mustyala. "Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 88-121.
2. Biswas, A., and W. Talukdar. “Robustness of Structured Data Extraction from In-Plane Rotated Documents Using Multi-Modal Large Language Models (LLM)”. *Journal of Artificial Intelligence Research*, vol. 4, no. 1, Mar. 2024, pp. 176-95, https://thesciencebrigade.com/JAIR/article/view/219.

3. Bojja, Giridhar Reddy, and Jun Liu. "Impact of it investment on hospital performance: a longitudinal data analysis." (2020).
4. Vemoori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.
5. Tillu, Ravish, Muthukrishnan Muthusubramanian, and Vathsala Periyasamy. "Transforming regulatory reporting with AI/ML: strategies for compliance and efficiency." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 145-157.
6. Bayani, Samir Vinayak, Ravish Tillu, and Jawaharbabu Jeyaraman. "Streamlining Compliance: Orchestrating Automated Checks for Cloud-based AI/ML Workflows." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 413-435.
7. Tomar, Manish, and Vathsala Periyasamy. "Leveraging advanced analytics for reference data analysis in finance." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.1 (2023): 128-136.
8. Abouelyazid, Mahmoud. "Comparative Evaluation of SORT, DeepSORT, and ByteTrack for Multiple Object Tracking in Highway Videos." International Journal of Sustainable Infrastructure for Cities and Societies 8.11 (2023): 42-52.
9. Prabhod, Kummaragunta Joel. "Leveraging Generative AI and Foundation Models for Personalized Healthcare: Predictive Analytics and Custom Treatment Plans Using Deep Learning Algorithms." Journal of AI in Healthcare and Medicine 4.1 (2024): 1-23.
10. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
11. Shahane, Vishal. "Security Considerations and Risk Mitigation Strategies in Multi-Tenant Serverless Computing Environments." *Internet of Things and Edge Computing Journal* 1.2 (2021): 11-28.
12. Althati, Chandrashekar, Manish Tomar, and Jesu Narkarunai Arasu Malaiyappan. "Scalable Machine Learning Solutions for Heterogeneous Data in Distributed Data Platform." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 4.1 (2024): 299-309.