Cognitive Load Analysis of Cybersecurity Interfaces in Autonomous Vehicle Control Systems

By Dr. Neema Balakrishnan

Associate Professor of Information Systems, University of Dar es Salaam, Tanzania

1. Introduction

To assure the functioning of such semi-autonomous systems, it is vital for the operator to cooperate efficiently with both the vehicular human-machine interface (HMI) and the security systems. The driver's workload can increase due to both the manual control of the vehicle during the levels of low driving automation and the safety critical control to regain the manual driving of the vehicle from conditional and high driving-level automation based on mainly cyber and physical events systems failure. We shall delve into deep-dive details and outline analysis of the effects of the choices regarding the logic and HMI design of the cybertrail on the operation of the autonomous vehicles. The art-of-the-state interfaces to allow the operator to provide the Legal Request for The Control (LRfC) to gain the manual control during the cyber event and HMI designs to provide security aspects' logic are vital concerning the sustainability of autonomous vehicles. Such UIs also describe the cyber events or follow the various warning levels and possess separate logic units to decrease the cognitive load of the operators and thereby make it easier for interest to achieve satisfactory security status for traffic [1].

Cybersecurity-related usability and user interface (UI) aspects have been recognized as important dimensions in the development of autonomous vehicle control systems, where stagnation can ultimately lead to substantial risks to people's lives, and are intertwined with several bottleneck factors—so-called "black swans"—in the developing ecosystem of autonomous driving [2]. Autonomous vehicles cannot operate in isolation and they need to interact with the environment by relying on a plethora of systems such as automotive radar, vision and thermal cameras, LiDAR and GPS systems in addition to advanced communication systems such as Wi-Fi, Bluetooth and various V2X network APIs, as well as a Forensic Tachograph, OBU, TMS and EVE systems. The large number of interfaces between the on-

board systems of a smart vehicle and the external environment open up new exploitation scenarios to an evil attacker since each communication interface could be exploited.

1.1. Background and Significance

[2] Automotive systems have evolved into large-scale, complex, and dynamic systems with ill-defined boundaries of ownership and control. As connected and automated mobility (CAM) becomes a reality, organizations need to shift their strategy from simply selling vehicles to delivering robust engineering practices that address the potential threats from the cyber world. In the domain of cybersecurity research, vehicle cybersecurity has been studied to a large extent. The nature of the connected and autonomous vehicle (CAV) systems, despite technological advancements in vehicle cybersecurity, makes cyber attack analysis and defense quite challenging. In reality, a mix of a traditional attack analysis approach and a predictive approach is necessary to increase trust in the systems. Hence the probability of cyber event detection and CAV response need to be more accurate, with special consideration given to the introduction of more defective nodes [e.g.,>1%, an RQ1 in 1.2. introduced in 1.3 CyRes—Avoiding Catastrophic Failure in Connected and Autonomous Vehicles (Extended Abstract) 3 structured workflow in CyRes (RQ2 in 1.2). In order to deliver robust engineering cybersecurity practices, two more principles—engineer significant differences and implement proactive updates—are proposed in 1.2.[3] With any driver assistance system or features and approaches that have been investigated, the goal is to reduce a driver's cognitive load on the basis of a low-cost car-following scenario. However since the driver is responsible for the driving, the impact of a feature on the cognitive load must be carefully considered, balancing the context-specific information and cognitive load to improve rather than impair the driver's performance. In the context of this study, it has been demonstrated that Adaptive HMI strategies based on the driver's cognitive state have the potential to improve traffic safety even in a low-cost scenario. Cognitive Load is a measure of the number of simultaneous tasks, levels of mental complexity, datasets, tasks, and time pressure that all occur at the same time. Cognitive load and the driving load is an important field of research when developing new vehicles, features, and technologies, in order to further increase road safety in future traffic.

1.2. Research Objectives

[4] Potential cybersecurity threats are increasing. In autonomous driving the order of time required for responses is critical. This is due to the real-time, dynamic and interactive nature

of autonomous driving. Unauthorized access to infotainment, communication services and the safety-critical functions of the vehicle can both lead to vulnerabilities with the potential to pose a severe risk to vehicle occupants and other road users. An approach that should be widely applicable to autonomous driving content will be employed in this report. It includes an analysis of existing input interfaces and control units, a rapid prototyping and implementation case study on a control software/engine control system and experimental studies with test subjects. As it progresses this approach can identify new interaction and system design optimization aids that either reduce a user's cognitive load or increase their cyber-security awareness for better attack detection and response times. In this paper, we present a user study that sheds light on the distribution of user attention in different scenarios.[3] The control of automated vehicles will help shorten and simplify the drive, resulting in new opportunities for secondary activities. This allows the driver, for example, to pass through emails or to have phone calls. It is known that an increase in secondary activities may lead to a decrease both in arousal and in the mean reaction time, often called a load of cognitive. The rear-end collision is a common type of road event that has been investigated in driving competitions. The vehicle following is an example of these driving situations. The dynamic traffic environment complexity (DTEC) holds out the promise of developing more realistic experimental environments when analyzing vehicle following and other control behaviors. Post-platooning control was examined here because, like Post-platooning management, shared information has generated an increase in cognitive burden. If drivers with different amounts of experience had been examined, Post-platooning control and set of backward roads should be investigated also.

1.3. Scope and Limitations

The assessment of external trustworthiness—intended as the capability of a supplier to deliver self-contained systems that can operate safely and efficiently without fore- seeing external interventions—has recently been investigated. In accordance with existing automotive norms, including ISO 26262 and ISO 21434, in this framework, the production of an external trustworthiness report is mandatory to allow the vehicle to be put into an autonomous mode [5]. The streamlining of certification has been proposed in a recent normative framework in order to create a faster and more efficient assessment process and a clear evolution path for the introduction of new technological features even when they may require a general recertification.

Cybersecurity is crucial for safe operation of autonomous vehicles [6]. It is not only necessary to build re- silient control systems that can cope with onboard failures caused by the deployment of edge cases, environmental noise, or disturbances in the control loops, but it is also mandatory to consider the possibility of adversarial attacks that could lead to hazardous situations. In fact, the failure to show the trustworthiness of autonomous vehicle technology has been identified as a major challenge, also from the perspective of creating user trust in the new technology [2]; both a global coherent approach to guarantee cybersecurity and the development of new design methodologies aimed at assessing the impact of both classical failures and adversa- ries on the overall system are considered as fundamental enablers for the success of the autonomous vehicle revolution.

2. Literature Review

In our study we investigate if such an AV user interfaces effectively reduce cognitive load compared with passive monitoring, no monitoring and ENG-Self-driving (SD). Different levels of automated driving were examined: Levels 0, 2, 3 and 4. To objectively measure cognitive load in participants the Event Related Potential (ERP) P300 component amplitudes elicited by secondary task-evoked auditory oddballs were recorded via and 64-channel EEG. For the method, as for behavioural data, online and offline blockwise analyses comparing different levels of automation are presented, thus allowing the comparison of real-time and overt cognitive load of participants. This aim is to analyze secondary task processing advantages and disadvantages of engaging drivers in manual, partially automated (PA), and highly automated driving (HAD) and to demonstrate to what levels of automation users would appreciate control transfer knowledge letting them invest their attentional resources effectively.

[7] [8]User-interfaces and computer mediated control systems in autonomous vehicles (AVs) are increasingly vital interfaces particularly as AVs gradually increase in their levels of automation. To ensure effective and safe driver-Vehicle Interaction (d-VI) and to avoid mental underload and overload, cooperative and proactive user interfaces would learn to understand, predict, and optimize drivers' and passengers' driving intentions and attentional resource allocation a priori. One important way to achieve this is by preventing suboptimal situation awareness in d-VI, and by keeping drivers engaged and prevent they mind-wandering. Thus, especially as long as partially and conditionally AV operation necessitate

driver assistance or total envelopment in control under unexpected situations, respectively. d-VI methodologies are demanded to identify and handle difficulties when engine control is clumsy and quick restructuring is expected due to new and unpracticed situations. Consequently, it has turned out to be of the upmost priority to understand how a real-time Cyber-Physical Human-Machine-Interface (CP HMI) in AVs can facilitate improved situation awareness and optimized humans' information flow allocation and reduce Cyber-Physical Systems (CPS) imperceptibility for human operators in the driving control-loop.

2.1. Cognitive Load Theory

The cognitive load theory explains that limited capacity working memory usually leads to cognitive overload when a task exceeds a human's ability to process or perform, which results in information loss and decreased effectiveness and efficiency in the human-computer interaction process (Dehue and Borst, 2019). Three types of cognitive load, intrinsic cognitive load, extraneous cognitive load, and germane cognitive load, are defined. Intrinsic cognitive load mainly comes with tasks, and it is determined by nature and complexity of the task. Extraneous cognitive load is induced either by the instruction process or the bad design of the interface. The task performance can be affected since human's mental efforts are wasted to handle irrelevant stimuli or the redundant perception in the interface. Germane cognitive load is cognitive expenditure that contributes to the learning task. Based on this theory, the efficiency and the effectiveness of an interactive system can largely rely on how the interface design has taken these principles into account to reduce the cognitive load for the user. Therefore, this theory is part of a number of works that analyze human factors and interaction for autonomous vehicles (Yan et al., 2016; Shao et al., 2021; Wei et al., 2022).

Computational cognitive psychology considers knowledge as the internal representations and procedures of the cognitive system that are used in perceiving, remembering, reasoning, and performing actions in a complex, information-rich, and structured environment. However, it is not enough to study the architecture and hardware component (Fletcher et al., 1980) of the cognitive system, but the cognitive function itself. In a study jointly hosted by the National Institutes of Health and the National Science Foundation, Atkinson and Shiffrin published a seminal paper on the working principles and mechanisms of human memory (Atkinson and Shiffrin, 1968). Cognitive architecture and cognitive mechanism are two fundamental concepts On the design of human-computer interface, researchers have been working hard to

reduce the cognitive load of human-computer interaction to improve human-computer interaction performance (Zauner and Ye, 2021). Cognitive load theory has become one of the most representative theories applied widely to guide the design of human-computer interaction systems (Oppermann and Mey, 2018) [7].

2.2. Cybersecurity Interfaces in Autonomous Vehicles

The Cyber-Physical (CyPhy) Model 2 in figure 2 is a multimodal or mixed-initiative system in which the vehicle and driver take control decision. A typical application as of writing of this paper are the driver in the loop (DiL) simulations, where the algorithm is tested by a human driver in virtual reality (VR) [9]. That is, the multimodal and the mixed-initiative combined system repeatedly hands control back and forth between a human driver and an autonomous driving (AD) agent, from the vehicle it compensates the human driver's attention deficit. Marketing claims demonstrate unobtrusive interaction. However, it has to be mentioned that mixed-initiative fully engaged the human driver in the 15 s before contact was established by the vehicle, but among the CyPhy can be conducted more safely in certain failure modes. For failure modes on the automated driving agent side, the Volkswagen study investigated the best method to hand over control of the car and to alert the driver, in multimodal, where the majority of the respond time participating users were transformed [10], it took more than three times as long for users that had entirely forgotten to monitor the car to react to the alert compared to those users with no change. The multimodal mix was made up of a visual as well as an auditory warning signal. At the termination of the automation, however, none of these users were able to adjust the speed of the vehicle by braking on their own (no participants discussed it).

The current cybersecurity architecture of vehicles was designed for traditional signal control architecture, where each function performs through discrete control lines or isolated in-vehicle networks that control powertrain components or safety features [5]. In automated driving, the vehicle cedes control to the autonomous system, a nightmare scenario arises in terms of cyber-attacks. If properly targeted, an attacker could exploit any dissimilarity existing in the cybersecurity architecture between today's electrical architecture and the increasingly electrical- and electronic-based architectures of tomorrow's vehicles. There are two key interfaces in the automobile of which both must be considered and protected. One of these interfaces is the interface between the car and the outside world (connected cars). The second,

and most important for defensive driving ("at any time, the driver must be able to resume driving"), is the interface between the car and the driver. This interface will be considered more closely in this paper. In the following we differentiate three cyber-physical, i.e., the cyber vehicle control system is affected and the human driver has to correct the error.

2.3. Adaptive Strategies in Network Segmentation

For several topics in Human–Computer Interaction (HCI) and usability research, the need for adaptive strategies for the reduction of the increased learning demand has been shown. There are several existing strategies for the reduction of the extra cognitive load. One of these strategies is error, or lack of fit, management. According to this strategy, useful information about what is not correct, and how the user should correct the problem, should be provided. This strategy is useful for error management and quality of decisions [11]. Another existing strategy is just-in-time training, which suggests that training on specific topics should be done at the time that the user needs to use the knowledge in his or her current assignment. Giving an operator a new explanation about a new functionality that he or she does not need when interpreting a radar echo is poor programming according to just-in-time training. According to our survey of adaptive strategies in cybersecurity literature, just-in-time training should be unplanned and unsolicited from the operator, as it is only the system once that knows exactly when he or she lacks knowledge. In the context of cybersecurity, just in-time training is useful mainly when the system thinks that the operator needs new knowledge to be able to act in a situation. In the field test, 45% of the participants thought that they needed to have security knowledge that they did not have to fully understand how to react to an odd situation. This observation highlights the need for both increased learning demand and potential cognitive load.

The aim of network segmentation is to increase the cybersecurity of the systems. However, if the measure reduces the usability to such an extent that the operators cannot use the system, the measure is practically pointless. This trade-off is based on the learning process that the operator goes through. Network segmentation could thus be described as a necessary evil – it is performed to ensure the resilience of a system against internal and external threats, even though it might increase the learning demand, and thus the cognitive load [12] .

3. Methodology

Adaptive human-computer interfaces, the mainstay of autonomous vehicle systems design, consider multi- sensory perception processing in addition to task complexity, which ought to be aligned within the driver's secondary task-carrying capacity. Therein lies the design of the Autonomy and Driver Attention Capturing (ADAC) system [3]. From a standpoint of cognitive modelling, to enhance traffic safety, particularly for driver automation-substitution handover and attention level assessment, it uses scientific observation of the human's multimodal and spatial 3D sensory modalities of retinomorphic vision, cortical hearing, haptic touch, and brain biopotential processing and comprehension, such as comparison of autonomous ['tengo un bloqueo múltiple'] for control with expert human drivers' protocols on the partially observable environments [2]. A driver's secondary task-carrying capacity [13] is important because it determines the maximum complexity of the secondary task a driver can handle while driving safely. This maximum complexity, the limit representing the threshold of a driver's attention level decline and of carrying capacity threshold of distraction or burden when a driver begins to have to detach from a previously expert-mode-controlled steering wheel, resting from unnecessary driving, reading a book, or returning back even to settle a vomituous illusory relationship with the system environment. Using against eye scan distance image projection in cortical coordinates visual support for a number of and weighting of limited part-control feedbacks at a given time instant, the ADAC Systems' structured secondary task is steered and conducted to be less small perturbed, nonsystem dangerous. This state of being refers to an alternative certain optimality design for the Athena Parthenos Game Two best intelligence implementation. Without training and data collection, it is assumed that this hypothesis choice will not overlap any "dangerous" semantic map paths 2PR2 paths with either twistor hallucinating path inside twistor-null-circulating channelsconstituent ADAC momenta of paths-Chapter Two's multimodal 3D virtual or by Riemann-Rochification possibly not realized neutrinos component.

3.1. Research Design

In the context of the study, the terms he 1-Heuristic: Evaluate the impact of cyber security with distribution control. The second scenario that makes use of cyber security functions of the autonomous vehicle. An Heuristic evaluation will be performed to assess the use of heuristic guidelines to be useful in the detection of security issues. This research is intended to focus on the heuristic evaluation of security operations done primarily on the basis of a checklist. For this purpose, the participant takes the helm of the car. Heuristic Evaluations are

directed by experts who are leading the study. These experts have experience in cybersecurity and inductive or evaluation methods. The duty of the scores is to evaluate the results of usability, user experience and user interface. The experts' experience is representative. This will make the analyse more feature-oriented [ct: 7bac4f65-0771-4424-89f3-5b781c37c19f].

The research design was elaborated with the scope of evaluating the impact of cyber security role-based task allocation for use in autonomous vehicle control systems. The evaluation addresses the two scenarios of manual and automated control mode with high and low usability. The participant's workload on different tasks is evaluated. For this purpose, the task helmsman's workload is assessed for each user. The evaluation is carried out in the car of the test track. A test supervisor sitting on the co-driver's seat observes the persons and interacts with the study participants if necessary. Before the user enters, the driving mode and the current workload are now displayed in the vehicle's user interface. The user interface shall be a standard commercial User Interface.

3.2. Data Collection Methods

We argue that the typical concept of measuring cognitive load in cybersecurity can be extended in respect to automotive cybersecurity. At this point, the real-world implementation of our research-based ideas for the risk assessment of the various cybersecurity aspects becomes evident. Furthermore, the new use-case with respect to ITS shows how the general strategies – risk assessment, safety, and security measures, backed up by adequate methods for measurement and methodological concerns – have to be implemented. These findings have a direct impact on cybersecurity in the automotive context, and also hint at further possibilities for the development of respective theoretical maturity models. The findings about software security measures for real-time properties feeding into the hierarchical model are derived from the case study in the public presentation of that model [13,14]. The structured case study carries inherent limitations; the project of that case study—covering formal methods for risk assessment and formal definitions for measures relating to them—ends at the same level as the hierarchical model. Helping resilient and secure applications to use properties of real-time analysis as security measures finally is an ongoing further research focal issue. Inspired by Peddisetty and Reddy (2024), who highlighted the potential of AI in predicting and managing change in IS projects, this paper delves into the technical and organizational considerations for successful AI implementation

Measuring cognitive load in cybersecurity is commonly done in the laboratory or field [4]. Laboratory studies typically use an experimental design such as between subjects or within subjects and a self-report or computer-based task. Studies typically employ various cognitive load measures. Common measures include self-report measures such as the National Aeronautics and Space Administration Task Load Index, performance measures such as task completion time and error rates, eye-tracking measures, psychophysiological measures such as heart rate and eye state, and neurophysiological measures [14]. Field studies take place in either virtual simulations like driving simulators or in the real world. Field studies primarily employ driving performance metrics such as speed maintenance, lane keeping, headway, accelerations, vehicular control, and collision occurrences [8]. A review of literature identified eight primary measures over 12 studies. Throughout the 35 studies, a total of 24 unique measures are represented. A total of 41 unique measures are featured in the measurement combinations of the 35 studies.

3.3. Data Analysis Techniques

Through comprehensive analysis (SSTE, TTT, and A-Track), three cognitive-load indicators (RSI, PL, and GZD) were used to investigate cognitive load at different levels (low, medium, and high) and then explore through linear regression the correlation coefficients between the operating time and cognitive-load indicators. Through the data analysis of PL and GZD in various condition experiment groups, it was found that the change in cognitive load increased the time of task completion, providing a basis for the research topic of the cognitive load in different task environment experiment groups and then combined with the method of linear regression to analyze the correlation between different priority indicators and the completion time, we could see that the control factors of the experiment group could be accurately represented and the cognitive load as a second level of control, and the data obtained can support the relationship between control factors, cognitive load, and data analysis. In addition, we did a more accurate correlation analysis between priority indicators. According to the t test method, the significance of the correlation between priority indicators and task completion time was obtained. Meanwhile, adding eye-tracking data to the data analysis of "mental workload" is more comprehensive. And it can specifically reflect the changes of human operators' emotions in autonomous vehicle operating systems and the spontaneity and naturalness of actions by your body [7].

In our experiment, we didn't involve any psychophysiological data, although it has been widely reported in the literature [15]. The Speech Shadowing Task Experiment (SSTE) was excluded from this research mainly because it was different from the other three tasks in terms of characteristics and uncontrollability. The analysis of eye-tracking data (A-Track) used in our research is a technology that can help collect and analyze human gaze data. The analysis of average pupil size calculation was based on the signal collected by an Eye Link-1000 sensitive scene corneal reflection pupillometer, and only in non-distraction einvironment within 750 pixels (≈ 35% of the video screen size) was the whole task time used for data analysis. The tool operation time was calculated by the mouse click and mouse move of the system, etc.

4. Cognitive Load Analysis in Cybersecurity Interfaces

The driving scene was clear for the Simulation and Supervisor scenarios. At that moment, a choice was given to the users with the Brake group being significantly faster. The average reaction times to apply the brakes and when the participants in the non-braking group assumed a collision was inevitable, as well as their choice criteria were taken into consideration. There is plenty of evidence that the participants in the DS group select a higher incident threshold in the Simulation scenario. Respondents in the Simulation scenario who were in the CSF group were also less willing to brake. Moreover, the mean reaction time to press the brakes was longer. The DS and the CSF groups both took a longer time to shift from close to inevitable toward certain thanks to a control sensor failure when comparing means between scenarios.

Detecting possible cybersecurity incidents and understanding them as they occur is vital for achieving the trustworthiness of automotive systems [16]. The Discrete-Event Detection-Response (DR) task is the method used to measure cognitive load in this study [17]. A user supervises autonomous vehicles and must execute a braking command as soon as they are certain an impending collision will be unavoidable. To ascertain the braking decisions of the users, the type of collision they perceived and the use of the brakes were measured. Types of cyberattacks were represented by a control sensor failure (CSF) and a delayed sensor (DS) failure. A collision was presented unless the supervising driver applied the brakes and made the need redundant.

4.1. Definition and Components of Cognitive Load

The optimal calibration of a proactive redundant display in a preventive cyber-security environment is a topic that is relatively unexplored, as far as we can tell. Prior work has formulated proactive security advice displays as decision aids and shown that, with appropriate training, properly displaying this information can facilitate efficient and effective decision-making in a proactive security setting [18]. Further research has explored incorporating a security advice display into the control system user interface. Although there is a significant amount of research calling for the use of passive rather than active preventive techniques, tools and technologies, very little has been written about whether and when to augment quality of advice based on metrics such as cognitive load. Therefore, in our work, we seek to understand whether an augmented and adaptive cybersecurity display is possible without increasing and, ideally, with the aim of reducing the cognitive load experienced by the operator.

Cognitive load is a measure of the mental effort that is required to perform a particular task. A widely accepted classification distinguishes three types of cognitive load: intrinsic, extrinsic and germane load [19]. Intrinsic load refers to the inherent complexity imposed by the constellation of info elements that have to be processed simultaneously. Extraneous load refers to mental effort that can be reduced by a reorganization of the task-irrelevant info elements. The importance of extraneous load has emerged as it is closely linked to the design of the learning material. It has been shown that secondary, or extraneous, tasks can competently judge perceptional and perceptual load characteristics of a primary or focal task or cognitive domain by occupying cognitive resources. The concept of germane load was introduced to mediately address the rather limited explanatory power of the original two-component cognitive load theory. The germane cognitive load required by info processing in working memory and other cognitive processes is important for learning because it determines the extent and direction of cognitive resource allocation (i.e., optimization or overinvesting, affecting cognitive learning effort) [15].

4.2. Measurement Techniques

The ADABase contains behavioral and physiological data visual response, reaction time in milliseconds, facial expressions, pupil dilation (applied two filters), and full brain signals, and about heart activity. All the human subject(s) were asked to per form visual and auditory tasks on the non-invasive computer interface memory the Dual task n-back paradigm. The pupil

dilation can be measured by visual driving response choices. After the 1st of 10 presentations, a red square appeared in 12 different places In the next set of tests ADABase was implemented on the computer interface and a semiautonomous Tesla Model S for further costumers assessment. In the test trip, 11 subjects been asked to keep up their driving speed on a longitudinal profile of a German interstate requested to hit the emergency break in case of appearing critical driving situations or till the program would stop. A change in beat-to-beat interval was found between a condition of the quiet resting-state and an arithmetic task simulation in the ADABase of time. Smolarek, Dymek, Lebrun, Li, 2018 combined simultaneous fNIRS-EEG recording for intra-individual purposes to monitor neural activity, in the healthy aging brain while (enjoying) driving. [17]

The figure of Rasmussen provides a heuristic framework for the classification of decision-making tasks under time pressure: skill-based, rule-based, and knowledge-based activities. These decision-making tasks are connected with varying levels of cognitive load—physiological, cognitive, and emotional. Physiological load can be data-driven through the measurement of changes in heart rate, heart rate variability, skin conductance, and skin temperature. Data are processed with the help of blood volume pat terns and other physiological data to derive cognitive load. Video games and virtual reality games pose a virtual environment for pilot training, in which human workload management should be implemented for the evaluation of pilot's performance and long-term adaptability in the domain of working memory (WM), multitasking, and cognitive control. There are many examples of the design on virtual environment games for the electrical or neurocognitive recording of correlates to cognition, or for the design and validation of neuro/thrombotic risk scores.

4.3. Factors Influencing Cognitive Load in Cybersecurity Interfaces

Cybersecurity breaches can quickly increase user multitasking levels, leading to heightened cognitive overload. Dividing attention between distinct security interfaces also exacerbates this already hazardous phenomenon, potentially causing network vulnerabilities if cybersecurity is not carefully activated [1]. Thus, Moran et al. designed a comprehensive conceptual framework as a pivot to meet all current trends of the multi-faceted problem of cybersecurity interfaces. The study identified the main factors influencing how to maintain control of a vehicle in adverse scenarios, the relationship between system feedback and driver

stress, and the dynamic and gradient design of adaptive cybersecurity interfaces. Choose different implementation strategies to achieve the same cumulative effect.Decision-making is moving in the direction of models and mixed methods, which provides a new student-friendly direction for future research in human factors research.

The first factor influencing the cognitive load on drivers related to cybersecurity systems is individual differences in cybersecurity risk assessment This refers to the different levels of cybersecurity vulnerability recognized by users, and their impact on risk management behavior. Without considering users difficulty coping with heterogeneity, AI-based decision-making would risk communication. Algorithms should be adopted to personalize user experience to reduce cognitive load or minimize errors [10]. This would have the benefit of operating the system homogeneously. In Figure 13, most users' cybersecurity risk assessments are moderate in friction due to the confusion ability barrier created by statistical adaptivity, while a few have accurate assessments, AI's effectiveness and reliability are difficult to verify due to these impulsive assessments.

5. Adaptive Strategies for Network Segmentation

Coope!rative MOBILITY ROADSIDE COUPLERS (MRCs) allow the RSUs to accept messages from different vendors. RSU's behavior can be also programmed; no data or control sent by CAVs to the RSU is going to be accepted and collected by it unless it is not really the communication ground. Meanwhile, extra control can be executed on the RSU to limit the number of vehicles that send messages unless the vehicle-to-infrastructure (V2I) communication flow charts are considerably larger compared to the rest and there are not buffer overflows due to the message's age. Clever designs can influence both the behavior and the purp!ose of the RSU despite the fact that the updates rely on the security of the number encoding the DRM function implementation, for instance, it is possible to set the percentage of traffic that must use the average deviation insertion bandwidth as a function of the number. Restriction to the number frequency-dependent encoding is such a disproportion among the unique identities that it can have an essential impact preserving the security applications of some messages. Another example is the random walk conducted by the MRC, this is the possibility of skipping MRSU01 Checkpoint and eliminate expensive decryption and authentication operations. Let a timed markers family follow the unconditional approach. New generation V2I communication networks follow a leap-forward with the proposed

periodic dominancies. This is demonstrated either through an analysis made on the mixedmobility vehicle associations in a V2I-controlled-only continent or from evaluations which also envisage a large variety of flexible and adaptable protocols intelligent cooperative vehicle architectures assuming vehicle ECU high cybersecurity assurance points to state-of-the-art encryption algorithms thanks to the capabilities embedded inside the edge AI. [8]'

From these studies, it concluded that when the FDI system is challenged with a considerable level of noise, due to a cyberattack inflow source which is undisaccompanied by knowledge of the real cyber threat zero measurements, the FDI process gets very ineffective and in cooperative automated driving environments, variability in the diameter of the social gap oscillates values which are not acceptable when approaching safety-critical objects aproximately between 3 and ~180. And similar cooperatively driven environment translates into small fluctuations of the volume edge within the social gap and hence also of the dynamics of follower MOBILITY NODE inbetween the safety-critical obstacle, also in the absence of an actual cyberattack. And only, in case of a cyberattack there is a remarkable increase in the phase-locking time.

' [20]'Safety implications of cyber-physical systems emphasize the importance of security features in autonomous vehicles. Network segmentation has, therefore, become increasingly important to ensure safety. Several islands of development have been established while discussing the different levels of network segmentation that could be applied across layers of the vehicle architecture. Network security standards have addressed the first two levels (e.g., ISO 21434, UNECE WP29, SAE J3061); however, the discussion becomes more imprecise in the higher layers of integration. It becomes increasingly complicated in heterogeneous architecture, where legacy safety-critical systems meet commercial-of-the-shelf (COTS) devices. Under such circumstances, the identified cognitive load physiology, i.e. intrinsic, extraneous and germane, along with network architectures, have been identified for cognitive load level assessment and adaptive strategies, to combine physical and cybersecurity research needs to improve the security and safety tradition inherited by the automotive industry. This approach should fit into a resilient and recoverable model to ensure the adaptability of the network and cannot be discarded with a first high-intrusive failure. [21]The strategy proposed in this paper is based on the implementation of domain-specific cognitive analysis to find "the best fit" for meaningful elements invoicing strategic value to the node. Therefore, the network is dynamically redesigned to exploit its vulnerability. Special attention is given to the security

landscape of complex and hybrid systems such as the ones in endorsed subscribing to the CAV philosophy. An intensive case study on the modern and practical Intelligent Transport Systems (ITS) and security of Cooperative Vehicular Infrastructure Systems (CVIS) mobility systems that embraces automotive cybersecurity standards/regulations is defined by the Automotive industry and professional associations worldwide.

5.1. Importance of Network Segmentation in Cybersecurity

[22] AV CS is an intelligent sensing system, versatile connectivity, and intelligent data processing system that employs algorithms to perform analysis that could provide an autonomous performance to the vehicle. This working of AV CS needs a real time and cooperative functionalities from several sensors, actuators, ECUs, as well from all the CoSs. This fully automatic and the real time cooperation between the CoSs fully depends on the Ethernet network linage systems. The high protocol and Ethernet signals through directly and through CCUs, further reduces the diagnosis time.[23] The rest of the paper is organized as follows: A literature review is presented in Section 2. A detailed explanation of a cybersecurity in the autonomous vehicle systems is given in Section 3 including automotive cybersecurity use cases. The classification, use cases and types of the cyberattacks in connected and autonomous vehicle (CAV) scenarios are discussed in Section 4 and Section 5, respectively. The cyberattacks impact assessment in the harmonious CAV environment is presented in Section 6. Next security measures and architectures are discussed in Section 7 followed by discussion and introduction of both generative and discriminative models for the security and privacy processes and its potential set of future work in Section 8. Finally, overall cybersecurity and privacy status analysis in the CAVs in Section 9 and a conclusion in Section 10.

5.2. Types of Network Segmentation Strategies

Network simplification methodologies help to reduce the number of components required in the complete version of the traffic model, but guaranteeing that traffic conditions are correctly assessed. Several studies deduce these models from data logs that maintain connection tracking over the network, using them to compute traffic loads at each of the routers. It is said that attraction and danger traffic flow models are the most used methodologies. Communication traffic between any pair of LANs in the network can be aggregated and estimated through aggregation that responds the EW. EW is computed by drawing weights

for the end points of each connection from a uniform [0.1] distribution. Traffic exchange modelling... flow traffic, flows of flows traffic, P2P traffic and malicious Pakistan intruder traffic and MISC traffic. [24]

The communication profile. When network communication is an essential part of the security perimeter allocation, the classical approaches compute the allocation of all the communication profiles. As many real scenarios are not feasible in the case of security perimeter assignment. It is important to obtain the security pilots that their resource consuming is high only if the network elements are included in the same security zone. When a network node sends information to another, the receiver security perimeter must be equal or more restrictive than the protections applied on the information at the sender. [25]

The evaluated information. The security perimeter assignment of a system, including its nodes, specifies the classified (or confidential) information that the security services are protecting against network attacks. A node can access the information derived from the security perimeter to schedule the transmission in an efficient way.

Security perimeter design requires an organization to define the characteristics of various groups of elements (also named zones) according to their risk (or security requirements) and the networking characteristics of the components (ie, load, quality). To cluster together network elements that exhibit similar security requirements reduce architectural complexity, improve system scalability, and allow the possibility to apply efficient security services based on the calculated requirements for each security perimeter. To cluster together network elements with similar network requiriments (traffic, latency and bandwidth) allow network nodes to mutually communicate and therefore avoid keeping the computation of the security perimeter derived from the security requirements. The assignment methodology defines:

5.3. Adaptive Techniques for Dynamic Network Segmentation

More sophisticated mechanisms like trust-level signatures and routers could further distinguish secure traffic between zones without going need of the signature of the Gateway. Today, most ECUs use a Basic Assurance Level SAE J3061 compliant Secure Boot process which, if correctly configured already prevents a significant percentage of the threats an adversary could carry out if they gained physical access to the Vehicle. SAE J3061 advocates the Data and Control Plane Model. In the data plane model, the configurations allow the

device to only handle intended sensitive read-write safety critical Touch Points, device-internal COP based Memory Shadowing Data and messages from only known-to-the-vehicle valid sources. In the control plane model: ECUs validate message routing using security credentials like Diagnostics Security Access and Network management message Validation. So the EWV-ECU checks message routing information and blocks unauthorized messages while the secure internal communication between interconnected ECUs is also also boosted by Authenticated encrypted channels using two-way securely originated Known Boundaries and Assertion. System Control In the control plane also verifies that any modifying system configurations or disable physical chip security integrity or field security configurations occurred using Keys encrypted management control messages if a negotiation security variant level with higher levels of user interaction is not faulty which would potentially cause an intended security vulnerability.

Autonomous vehicle control systems often use manufacturers' proprietary in-vehicle networks, like the Bosch Controller Area Network (CAN) and CAN-FD interfaces, and Gateway modules to communicate with multiple interconnected Electronic Control Units (ECUs). The ECUs may be used for networking, telematics, body communication, control and monitoring of chassis, powertrain controllers and some vehicle safety equipment. While the existing networks and multiple ECUs are sufficient for the vehicle to function as a standalone system, the autonomous vehicle also minimally needs to be connected to external systems such as those managing navigation inputs, and updating maps and firmware Over read write access. Please contact us at chatsupport@springernature.com. One approach to managing network safety is to enforce dynamic network zone segmentation. Network segmentation ensures that effective firewalls, IDS/IPS, network access control, and network logging appliances can monitor and block unauthorized network traffic transactions, as well as manage and ensure that the vehicle communications architecture is no longer flat but follows a more sensible Layered Approach. This would segment the vehicle's spatial communication network into zones meant to be mutually isolated except through the Gateway. In a segmented network, traffic that is e.g., classified as from the Navigation and Telematics Zones could be permanently separated from Safety Critical and wEVE Data Zones and only be able to communicate with them through the Gateway. This would include messages like those coming from a cellular modem's cloud connection.

6. Case Studies and Experiments

Adding an emotion expression recognition feature to the eBIZ 4.0 platform will provide an automatic detection of user emotions and a decision support to the operator within 2 seconds in the case of a part or assembly operation. This paper shows the design of a database for research in HCI and affective computing. Cognitive load analysis of cyberphysical systems is a state-of-the-art topic with the increasing use of Human-Computer Interaction (HCI). This is true also in the automotive domain, where Cybersecurity (CS) and Human-Interface (HI) predict human interaction considering ergonomic and intelligent solutions. The work, entitled A discrete-event simulation model for driver performance assessment: application to autonomous vehicle cockpit design optimization, proposed and validated a Des model for the analysis of cognitive loads and attention in automated driving systems, integrated with a cooperative graphical interface adapted to the predicted mental status of the driver. What is missing in the state-of-the-art is a real-time comparison of existing HCI for active CS in HI for autonomous vehicles, proposed by text recognition technique, as a potential increasing of cognitive load, result of the HCI that is useful to lightweight and shallow protocol.

[16] A Discrete Event Simulation (DES) model of car-driver interaction is proposed for car cockpit layout optimization in terms of user comfort, physical comfort and driving efficiency. A theoretical model of driver cognitive load is integrated in the DES model to predict the mission success rate in the alternative car-cockpit architectures. The model is based on Analytic Hierarchy Process (AHP) and allows the estimation of the influence of architectural factors (namely age, driving experience, screen's luminance, fonts dimension and contrast, user's objective,…) on the driver's operation time, performance and waiting time. This original solution is validated by a real case study. [17] In this work, the applicability of the four previously described experimental paradigms based on the detection-response task for the assessment of driver cognitive load while interacting with in-vehicle information systems (IVIS) has been outlined, covering the different cognitive load levels imposed by the cognitive task and commensurate with the influence of the driving situation on participants' behavior. UulmMAC is a multimodal and multichannel multimodal database of audiovisual recordings of spontaneous emotional expressions for the application in affective computing in HCI. The database already includes many recordings as well as pre- and post-processing results from technical processes in which essential physical and computational aspects were taken into account.

6.1. Real-world Implementations of Adaptive Network Segmentation

Car door control systems (DCSs), later considered as E/E architectures case studies, are used in this work to demonstrate practical implementations of principles of network segmentation, with this separation mode devoting itself to being implemented on automotive switches [26]. We conceive of concepts following a build-to-the-needs paradigm with adaptability and future measures being practice-oriented protective methods against attacks. It is demonstrated that tapping flows of real network traffic can bypass dedicated physical security measures if these measures are not end-to-end realized anyway. With the presented experiments, we show that one can subdivide network assessments to characterize effects on traffic routing. Such routing efficiency is essential for the wide-spread establishment of R-NS as proven within our E/E architecture case study. It is also shown in our actual setup that certain changes of real-world interconnections, in particular at certain implementing network segments, may help raising attack detection rates and lowering reasoning error rates.

The automotive industry is among the fastest changing industries of the present decade. Apart from issues related to climate protection, sustainability, and shifts in mobility behaviour, major issues include digitization and the aspects of information security. This reveals a growing discrepancy between currently available security measures and the rapidly changing threat landscape. It has been shown that aspects of information security need to be incorporated within the development of technological platforms for future on-demand mobility solutions, no matter if such offers are based on conventional cars, electric vehicles, or self-driving cars [21]. Consequently, in the automotive industry, requirements on secure information flows over platforms like automotive buses and the infrastructure at large, change extremely fast. It is for this reason that this article discusses reactively secure and adaptively secured automotive Ethernet, including a new hardware and its conceptual extensions (SOFC, IRRR), hardware adapters implementing network segmentation (DCCP), a network segmenting automotive switch (RAB-SWC), specified security protocols for automotive network segmentation, network- and protocol-level security risk assessment with the composed concept (R-NP-R), and a security system for detecting automotive cybersecurity in practice. All these aspects are demonstrated within dedicated use cases such as car door networks (DCF) and E/E architectures, all of which satisfy automotive standard ISO 26262 (ASIL C) requirements [27]. A prevailing, comprehensive understanding for network segmentation in automotive Ethernet (ASE) and principles at which IT-security mechanisms,

systems, and concepts at large need to be applied and developed is by far missing in public research and scientific discussion.

6.2. Experimental Studies on Cognitive Load in Cybersecurity Interfaces

A large variety of modalities such as audio, video, or physiology signals are employed for the development of multimodal datasets [28]. The latter type of information concerning human affect, stress level, or cognitive load can be vital in providing assistance. It has especially become important in recent years regarding various Human-Computer Interaction (HCI) systems, which can even frequently allocate the omission of the input sensors used for enabling situation- and user-adaptive capabilities, without violating new legal European regulations regarding privacy sensitive information withholding in milliseconds. Given all these challenges, often the prediction capabilities of the models that are trained and designed to assess the mental burden people experience by interacting with any system are considerably affected.

For the consistent performance of reliable and robust sensor-based security methods in real-time, vital importance is laid upon the elimination of undesired information that results from the interference of various types of noise such as environmental noise and interference during the operation of the system. In this study, an attack-aware multi-sensor integration algorithm has been presented and applied to autonomous vehicle systems that are interconnected with a wide range of sensors, including Motor Control Unit (MCU) diagnostic sensors, to detect and isolate sensor faults [15]. In the first stage, unscented Kalman filter (UKF) and Gaussian Mixture Model (GMM) are used together in order to isolating sensor faults on MCU. Thus, taking a common vehicle cybersecurity scenario comprising a remote cyber attack on the electronic control units (ECUs) of the autonomous vehicle into consideration compellingly demands incorporation of a specifically outlined cybersecurity unit by integrating with: the navigation sensor that is, indirectly steering sensor that is, directly related to the cyber attacked ECU, and fuel level sensor that is related to the MCU, thus substantially involving little redundancy element between the sensing and actuation layer.

During the study utilized a relatively simple problem scenario to keep the number of interfaces and tasks to a manageable size. Specifically, we considered three pairwise indicators or alerts requiring the operator's attention: two regular alerts, such as lane departure and backward vehicle threat, and one cybersecurity alert about the threat of a remote cyberattack

on the vehicle [6]. Similar to the problem scenario of the first study, we designed the task to require the participants to proceed forward in their lane while being attentive to the instructions displayed by the simulator's interfaces. To compare the cognitive load imposed by the task of processing cybersecurity alerts to other, more typical, vehicle-related tasks, we added two control conditions to the experiment. The first control condition involved the original task of monitoring the two regular alerts only. The second control condition was further designed to be less demanding compared to the first control condition, because it required the subjects to pretend they were leisurely driving. The latter condition was included to provide an ideal psychological baseline for other conditions relative to which their increasing cognitive load could be evaluated with greater precision.

7. Discussion and Analysis

There are multiple implications from the cognitive load analysis presented in this chapter. For example, the versions of the status display should be more intuitive and display multiple negotiation agreements between the version and car manufacturer. The engineers should conduct efforts to monetize the amount of cognitive load that the skyline display version adds. Another consideration is that the user will make petter driving-related decisions with the skyline default version as it provides relevant information which makes it easier for the user to judge the current security posture of the vehicle. Further studies here will primarily address the concept of device associations within our study. We posit that, by managing a stronger connection and understanding user's context, the designed future interfaces could influence their decision- making potential – a prominent target for improving well-being benefits [29].

[5] This chapter showcases the results from a quantitative observational study to obtain an understanding of the impact of cybersecurity user interfaces (UIs) on human factors. Three distinct sections formed the main focus of this chapter. Firstly, we carried out a load analysis to understand how much cognitive load (of a human) the default and alternative cybersecurity UIs for status displayed impacts. Overall, a lower average cognitive load was exhibited by users for the default (HM) UI than the alternative UIs. Secondly, we explored the time that users took to complete the primary tasks and the overall usability of the interface. The results demonstrated no real significance in the time taken by the users to access a UI to perform a critical task for all agents. Finally, we analyzed how the context supplied by the default system

impacts the quality of the user's decision-making capabilities and thus ascertained the trust and confidence users had in the information provided [30].

7.1. Integration of Cognitive Load Analysis and Network Segmentation Strategies

Cognitive load classification was successfully evaluated in order to take a significant step in the roadmap towards reliable state-of-the-art decisional mechanisms that may come in handy automakers and Advanced Driver-Assistance Systems (ADAS) manufacturers for the enhancement of safety of the transportation road domains [31]. Road accidents are often caused by driver-related factors. The data are produced in normal driving and distraction caused due to reading. Early identification of the distracted drivers and taking a defensive action were proposed. Therefore, simple experiments were carried out and the physiological signals ECG, GSR and vehicular features obtained from the car control interface were measured in autonomous vehicle control settings. Stimulus onset synchronisations were observed in the cognitive load observer.

Beside the immediate consequences for car manufacturers, the automotive industry could see potentially long-lasting repercussions after recent hacking attacks targeting connected and autonomous vehicles [32]. Automotive cyber security incidents have been unveiled since years with potentially critical consequences harming passengers and interfering with normal vehicle control. Moreover, recent hacking evidence has stressed the scenario of public dissemination of ransomware for connected-and autonomous vehicles and legal demands for features disabling user access to personal and/or mobility functionalities proportionate to services and privacy violation.

7.2. Key Findings and Implications

[10] The comparison of three different interface designs in understanding how typical dashboard display interfaces for the rear camera contribute to deal with pressing button secondary tasks while driving in a highly autonomous vehicle has shown, through the system model, long and medium-term retention periods and in the context of time pressure, a comparable number of performance improvements. The exit increase on account of the operational simplicity in a pressing button task decreased all response times. In the rear interface with menu naturalistic environment while driving, better operational safety was confirmed intuitively because the time needed for button operation decreased, or the DRT

method predicted its cognitive response for subsequent mental tasks.[17] The smart seat to reduce cognitive load and driving distractions. The ReDriving Safety Intelligent Seat used the headrest, seat cushion, and pedal cover as input/output devices to support the operator's ability to stay focused and keep seated while driving; Amazon Rekognition and voice input were used to determine the driver's cognitive independence. Emotional control and virtual parent interfaces were provided to increase and decrease cognitive load, respectively. Adaptive human-computer interaction systems can improve traffic safety by considering drivers' cognitive state. Evaluating driving load involves analyzing driving performance, response times, eye movements, and physiological and psychological indicators.

8. Conclusion and Future Directions

elli_nikolaou1.pdf

This study confirms previous findings from HMI research in AVs as well as in driving and simulations. The more the vehicles rely on autonomous systems or even become self-driving, the more important the role of the human in the communication system becomes, in developing seamless human-machine interaction. The analysis of the interfaces of AVs is performed by applying a constructive-sorting method, and captured significant differences between the interfaces of the manufacturers. Furthermore, three critical themes emerged that may impact user satisfaction with the interface and inhibit downloading of cognitive resources from the interface: anxiety and stress-sourcing factors; deflection by the medium; and forgotten expectations. There is therefore a risk that the communication between the AV and the user becomes a cognitive burden, during which the user worries more about the decisions already made by the AV and less about optimally exerting those that remain.

[12] [6] This paper presents an analysis of interface designs found in AVCSs in order to identify potential human-machine interaction (HMI) challenges resulting in cognitive load. The analysis serves as a basis for future experiments with human participants in a virtual driving task and seeks to critically investigate the cognitive load that might arise from interaction with modern automated vehicles. The findings show that AMs often provide strong emotional satisfaction and enhance users' overall experience. However, some form of annoyance still persists, usually in relation to the need to interact with the AM at all, with technology temporarily failing to understand input and output issues. When such experiences

are also seen in AVs, such as when using the interfaces that are the focus of this study, they may put additional cognitive load on the user.

8.1. Summary of Findings

Furthermore, the rush to launch driver-assistance systems on the path towards self-driving cars has created a number of safety problems as well as advantages. In fact, autonomous vehicle control systems (AVCS) rely on the user's trust and management, which means that the adoption of AVCS by users depends on how much they trust them. Researchers should develop more comprehensive, rigorous, and comprehensive Cyber-Physical Systems (CPS) evaluation and analysis techniques, and balance security and privacy to increase policies and strategies. It can support general complete causality based on cross-domain and cross-platform attack vectors between vehicle, future infrastructure, and the attack surface of driving platform [13].

Automotive cybersecurity is a critical concern in modern cars with advanced driver assistance systems and connectivity features. The automotive cybersecurity threats have evolved and increased in sophistication, and a new set of vehicle attack surfaces have emerged. Our findings suggest that the complexity and scope of cybersecurity issues in are multifaceted and include not only the vehicle's module connections and network faces, but also the vehicle-to-infrastructure connectivity, infrastructural security, and external environment safety. The research community needs to focus on factors such as the safety and security issues in intelligent vehicles, the development, production, traffic control, parking, and modification of the specific conceptual model, and vehicle systems that need to be focused on, in order to obtain safety-critical system security and privacy issues [33].

8.2. Recommendations for Future Research

Adversarial machine learning (ML) attacks pose a significant concern for the security of autonomous vehicles because of the potential catastrophic consequences of attacks. This underscores the need for secure and resilience-by-design autonomous navigation and control systems, including low-level safety-critical functions. Resilient and secure autonomous systems must move from digital protection and detection mechanisms towards HCRM cybersecurity approaches such as: real-time cognitive load monitoring, the use of soft and hard security adversarial machine learning models and prognosis and strategic decision

making in the presence of adversarial machine learning attacks and human-factor-conscious safe-by-design adversarial ML countermeasures in secure autonomous driving scenarios. Research can be extended beyond simple SIL/HIL/ bed tests to railway, drone, airborne and spacecraft traffic and control systems. A full compliance of the proposed methodology and criteria within Magistrale Program intense short course projects in real-time, state-of-the-art problems can be very interesting to be conducted.

Security is achieved not only by technical solutions but also by setting codes, standards and regulations. Beyond certain regulated requirements and security standards, cybersecurity can also be positively addressed in-vehicle interfaces [33]. The enhancement of cybersecurity in autonomous vehicles can also be achieved at the human–vehicle inter- face (HVI) level by potentially supporting practices that increase driver cybersecurity awareness, such as visualization and warning systems. To this aim, user experience design principles should be followed by considering potential human factors which are useful to indicate potential vulnerabilities within cybersecurity.

9. References

Furthermore, a new approach is presented to measure the cognitive load arising from the constant interaction with the Cybersecurity Assistant. The system is about highly automated driving (SAE level 4) in a defined area with the necessary and necessary and sufficient measures that have to be put into place to deliver autonomous drive in public space. The modular components of all passenger compartments are ideally decoupled from each other. However, a very important safety aspect of highly automated driving is that the passenger compartment must be linked to the rest of the vehicle via security- (from attack) and safety-related (e. g. airbag deployment) interfaces only. This is addressed in a joint DFG research project between the departments MGSE at the Hochschule München and Mechatronik at the Technischen Universität München. This research is focused on not only determining the necessary measures which must be taken in the gateway, but also proposing a systematic approach to derive concrete security mechanisms with individual brightness for different messages/interfaces that cross the gateway. [34]

The work developed cyber-resilience strategies to protect a reference architecture for connected and automated mobility (CAM) from cyber-attacks on interfaces with communication partners. Also, we are enhancing the Cyber Resilience Working Group at this

time with penetration testing from the cybersecurity research area on collaborating with EDAG/ Böblinger Consulting on risk analysis data from the Automotive Security Research at OEMs and Tier 1 suppliers. The CAM Defense WG plans to provide a gap analysis of cybersecurity measures and to analyze and choose best practice countermeasures. Investigating the state of the art in cybersecurity, and analyzing new trends in cyber-resilient defense CAPSIM can provide recommendations and assist the members on protecting their CAM ecosystem. [2]

The transforming transportation with autonomous vehicle technology brings untold benefits to humans, alleviating human errors, reducing environmental impacts, and enhancing the overall efficiency and safety in the ecosystem of intelligent transportation systems. For this brand-new promise of autonomous vehicles to drive on public roads, besides the traditional key technology concerns such as perception, decision-making, control execution, connected and automated vehicles (CAV) also extend tough challenges with cybersecurity, mainly on account of so much more opportunities and exposure to cyber-attacks.

References:

1. Sadhu, Ashok Kumar Reddy, et al. "Enhancing Customer Service Automation and User Satisfaction: An Exploration of AI-powered Chatbot Implementation within Customer Relationship Management Systems." *Journal of Computational Intelligence and Robotics* 4.1 (2024): 103-123.
2. 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.
3. Perumalsamy, Jegatheeswari, Muthukrishnan Muthusubramanian, and Selvakumar Venkatasubbu. "Actuarial Data Analytics for Life Insurance Product Development: Techniques, Models, and Real-World Applications." *Journal of Science & Technology* 4.3 (2023): 1-35.
4. Devan, Munivel, Lavanya Shanmugam, and Manish Tomar. "AI-Powered Data Migration Strategies for Cloud Environments: Techniques, Frameworks, and Real-World Applications." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 79-111.

5. Selvaraj, Amsa, Chandrashekar Althati, and Jegatheeswari Perumalsamy. "Machine Learning Models for Intelligent Test Data Generation in Financial Technologies: Techniques, Tools, and Case Studies." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 363-397.
6. Katari, Monish, Selvakumar Venkatasubbu, and Gowrisankar Krishnamoorthy. "Integration of Artificial Intelligence for Real-Time Fault Detection in Semiconductor Packaging." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023): 473-495.
7. Tatineni, Sumanth, and Naga Vikas Chakilam. "Integrating Artificial Intelligence with DevOps for Intelligent Infrastructure Management: Optimizing Resource Allocation and Performance in Cloud-Native Applications." *Journal of Bioinformatics and Artificial Intelligence* 4.1 (2024): 109-142.
8. Prakash, Sanjeev, et al. "Achieving regulatory compliance in cloud computing through ML." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).
9. Venkataramanan, Srinivasan, et al. "Leveraging Artificial Intelligence for Enhanced Sales Forecasting Accuracy: A Review of AI-Driven Techniques and Practical Applications in Customer Relationship Management Systems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 267-287.
10. Makka, A. K. A. "Implementing SAP on Cloud: Leveraging Security and Privacy Technologies for Seamless Data Integration and Protection". Internet of Things and Edge Computing Journal, vol. 3, no. 1, June 2023, pp. 62-100, https://thesciencebrigade.com/iotecj/article/view/286.