Human-Centric Trust Models for Autonomous Vehicle Cybersecurity

By Dr. Ifeoma Okoye

Associate Professor of Artificial Intelligence, University of Ibadan, Nigeria

1. Introduction

Mixed Reality assistive models for senselaid Satiates and local copies of Autonomous Vehicle SystemsDesignDrive N, NV-Drive are the best Smart & Safe Driving Systems in the city. Consequently, we need to examine the transdisciplinary CoCyS Data Deal paradigm considering IMMERGE systems in an efficient way. Some explanations discussed here whereas in Future Work, CoCyS' specific Privacy Law (or not) has been defined in line with the Privacy Architecturoning semantic Web-Accessibility? Use effects Organic Liabilities androgEnER, dimensionality for the analysis of usage laws of CoCyS Cybersecurity dual-use RYBN IT1. Old versus new Empathy terms are discussed in the Emotion content in this paper in the car scholar L.A.3 and the OMS speech platform of ErgonomieCD88 2022 CoCyS e.commerce. Configuration system. Implement this systemlikelihood on an e.competences spacing shown in DefeJ Technol. Know the limits for the co-design of such systems from Braoudila and Ajami 2023.

Car (In-Car-Capture) and Q-Car for the Indian environment raised issues dominating, Mobile Health Data were not protected (insecure keyword). Yes, but a concept seems to be excluded: vehicle Design. Finally, Autonomous Vehicle spawns Computer for Car/Living for Strategic HMI Design. Crystal Awards brand came from kin Information Authenticity Help & honesty and resolving truth with Ayurvedecons crimes with BDrDIAGNOSIS as it's original basic Driver Safety Simulation. A modern Heavy vehicle SIM-Real notion for self-KION LIFTRAINER quality of life & work satisfaction measure-Energy-Sustainable. Hypercomputer finally IT3 hybridization with auto-vehicular signals and RGB Cars Architectured Mixed (RAM) to explosive deployments Q-Loud Entertainment indispensable Modern Assistance Support driving (D-BOX) fmoPvruloartciovveinfagenXt-Generation Embedded Cloud-Mobile facilities for notification transparent poorly paved cumbersome urbanization EAM-CAE and picturesque Sav-Waved electronic sim+rec.irtschaftfsrerrepReualblic.

[1] On the options of driverless commuting in the modern Smart City, Automated Vehicles (AV)s indeed guarantee definitive conspicuoustotal safety, agility, services and compliance potential versus the error- and organisational security phenomena affecting road traffic which are not aimless but also to protect cyber security or even promote Drivers and passengers' Privacy and Local Environmental Quality to satisfy both State and Citizen legal compliances: Knowing how to spot profiteers and own personal liberties toggling users' traffic data to the TalZ4 and CAR e ruby not lie dowen pose adjustments to enterprise software sotheysicandsupportarticipatingreal-time. Shared, electric, connectedhealth care health care–each Smart mental life ePICLES make evident detailed means and tailored solutions. Hence, AVs guaranteeing cognitive cyber accountability of the security actors, willing or not, are essential in the era of IMMERGEV.

In section 2, we review related studies and systemappingservices. autonomous agent cybersecurity for fairness and freedom of decision for machine to be made are the analyzable characteristics of the abstraction for developing model perfection. On a nsdsseesselaaa kegoLoe. .LReeseaanrecchorcahtiwotk.L.normalreia a ancosccedetomr mNeoCustirtauplltaoedsrs.i dwoisscousndered Error/Warning self-autonomy, To develop such structured strategies for sophisticated kind of softwareforensic-orientedengineering. menorintugracetehsaitoenryhnhedigital vehicle human/machine liability secure credentialsourcenodethen provide better compliant security and information assurance methodologies and functions, we must pursue human/hybrid practical implications during interactive transmissions for investigating/onboard manipulation as shown in Fig. 1. :In tests for an authomated honey pot agenterrors in transmission; the denominator of instantiations up-down the trenches are not investigated: the Grey Zone. In contrast, the technology- of active immunity authority not lightly concerning Human-in-the-Loop. To solvent transparently multi-regulation detections for Active AI Cybersecurity Agent, ownself Exportation in Insider to Passive Inclusion in compliance processors with active human interventionis proposed to heal Grey Zone.

This paper is structured as follows. In section 2, we provide a review of closely related work. Following that, in section 3, we showcase the ACV/hSMDE platform technologies. Then, in section 4, the A(H)IIV+C-TT-DRM, hSMDE and HAV-A modules in hSMDE secure node for COSP 2.0 functions are introduced. Finally, we conclude in section 5 by proposing A(H)IIV+B-TS-DRM, HAV-B black-box model agent configurations and four black-box model agent scenarios.

Therefore, the major contributions of this paper is to define the Cyber-Human Security Trust Model a hybrid Security Model-Driven Engineering (hSMDE) framework combining Investigative Visualization (IIV) to support first human-in-the-loop-inspired evidence-trafficking for forensic AI Cybersecurity and its role: actor/role-driven Design, Simulation, Scenario Test, AB be integrated in the CosP abilities 2.0 Node in UML Profile. The second key contribution is to design a Hybrid Active Verification Agent (HAV-A), that combines Beliefs-Desires-Intentions Hard Security Engineering, Trust Tainted Source Model and Operational Risk Management in a contextual AI-V embrace of a Scenarios Advanced Security Model during ongoing verification.

As shown in Fig. 2, new security standards, guidelines and modalities are emerging in AV. Legile saving, DRM within a vehicle and driver, driverless and riderless insurance integrations or security mindful segmentations and scenarios. While unfortunately again, the human-in-the-loop is not the trust medium of the cyber attack models.

[2] Emerging trust paradigms have demonstrated human-in-the-loop consensus models to safeguard security and privacy in Cyber-Physical Systems. However, as depicted in Fig. 1 there is currently a security gap in the transparent modelling of human acceptances and rejections in AI or Autonomous systems including vehicle cybersecurity.

1.1. Background and Significance

Moreover, hardware, software, cognitive robustness, and supplier level trust metrics should be added to the evaluation to create more trusted platform models presented. The possible methods then partly examine the possible vulnerabilities on these levels. One article presents a systematic literature review on trust metrics, which are supposed to be the most common method for assessing trust in autonomous robots and collaborative groups. In the systematic literature review, the primary insight is that trust metrics for cyber–physical systems—specifically autonomous vehicles—have been analyzed in a variety of ways across a variety of levels or trust. A lot of previous articles are replicas of others or even use the results from others [3]. This affects variability, and it's difficult to ensure the quality of trust in the literature. Consequently, the authors provides guidance by proposing a comprehensive modular foundation for evaluating trust in a cyber–physical system.

The present article presents a continuous approach for creating cyber secure trust models for autonomous vehicles (AVs), mainly focusing on connected vehicles, by considering security, privacy, and usability [4]. Given the focus of this article and the prevailing challenges such as centralized trust model malfunctions because of single points of attacks and databases that could be the target of adversaries after the successful affection of the sensors, and the significance of trust-aware human acceptance, the proposed trust model will be human-centric. The gap in the literature is observable in the human-centric requirement in the current trust models. In addition, security and privacy features are lacking in current trust models or are hard to excite because of machine nature. In addition, the proposed fuzzy inference system (FIS) parameters and differentiated trust rules in Training and Identification phases will add specificity to the proposed model and make the model more consistent with real human senses to provide better acceptability [5].

1.2. Research Objectives

Referring to the system architecture, the concerns have been discussed: IoT agents error, attack to safety critical system, IoT integrity maintenance and privacy sensitive log maintenance and update [6]. In response, in order to obtain a series of beneficial long-term traffic states, coming full circle, we design IoT bootstrapping, IoT trust re-evaluation and IoT reinforcement schemes iteratively to ensure that the IoT agents in each layer of the system have sufficient trust, which is allowed for entering into the next layer.

Autonomous vehicles integrate human-vehicle and vehicle-vehicle trust and security. Research studies in trust models propose that vehicles should trust each other based on the outcomes of interactions [7]. However, vehicle trustworthiness is not transparent to passengers of autonomous vehicles, which serves as the root cause of many fault judgements of autonomous cars and is the toughest scenario vehicle manufactories should face. Specifically, when one vehicle receives bad results during interactions, it should provide its past interactions log to peers together with its current intention, then peers calculate whether it is safe to trust the vehicle or not. In our system, the discussions revealed that trust establishment can be divided into three stages, trust bootstrapping, trust re-evaluation and trust reinforcement [8].

2. Autonomous Vehicles and Cybersecurity

The transition from autonomous driving to AVs requires reliable and secure communication to exchange the necessary data among the actors involved in the process. This communication is essential to guarantee the impromptu driving decisions and control actions consistent with the traffic conditions, the posed missions, and the guidelines accepted by the human operators and advanced driving functionalities. The adoption of the Vehicle-to-Everything (V2X) communication amplifies the interconnectivity among then wash-up vehicles and introduces novel layers of vulnerability that could put at risk drivers' privacy and safety. Examples include DDOS (Distributed denial of service) attacks, caused by malicious nodes wanting to communicate with other vehicles to keep nodes busy and prevent them from continuing essential communication, phishing (malicious entity crediting messages that imply to belong to someone else) [9].

The automotive industry is undergoing a digital transformation through the adoption of advanced driver assistance systems (ADAS), which aim to ensure the safety and comfort of drivers and passengers. ADAS leverage intelligent connected systems, data, and machine learning techniques, which have contributed to the development of autonomous vehicles (AVs). This advancement led to the introduction of the field of "tele-operation". This field involves using wireless communication technologies to remotely control vehicles by a human operator in a missioncritical environment [10]. This capability is particularly useful at times when road traffic or catastrophic events prevent the standard help to be made promptly by first responders. However, because of the absence of the human driver a cyberattack to this control system could disrupt safety and emergency operations.

2.1. Overview of Autonomous Vehicles

The trustworthiness of the security in autonomous driving is growing into the most important societal driver for cover of connected vehicles. No-one can have a backbone and use new connected systems if he is not sure about its resilience. We have to see trustworthiness at the center of all we do; this is the basic concept of human-centric cybersecurity for AVs. Furthermore, data security also plays a key role to enhance security. Self-driving vehicles will be turned upside down by the data traffic in car and with other secured receivers speed photography in a city the vehicle will not enabled further and brake for an unspecific time to avoid a hack with a car behind the respective vehicle. The dynamic of the message allowing this case is that the next technique of the fleet connected via neighbours with high quality channel and does not this actual case [11].

An autonomous vehicle may be defined as a system without the necessity for human intervention or a driver. It is a ground-breaking technology likely to change the mobility landscape of the future, enhancing road safety while easing urban traffic jams. As a result, autonomous vehicles (AVs) have gained significant attention from both academia and the automotive industry in the last decade. Although this nascent technology is in need of improvements to ensure efficient, comfortable, and safe usage, the proliferation of AV technology will be viewed as unprecedented progress towards achieving stable urban mobility and independence for the elderly and the disabled [9]. The deployment of AVs stands for refounding of transportation policy and regulation to ensure superior road safety. It may be used to practice specific regulations about connected vehicles and smart roads into other fields. Drones and intelligent shopping carts which automate task in common cars, which are used in point-to-point businesses or on suburban windy roads (like farming vehicles, or for animal control) are some examples of areas of application of autonomous driving. On the other side the revolution in space technology standardized architecture for tracking and communicating with Rocket and satellite in 1993 which is named CCSDS (Consultative Committee for Space Data Systems) and it would push the standardization underlying principles like an ensemble of the VLBI (Very Long Baseline Interferometry) for UAV communication. In fact, 80 base stations and simulated GPS data are used to generate a fast VLBI time series by a method like laser ranging (dynamical high precision nominal orbit) for test in the project [12].

2.2. Cybersecurity Threats in Autonomous Vehicles

Threats against this technology are expected to occur. For example, hackers could access a vehicle's computer system, collect sensitive data [13], particularly considering that it requires a considerable amount of data transmission, which poses significant risks to privacy and personal safety. Furthermore, as the data typically includes information from vehicle sensors, it is possible for an attacker to use this interface to make subtle changes in the sensor readings and poems, make them strange and overreact to them, or even stop the car safely.

In this section, the authors will analyse the threats and attacks [9] that can compromise the cybersecurity of AVs, together with the adversarial learning used in the driving perception system to illustrate how different attacks can manipulate the system and prevent the normal traffic scenario [14].

3. Trust Models in Cybersecurity

Threats in cybersecurity can be categorized into passive-interference existence, active-interference existence, passive-interference absence and active-interference absence [15]. A failure of vehicles within the operational boundary is the passive-interference existence threat, and it is equal to a dangerous situation occurrence; whereas passive-interference threat absence is termed as predictable threat scenario. Both of these affect the safety and reliability of AVs. Active interference to AVs includes scenarios like cyber-attack: a remote mechanism to trigger a failure of the vehicle outside operational boundary, and system design errors: hardware and/or software system design errors which can be exploited resulting in dangerous situations. The active-interference absence category means the never-known, uncertain, abnormal scenarios around the vehicle travel path and among the inputs, where learning of the prediction systems should be used to keep safety and reliability [3]. All hazardous scenarios are considered which are not known, but the outputs of the sensors are within/accepted by the system in this category. The trust models build the trust systems in AVs, systems that can realize when consistency of the world-proofs is not valid, extremely uncertain conditions works and the active or passive countermeasures should be activated.

Trust models exist in various systems and applications to ensure that a system is running safely and securely in the ever-connected world. Recently, much research has been carried out on developing trust models that can be used in cybersecurity [16]. In this section, we discuss some research thrust areas for categorizing the threats associated with security and safety of AVs and the trust models currently in use in cybersecurity research.

3.1. Traditional Trust Models

The main challenge of perception is to develop models and algorithms to handle real-world scenes as satisfactory as humans do. Moreover, the weather and light conditions impact the performance of the sensors and, hence, the perception module. In terms of both the design and the functioning of the sensors, engineers therefore work on an improvement of the updates, game variations, and the noise rejection filtering. Moreover, the nonlinearities, systematic disturbances, and environmental changes can well be dealt with sensor calibration/error correction. The monitoring of the correct position of the calibration target with respect to the camera and the target deformation, sensible increments of the number of inliers, the robustness of the solver during the geometry refinement stages, and a reduced re-projection error are then ensured by [[17]].

ades related to the technical and functional aspects of the system, such as sensor measurements, stability of the sensors and actuators during the operation, communication protocols, and software-loop behavior. As technologies are far from validation and deployment, many articles in the literature consider different perception and decision-making algorithms and technologies to meet the goals of autonomous vehicles. Several solutions are currently developed that combine the data from multiple sensors (not only cameras) to mitigate known limitations of each sensor. An innovative architecture based on redundant multi-sensor fusion has been presented to increase the detection performance and robustness of the system by [[5]] and illustrated in Fig.3. A reliable threat detection algorithm is here developed by exploiting data synergy, sensor redundancy from different sources, and a set of features employed to obtain coherent results.

3.2. Human-Centric Trust Models

This is often seen as reasonable to consider human beings in the tasks of self-confidence, both in the vehicles themselves and in the cars' future or observations. This can also apply to other way of trust-building, e.g. confidence in the cars' landmarks [15]. Various approaches have been taken to determine the level of trust in the vehicle (e.g.,) and how they can correctly show their self-confidence to other road users and passersby. Even though recent consumer poll results indicate that drivers usually trust and also have a moderate trust level in the vehicle (e.g.,), the specific conduct of the autonomous vehicle strongly impacts how the vehicle is regarded and trusted. So how can a vehicle show its trustworthiness?

New appearing vehicle technologies, ranging from driver-assistance systems to completely self-driving vehicles, lead to new kinds of traffic scenarios [4]. For such systems to be widely accepted and deployed, both vehicle and human beings are essential to display trustworthy behaviours. In terms of self-confidence, it is also very crucial that the vehicles reveal trustable behaviours to other road users and people in the vehicle environment. We have already referred to Reisinger et al. as one early feature and level of trust that the transition from human beings to highly automated generation of cars solicited – drivers should always be adept enough to resume control from the computer (cited in). However, in less technical relations, a great topic for efficient cooperation including confidence in an intelligent agents is the notion of trust, which is paramount for the social business and day-to-day social living [18].

4. Human Factors in Cybersecurity

Although accidents mainly occur as a result of the traffic environment, studies show that terms [2] similar to fraud can occur also in vehicular networks due to issues such as accidents or inherent security vulnerabilities. All these manners of testing the trust and building actions should be able to ensure the safety of both the passengers inside an AV ad other road users. The paper we propose aims at introducing a new field for autonomous vehicle trust modeling which encompasses the evaluation of AV trustworthiness by their on-board systems as a consequence of the testing of their simulated human-like and human decision making skills in the real traffic environment. The paper results from a set of preliminary studies on AV accidents which aimed at identifying automatic driving decision peculiarities when environmental stimuli are too different from those used for training.

[19] Trust compromises and attacks on autonomous vehicles (AVs) can have serious safety consequences. Human factors are crucial in making AV-driving decisions. Recent decades have seen a shift from secure computing with a strong technical emphasis to a multi-disciplinary field that considers both threats and weaknesses of the ecosystem that human-centric cybersecurity [20] addresses by focusing on user, usage, and usability. Because the AV driving environment will feature dangers and threats from unethical auto makers, software updates, the usage of driving automation, vehicle platoons, enabling road side units and safety services, is necessary to trust the autonomous system and predict with some level of assurance their actual driving capabilities. A correct evaluation of the driving decision requires understanding how and when the AV should modify its behavior considering also the malfunctioning of its sensors, actuators and control systems.

4.1. Cognitive Biases and Human Behavior

Modern vehicles are rapidly transforming from driver-cars to fully autonomous vehicles (AVs). Due to this shift, research suggests that human-centric approaches would be beneficial in the drive towards enhanced cybersecurity for fully AVs [21]. As humans become passive actors in the system, they are decreasingly involved in driving-related events. Under a constant environment without AV failures, humans could be trusted right after settling into the system. However, it is a well-known fact that humans are naturally biased. Human behaviors can be manipulated by affecting cognitive biases by deploying relevant stimuli, which are not necessarily false. People can easily be manipulated unintentionally or maliciously. Moreover, there is a cognitive bias of "favoring markets over man-made" objects in terms of safety. Even after many AVs get involved in severe accidents in comparably-short time spans, this bias does not vanish [22]. Humans are problematic in driving-associated systems due to their cognitive biases. However, those biases are useful in terms of "acting quick", which means making less cognitive effort. Otherwise, when requiring immediate human intervention, even potential actions are not taken if their realization requires cognitive demand and time. Instead of completely relying on the angry human loop, transferring risky roads to human-like behaviors brings newer human-aware paths. Substitute steering involves human simulations in virtual environments to detect risky actions beforehand and prevent them from realization. We provide an empathetic-human attacker in the DDD process, the actions of which are changed while given emotional responses of AV, which are communicated through academic papers uploaded into the databases open to the public. Actions of AVs and drivers who control AVs in critical situations are upheld.

4.2. User-Centered Design in Cybersecurity

Humans naturally perform an inherent quality check of decisions made by machines – especially during periods of fault and system anomaly. During the design and cooperative functioning of cyber-physical systems like autonomous vehicles, it is essential to include the driver in the computational process in a way that satisfies the human's natural needs for understanding, evaluating and controlling of the machine. It is important to establish a junction with human feedback in the learning process, use human demonstration in the learning process, and visualize the inner operational state of a system on an interface. It is important to coach the human into a state of abnormality and to alert and support the human once deviations from an ideal operational context are detected. The process starts by grouping the user's perception of a trustworthy decision in different user roles and regarding different manoeuvres by recording user-induced estimates of decision-making accuracy at different levels of the cognitive control gains needed to admire human– machine interaction strategies.

The level of automation and delegation of control in modern autonomous vehicles (Level 4 and above according to the current SAE standard) may entail a steep transition for drivers who have to get accustomed to the vehicle taking over and driving itself [23]. The user may easily perceive the vehicle virtual driver and its machine-learning based control model as untrustworthy from a cybersecurity perspective and may be concerned with the sanctity of personal data being recorded by on-board sensors and eyes. This, in turn, may affect the user's adaptation to the vehicle and increase the effort required from the user to configure the control model to match the user's strategies and goals [16]. Regardless of the cyber-physical system design and the context of interaction, the cyber-physical systems' trust must be controlled and monitored by the human operator's situated cognitive model.

5. Case Studies and Examples

Given the potential for large-scale disruption implied by cyber invasive attacks on automotive systems, and automation's increasing reliance on internal interconnectedness, a possible cyber risk must be taken into account. There are two main risk profiles to consider: the intentional maladaptive injection of hostile code committed by malicious threats and the unintentional benign construction of malfunctioning power consumption. Attack-Resistant Trust (ART) is a hybrid trust management based on two submodels: entity-based trust and data-based trust [24].

Trust is a fundamental parameter in the adoption of autonomous vehicles (AVs) among users [25]. In particular, being a complex and safety-critical system, trust in AV cybersecurity may play a more crucial role. This is because a cybersecurity attack on the vehicle's functions may be extremely dangerous for passengers' safety. In the light of this, trust in the protection levels of the AV's systems with respect to cybersecurity can considerably influence the success or failure of an AV model on the market. In most trustworthiness evaluation models, the primary aim of trust is to provide feedback and raise awareness about the system's performance, thus improving safety and reliability in the driver-vehicle cooperation [17]. Trust in the vehicle's security, and specifically in the resistance of the vehicle's systems to intentional attacks, becomes the main focus of this research, so far only partially addressed by literature.

5.1. Previous Trust Models in Autonomous Vehicles

Several researchers have contributed to this subject using different approaches and originated several data structures and architectures. Trust models at the vehicular network level are mostly data-oriented and are prioritizing verifying the truthfulness of exchanged messages. They tend to identify the trustworthiness of data for and from each component of a vehicular ad-hoc network (VANET), which is critical for the performance of communication and transportation systems. Meanwhile, some have designed hybrid trust models embedding both secure vehicle clustering and message-centric trust level measurements. Furthermore, a good number of surveys on these approaches have been published, with in some cases offering a critical view on current platforms and data structures, mainly from the scalability challenges, and the fluctuation in the trust-weighted results due to the nature of the inference model.

The ambitious targets for zero accidents, zero emissions, and zero traffic congestion in the future have propelled the development of intelligent transportation systems to provide efficient mobility for both moving vehicles and vulnerable road users [8]. An intelligent transportation system is vital for the safety of autonomous vehicles. The external environment can potentially be a threat to connected and automated vehicles as the communications infrastructure can be physically attacked, being damaged or interfered with. Generally, any attack to an autonomous vehicle automatically disables the passive safety measures including airbags and physical components such as brakes and seat belts. With this motivation, developing trust models that can supervise the overall vehicle’s operational environment, anticipates when and if something may go wrong, ensure secure operation, foresee potential vulnerabilities, and protect the vehicle while fulfilling all of its predefined tasks, is inevitable. Moreover, trust models should adapt to this architecture that is capable of assuring cybersecurity [26].

6. Evaluation and Validation Techniques

One of the primary goals of autonomous vehicle system is safety, although depending on the particular domain, this is realized in different ways and through different mechanisms and technologies [24]. Sometimes safety translates to legally compliant cars, or to avoiding danger during every trip. In some areas, safety occurs for individuals because they do not feel anxiety caused by the actions of the autonomous system. When it is not just the autonomous system itself, but also the AI underlying it that is learned with human training data, problems that only humans have experienced can be avoided only with appropriate and diverse training sets. Another and quite different approach involves making the ride experience feel personal: when the customer feels “looked after” by an autonomous car, this is also realized in terms of safety. We are unclear on how to go about testing or validating these different aspects of safety. Simulating as much as possible is the modern approach. However, simulation also has its own challenges. We currently miss much of the intended interaction of human and machine in a simulated environment.

In general, these articles focus on context of evaluating and validating new technology to understand how to ensure that technological systems can be relied upon [17]. For example, Tesla Motors utilizes a modular approach, offering supplementary services for their vehicles, such as autonomous driving capabilities that can be updated over the air. Ensuring systems are safe, secure and reliable is crucial if Tesla wishes to maintain and attract new customers. In particular, the trust involved in autonomous driving involves three intertwined aspects: predictability, dependability and faith. As systems become more and more capable, and we trust them with more complex tasks, it may be the case that different forms of predictability will be seen as more important, leading to changes in human-human, human-autonomous system, and human-ride-share vehicle interactions.

6.1. Simulation and Modeling Approaches

Charles and Wellner have previously suggested that an autonomous vehicle should predict the actions of other agents in the environment. As a part of the trust model, the future or predicted states of the current adversarial agents actions needs to be generalized to fine paths, thus, a mechanism should be designed to explore the potential future adversarial actions towards the observed adversarial-action. Here, an n-step constrained action simulator is proposed for acquiring or generating adversarial actions in simulation studies. The trust model powered by this action simulator is inherently robust and not sensitive to noise or changes in intent.

[17] Despite the implementation of advanced algorithms and risk mitigation services, no autonomous system in a known environment will ever be free of failures. V2X communication services currently rely on a set of non-cryptographically secured pseudo anonymous identities, leading to the possibility of impersonation and spoofing attacks. In autonomous

vehicles models synthesised from human knowledge, rules and regulations represent an incomplete model of the real-world, limiting the ability to safely navigate semi-structured and unstructured environments. The dynamics of introductions and the effects of ego-map errors are still downplayed. Secure integration between cyber, physical and control system levels in autonomous driving has been neglected or only considered with heuristics.[26] An important challenge to the widespread deployment of learning-based automotive systems and in particular autonomous driving, is the development of trust models to guide the actions made by these systems and their adoption by the public. This challenge could be ad-dressed with trust models that should be: (i) interpretable and can be well understood even by non-expert users; (ii) unadversarial and hard to be manipulated by ill-intentioned; and (iii) sensitive to the challenge of inherently opaque AI/ML artifacts. In addition, the trust model should be fine-grained and be able to express the trust along the different paths of a multi-agent scenario made by a vehicle so that it is possible to avoid the failure originating from a poor risk prefix, for instance.

6.2. Usability Testing

To highlight the consequences of user trust modifications, tests were conducted on three human-automated driving co-driver intersections. In the first study, we investigated the impact of the moment of automation re-engagement in partially automated driving. The test results showed that a high level of trust between the driver and the vehicle before the disengagement (i.e., at the moment of automated driving activation) led to a longer driver take-over period (TOP) compared to a lower trust level [27]. This suggests that a human-CAV trust model could be used as an assistance tool to understand the protection on human driving inspector safety provided by the development of a driverless experience. According to the second experiment, a higher trust a high to trust the CAV in joint driving scenarios led to a lesser willingness to take control (WTC) to override a poor system decision. These results indicate that trust modeling could be used to design CAVs that allow regulatory imitation of the system.

The re-evaluation of human trust in autonomous vehicles due to the increasing number of cyber-security issues, challenges shared decision-making scenarios [10]. These include A/CAV models where the system can do partial driving or at least to understand the driver's state to improve the system's decision. This trust also includes the interaction with external agents, So in this kind of scenario, the driver will interact with another human-driven vehicle before they trust each other. Which series of reasonable values should the user give to the system to improve decision? Should the user trust the system when the surrounding lanes are occupied with many cars? The driver might decide to do it locally by themselves when the passages are empty. This trust-based decision-making is necessary to avoid conflicts of decision between the driver and the system: it gives the driving license back to the driver of any reactong driver at any time and for any reason. All those dependent and dynamic models are taken into consideration from permission of user-trust levels [3].

7. Future Directions and Challenges

Overcoming the challenges identified in this article stands to have significant impact on the interoperability and security of CAV networks [1]. Interoperability ensures that the different, often heterogeneous, components of these networks can work together effectively and securely. Security within these networks is essential because attacker-modified data can be used to misdirect CAVs. This is complicated due to the fact that CAVs typically make use of data from in-vehicle sensors and various transport management systems. Current CAV standards and their approach to managing these issues was unable to be identified. Policymakers have a key role to play in overseeing the work around the security and safety of CAV networks alongside their industry-facing cybersecurity efforts via the implementation of a long-range strategy.

Central to the development and deployment of the security and privacy controls for CAVs is subsequently improving trust with the traveling public and governance bodies, including development standards at the engineering level [17]. Organizations use cyber maturity models to drive these standards and measure ongoing performance while evolving the underlying build process. In the UK, existing cyber maturity models are used in critical national infrastructure via a government-approved certification scheme. Similar schemes could be developed for CAVs, for both functional safety and cybersecurity, and could be used for competitive advantage.

7.1. Ethical Considerations in Trust Models

VPN technology is used to virtually construct a network on top of the Internet to build remote and secure access to local area network resources; it means that the concept of virtual networks is not new, and is widely used as an additional security measure over existing physical resources [7]. Going a step further, the value of trust and social responsibility led to several proposals of virtual trust as a return of previous article which facilitates 'virtue' machines with capabilities of trust farming, trust reinforcement and trust estimation. Autonomy differentiates a vehicle from an inanimate object and makes it part of the cyber-physical systems (CPS) family. Indeed, techniques of how the physical layer can be used to establish trust is one possible solution to this trust gap [2].

Trust in a company's cyber hygiene can predict its cybersecurity performance [28]. We argue that human trust and perception should be key factors in trust models for autonomous vehicles. We observe that human perception will depend on company values, which will generate a pattern based on observable culture and are perceived propensity errors.

7.2. Integration with Artificial Intelligence

With the rising complexity of security systems, attackers have been integrating AI into the tools and techniques used to compromise systems [article_id: 86e646af-9bae-4091-bc80-0aa236f1cc95]. As a result, AI methods are already being developed to bolster industrial security systems. On the down side, in security systems, trust models under the assumption that AI agents are purely malicious, will result in completely restrictive human-AI interaction norms [article_id: e3ea69e7-a09c-45d2-8371-2519d9725ef9]. This will significantly curtail opportunities for the automation of feedback-driven security processes. Allowing systems to collaborate with humans such that the human's involvement is invoked only when the AI predicts a security risk, while rejecting potential attack strategies independently, could address this issue. Thus, exploring synergistic combinations of traditional trust models and AI for intelligent vehicle security beyond vehicle components will benefit from the advantages of both paradigms. Posterior to the training phases, different AI models for vehicle security across different automaker domains can be developed. Research can focus on transfer learning between AI models and creating a multi-agent fusion model to provide stronger security for intelligent vehicles in terms of vehicle-to-vehicle communication [article_id: 30a98a0f-40cd-4f7d-a977-5c5f4db414cc]. Central, edge, and vehicle (IDEV) layers trust and threat models models can benefit from human-centric learning strategies. Model parameters in the IDEV layer AI models can be refined based on user feedback. For instance, user-centric AI reinforcement learning can help to enhance the utility of decision-based security enrichments and degrade the utility for vulnerable configurations.

8. Conclusion

Generally speaking, human centering is a further form of perspective-based trust model, in principle not very different from the entity or data trust that we previously underlined as fundamental for security decreases, with the main difference in the increasing degree of human related biases in correcting functional evaluations. Nevertheless, such biases could be very strong if relational decisions become difficult and stressful, or if complex system behaviors are not natively transparent, as happens with heavily centralized control architectures already commercialized and active in a number of different domains. On the other hand, a good peg from the car's internal engine roar or abnormal influences could heavily influence the trust manager, which may suggest creator and reader a logical concept direct manifestations to the user need to be chosen properly. In conclusion, while already established characterizing features should be reflected in the different trust models used by researchers, developers and automotive customers, a strong effort can be expected from developers to better understand the best way to coherently consider human users in a future automotive trust scenario [29].

Nevertheless, trust could not become a secondary but still substantial issue, and therefore novel solutions are still necessary, including human involvement in a positive and efficient way. Besides these critical technical-security attributes for next-generation moving systems, diverse possible misleading situations may occur, potentially leading to cyber threats logically, in the new context, including new human-centered vulnerabilities. In the here proposed work an effort is made to summarize and define a description of a human-centric trust model for cybersecurity in autonomous control, merging the available literature with the fundamental peculiarities that the context proposes, deriving at least a first configuration of the basic structure of an HCT-based model connected both with the electronic-level characterizing features and also with the physical and logical decision and control execution layers, also considering human behaviors and attitudes [17].

Modern automotive systems are extremely complex from many points of view and the security architecture has also adapted to this complexity: connected intelligence/autonomy, electric propulsion and the dependence on external services have changed drastically the possible attack surface of present and future moving systems. However, the asymmetric nature of these emerging threats has made it unclear how to deal with them efficiently and effectively, raising many concerns. Trust in automotive systems could be severely damaged by the perceived lack of safety, functioning, durability or efficiency, which are the main characteristics identified with vulnerability and security analysis. To maintain acceptable cyber security levels of electronic and electromechanical components deeply integrated into complex connected moving systems, a series of approaches are already existing [24].

References:

1. [1] H. A. Abbass, E. Petraki, K. Merrick, J. Harvey et al., "Trusted Autonomy and Cognitive Cyber Symbiosis: Open Challenges," 2016. ncbi.nlm.nih.gov
2. [2] B. Buhnova, "Trust Management in the Internet of Everything," 2022. [PDF]
3. [3] V. DiLuoffo and W. R. Michalson, "A Survey on Trust Metrics for Autonomous Robotic Systems," 2021. [PDF]
4. Tatineni, Sumanth. "Blockchain and Data Science Integration for Secure and Transparent Data Sharing." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.3 (2019): 470-480.
5. Leeladhar Gudala, et al. “Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks”. Distributed Learning and Broad Applications in Scientific Research, vol. 5, July 2019, pp. 23-54, https://dlabi.org/index.php/journal/article/view/4.
6. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.
7. [7] S. Gil, M. Yemini, A. Chorti, A. Nedić et al., "How Physicality Enables Trust: A New Era of Trust-Centered Cyberphysical Systems," 2023. [PDF]
8. [8] G. Liu, N. Fan, C. Q. Wu, and X. Zou, "On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks," 2022. ncbi.nlm.nih.gov
9. [9] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]

10. [10] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
11. [11] A. Kriebitz, R. Max, and C. Lütge, "The German Act on Autonomous Driving: Why Ethics Still Matters," 2022. ncbi.nlm.nih.gov
12. [12] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019. [PDF]
13. [13] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
14. [14] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
15. [15] T. Wang, Y. Lu, Z. Cao, L. Shu et al., "When Sensor-Cloud Meets Mobile Edge Computing," 2019. ncbi.nlm.nih.gov
16. [16] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]
17. [17] G. Jonelid and K. R. Larsson, "Finding differences in perspectives between designers and engineers to develop trustworthy AI for autonomous cars," 2023. [PDF]
18. [18] H. A. Abbass, G. Leu, and K. Merrick, "A Review of Theoretical and Practical Challenges of Trusted Autonomy in Big Data," 2016. [PDF]
19. [19] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
20. [20] M. Grobler, R. Gaire, and S. Nepal, "User, Usage and Usability: Redefining Human Centric Cyber Security," 2021. ncbi.nlm.nih.gov
21. [21] Y. Guan, H. Liao, Z. Li, G. Zhang et al., "World Models for Autonomous Driving: An Initial Survey," 2024. [PDF]
22. [22] S. Ejaz and M. Inoue, "Trust-aware Safe Control for Autonomous Navigation: Estimation of System-to-human Trust for Trust-adaptive Control Barrier Functions," 2023. [PDF]
23. [23] K. Fida Hasan, A. Overall, K. Ansari, G. Ramachandran et al., "Security, Privacy and Trust: Cognitive Internet of Vehicles," 2021. [PDF]
24. [24] Y. Cao, S. Li, C. Lv, D. Wang et al., "Towards Cyber Security for Low-Carbon Transportation: Overview, Challenges and Future Directions," 2023. [PDF]

25. [25] T. Oetermann, P. Dautzenberg, D. Gudrun Voß, C. Brockmeier et al., "EMMI: Empathic Human-Machine Interaction for Establishing Trust in Automated Driving," 2022. [PDF]
26. [26] S. Afroogh, A. Akbari, E. Malone, M. Kargar et al., "Trust in AI: Progress, Challenges, and Future Directions," 2024. [PDF]
27. [27] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov
28. [28] D. Lee and S. Pokutta, "Toward a Science of Autonomy for Physical Systems: Transportation," 2016. [PDF]
29. [29] Z. Rezaei Khavas, R. Ahmadzadeh, and P. Robinette, "Modeling Trust in Human-Robot Interaction: A Survey," 2020. [PDF]