Artificial Intelligence for Predictive Change Management in Information Systems Projects: Cognitive Load Analysis of Cybersecurity Interfaces for Autonomous Vehicle Operators

By Dr. Byung-Woo Kim

Professor of Automotive Engineering, Korea University, South Korea

1. Introduction

The integration of cybersecurity interfaces within autonomous vehicle systems presents significant challenges, particularly in understanding the cognitive load on operators. This study investigates the impact of command, control, and monitoring interfaces (CCMI) on the cognitive load of both expert and novice operators within an AI-driven Predictive Change Management framework. While prior research has largely overlooked this aspect, our work evaluates and compares the performance of various cybersecurity interfaces by utilizing actors from different user groups. By analyzing cognitive load data from experimental mock-ups, this paper offers valuable insights into how AI can optimize interface design to enhance user performance in dynamic, change-driven environments. The findings also support the certification of interfaces for human factors engineering, ensuring that both novice and expert operators can manage cybersecurity effectively during organizational transitions in autonomous vehicle projects.[1]

Cognitive Load Analysis of Cybersecurity Interfaces for Autonomous Vehicle Operator[2] Autonomy in many vehicles ranges from low levels where it offers driver assist to full autonomy where no driver intervention is expected. The autonomous system in the connected and autonomous vehicles (CAVs) is operated at one level of autonomy of partial to full automation with a human operator. In case of an autonomous vehicle, the human operator has to be ready to take over control in case of a system failure and, in case of a partial automation vehicle; the human operator has multiple tasks at hand: monitoring of the environment, controlling the vehicle, and monitoring the highly automated system. Thus, there is already a high cognitive demand in operating autonomous cars [3]. The introduction of cybersecurity uprisks the passive threat like sending unauthorized data packets to active threats like injecting virus and malware. In this scope, efforts are being directed by the research community to the enhance the proposals for Command, Control and Monitor Interface. Analogously, cognitive load studies are widely conducted in various real-time system cockpit interfaces. It is important to note, that such nomenclature term used is dependent on the drive by suggest relation between nomenclature term used and mandated certification.

1.1. Background and Rationale

These sketchy considerations motivate a detailed study of the issue to analyze the security aspects of an embedded System-on-a-Chip (SoC) defensible protecting the VCN ecosystem. Any high-performance Real-Time Operating System (RTOS) with minimal execution overhead, such as e.g., MDV3, needs to ensure a reliable/secure execution, which forms a line of passive and active measures against threats and attacks by a complex adversarial model [4]. Regulatory bodies in the automotive domain devise standards and guidelines concerning functional security and directly related safety matters, e.g., ISO 26262. However, security "absorbs" safety, eventually extending the scope of these standards across the whole electrical, electronic, and embedded software in vehicle. Hence, a basic automotive security standard was released in 2018, motivated by the automotive environment's high complexity and connectivity, i.e., ISO 21434. There still are numerous mandatory security check-ups like network attacks evaluation during a vehicle's type procurement. However, apart from Internet-related attacks, other exceptional, still-incomplete danger sources are under retired consideration only. For example, sensor attacks are preferably examined only in the quality-related domains. Thus, the quality among domains is guarded by several approaches, such as hardware-in-the loop (HiL), model-in-the-loop (MiL), and software-in-the-loop (SiL) [5].

In recent years, the automotive industry has experienced a considerable evolution regarding autonomous driving, where the vehicle may assume the driving task at different levels from performing low-speed convoy driving to advanced levels of full automation under different driving conditions such as highways, urban or rural roads, parking, etc. These complex systems require more capable and autonomous control methodologies allowing, among others, the monitoring and re-planning of safety-consequence critical sub-tasks in a coherent and reactive way. Under all of these operational domains, it is clear that every vehicle's subsystem must ensure a proper control and supervision execution [3]. Nevertheless, new vulnerabilities and threats have arisen since the introduction of this new hazardous and extended connected environment, i.e., the Vehicle-Communication Networks (VCN). It is imperative to provide mechanisms to protect this critical infrastructure, including the security of data communication, considering a wide range of vehicular applications.

1.2. Research Objectives

Nevertheless, the initial proposal of the socio-technical analysis should be extended for a better consideration of these concepts for the design and assessment of Autonomous Vehicles, with a focus on the design (where the burdening of the sensor is likely to be minimized by MO-RO-based cognitive (and smart) combination of different sensors) these dispensable data taking are likely to be optimized design, that how should the final open door interfaces of the autonomous vehicles be assessed in order to guarantee that the operator's unsafety due to unsure focus or fragmented attention does not occur. Keep in mind that, in this work, the design of the autonomous vehicle is taken as already set and finished, as done here in line with [6], with the emissions-objective electric trains without drivers and with dynamic promotion for the safer planning of the human–machine interfaces in the consideration of the MLS–VIP categories. Therefore, it should be noted that the final evaluation of the cognitive safety of the "driver" (where the quote mark reports about the meaning difference due to the long time driverless driving time on board, better the autonomous vehicle operator) of the autonomous vehicles is taken as the main novelty and original contribution of the current paper. Building on the insights of Peddisetty and Reddy (2024), who investigated AI's role in predictive change management for IS projects, this study explores how AI technologies can enhance change management effectiveness.

The contribution of cognitive sciences to the study of the broader aspects of human interaction and involvement in technology-assisted activities, and most specifically in the design of Cyber-Physical Systems (CPS), is an emergent issue with its quantitative application to average human users not in favor. Nevertheless, in the literature, computer-aided tools and methodologies for analyzing cognitive load have been widely disseminated. In fact, different aspects of a workload in a vehicle (regarding e.g. reading an objectively difficult instrument or navigation activity) have been classified according to Hall's cognitive load categories [7]. In this context, it does exist an international standard which provides guidance for cognitive and perceptual aspects, including those aspects pertinent to human cognition, that are important for the design of physical and computation-based devices [8]. Therefore, this study aims at schematizing the canonical application of such a multiple-source elaboration standard to ROS-based (Robot Operating System) applications of the Cyber-Physical Systems.

2. Autonomous Vehicles and Cybersecurity

These three built-in systems are also the weak points against which potential cyber-attacks can occur. Cyberattacks can directly target self-driving cars or attempt to disable LIDAR, RADAR, ultrasonic, and GPS sensors. Attackers can induce random errors, delays, and lung attacks on sensors. These attacks lead the perception system to capture incorrect information and provide incorrect location and speed data flow through the Control and Decision-making systems. As a result, the vehicle can switch from the correct lane to the opposite lane, and accidents can occur. The most significant risk of man-in-the-middle attacks is that they create a data grid between the controller and the processes which can manipulate the information flow. The control system and the self-driving vehicle directly interact with the physical environment and many smart device networks with two advantages. 1) They change the environment by performing actions to reach the destination. (2) They collect information about the environment to make inferences. Vehicle-to-Vehicle and Vehicle-to-infrastructure applications, as well as vehicle-to-everything communication, are designed to solve problems in today's traffic [9].

There are three main built-in systems in a self-driving car: the perception system, the control system, and the decision-making system [10]. The perception system is the vehicle's "eyes," responsible for capturing information about the world around it via sensors such as cameras, LIDAR, and RADAR. The control system is responsible for executing the commands given to it by the mission planning system and executing the necessary control actions that translate the given commands. The mission system is where the vehicle decides to send the control orders to the control system by combining the captured data and deciding on the course of action to be taken.

2.1. Overview of Autonomous Vehicles

The automotive industry has recently started to undergo its own form of digital change—the resulting new mobility models play a fully networked role within the scope of potential future car developments. With potential future fully autonomous driverless cars in mind, there needs to exist an intrinsically safe and solid automation of road traffic. Here within the newest digital architectures, latest communication, and transmission technologies play a significant role. This is accompanied by new digital telecommunication technology: 5th Generation (5G) mobile network communication. There, the introduction of 5G mobile network communication as carriage / transport technology will offer the exchange of data at high transmission speed and minimal latency. Hence, there will albeit remain an actual telecommunication anchor between surroundings and vehicles (to implement complex applications such as intersection motion), but mainly telecommunication will further migrate from vehicle to vehicle and also encompass every device within the scope of so-called Internet of Things (IoT) type of concept.

The automotive industry is experiencing a digitalization process based on revolutionized mobility models, such as Mobility as a Service (MaaS) and car sharing [11]. As a result, the focus is shifting towards connecting vehicles and gradually automating road traffic to create safe and reliable fully autonomous driverless cars. The current extensive digitalization inside the vehicle will necessitate addressing multiple functional areas, such as modern in-vehicle communication networks (IVNs) and cybersecurity. This paper provides an answer to the question "what could be core cybersecurity attacks and issues within the future digitalized vehicles?" The ground idea in this study is that, at first, there will be various vulnerabilities together with the in-vehicle networks in all current and future vehicle generations. Also, as it is shown based on the reviews of recent attacks and vulnerabilities available in the literature, the IVN attacks could affect the entire vehicle functionalities [12].

2.2. Importance of Cybersecurity in Autonomous Vehicles

The paper [13] outlined the immediate need to enhance security in autonomous vehicles and showed that although cybersecurity technologies have significantly improved in the past decade, research focusing in-depth on vehicle cybersecurity is relatively limited. The authors highlighted that Autonomous Vehicles (AVs) are more vulnerable to cyber-attacks compared to traditional vehicles since AVs are equipped with software-based subsystems on top of traditional hardware. As a result, model-based attacks and data attacks are some of the potential vulnerabilities in AVs. Threats such as DoS (Denial of Service), false data injection, timing alteration, and malware insertion could disfigure data coming into the car, affecting the perception, decision-making, and control parts of the AV's driving framework. As a result, operators' visual perception and decision-making might fail to recognize a non-existing problem while performing any life-threatening maneuvers which could seriously affect the safety of the AVs [2]. Additionally, the authors summarized that cybersecurity technologies aim to protect networks, devices, and programs from attack, theft and damage of data. In comparison to the defense mechanisms in traditional vehicles, AVs employ various techniques such as behavioral modeling, deep-learning-based anomaly detection, deep-learning-based intrusion detection, and so on. Thus, an individual or group can control the unauthorized ways to access vehicles to avoid any cybersecurity risks efficiently [14].

3. Cognitive Load Theory

The design of this study using a mixed method makes it innovative. The VR interface and the interface-independent quantitative cognitive load measurements can complement each other. Either ones' results can be inappropriate to provide a complete conclusion but combined, rich inferences can be made. Regarding our methods, the VR interface was evaluated at four different cognitive load conditions using quantitative measures and then by experts through qualitative interviews. Our results indicate that the VR interface imposes additional cognitive load upon operators' visual working memory, which may result in the degradation of their real safety-critical tasks, managing cybersecurity for autonomous vehicles during their operation. Furthermore, we provide active guidelines for designs of safe cybersecurity interfaces after a careful examination of the results [5].

We design a VR interface for autonomous vehicle cybersecurity monitoring. Our goal is to evaluate the interface from the cognitive load perspective. Human cognitive load, the amount of information processing imposed on working memory, is the theory's driving force [15]. It has been used traditionally to evaluate different interface modalities in safety-critical domains like aviation, medicine, and military. Here we apply it to autonomous vehicle cybersecurity where similar concerns are present. The two primary objectives of the mentioned study are to examine the information processing imposed by the interface while a human operator uses it and to explore if variations in cognitive load are associated with participants' cybersecurity management performance. We assume that higher load will degrade the operations.

3.1. Definition and Components

According to the generative model proposed by Young and Stanton [16], extraneous and intrinsic components of cognitive load are dependent respectively on the qualities of a cognitive task, and on individuals' peculiarity/differences, mainly related to cognitive abilities, skills, and knowledge. Instead, the mental effort devoted by the learner to successfully achieve a cognitive task is called germane cognitive load, and depends on the regulation of individual cognitive activities. In other words, extraneous and intrinsic cognitive load are responsible for the mental effort imposed by an instructional design or by a task, while germane load is engendered by the regulation of these resources.

Cognitive load is a multi-dimensional, multi-componentialer construct that represents the load on working memory during a cognitive task. In this context, working memory is the cognitive system responsible for the control, temporary retention, and manipulation of information received from sensory organs or retrieved from long-term memory. According to cognitive load theory [17], distinct capabilities of working memory resources are separately dedicated to perform distinct cognitive operations, such as processing of information germane to the task (intrinsic load), or to manage the cognitive operations needed to handle extraneous information helpful for learning.

3.2. Relevance to Human-Computer Interaction

[18] To some degree, the experiment findings on driver's cognitive demand in general might not just rely on the relevant domain according to the target of the driving data because the environmental visual question might distract him. Also, those brainpower could simply go way of vehicle control activity. In other words, we could tell a driver's cognitive effort in working while he is driving based on measurement of brain biometric characteristic. A research program explores new options for brain biometric-based measurement of driver's cognitive effort indicator, including qualitative electroencephalogram (q-EEG) main wave on driving a continuous tracking task and d_PREDICT for drivinglicate the longest interval of time domain detection-response task performance in driving while the protocols.[19] The driving safety-oriented field is driving task, while, other cognitive-active information with his attention occupation then induce Diverted attention, could make a driver himself Rocket risk Thus predicting and preventing this kind of diverted driving factors has been a focus of the Transportation safety exposure research field. External cognitive demand test mind, we separated the Drivers Binary cognition Operating in the two cognitive tasks and analyzed

patient Implement kinetics and the Brain characteristic of the reaction. Its is determined that on the basis of an accurate reading extensive cognitive resources. Certain situational may lead to Diverted attention drivers the Market for visual and cocktails Prions, by predicating the effect tools could submit to the estimated Other Homicides Rates.

4. Methodology

The choice of methodology to evaluate the impact of either new automation or new human-machine interfaces has mainly been backed by two approaches: the Operator Load Model, as proposed by the Swiss Cheese Model, and the Driver's Activity Model. Even though relevant and interesting drivers' data are acquired in naturalistic studies, driving simulator studies and field operational tests, researches are lacking on actual data from the operation of autonomous vehicle. For the development of human-automation interaction, methodology and methodology validation are thus desirable. In their study, Engström et al. [17] worked as a driver in an L3 experimental vehicle equipped with five different interface solutions: A. Control panel, B. Steering wheel buttons, C. Side screen with touchscreen, D. Driver's image in HMI, and E. Steering wheel buttons and side screen. They performed the driving task one time for each interface and on each route, adding in additional tasks on some sections-the Raven test, the Operation Span test-in the random presentations. By recording their performance and subjective impressions when handling the interfaces, Engström et al. aim to further the understanding of the cognitive load induced by control, interface and automation design in autonomous vehicles.

When considering human error in the domain of autonomous vehicle operations, it is useful to apply the Swiss Cheese Model, which explains how accidents and incidents are not caused by a bad person or set of individuals but rather a set of 'holes' – individual weaknesses present at different stages of system operation aligning to result in adverse consequences. In their application of the model to the automotive domain, Ferdinand, Engström, and Kolamyasenkov [20], divided operator load into five groups: work load, task load, information load, communication load, and mental load. Their research also proposes that as operator workplace environments become more complex, the amount of information gained from vehicle systems also increases. Hence, proper communication is achieved by choosing an appropriate amount of information relevant to the task at hand and finding ways for this information to stream inevitably to the operator.

4.1. Research Design

Operators of technically complex systems often need to monitor quite large sets of quantitative and/or qualitative data in supervisory control to detect more or less subtle system states deviating from normal ones. The amounts of data that need to be captured have increased widely addressed, and a lot of additional monitoring techniques are available for systemic contributions from human–machine interactions summated in the overall load of human operators. Nowadays, controller to system like autonomous vehicles, automated industrial machines or B-presses evolves one step further towards more or less autonomous or possibly fully automated 24/7 and autonomously operated systems. The original operator role shifts from active control towards more or less passive monitoring, possibly only in case corrective actions are necessary operators are forced to intervene [5].

Operators of technically complex systems often need to monitor processes to detect system states deviating from normal ones in supervisory control. Nowadays, many systems evolve towards more or less autonomous systems with the aim to reduce operators monitoring efforts. The Swiss Cheese Model is a representation of how multiple human errors or system failures can align to influence each other in complex systems and finally lead to accidents or incidents. Such accidents or incidents are typically caused by a set of errors, each only having a small impact. Redesigning Endsley load model is necessary but there are some other opportunities to quantify operators' mental' states [20].

4.2. Data Collection Techniques

As detailed in [21] the workload is defined as the total amount of processing capability required to perform a task, and it includes three types of cognitive load: intrinsic load, extraneous load, and germane load. This particular study focused on monitoring the total processing capability of the subject as the workload measure. In intrinsic load demands of the sensorimotor and cognitive processing which were required for performing the task are also considered. In certain studies the intrinsic load according to the mental workload theory is contributed by forced and transient load, highlighting the peak and momentary demands placed on the operator due to the environment and upcoming tasks respectively. The extraneous load is due to the way in which information required for performing a task is presented. The extraneous load arises when the subject struggles to map their internal representation with the task's physical representation. This load can also occur when the task design encourages a misplaced allocation of attention.

1) Which combinations of tasks result in the highest reported and objective load values e.g., NASA-TLX and HRV at which part of the drive mode interface? 2) What were the shared visual attention patterns as they engaged with the autonomous mode management (ADAS activation and deactivation) task?

One of the vital accessories to solving the problem of cognitive load in operators and facilitating the ease of accomplishing and understanding the tasks based on the information provided within the ADAS HMI is by understanding the multiple underlying problems causing the cognitive strain on the operator [20]. In order to perform said task, the following research questions were developed:

5. Literature Review

The visual interface complexity for cybersecurity ID, the simulation of autonomous driving, presents uniformity visual interfaces showing the vehicle Dashboard (Vehicles' Speed), a radar showing the vehicle environment, a sensor showing the cyclist crossing in front, a second radar identifying a pedestrian approaching laterally, a GPS (checking the vehicle's location), a system to identify the road signs and, finally, a control system called ADEFIS MANAGEMENT that check, in real-time, the status of the foreseen intervention. These interfaces were designed to compare five different levels of perceptual complexity [5]. Results showed that systematized interfaces with an intermediate level of perceptual complexity, in fact, are visually attractive and perform the task well. By contrast, the interface of status which counts both a high level of complexity and a high degree of fluctuation and mutation on the initial scheme appears to be demanding and a graphic which subtracts attention from details useful for understanding the situation to the operator, therefore generating a significant increase in cognitive load.

Efficient automatic detection of cognitive overload can be critical in preventing human-related breakdowns and malfunctions [21]. This feature becomes particularly relevant for complex domains, such as cybersecurity, which involve critical decision making and interpretation that require cognitive resources particularly sensitive to the cognitive load (CL) variations caused by different interfaces and levels of perceptual complexity [6]. To our knowledge, no study has investigated the correlation between the type of interfaces in cybersecurity for autonomous vehicles, that is mainly professional drivers, and their effect on the subject CL and, as a consequence, on the cybersecurity operators selling campaigns, with the aim to propose new tools for tutoring and training. However, this experimental study on the usability of different types of graphic interfaces within the spreading production of driverless vehicles can contribute to new interesting results in order to prevent human errors, focusing on their cognitive load.

5.1. Previous Studies on Cognitive Load in Human-Computer Interaction

In a previous study, electrical cardiography (ECG) was used as measurement of cognitive load in a VR application [15]. It was shown that an autonomous car's user interface displaying indicators of car states (like temperature and charge) and no alerts were perceived at least as demanding as an interface with additional explicit alerts [6]. In their study, subjects were shown situations where the car was not driving autonomously (creation of experimentally varied waiting times for the driver in which they had to monitor/review/control the system) and had to evaluate the demand of these interfaces. A significant relationship was found between the MPI value (a combined measure) and the number of visual and haptic alerts received by drivers, but not with their impact on the cognitive load (as measured by the TRS). Drivers who reported a greater perception of the alerts claimed a higher cognitive load. This indicated that despite in both experimental conditions, high and low alerting frequency, MPI values were on a similar level, there were significant differences between them. As such, the theoretical background was proven: Some drivers experienced no reduction in unnecessary and useless alerts and over time reported a higher perceived load although the measured cognitive load did not differ [22].

6. Analysis of Cybersecurity Interfaces

According to Jonna Hakkila et al., there is overwhelming evidence of the influence of varying automation levels on different workload aspects. They believe that both unpleasantness ratings and situation awareness in Level 3 significantly differ from Level 0. However, the most significant differences are found between Level 0 and multiple automation levels in a bimodal distribution of rating scales among different conditions. In this study, individual cluster analysis was conducted in order to better understand how participants strategically allocated attention to the driving task or supervisor task based on individual differences while using multiple driving automation levels. The results demonstrated that although brain activity and unpleasantness ratings confirm a bimodal distribution of attentional resource allocation, SaRA does not fully follow the same pattern. This might suggest that by solely using psychophysiological responses to assess automation-related workload or cognitive state may have limitations.

[7] [17]Factors such as vehicle control, cognitive load, trust, workload, and emotional state affect human task performance and system reliability. Understanding human cognitive factors can enable the effective design of systems that ensure user safety, task execution efficiency, and user trust. According to Ladan Haghighi, a large number of studies have shown that monitoring for cybersecurity alerts can substantially load a user's working memory and impose a substantial cognitive load on operators. There are important trade-offs that need to be considered when designing a security interface that is deployed in a high workload environment, especially in semi-autonomous or autonomous vehicles. Cybersecurity alerts have to be presented to the driver with a trade-off between being transparent and being cognitive load. We must investigate the effect of different cybersecurity interfaces under different autonomous levels on operators' workload, trust, and driving performance while manipulating task workload through a common in-vehicle system. For this research, the common in-vehicle system is an infotainment system that is used in the EuroNCAP standard crash testing.

6.1. Interface Design Principles

In this work a technical cybersecurity interface design demonstrator for such dynamic transitions between full manual and full autonomous (teleoperation) control is discussed and evaluated with respect to cognitive load implications. Schneider et al. developed an analysis platform for the measurement of eye-tracking and body movement in conjunction with scripted test scenarios while operating two versions of the demonstrator with different cybersecurity user-interfaces [23]. The user-interface alternative of the demonstrator had a visual representation of the cyber-situation at a traffic light as well as a textual description. It was successfully demonstrated, that the less animated visual interface implementation performed better regarding an operator’s mental workload as well as from a workload assessment point of view.

Cybersecurity is not only an essential technical requirement for modern autonomous vehicles but can also heavily influence the user-experience and cognitive performance of the human operators of such vehicles. Cybersecurity incidents with autonomous vehicles can result in unauthorized driver displacement, e.g., via GPS manipulation [4]. In future fully-autonomous vehicles, human operators are expected to hand full control over to the autonomous vehicle's automated driving system when shifting from normal road to teleoperation mode in case of a security-critical event. The shorter this transition, the more effective the intervention and consequently, the higher the probability of safety being restored. Therefore, the cyber situation awareness of operators must be supported accordingly and as unfatiguing as possible [24].

6.2. Usability Factors

[19] While the presentation of information only introduces little driving cognitive load, computer-generated content seems to cause high levels of effort. This is especially the case for automotive use cases. Accordingly, even though touchscreen tabletop AR interfaces could offer functionalities such as a depth-cue simulation to convey state information (e.g. the interactive table-top is used as a simulation surface), care must also be taken that the information is arranged in a manner allowing for an easy association of similar information covering different surfaces, e.g., perhaps by having all information concerning an application shown on top of the application's window. Furthermore, for during travel use contexts, a table-top might not be reachable by all occupants which could further complicate touch-interaction workflows. While large displays could emphasize the hierarchical curve-following information structure for a given alternative, an alternative might not only affect the ego-vehicle, but also other traffic participants under autonomous driving modes (cf. bugs on the windshield metaphor). When operating with a very large heading curve, even though heading correction requires relatively low torque values, an increasing over-steer could make it difficult to track the tree-to-distance-difference state with structured motions, e.g., a telescope hand motion; if the ECU is unaware of the human nature to adapt finger motions to the specifics of the current interactive surface, a motion tracking system might also misinterpret commands, and a high cognitive load might result for the occupant from iteratively verifying desired heading commands (touching and checking the resulting motions).[25] Our results show that drivers consider the quality of their relationship when revising their position settings during a drive. Moreover, when drivers want to tell something

they look at a position partner that they trust more, maybe because they are sure that the partner recalls real partner gestures that the sender avoids to demonstrate. This can contribute to the fact that drivers can share more information with their position partner, regarding the drive. That position partners look; even if from time to time; at a driving-related agent of the same driving situation might serve to regulate attention of drivers and position partners to possible important sources of information. Also, whenever verbal communication will be possible, and while being primarily focused on a driving-related agent, listeners tend to also from time to time; actually look at the; acquiescent and eye contact giving partner. This can relate with nonverbal regulatory activities such as smiling and h-, which is also described in. Such nonver,al inventory inter-,es and other controlling behaviors are so important in informal conversation that, if they contradict the verbal signal behavior, the partners are tempted to consider the verbal message to be false.

7. Cognitive Load Assessment

It is expected that a high cognitive load would be experienced by operators who are responsible for monitoring various internal and external vehicle-related processes, events. and vehicle system states, while controlling and managing various Cybersecurity-related tasks, complying with regulations, and possibly being required to respond to Cybersecurity warnings, alerts, and incidents [20]. In contrast, the ability to monitor multiple streams of information, search for and encode new information. and maintain focus in the presence of cyber-attacks might not consume excessive cognitive resources. It is plausible that consistent passive Cybersecurity awareness through prompts will not heavily impact the operator’s cognitive load. In sum, different Cybersecurity interface solutions demand varying loads on the vehicle operator’s cognitive system.

The assessment of cognitive load provides information about the capacity of an individual’s cognitive system. Optimal performance can be maintained when the cognitive load matches the level of human cognitive capacity, such as working memory resources [26]. In the context of cybersecurity for autonomous vehicle operation, it is important to understand the cognitive load experienced by the vehicle operator in monitoring and managing different Cybersecurity-related tasks, e.g., monitoring the Cybersecurity real-time attack detection system of the vehicle.

7.1. Measuring Cognitive Load

A mastery learning approach demonstrated by a serious game environment allows educators to ensure engaged scaffolding and challenging learning materials. However, balance between these two factors is critical for a game to be effective in the context of skills training. The study presented a feedback system that addressed its user's perceived graph in terms of dependent skills required for enhanced performance. The performance of the game was regulated based under different experimental conditions to determine the best form of feedback while increasing cognitive load. Categorizing the content of cognitive load in game designed for cadets was also evaluated and results suggest that learners complete the game at a high level of utility in the system.

The cognitive load of learners was recorded in the process of playing and learning utilizing serious simulation games [27]. Learners' performance and behaviors were analyzed during game-based learning activities at predefined experimental conditions. Statistical and machine learning algorithms were utilized in the analysis, establishing a cognitive load model. The results suggest that the evaluation method, i.e., monitoring the performance metrics and behaviors of users engaged in serious games, could be applied to learning activities to ensure optimal learning outcomes. The present approach yielded a compelling balance between measuring cognitive load and actual utilization within the context of serious games.

7.2. Tools and Techniques

Multimodal stimuli combinations of computer operated modes and interactions and virtual environment and physical world interfaces should be implemented to enable the highest range of cognitive load requirements. These requirements should be as natural and authentic as possible to reify the training framework inherent to artificial interface technologies [26]. Appropriate experiments for Wearable Augmented Reality (WAR) interfaces using multimodal Hyperhuman Machine Interfaces (HMI) should include evaluating pilots' handedness during 2000 km high altitude flight after refresh-training with Above HMI Cockpits (HMI)! Incorporate and introduce more abstract Swagger-Interactive HMI (SIHMI!) to build-up pace-of-adoptation models.

Several criteria must be met to satisfy the quality of this usability investigation. The five principles listed below will naturally follow the necessity of the evaluation of a cognitive load estimation technology after a software application or hardware intervention [20].

Cognitive load monitoring is essential to human-computer interaction for skill acquisition, multimodal, and augmented reality interfaces. This study presents recent advancements in cognitive load measurement for interface design and presents a critical analysis of the design process. Planning and performing a human experiment require multiple design sub-activities to assess cognitive load, whereas very few authors presented details of their step-by-step procedure [28]. In this section, we provide a detailed guideline on how to design and perform a cognitive load experiment by rectifying the mistakes and limitations addressed in the previous sections.

8. Case Studies

Similarly, in the context of continuous input, there are instances where a user may intentionally want to stop conversing or control management even when the sensory data can be interpreted as the continued or, in some cases, the same as, the present intention of the user. Thus it is clear that a task can be managed with both continued or remained the same expressive or conversational utterance; this statistic was included as a feature. The endorsement of this design might be congruent with the fact that an alert reinforced with a sonification can be two times more quickly recognized than a user interface alert [29]. This might also have implications for modeling human behavior during driving and also designing driver–machine interfaces.

Various HMI (human–machine interface) designers need to rely on measures of cognitive load to assess the effect of their designs and guarantee that the vehicle operator is better prepared to take control of the vehicle when necessary [21]. Two immediate applications of this new CLD (cognitive load detector) will focus on how different types of HMI--such as visual complexity, modality of presentation, workload, etc.—interfere with vehicle operations. Taken together, our results indicate that participants were able to navigate adequately through formal DP (dialog policy, i.e., the graph of system actions) and execute low-level actions without significantly lagging behind reported mental effort levels. Our work also shows potential methodological issues in the selection of the right response to handle erroneous input from sensor data during continuous control tasks in the vehicle [15].

8.1. Real-World Examples of Cybersecurity Interfaces in Autonomous Vehicles

Simulation was applied for the evaluation of a manually controlled vehicle(s), AVs with different grades of vehicle automation for vulnerable road user (VRU) traffic safety, advanced driver assistance systems (ADAS) testing, and vehicle-to-everything (V2X) evaluation. To the best of our knowledge, we believe we are the first to present the possible scenarios and selected reusable and digitized security threats and misbehaviors facing the V2X context to corresponding traffic flows in urban and highway traffic [1], and benchmark a simulation-based evaluation setup to testify the threat levels and impact on the safety, privacy, usability, and economic status of V2X-equipped vehicles. As for the outcomes of this contribution, we expect to provide a better grasp of the scalability and practicability of our scenario-based approach transitioning from simulation to real-world evaluation, which lends extra credibility to the threat-proofed safety and convenience of V2X vehicles.

Autonomous vehicles are a rapidly evolving technology that are now in use around the world. This has further increased pressure to consider the cybersecurity of the system, as previous incidents have raised concerns that the attacks that can affect the system pose dire consequences. The necessity of cybersecurity for self-driving vehicles (SDVs) is being recognized, and policy and regulatory frameworks are being developed at national and international levels. For this review, we collected 18 SDV cybersecurity interfaces (CI) for evaluating components and/or functionalities. However, due to some sensitive or private materials used in real CIs such as digital twins or sensitive production data, we only include CIs that are published in public for this paper [3].

9. Discussion and Implications

We use the concept of situational awareness to help motivate and drive the analysis. Our results show that the simplified smartwatch interface significantly aids in reducing the cognitive load of the task. This result aligns well with recent research, as we outline in Section 8. The lower load that the smartwatch interface produces suggests that simplistic and intuitive interfaces are favorable in the context of CPS cybersecurity user interfaces. Like many other interface design studies in automotive, there can be a risk of getting too abstracted from the actual driving task, which would make the results less ecologically valid. However, we compared to no Cybersecurity information at all (i.e., No CI), meaning that we were essentially measuring an incremental amount of information presentation in the car management task. We acknowledge that baseline measurement with the smartwatch interface in a realistic driving scenario is still an important step outside of our focus in this study on cognitive load. In future, we hope to conduct such a study to replicate and confirm our initial findings. We found no other significant differences between any of the other conditions and propose this is probably due to the somewhat arbitrary level of difficulty associated with the car management scenario [8].

Cyberphysical systems (CPS) such as automated vehicles promise to support diverse use cases, from autonomous driving to personal productivity and entertainment. Regardless of the specific domain, well-designed cybersecurity user interfaces are essential to maintaining user trust and confidence in systems and, as a result, to the sustained learning and adoption of these systems. In this study, we consider that an important step in establishing the validity of specific trust, workload, and situation awareness user interfaces is to evaluate those interfaces against a common metric which defines, at least in part, the difficulty of using the interface or interacting with the system in general. This common metric is cognitive load [30]. We provide an analysis of the cognitive load associated with human interaction with four different cybersecurity interfaces for an automated car scenario: a generic indicator mixed with a task-level little's law indicator, a generic indicator coupled with a task-level divided attention indicator, a simplified low-resolution smartwatch, and a high-resolution in-situ augmented reality dashboard.

9.1. Interpretation of Findings

For the Expert Mode interfaces under investigation, findings indicate a decreased secondary task score and higher scores of perceived workload for ADAS-like than TL-like information presentation. This was not reflected in immediate changes in SA as in the Lane Keeping Task example presented earlier. This provides some new insights into the interpretation of our observed effects: it seems that TLexiable expertise-provided interfaces also mitigate the adverse effects of visual cluttering. Nonetheless, in the light of our overall findings, TL-like interfaces still seem to cause less experienced cognitive load and smaller costs with respect to secondary task attenuation in the ADAS-like information presentation. A better understanding of the interaction between the functionality-driven informational needs of expert drivers and layout-specific differences as found in our ACL investigation remains an essential factor to consider in future developments of ACL-based ADAS-like interfaces.

[8] [4] [6]The results of the laboratory study presented here can be interpreted in terms of the immediate effects observed on situational awareness and perceived cognitive load, as well as possible long-term implications for the development of more robust interface concepts. We first review the immediate findings, which we consider relevant for any real-world development of ADE interface designs. Furthermore, we systematically compare the impact of different interface concepts on end-of-drive situational awareness. For easy interfaces, we observed a significant positive correlation between the secondary task– divided attention score and the information seeking score; this relation was diminished for TLxing interfaces. Further, we observed differences in perceived workload across the different interface concepts, indicating a diminished mental demand and lower frustration for TL-like concepts.

9.2. Implications for Practice and Design

[18] Older adults are often more susceptible to becoming distracted by in-vehicle interfaces than younger adults and this distraction can lead to an overall increase in both mental workload and response time. When discussing the implications for practice and design, it is important to remember that these findings can be used to help design in-vehicle interfaces, particularly for autonomous vehicles, that can be tailored to the cognitive abilities of an aging population to a greater extent than is considered the norm today. When considering largely autonomous cars, it is conceivable that older adults would benefit from an adjustment of some components of the designs of the Digital Lab GTI (Blue and Yellow), Email System and Maps System to include only the most crucial information at the time of the expected handover. For example, the blue interface cluttered with information was identified as particularly cognitively demanding and it is proposed that the most dominant elements of this interface should be moved into visually noticeable areas and the most dominant elements of their remnants temporarily replaced by more basic, legible interfaces.[6]In combination with the relatively high number of older, well-functioning participants among the sample, it may have been beneficial to adjust the design of the IVI to align with their current cognitive abilities. This is not to assume that all elderly individuals have poor memory, but if possible new in-vehicle functions should consider potential benefits for the older population by intentionally designing a gradual, logical and memory-supportive information display. When considering the implications of the present results for an older population during vehicle automation, it is hypothesized both from the present data and in relation to previous research that it is essential that older drivers are still able to comprehend and respond to safety-critical information in

autonomous vehicles even in the presence of system cognitive demand. For instance, a robust multimodal warning that scaffolds comprehension of the auditory alert component was necessary to ensure older adults retained awareness of the driving environment and were still able to react effectively to sudden changes, irrespective of the driving environment.

10. Future Research Directions

As a result of ongoing research, we plan to prepare an article for the journal "Applied Sciences" and take into account all relevant suggestions and comments. We also plan to carry out cybersecurity tests on the constructed model that can be visualized. The hierarchical layer of the conoscopic window will not include automatic selectioning by the program decision. The purpose of such experiments will be, on the one hand, to increase the tragic error rate and, on the other, not to optimize the results by the system prior to the field tests [22]. In addition, we have planned to conduct cognitive ergonomic tests among people using two different system designs (without the conoscopic window and with the conoscopic window), in the natural functioning of the autonomous vehicle, i.e., during travel. At a later stage, we will obtain professional (10 subjects) feedback and consumer feedback (approx. 150–350 subjects) during tests. This will allow for final conclusions regarding the use of the conoscopic window in an autonomous vehicle as a cybersecurity operator interface and should enable simulation of specific repeated sequences of interactions.

In this paper, the primary goal was to evaluate cybersecurity interfaces for autonomous vehicle operators from the cognitive architecture of the modeling perspective. The proposed approach did not exclude human in the loop for system security but provided insight into the best practices for human–machine interface design, given the available architecture of autonomous vehicle systems. Our cyber security evaluation at the cognitive level shows that the design-specific conoscopic windows can train an expert in a correct self-identification of patterns. Moreover, the design specific knowledge and skills are also necessary to operate the on-board cybersecurity system (defense). Surprisingly, the fact that the experimental groups, representing professionals with similar qualifications regardless of the interface analyzed or their operational design, obtained bull's-eye was the average number of fixations at computer monitor: 0. This fact indicates that the majority of the respondents were unable to find the proposed object in the test arrays and the mental process of remembering and matching the analyzed icons (potential candidates) in order to select the icon that would apply was omitted in practice.

10.1. Emerging Trends in Cognitive Load Analysis

[8] Road transport stakeholders expect autonomous vehicles (AVs), with their assistive and fully automated driving functions, to revolutionize future traffic management by reducing road deaths and improving the efficiency and comfort of daily commutes. The potential of AV drives to spark a transport revolution is tied to the assumption that the operators they assist will primarily play a passive safety net role before AVs reach full autonomy levels, as defined by the Society of Automotive Engineering or SAE International standards. Following the distinct definition of the capability of an automated driving (AD) system to reconcile with the necessity for an attentive, ready, and responsive operator or driver to retake control of an AV, the SAE introduced six levels of automation. These levels range from driving automation levels 0–5, where Levels 0–4 rely on the need for specific observed aspects to retain the driver's partial monitor responsibility in a certain driving context and thus require drivers to be in a state of perceptual and cognitive readiness to take over driving back from the AV, as required, depending on the situation. Levels 0–4 are operating as the primary focus of this chapter.[3] All of the automation impacts conveyed above are based on the SAE J3016 taxonomy, according to multiple AV development strategies and availing the customers. This model can be highlighted as the framework encompassing all of the theoretical and experimental studies concerning the interplay between AV and operator characteristics in the human factors domain. Hsieh proposes a comprehensive review of the cognitive requirements of human operators in their interaction with AV systems in driving tasks in the subsections "The Basic Process of Human–AV Interaction" followed by the sections "Ethical, Social, and Legal Issues," and "The Paradox of Human Inattention with Increased Automation." The principal challenges and opportunities for AV safety, security, and privacy in the human factors domain as explained in this chapter are detailed. The empirical insights of human operators at the perception, cognition, and psychology levels guides their overall trust, usability, and interactions with AV function perception.

11. Conclusion

[6] Autonomy brings complexity to the human–machine interface in vehicles, which could lead to an increase in cognitive load and in turn, an increase in operator error. The primary

aim of this research was to analyse the cognitive load and its cumulative effect on operators while using different Human-Machine Interfaces (HMI) in autonomous vehicles. The outcome of the study will help inform the design of future cybersecurity user interfaces.[4] The measures of cognitive load (performance, subjective rating, and physiological measures) showed an increased cognitive load subjected to a high cyber risk interface. We combined the performance, subjective rating, and physiological measures to create a flow model of cognitive load providing an overview of how operators responded to the cyber risk during the simulated autonomous vehicle driving task. The results suggest adding a cybersecurity interface increases the operator’s cognitive library and adds stress, noise and the need to find information at short notice to the flow condition. We plan to investigate further by exploring an auto-generative explanation model of cognitive overload and compose the study into mitigative measures by using artificial intelligence seed models.

11.1. Summary of Key Findings

An adverse effect from cybersecurity-based interface warnings may additionally increase the driver's cognitive overload. Moroń, Oniszczuk, Majer, and Służalska [31] stated that some drivers facing a cybersecurity attack might experience cognitive discomfort, a cognitive and perceptual problem, while driving. Smolen, Horoba, Molendowska, Stanczyk, and Łukaszewicz suggested cybersecurity warnings could do harm to drivers and passengers because they may disturb the attention, interfere with tasks that drivers deem more important, and place extra requirements on the driver. This concept is known as attentional disengagement. This special problem is the largest potential obstacle to the successful completion of the study's purpose. The cognitive load associated with cybersecurity information warnings should be determined under the with-cybersecurity information warnings and without-cybersecurity information warnings.

It is well known that interfaces have the power to increase or decrease the overall perception of the vehicle. With a growing interest in developing autonomous vehicles, the hacker's interest in finding a gate to reach onboard subsystems has also grown. Sensors, the processing unit, and the underlying mechanical systems are all prone to different types of cyber-attacks that may lead to tragedies [4]. As for level 3 autonomous vehicles, cybersecurity is a major concern because there is a possibility that the driver may be busy doing some other tasks and may not continuously monitor the road. This enables any onboard cyber-attackers to make a core role failure which could lead to passenger's lives being in danger. A warning system, which continuously notifies the driver about any cybersecurity breach, is in demand. We built a cybersecurity aware system to consider driving behavior which can detect fake warnings/severity of warnings [21].

11.2. Closing Remarks

[4] As connected and autonomous vehicles are just starting to fill the roads, the focus of our future work in the automotive domain will be on the ways tyres send infrits. Tire sensor technology is progressing rapidly every year, but it is also spreading sensitive and critical information. The transmission of such data is crucially important exactly because it is of high relevance or very sensitive. Hence, this study will focus on the potential ways to misuse tire data and tyre sensor communication for cyberattacks. Attack vectors will be presented, and a test platform for carrying out such hypothetical tire cyberattacks will be proposed. Furthermore, the current European and U.S.A. obligation regartheir privacy and cybersecurity of tyre data are analyzed, alongside with other relevant legislations and concepts. Certain legal instruments which could be used in litigation proceedings connected to the studied cyberattacks will be analyzed, and possible countermeasures necessary for aptheirprotection of vehicles and vehicle users from the proposed cyberattacks will be researched. The results of our study will be applicable in e.g. implementing higher-security standards for tyre sensors and their communication protocols in order to prepare for the integration of cyber-resilience into Connected and Automated Mobility services in the future.[32] The growing use of data by people with smart and connected technologies has resulted in increased cyber-sxiety about data privacy, including mischievous activities, fraud, or any form of cyberattacks. The main security problems faced by cybersecurity are endpoint cybersecurity, secure and usable authentication, and measurement and mitigation of dynamic risks. However, compared to the wide availability of smartphone and device usage data, other information such as tyre sensor data is relatively scarce. The large-scale analysis of existing user requirements, legal framework, and their impact on the vehicle domain due to the spread of tyre Tyre sensor data provide new perspectives in cybersecurity terms. The research will be conducted in public opinion, tyre sensor product description and market vulnerability research, standardization influence research, tyre sensor data in the European Union legal framework analysis, legal framework for tyre sensor data in the United States investigation and case studies of their under research case. This study is the first paper to focus on

cybersecurity of tyre data and its communication, and it fills the gap in the broad understanding of the cybersecurity in the context of the data-rich smart and connected tyre era.

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, Chandrashekar Althati, and Muthukrishnan Muthusubramanian. "Leveraging AI for Mortality Risk Prediction in Life Insurance: Techniques, Models, and Real-World Applications." *Journal of Artificial Intelligence Research* 3.1 (2023): 38-70.
4. Devan, Munivel, Lavanya Shanmugam, and Chandrashekar Althati. "Overcoming Data Migration Challenges to Cloud Using AI and Machine Learning: Techniques, Tools, and Best Practices." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 1-39.
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. Makka, A. K. A. “Comprehensive Security Strategies for ERP Systems: Advanced Data Privacy and High-Performance Data Storage Solutions”. Journal of Artificial Intelligence Research, vol. 1, no. 2, Aug. 2021, pp. 71-108, https://thesciencebrigade.com/JAIR/article/view/283.
10. Peddisetty, Namratha, and Amith Kumar Reddy. "Leveraging Artificial Intelligence for Predictive Change Management in Information Systems Projects." *Distributed Learning and Broad Applications in Scientific Research* 10 (2024): 88-94.
11. 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.
12. Althati, Chandrashekar, Jesu Narkarunai Arasu Malaiyappan, and Lavanya Shanmugam. "AI-Driven Analytics: Transforming Data Platforms for Real-Time Decision Making." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 3.1 (2024): 392-402.
13. Venkatasubbu, Selvakumar, and Gowrisankar Krishnamoorthy. "Ethical Considerations in AI Addressing Bias and Fairness in Machine Learning Models." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2022): 130-138.