Human-Machine Collaboration for Incident Response in Cybersecurity Operations for Autonomous Vehicles

By Dr. Aicha Belaïd

Associate Professor of Computer Science, École Normale Supérieure de Kouba (ENSK), Algeria

1. Introduction

n addition, in a shared control setting, both (a) mode changes and (b) period changes require the driver to give a reaction swiftly, while still being insensitive to the current instance, and to be timely in closing the loop. In shared control settings, state of affairs can be different than in shared control settings. This means that effort allocation can fall below desired level when the system has autonomous and interlaced tasks which supplement to obedience in autonomously eradicating the duties assigned by a human, and whose inspection speeds subsides only when the gauge developed to sense the goals and then finding inspiration from it tells that changes can be timed from the driver. for accommodating this recent layer tasks for only the human is affected unlike traditional shared control where cooperation can be damaged. However, planning the amount of individualized autoes successive driving is formidable task for humans and can lead to inefficiency [1].

[2] Existing autonomous and semiautonomous vehicle technology has enabled corporations, particularly in the transportation industry, to push the frontier of innovation—encompassing future autonomous vehicle release, energy savings, and the possibility of preventing collisions by monitoring all sorts of traffic situations. A key unsolved problem is that drivers' input is appropriate when it is required, given the outcomes of current research that look at incidents from a driver's response perspective. This exceptionally difficult problem has gained the most attention of organizations involved in several domains of research to now—safety and insurance industries (manufacturing, public transportation, and healthcare services individuals), user claims in consumer reviews, and—from a theoretical viewpoint—safety researchers [3].

1.1. Background and Motivation

They were also able to tamper with real-time sensor data, make vehicles drive more erratically and even erase logs of any evidence of an attack. Experts say that the vulnerabilities could endanger future autonomous vehicles that the military wants to operate on battlefields as fully autonomous killer robots or supply line robots [4]. Allowing potential attackers to trivially disrupt supply would undermine the U.S. military's war plans and potentially also the high-cost vehicles the hackers seek to attack, armed with weapons and relying on sensors to perceive the world around them. To help understand the challenges both conceptually and practically in combining AI and human operators, we will first discuss how human supervision has been conceptualized in the broader context of autonomy – emphasizing the role of human trust and skepti-cism, operator reliance on automation and its drawbacks, and the importance of incorporating adaptive automation into future systems [3]. Furthermore, we will describe how recent AI research focuses on human AI col-laboration in the context of autonomous cars and what the collaboration entails, including how autonomous cars' AI, and humandrivers can cooperate with each other in the real world.

Flaws uncovered in the cybersecurity of the U.S. military's latest autonomous tanks and robotic supply trucks pose a significant threat to America's efforts to modernize its armed forces [5]. Researchers at the Pentagon's Defense Digital Service (DDS) mounted a series of attacks on the U.S. Marine Corps' new Warfighting Lab autonomous vehicles – and repeatedly found chinks in their armor. Using no more than a small amount of readily-available equipment, they were frequently able to hack into a Marine's self-driving vehicles and make them "unresponsive" or veer off of their lanes.

1.2. Research Objectives

Nevertheless, the mutual influence between the human's intention, the autonomous driving model, and the road environment make the study of the human–vehicle– road system a relatively complicated cognitive process that presents a series of requirements due to its various constraints such as the engineering constraints, the relevant driving environment, the human-vehicle interaction, the different behavioral patterns, the feedback of intelligent vehicles to human behaviors, and the evolvement of the human-vehicle system [3]. The accident coefficient confirmed by the ocial data, although the injury and death of the non-autonomous vehicle occupants caused by the accidents in autonomous driving are reduced

by 85%, but the autonomous vehicle human injury and death accident coefficient almost unchanged than the non-autonomous vehicle accident.

As we have discussed earlier, human behaviour is an important factor in deciding the health status of the system [6]. In the case of human supervised autonomous systems, when the human is involved in the loop of the system working he intentionally or unintentionally can change the output of the system. In that case the behavior of humans can be characterized as a stochastic feedback policy based on new perception to change the autonoumous system's trajectory. There are many factors that can affect human's behavior while driving autonomous vehicles accidents are some of them. Expectation violation, such as unexpected system underflows or overflows specifically in critical states are one factor that can affect human behavior while driving [7]. According to the traffic code human are needed to control vehicle based on the traffic code at the time of car autonomous system's malfunctions but unfortunately human can not adjust the vehicle according to the situations due to system malfunctions and these malfunctions can lead to accident.

1.3. Scope and Limitations

This motivates the development of novel tools for creating a resilient, human-aware, and intelligent Incident Response system for advanced Autonomous driving systems. The goal is to provide teams of professional security operators, incident responders, and autonomous driving experts with comprehensive, multi-modal insights and situational awareness, in real-time, during critical incidents.

This motivates the development of novel tools for creating a resilient, human-aware, and intelligent Incident Response system for advanced Autonomous driving systems. The goal is to provide teams of professional security operators, incident responders, and autonomous driving experts with comprehensive, multi-modal insights and situational awareness, in real-time, during critical incidents. This motivates the development of novel tools for creating a resilient, human-aware, and intelligent Incident Response system for advanced Autonomous driving systems [5]. The goal is to provide teams of professional security operators, incident responders, and autonomous driving experts with comprehensive, multi-modal insights and situational awareness, in real-time, during critical incidents.

According to the World Economic Forum, the biggest challenge to human-robot collaboration is to involve humans in system development in a way to anchor the relevance and applicability of autonomous system technologies in the human society [6]. From the mentioned perspective, a recent research proposal in the area of cybersecurity focusing on human-robot teaming in the domain of intelligent transportation systems is captivating and cognitively challenging [7]. The global motion towards the development of autonomous driving systems is offering several advantages; however, a significant cybersecurity threat should not be ignored. Autonomous systems are highly complex, dynamic, uncertain in their behavior and require computational real-time decision making. Besides, it is expected that autonomous systems will be a preferred target of terrorist attacks and those with malicious intent.

2. Literature Review

Recent Advances in Artificial Intelligence and Tactical Autonomy" [5] constitute a growing interest in the application of A.I.-enabled software development for automation of critical tasks in complex systems. Therefore, in this review, advanced A.I./machine learning algorithms have been discussed to accomplish variety of robotic and autonomous tasks under different applications. The development of robotic autonomous systems is being accompanied by major technological breakthroughs, particularly in the domain of A.I. for tactical autonomy that has advanced dimensions of decision-making, critical reasoning, and autonomous mission and path planning. Safety and security in real-time software processes for autonomous auto-driving systems have been discussed via the potential physical impact on passengers. Autonomous vehicles provide extremely complex and safety-critical scenarios for their safe operation, as autonomous controls could provide several vital entry points for cyber-attacks. Thus, imposing software safety and security subjected to ethical and technical constraints for timely incident response poses a crucial problem for automotive variants of A.I.-enabled machines. Because of the cases related to software malfunction, it is crucial to have an incident and response system in place for automotive systems such as automated ambulances. In this paper, a system has been proposed, HCI^3 (Human-Computer Interaction and Incidents Incident detection) for responding to such incidents both at emergency and non-emergency levels. In our methodology, we are attempting to predict potential incidents utilizing sensors within the transition from vehicle automation to (partial participant's) responsibility in order to address a security and perform-ability challenge. Reducing the

response time of a human agent is principal in ensuring passenger safety. The system consists of a Computer system analyzing the Human computer interaction so as to identify any discrepancies in the transition period and then it will be relayed to the human level in the participant or the staff. HCI^3 enables many scenarios that are associated only with automotive industry. For instance, a driver who get his attention away from the road, an intruder on the vehicular radar, the process of fast moving from the vehicle a car starter can be actions that can be considered. Autonomous vehicle control systems where human-machine collaboration is key are becoming the backbone of a modern technological era with extremely complex use-cases, especially in an automotive context consisting of A.I., machine learning, and autonomous driving systems. In catastrophic scenarios like vehicular cyberattacks, A.I. sexes can be directly utilized for kidnapping(sp)/hijacking an automobile or car which puts lives at potential risk. If it can no longer rely on the respond from A.I. algorithms then the response time for human agents becomes the crucial factor for protecting passengers, pedestrians, and animals from severe physical threats that originate from compromised A.I. implementations or system robotic software assurance methodologies. " [4]

2.1. Cybersecurity in Autonomous Vehicles

In the context of security, [8] vulnerabilities in the underlying infrastructure can affect the functioning of any AV's component or system. For example, in 2015, hackers hijacked a Jeep Cherokee remotely. Even coins sized reflective material can trigger an AV's sensors to suffer from 'confusion' – from the attacks via radio frequency (RF). Deployment of deep neural networks (DNNs) have been demonstrated to be easily misled through the insertion of unnoticeable perturbation in input data. Even the near-accurate, and genuine, AVs can potentially be forced to perform actions causing catastrophic consequences.utura. Hackers took over a commercial drone from a distance of two kilometers.riage can be exploited to cause fault in AV's operations, which essentially causes real-world jeopardy in equipped AVs. These attacks that potentially cause AV's unavoidable crash without any driver control, intentional wrongdoing is considered to be serious cyber-physical safety issues in AV scenario.

[9] An autonomous vehicle is an artificial intelligence (AI) in physical form, handling all elements of vehicle operation that are typically performed by a human driver. Instead of a person behind the wheel, AVs rely on machine learning algorithms for decision making. AVs

can function in one of six levels of automation: Level Zero is the standard car driven by the human; and Level 5 is where AVs are achievable everywhere, at any time, with zero human intervention. The development, testing, and deployment of these systems are ongoing, therefore, it is important to account for the cybersecurity and safety aspects.

2.2. Human-Machine Collaboration in Incident Response

As noted by article [10], when the ISO27002 framework is used together with IEC62443, the regulations in the 21434 standard can be followed and necessary specific RM (risk management) processes are integrated. Since the proposed architecture also includes real-time intrusion detection technologies, the system classifies the incident as soon as it is detected and initiates an incident response in a short period of time. Level 3 has not been established yet, which describes intruders who want to capture the system, thereby subverting its normal capabilities. In the created profile for vehicle firewalls, the access is given only to the communication channels that are needed for the operation of the IV control units.

It is known that one of the most common and oldest techniques to inspect, analyze and develop resilience to new vulnerabilities and potential exploits on various platforms is vulnerability analysis [11]. To expose potential malfunctions in IV (intelligent autonomous vehicles) due to the attacks and provide secure and trustworthy transportation services, an analysis should be conducted focusing on systematic control implications in the physical domain. Given that potential cybersecurity incidents can cripple the actuators and other critical vehicle operation facilities that require physical dynamic control, this article proposes a new physical classification of the potential IV (intelligent vehicle) cyber incidents

3. Theoretical Framework

In safety-critical domains, vehicle-to-X communication (V2X), as well as vehicle-to-cloud communication will be able to pre-warn infrastructure components or other traffic participants, even before the expected incident causes a breakdown. Our framework is developed for L4 autonomous vehicles, in which an operator is requested to take control in case of occurring threats. In the event of a threat, the L4 vehicle reacts by minimizing danger, while the operator takes on responsibility incrementally, by expanding the threat model and formulating an appropriate rescue strategy. To allow such a division of work, an efficient workflow between human, vehicle and infrastructure components are addressed in this

paper. Initially, vehicle-to-infrastructure communication helps in recognizing the highest affected danger zones, reduces the safety distance, and introduces a deployable rescue strategy later. In a dynamically changing traffic environment, it is noted that immediate intervention of the operator is essential in case of direct lethal threat initialization_seconds_needed. Dangers which the vehicle cannot address (emergent safety critical threats) will also be communicated to the infrastructure so that appropriate emergency teams can be assembled.

[12] [13]Autonomous vehicles are part of a larger area where cyber-physical and human-machine systems work together. To ensure reliability and resilience in such environments, it is critical for the involved human and machine entities to collaborate productively. In the scenarios considered in this paper, this collaboration occurs in emergency situations according to pre-defined interventional levels. To ensure safe and efficient collaboration, we have to ensure that humans understand the current threat; whether the autonomous vehicle's response was a topic of an attack; or what triggers are sensitive to attacks. Therefore, we will introduce a theoretical framework for the safety evaluation of human-machine collaboration in such environments. This framework provides various levels of responsibility for the humans in an L4 autonomous vehicle, i.e. in a vehicle ready state for Level 4 self-driving features up to the protection of time-critical infrastructures (e.g. presentation of hazardous materials). Such human-machine collaboration levels not only allow for a precisely defined division of responsible areas, but also provide an understanding of the different situations the human controller can adapt to, in terms of time and complexity required for the behavior mediated by the human user.

3.1. IoT Security Principles

Security issues can originate (i) from each node in an IoT-connected system, such as low-cost sensors that have been designed without abuse and security threats in mind, (ii) from communication and network-related attacks that are carried out on the user equipment, IoT interfaces or middle nodes in the route, and (iii) through IoT-cloud interface level attacks that are coordinated to create False Data Injection (FDI) in fake user activities. Then, with the data accumulated in the cloud, critical failures can be simulated, data quality assurance errors can be generated about readings taken from sensors with reasonable garbage results, simulation of incorrect data on active flows can be created in accordance with the scenario, and finally, a

direct attack can be carried out on the targeted institution using legal automation results based on this wrong data. The identified challenges and corresponding solutions are categorized under the principles of IoT security as End-Point Devices, Communication Security, and Cloud Security. Therefore, to manage and solve the difficulties and possible threats in each IoT security-related sub-group effectively, employing an overarching IoT cybersecurity framework for connected, automated, and IoT-connected vehicles is in a high quest. Hence, the proposed comprehensive solution bundles the golden contributions from the IoT security principles, incident response actions on the network and cloud security layers having a high focus on unified vulnerability-disclosure of IoT policy updating with an automatic approach.

[14] [9]Connected cars and automated driving heavily rely on Internet of Things (IoT) technology, which brings the threats and vulnerabilities which can be exploited in potential car hacking scenarios [15]. Consequently, ensuring the security of cars and their ancillary devices and ensuring the privacy of the occupants, cause new challenges in the automotive domain. To overcome these limitations, different solutions were proposed to enhance the automotive security, e.g. (i) the use of secure software development practices in new cars, (ii) employing encryption methods for securing car communications, (iii) designing secure network security protocols for connected vehicle environments, (iv) integrating artificial intelligence (AI) and machine learning (ML) methods inside cars and (v) employing blockchain technology to secure car and IoT communications. Research focusing on car hacking is ongoing and promising for securing the connected and automated vehicles in the future. Vehicle networks that are used for facilitating E/E architecture components (e.g. the diagnostic, infotainment and telematic units of the in-vehicular resources, the personal smart gadgets, and the external systems/cloud servers) are the most critical points where mainly cybersecurity issues in vehicles emerge.

3.2. Firmware Update Mechanisms

The main problem of automatic updates is that it assumes highly trusted servers. In a TLS session with mutual authentication, a firmware update is downloaded from a server certified by a Certificate Authority (CA) entity [16]. It would be enough for a hacker to get access to the certificate of a vulnerable certification body to be able to impersonate a certified server and deliver an altered version of the firmware in question to the vehicle. Even an attacker who

breaks into a server at the update software manufacturer's site would be able to produce new emergency certificates.

The firmware update process used to include updates obtained from embedded systems or vehicle manufacturers in the case of official updates. This model is no longer compatible with modern vehicles, in which firmware is automatically downloaded by software delivery platforms [17]. Unfortunately, having an over-the-air (OTA) update capability can become an open door to attackers [18] (ISO/SAE 21434:2019, 4.4.7.2 g). The management of the FIRUM's firmware update mechanism (ISO 21434-10:2021) regulates the life cycle of domain applications - new or new versions of ECUs for the execution of the applications. The update mechanism has become responsible for verifying the integrity of the firmware to be installed using cryptographic mechanisms, not to mention the authentication of the exchange to prevent its manipulation by a third party, and correctly performing the download and installation of the firmware. These processes must take into account the potential risks such as a vehicle supply chain hijacking, a MaaS (Mobility as a Service) sexual harassment attacks or a fault injection attack up to the checksum for a Data integrity fault. A suitable set of technical and organizational measures is therefore essential because automotive Electronic Control Units (ECUs) are a perfect target for attackers.

4. Methodology

The premise to assist drivers with cybersecurity incident response in autonomous driving systems are twofold [1]: (1) The cyber–physical interaction put from now on into place by the AIs embedded in such vehicles should not be carried out in back boxes. Rather, such complex AI decisions should be brought to the attention of the human, because of the reciprocal influence from driving to cybersecurity incident response and vice versa (it might be necessary the human involvement to solve what has been entered into deadlock, depending upon the result of the breakdown assessment, which again might dependfrom the trust buildup during ordinary driving operations); and (2) a good collaboration dynamics should be informatively managed (introduced and then updated in time) so as to improve its human–AI interface, thus augmenting human cockpit performances, also taking into account a situationally aware driving path selection, a behavior that it is strongly affected by the cybersecurity cognitive loads.

Researchers have proposed developing human-AI joint cognitive systems, instructing autonomous vehicles by taking seriously into account reciprocal dynamics that are involved in collaboration [7]. The EYE-on-HCI framework was proposed, for monitoring human–machine interactions in driver-monitoring systems aimed to note the cases of misuse of HMI functions and elements by the drivers [19]. Both works point out the role of the cognitive state of the human in codesigning human–AI interfaces. This section presents an alternative system for entrusting drivers to assist with cybersecurity incident response, showing how some critical findings in Human Factors can be exploited for a double purpose: improving the decisional outcomes thanks the drivers' knowledge and control over driving, as well as taking the utmost care to preserve a driver's expending cognitive resources.

4.1. Research Design

[20] There are autonomous vehicles (AVs) on our roads in increasing numbers. Within the next five years, 11% of European new cars are supposed to be AVs. AVs come with large potential benefits for drivers and other traffic participants concerning comfort, road safety and traffic efficiency. However, they also come with new challenges. Cars experience around 40 so-called disengagements per 1,000 miles even as tested by Google now-Waymo, and 20% of these disengagements had the impact of needing on-the-fly human intervention to avoid a crash; e.g. via taking manual control over steering wheel or braking. The time needed to hand over (or hand back) driving to a human driver in such a situation has been buzzworthy among researchers and policymakers and Frings discusses in unison what kind of promises need to be made about autonomous drive functionalities and how this also gives rise to new human factor challenges and thereby introduces these into driving and traffic: Can trust be established if cars—like Lucy—already stop on a 95% red onset light? How does this change driver sitting and working behavior? What risk potential is associated with these issues, not least in view of unexpected technical issues in these cars?[4] Whenever automation is replacing human manual work, important challenges emerge, including the monitoring of system failures, critical situations, regular work safety and efficient human-automation collaboration. Especially in hybrid systems that are supposed to be operated by both human workers and robots, this can be necessary to avoid human errors and also to improve cooperation of humans with the software/hardware structure and algorithms. The main goal of this contribution at hand is the introduction of a reliable, effective and safe approach to automatically detect relevant incidents, which cannot be handled by autonomous driving

functionalities, and to hand over this work to a human backup agent as quick as possible. The final system will include real-time methods for threat detection and will be implemented together with driver and remote control station concepts for human situation awareness in presented research settings. This problem has to be solved in real-time. These contexts will elaborate underutilised pillars from the execution design and human-factor design of intelligent transportation systems by making is used to using real-time threat detection during human–machine interaction in driver behavior or in conflict with the traffic environment as starting points.

4.2. Data Collection and Analysis

The main objective of this research was to monitor the willingness of the general public (N = 169) to use cybernetic grid systems for networking. The emergency response system's willingness was assessed as 78.1% for e-health systems and 74.6% for security and relief management systems. In these two security management sectors, 4.1% of the participants were afraid of technology failures, 3.5% were fearful of cyber-attacks, and 1.7% were fearful of the wrong method of use. The attributing factors explaining cybersecurity willingness to use emerged as data awareness ($r = 0.289$, $p < 0.0001$), intelligent e-health management ($r = 0.261$, $p < 0.001$), and data privacy ($r = -0.169$, $p < 0.047$) [21].'autres ressources : christophe-damm_metafor_043_analyse_structurale_des_tensions_entre_les_professionnels_de_la_solidarite_et_les_riverains_cas_des_services_publics.pdf AMMC_44-352_les_assoces__e__s_mal_place__e__s_au_service_d_un_consortium_de_formation_apprenante.pdf =- LES DÉFIS DE LA VOIX QUESTIONNAIRE SUR LES PRATIQUES VOCALES DES ÉLITES LES MEDIATIONS PSYCHOSOCIALES DE LA VOIE DE VOIX, DU SERMON ET DE LA PERFORMANCE VOCALOLOGIE PSYCHOLINGUISTIQUE HAL-01263877.pdf

The research utilised the data collected from 169 participants, with a mean cybersecurity experience (62, 36.7%) of 3–6 years followed by 1–3 years (57, 33.7%), 6–12 months (28, 16.6%), more than 6 years (12, 7.1%), and not at all (10, 5.9%). The questionnaire was developed and distributed using Google Forms to assess the willingness of participants to communicate with emergency management systems [20]. The participants were divided into various age groups, with the majority (61, 36.1%) of participants from the age group of >30 years, followed by 24–30 years (59, 34.9%), 18–24 years (52, 30.8%), and preference to disclose the age (9.2%).

5. Secure Firmware Update Mechanisms for IoT-Enabled Components

Given this context, the attack can target server downtimes and printers infected by network worms, and car manufacturer or part supply-chain virus infection, or Dynamic Host Configuration Protocol (DHCP) updates via DNS and Internal Protocol (IP) address distributions. The in-vehicle wired or wireless potential external input interface can lead to increasing security risk, not only following the fact of already described attack vectors. The external software systems, which are accessed directly via ports, can comprise all part supply-chain products and part supply-chain support hardware lists and demonstration platforms, software development kits (SDK), and OEM-oriented/III- and IV-Generation Car-Around View Monitor (CAVM). Owing to an increasing number of main appended third-party vehicle devices, each will provide its own Internet of Everything (IoE)-observing threat level. The investors fear whether the OTA final system will be attacked.

Over-the-air (OTA) updates are significantly altering the automotive industry by enabling firmware updates for millions of cars without requiring vehicles to return to vehicle service locations. Therefore, OTA updates apply to Intelligent Connected Vehicles (ICVs), not only to support the economic update but also to support continuous smart concept updates in the autonomous vehicle ecosystem [17]. OTA updates promise to cloud-enable, even for a future fully autonomous vehicle, the end-of line (EOL) vehicle electronic control units (ECUs) and the over-the-air software updates to implement new IoT-features, including Vehicle-toeverything (V2X) communications. OTA updates may thus facilitate the modern automotive industry, thus, extending automotive business model functions. Meanwhile, they pose significant security vulnerabilities, as attackers could introduce malicious content during transmissions. A successful attack could disable the vehicle's important feature sets of advance driver assistance systems (ADAS) and even powertrain. In the event that a vehicle gets infected by malware, part of the attack can even make the customer personally victim. As regulation framework for automotive industry the European Union eCall regulation EU 2015/758 responsible for the implementation Phase2 requirements on IP-Protocol and complete Europe country wide coordination, in effect as of 31st March 2018, but ongoing still best practice updates, declares the public emergency call service (eCall) as a mandatory EU deployment [22].

5.1. Overview of IoT-Enabled Components in Autonomous Vehicles

It is realized that in [Jose et al., 2020] V2I communication is based on intelligence information as V2V communication is based on the route and traffic information and these communications are through different channels: DSRC/WAVE, 3G, 4G, 5G, etc. by developing authentication algorithms as Pairing-Based Signature (PBS) and Key Aggregate Cryptosystems (KAC) for lightweight V2I communication. In Section 5.2, we further provide a solution on how IoT-based components such as the smart energy–beam control–beamforming AI–driver-personal communication–mHealth and eHealth communication models, etc. may introduce secure autonomous vehicles.

[23] [24] A vehicle collaborates with different components including the vehicle and infrastructure internet of things (IoT) security and communication – (1) V2V and V2I security and (2) V2I communication in the main scenario although other correlated scenarios must also be considered. The V2V and V2I security and communication components enable the connection of a vehicle with other vehicles, traffic lights, and such traffic infrastructure, and these all are involved in visual, sensorial, and artificial intelligence-based V2I communication. Autonomous vehicles are equipped with various connected and controllable devices and their interactions with vehicles and infrastructure components must be managed securely. The challenges and threats in connecting vehicles to various components and solutions need special attention. The V2V and V2I security and communication in an autonomous vehicle are concerned with the secure interaction of the vehicle with all the components of the IoT devices such as signing the communication messages, visibility to the immediate sensors, controllable devices, vehicular/traffic conditions, etc.

5.2. Challenges in Firmware Updates for IoT-Enabled Components

Improved levels of vehicle automation for transport systems reinforce the uptake of internet of things (IoT) in transportation, with massively interacting and interconnected mobile and infrastructure components and a multi-modal user environment as its key characteristics. With the advent of 5G, connected and autonomous vehicles will interact with other vehicles and infrastructure components, taking advantage of its ultrareliable low-latency communication services to update information on vehicle and environmental state with low latency for balancing network load, avoiding accidents and providing intelligent and autonomous, self-optimizing traffic alerting and routing. Autonomous systems and transportation in general represent settings where the cybersecurity is not only relevant per

se, but also by means of an interacting system with all its components in need of secure operation. Autonomous vehicles are no exception from this [22]. In contrast to conventional vehicles, autonomous vehicles are in principle already capable of performing all necessary driving tasks without human intervention. Nevertheless, in complex traffic situations, a human operator will still be in the driving loop to guarantee correct and safe operation in case of uncertainty and/ or malfunction.

Software-controlled vehicles (SCVs) have been recognized as the wave of the future for the automobile industry. Such systems, also known as self-driving cars, are part of a broader vision of autonomous mobility with the potential to address many societal needs, including provision of transportation for the elderly, people with disabilities, and others who may not be able to drive, reduction of environmental impacts, reduction of gridlock through increased road capacities, reduced need for parking space, reduction in demand for owned vehicles, and more efficient utilization of transport capacity [25]. The correct operation of these autonomous systems will require effective solutions to ensure their safe and secure operation.

6. Proposed Mechanisms

Bidirectional communication is a need of the hour, and a prerequisite if the autonomous vehicle network had to reach the state of trustworthy autonomous operations. This study has delved into communication in both directions. Directionality determines the pattern of attacks one will have to prepare for, and it will also affect the priority of developing each component of the autonomous commands and responses [26]. Assessments done on drivers for various debatable categories are mapped into a vector space, which was processed by the system itself as part of its template matching system, while the machine learning system filtered out the noise. The use of synthetic variant datasets and state-unknown methods enhances the cybersecurity feeling on the machine side. The MONICA framework has been successful in making cyber-physical systems secure up to now. Despite a large number of optionally active countermeasures, the proposed changes to them are seen as the most relevant— consolidating them under a security framework will be a necessary step in the next phase.

To enable mankind with cybersecurity toolsets, one needs to understand the scenarios, both for autonomous and remote operations. Functions that currently require some level of human involvement for cybersecurity tasks, such as pattern recognition or understanding of situational awareness, risk assessment, and consequence modeling, are rather human biased,

with different levels of cognitive capabilities inherently required [19]. Still, creativity and adaptability, which are easily handled by humans (but not yet machines) adding up to local context bias (Online-only) are necessary ingredients to address. It's particularly important in cybersecurity aspects, where coping with yet unknown attacks, and fast lapses in security can bring in disastrous consequences. To create a resilient, automated responder, where the efficiency of a combinatorial human-introduced capability handles the mentioned scenarios, and issues are taken care of in this proposed model. The proposed solutions span from endpoint handling, monitoring, and anomaly detection in nodes, host, and network levels depictions, elaborating in section 4, in particular, for vehicles.

6.1. Mechanism 1: Secure Over-the-Air Updates

Options that do not require extra structure include privacy oriented and trajectory predictions, which are top of mind for most AV cybersecurity research, we adapt these two examples to highlight current HMI and challenge spaces in current trajectory predictions. Resiliency oriented HMI techniques are examined last, as these areas do not yet have enough cross-community data to provide simple examples.

Secure over-the-air updates (SOTAUs) are crucial to the operation and security of the new connected and autonomous vehicles (CAVs), yet malicious code can be injected directly into the SOTAUs themselves. In this sense, a deployed CAV system with a weak SOTAUs system can be thought of as allowing an ever-present intruder function to have high power at any time. A fundamental effort in this direction must effectively balance the trade-offs of maintaining the intrusion of future SOTAUs both in the computational capabilities and the attacker's uncertainty. Through a sequence of examples, we have demonstrated the practical importance in considering these various trade-offs. Future work focuses on streamlining these insights and applied to the problems of decentralized patching, platform strategies for how to promote SOTAUs 823, iterative intrusion functions, applications of this timeliness.classification tradeoff, and exploring the role of machine learning in making selection decisions with respect to intruders and the operational tactics they use to leverage. Here we break down our results to time-ordered enumerate current trends, known in the cross the science community as some important areas of opportunity for HMI. [12] Through this process we also identify specific areas where new metrics provide a unique opportunity for

deploying MLaHS. Related to both collaboration and adversarial machine learning and detection, continual learning maintains the rapidly changing information as it balls in.

"Secure Over-the-Air Updates (SOTAUs) are needed for connected and autonomous vehicles (CAVs) due to the increasing complexity of CAV software architecture and the presence of human drivers. These updates, however, create avenues of vulnerability for CAVs [27]. In this section, we design theoretical frameworks for SOTAUs to assist in these tradeoffs between security and recovery. In Section 6.1.1, we study the tradeoff between the risks of falling back to outdated code versus the uncertainty of new risky code. We show (Theorem 6.1.1) that the decision of whether to accept a new risky update may still be made with tradeoffs based on when the risk is learned, how much was expected of the attacker, and the penalty of falling back on outdated code. There is some chance where it is the best decision not to update partially deployment because the penalty for falling back on the old code is too severe. Finally, in Section 6.1.2, we begin to discuss the problem of patch rates [20]. Here, an attacker can learn about the SOTAUs of a system by inferring the schedule of patches, we give a framework for determining the best patching behavior for a CAV to protect itself for these revelations, under the same kinds of tradeoffs as before."

6.2. Mechanism 2: Blockchain-based Verification

In particular, we considered Attacks and associative countermeasures for the following ICT systems: - Network intrusion detection system (NIDS) for the case of SQL Injections attack which aims at discovering side-channels in the C-ITS. - Malware Detection in IoT Edge Nodes to counteract Dos Attacks. - Data privacy/forgery prevention in security-critical vehicular P2P and V2X communications counteracting Collision Attacks. To ensure that the Automotive challenge can be really solved and as well as to demonstrate a clear advantage of using the blockchain approach in these scenarios with respect to the traditional ones, we have embedded the above Mechanism into the logic of Operating the Autonomous Vehicle Machine-Learning Functions [28].

In addition, considering the Cybersecurity operations for case studies of two-instance incidents, related to two side-channel attacks, a typical DoS attack and a Collision attack, several information and Communication Technology (ICT) systems have been developed enabling Human-Machine collaboration for Autonomous Vehicles Incident Response. This approach relies on a novel blockchain-based verification mechanism in order to counteract

Security threats such as Data, DoS, and Collision attacks. Blockchain-based mechanism ensures for each ICT sub-system a tamper-proof the log of the security-related records appealing for Forensic Analysis after the "crisis" resolution.

In cybersecurity operations for autonomous vehicles, it is critical to take security very seriously. In this work we are particularly interested in tackling security issues such as side-channel attacks and Denial of Service (DoS) attacks affecting Machine Learning (ML) algorithms integrated into sensors for road infrastructure pervading Autonomous Vehicles scenarios. We propose a framework, named Autonomous Vehicle Incident Response (AVIR), which includes a novel hardware architecture for boosting security in the context of Incident Response via Human-Machine collaboration [29].

7. Evaluation and Validation

In essence, cybersecurity operations for the protection of CAV, especially a post-attack scenario, consist of several steps: auditing, response, predictive analysis to create a self-defense mechanism, proactive defense and mitigations, and a complete lifecycle view of security engineering [30]. In this context of incident response strategies for CAVs, human-machine collaboration is increasingly being viewed as a new strategy to contribute to the mitigation of some forms of cyber attacks on automated vehicles. Human-machine collaboration has the potential not only to speed up the processes of threat detection and reaction but also to be instrumental in situations where malware detection is not straightforward. When an attack reaches and affects the CAV, then it is detected. The front line software also has an autonomy to react to the attack or as a part of the DRM protocol, report it to humans for further action research. Notably, findings that are similar to ours point out how learning from historical and perceptual data strategies may offer the best potential to accelerate malware detection [31].

Cybersecurity is tested beyond its limits with increasing connectedness, digitization, and integration of autonomous systems. Advanced persistent threats can infiltrate the more interconnected, open, and monitored networks to launch advanced cyberattacks [32]. An autonomous vehicle integrates with multiple systems and contains crucial data and human life and is therefore an attractive target for adversaries. While connected and automated cars are expected to improve mobility and reduce accidents, security experts fear their dependence on centralized servers, and worry about hackers' abilities to remotely attack vehicles in several

ways. The vast number of autonomous vehicles at times is itself considered challenging for potential cyberattacks, specifically Distributed Denial-of-Service attacks. Incidentally, much research argues that the increasing interconnectedness of CAVs will lead to hyperconnectivity, where a plethora of devices and networks will not only facilitate integration and communication but will lead to vulnerabilities that can be exploited.

7.1. Simulation Setup and Parameters

Collisions happen frequently between vehicles, and collisions between vehicles irrespective of manufacturers or types will cause a series of hidden dangers. Thus, it is extremely necessary to do the research on the model of V2X transportation. This paper constructs three traffic models:firstly, a model based on cellular automata to characterize the performance of V2X transportation. Then, it builds a peripheral model of pedestrians and vehicles to evaluate the influence of V2X on crosswalk traffic. Finally, it constructs an influence index to evaluate the congestion state of V2X transportation in real life. The results show that V2X transportation is more likely to cause congestion under small disturbances than traditional transportation, and the proposed algorithm in the paper can effectively reduce the congestion caused by V2X transportation [33].

Recognizing that these are inconvenient orders, the authors consider the quantum Zeno dynamics observed in the coherently driven first-order phase transitions in extended quantum systems. Stated more precisely, the quantum version of the celebrated Zeno effect has already been discussed in many conceptual and experimental contexts, including the control or suppression of decoherence through frequent, perturbative measurements of the environment. However, the coherent dynamical analogues of such effect have been less considered and understood. For this purpose, the authors provide an analytical explanation to the suppressed relaxation rate related to a pair of specific topological and non-topological contiguous hierarchy of coherently-driven quantum transitions. It is observed that the topological phase causes a stretched-exponential relaxation hindering a diverging relaxation time. This is referred to the topological coherent quantum Zeno dynamics [10].

7.2. Results and Analysis

The results from this experiment showed how human-vigil and machine-automation can collaborate to perform incident response tasks in cybersecurity operations for autonomous

vehicles. The study incorporated performance, vigilance, workload, and team dynamics to holistically observe human–machine collaboration. They collected valuable insights about human–machine collaboration that could potentially integrate into an AI-driven incident response system. Hence, the perfect entry point for the study is in extending existing intrusion detection models in the domain of cybersecurity to provide cognitively-inspired automated cybersecurity incident detection mechanism for future autonomous vehicles [12].

An empirical evaluation of human–machine collaboration for incident response in cybersecurity operations for autonomous vehicles is presented. The effectiveness of collaboration based on the symbiosis model [5] of human-vigilance and machine-automation was investigated by conducting a user study. The participants were the suitable surrogates for a cybersecurity operations engineer (COE) which would be in an incident response scenario for a future autonomous vehicle.

8. Discussion

The present article now has as theoretical nucleus the human-machine collaboration in the interaction of a human being in front of computers : Post-hoc analysis is conducted to identify direct and indirect effects of human performance, as influenced by system (i.e., AI system and computer software system), on researchers' trust in the AI. REACT is designed to provide quick and efficient responses to system-relevant incident scenarios without always contacting a remote Cyber Security Operations Center (CSOC). TRUST also plays a vital role within this collaboration and decision-making network. AI's technological development has greatly impacted the way individuals work and live, especially for those working with AI [3].

To understand better how to build systems to be cognitive to the reality of autonomous vehicle management, it is important to stop and ask: what models of knowledge are these human sympathy with the reality already playing when compared to the classical mathematical models commonly adopted in the technical solutions of the current active cybersecurity of autonomous vehicles? This is not a rhetorical question. It is analyzed to what extent the models of human significance in operation represent a challenge for the traditional cybernetic models and information theory: the traditional mathematical models for the construction of the information theory and of autonomous vehicle cybersecurity.

8.1. Key Findings

Over the recent years, the intrusion of connected technologies in automotive industry has augmented the risk of cyber-physical attacks and presented an increasing challenge to the design, development, and management of autonomous vehicle technology. It is felt that a change in perspective is urgently required to address significant questions of technologies in roadway and vehicles. deploying AI-based systems and robotic models to create a secure, cyberattack-resilient or antifragile driver-in-the-loop on-road environment. The mainstream studies and technologies are inclusive of AI enhanced adaptive cyber resilience, blockchain for AI based HMI security, Cyber Security in Autonomous Vehicles (ISO-CS-AV), cryptography for connected vehicles, data authentication and access control, Encrypted Database Management Systems, machine learning threats and security, privacy, security, Protection of Critical Data, Security Consideration For Artificial Intelligence [19].

In the field of city traffic, artificial intelligence and data fusion algorithms are employed to detect, recognize, localize and react in real time thanks for connected and autonomous car. Uncertainty analysis is a fundamental concept when robots and autonomous vehicle are employed to perform human–computer interactions (HCI), especially in this security critical tasks. Hansen presented a Robust Real-Time Object Action Recognition (RobARTOAR) pipeline that uses LSTMs to recognize actions performed by objects or groups of objects. A unified probabilistic data association filter (UP-DAF) based fusion strategy for multimodal asynchronous sensors COTS data is proposed, with the aim of enabling better decisions. Collaboration in the city traffic may be strongly useful as distributed machine learning techniques for robotics can overcome some limitation of the centralized control design.

[Cyber-physical systems (CPS) aim to create a full-fledged collaboration between the physical world around us and digital computing and communication systems. The interaction between the physical world and automated machines in autonomous vehicles is an emerging field, which poses challenges in human–computer interaction and machine learning algorithms with respect to scenarios and techniques for cybersecurity detection and reaction. Specifically, it is crucial to understand cybersecurity tasks in the new domain of driver monitoring (DM) human–machine interaction in semi autonomous vehicle (SAV). It is necessary to offer manned or unmanned robots collaborating with human operators and emergency responders in credible and useful scenarios for everyday life, to help the controlled environment including cybersecurity scenarios. The use of robots can also be an effective solution when

extraordinary events, such as natural or anthropic disasters, give rise to the necessity to carry out activities that would be dangerous or impossible for humans to accomplish.

8.2. Implications for Cybersecurity Operations

To showcase the potential impact of HMC, especially in cybersecurity operations, I will use an interesting example outlined in a recently published article addressing the vulnerability of autonomous vehicles to ransomware attacks [12]. The authors described a scenario where AVs are attacked with ransomware. The attackers demand money from the vehicle owner/car manufacturer in exchange for relinquishing control of the vehicle. To illustrate the limitations of today's systems, the authors used checks based on driving policies (set in off-line mode, before the vehicle's trip) and periodic verifications during the mission. Note that, in realistic scenarios, it is possible that some elements of the knowledge use-cases requested by the vehicle's owner are disabled in the HMI to prevent (unwanted) actions from the driver. Furthermore, each time a safety intrusion is verified, at least three requirements should be met.findFirstMar2022. First, we are supposed to assess the countermeasures to recover the mission. Second, we must carefully verify that the countermeasures do not have unexpected side effects. Third, we are supposed to manage the conditions to maintain safety intrusion detection capability. Despite the richness of the formalism, two linked-closed loop cyber attacks, which the model unfortunately describes, yield hard-to-verify safety intrusion detection, recovery, and resumption [6]. In this perspective, a brief excursus regarding formal verification was useful.

Autonomous vehicles (AVs) are complex and are expected to leverage various communication technologies and sensors working in a wide range of conditions, both during normal and degraded operation ([7]). Consequently, cyber threats targeting such systems are of increasing concern for the automotive industry. Well-known cybersecurity weaknesses in AV technologies (e.g., V2X, DSRC, OBD) have been demonstrated by attackers able to deceive the system by tampering the control logic. The multisided attack space targeting intelligent transportation systems (ITS) is broad and includes network, internal/external environment, and vehicle attacks. As an inherent part of the ITS, AVs are just as vulnerable to cyber attacks and therefore must be equipped with adequate cybersecurity protection mechanisms.

9. Conclusion and Future Directions

Moreover, since the attack prediction performance is susceptible to variations between different actors and hubs, improving the robustness of the trained ML model by introducing human affects could significantly affect the model's performance in the real world. Short-term behaviour, naive and ignorant user models, long-term non-adaptive behaviour might support training the ML models to generate accurate predictions in real time. Integrating non-expert behavior as well as the attacker model with the proposed framework could generate more informative results to estimate security risk accurately.

Including both positive (fact or fiction) and negative scenarios in training could assist in generating a broader set of correct responses. This trained AI perception can be employed to predict attack interactions and actor's behavior in a human-in-the-loop model and reduce security risk. Testing and training the model with varying human impact severity in attacks would yield better prediction accuracy.

9.1. Summary of Findings

Nowadays, one of the main pillars in the development and validation of machine learning (ML) algorithms is their robustness under adversarial conditions. This design pattern has proven to also be an effective tool against adversarial attackers. While some authors propose to break down the adversarial resilience barrier for the addition of human information in the process, a new field emerge oriented to the domain of Human Machine Collaborations (HMC). Human Machine Collaborations (HMC) could enable reduce false positive and negative responses. However, the design of the resilience mechanisms in HMC complementing ML systems and ensuring an efficient Information distribution between human and machine will define the impact of remaining vulnerabilities as opposed to the vulnerabilities yielded by adversarial attack direct responses [34]."

"An autonomous vehicle (AV) is a modern transport method, which allows the vehicle to operate under environmental control and automated driving functions without human intervention. The need for more resilient automated driving technology raises the expectations to perform massive validation and testing not only at the quality assessment level. However, we have to verify and validate the robustness of the system in adversarial and stressful scenarios to prove a certain level of attack-through resilience. Evaluation methods based on the classification and assessment of different countermeasures increasingly emerge, and in some studies the human factor is set as the bottleneck of the future research [35].

9.2. Recommendations for Future Research

The following recommendations are helpful to guide researchers and engineers interested in diving deep into the human-AI collaborative incident response. Specifically, insights or experience reporting, such as after-action reviews, should be encouraged and extended to cybersecurity operations in autonomous vehicles. Human factors researchers in human-machine collaboration and human-machine interaction are especially poised to lead these cross-disciplinary developments. Notably, emerging recommendations are available about how knowledge, behavior, and social factors in HCC may counter adversarial attacks. However, only few attempts have been made to introduce human factors ideas within the area of security with autonomous vehicles. From an intersectional perspective, probing into the gaps between traditional machine learning and human components in security-related vehicle incidents, including adversarial attacks, will also be a promising research direction. Moreover, attention should be paid to largescale incident responses and systematic improvement using hybrid intelligence for security scenarios in autonomous space. Representatives could be cyber-physical attacks on an autonomous vehicle development or a fleet to evaluate the cyberphysical resilience in the face of a cyber-physical attack. [36]

Despite the promising perspective demonstrated in autonomous driving, the emerging safety challenges of such system featuring insufficient fall-back capabilities require improved approaches to ensure safety and security of autonomous vehicles. Adequate human-machine collaboration schemes are a main enabler for autonomous vehicles to modernize and strengthen traditional fail-over strategies and carry a stronger resilience to adversarial behavior. Therefore, it is imperative that human factors research evolves in parallel to AI enhancement. The interdisciplinary hybrid intelligence perspective includes human expertise and knowledge is often suggested for addressing these adversarial attacks in an era of big data. Nonetheless, this may impose new challenges to the human cognitive system (Huang et al., 2018). This study thus shed new light on leveraging human-machine collaboration in particular to mitigate cyber-physical adversarial risks in the context of autonomous vehicles. [7]

Reference:

1. Tatineni, Sumanth, and Anirudh Mustyala. "AI-Powered Automation in DevOps for Intelligent Release Management: Techniques for Reducing Deployment Failures and Improving Software Quality." Advances in Deep Learning Techniques 1.1 (2021): 74-110.
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, Jun Liu, and Loknath Sai Ambati. "Health Information systems capabilities and Hospital performance-An SEM analysis." *AMCIS*. 2021.
4. Jeyaraman, Jawaharbabu, and Muthukrishnan Muthusubramanian. "Data Engineering Evolution: Embracing Cloud Computing, Machine Learning, and AI Technologies." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2023): 85-89.
5. Shahane, Vishal. "Towards Real-Time Automated Failure Detection and Self-Healing Mechanisms in Cloud Environments: A Comparative Analysis of Existing Systems." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 136-158.
6. Devan, Munivel, Ravish Tillu, and Lavanya Shanmugam. "Personalized Financial Recommendations: Real-Time AI-ML Analytics in Wealth Management." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*2.3 (2023): 547-559.
7. Abouelyazid, Mahmoud. "Natural Language Processing for Automated Customer Support in E-Commerce: Advanced Techniques for Intent Recognition and Response Generation." *Journal of AI-Assisted Scientific Discovery* 2.1 (2022): 195-232.
8. Prabhod, Kummaragunta Joel. "Utilizing Foundation Models and Reinforcement Learning for Intelligent Robotics: Enhancing Autonomous Task Performance in Dynamic Environments." *Journal of Artificial Intelligence Research* 2.2 (2022): 1-20.
9. 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.
10. Althati, Chandrashekar, Manish Tomar, and Lavanya Shanmugam. "Enhancing Data Integration and Management: The Role of AI and Machine Learning in Modern Data

Platforms." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 2.1 (2024): 220-232.