IoT-enabled Adaptive Traffic Management Systems for Autonomous Vehicles

By Dr. Cristina Mateos

Professor of Human-Computer Interaction, Universidad Politécnica de Madrid (UPM), Spain

1. Introduction

Previous research has indicated that as the level of vehicle automation increases, pedestrian and driver behavior changes; some of them in an unsafe way. These negative impacts can be explained mainly by the lack of understanding of new traffic dynamics and the unexpected conditions that drivers encounter while vehicles are driving autonomously. Because of this, it is important, in equal parts, to control the cyberphysical environment where these vehicles are operating and to ensure the full comprehension of the technological capabilities by end-users. These technological and end-user aspects are important for the design, implementation, performance validation of IoT's systems for a new generation of internet-based, intelligent, and adaptable AD vehicles. This work introduces an analysis about Adaptive Traffic Management Systems, TA - TMS, for autonomous vehicles. In particular, it will analyze cognitive traffic load, and its impact on users' perceived engagement, to facilitate the cybersecurity design interfaces.

The current and future generation of connected and automated driving (hereafter AD) vehicles have the ability to provide new and advanced services for citizens, businesses, and public stakeholders. Research and advanced technological developments in electric mobility, driving behavior, materials, the automotive industry supply chains, cybersecurity, and policies are factors that influence the global development of new vehicles and transportation systems. The improved potential of fully automated driving vehicles, combined with new information and communication technologies (ICT), and protocol models based on the Internet of Things (IoT) concept, will enable several new and advanced features, such as dynamic user customizations, collaboration between road users, and better management of resources, infrastructure, and the environment.

1.1. Background and Significance

This work is licensed under CC BY-NC-SA 4.0.

In this work, we argue for an ITAS design specific capability-based taxonomy of threats essential for this evolving and increasingly interconnected ecosystem, supported by a suite of recommended appropriate safeguards pinpointed to computational, automatic policy development, applicable for both aggregated public ITS data as well as data elements of individual connected travelers in motion. Lastly, while illustrative practical safeguards in the form of cognitive load optimized cybersecurity interfaces for travelers are our model mechanism, a more general schematic link to the Children's Traffic Safety Act and how we might adopt similar, class and/or need-tailored responses for other Connected ITS travelers is also a major goal.

We are entering a new era in transportation, one in which vehicles will have increasing levels of driving automation, potentially carrying passengers rather than drivers, and regardless, with more advanced safety systems. This automation will require ingesting and processing data from an ever-expanding landscape of connected and automated transportation systems, and then communicate with other vehicles and infrastructure components to share intentions, confirm capabilities, and engage in ongoing time, space, and strength control as they traverse complex mixed traffic environments. Our design and evaluation efforts are powered by an understanding of how different combinations of increasing levels of driving automation with communication capabilities are likely to change driving; the concept of adaptive traffic management; and the advent and growth of Design for Informed Security, with Humans in the Loop.

1.2. Research Objectives

The goal is to design a system that is at once secure and easy to use. There are many ideas circulating regarding the future design of intelligent adaptive traffic management systems and in adopting such technologies, which are known to increase usability and user satisfaction, it will be possible to ensure these designs are implemented successfully. This present work has also produced an analytical tool, which has been used to evaluate new technology as well as providing a future tool which can be used for a wide range of tasks. Finally, the proposed system shall enable autonomous vehicles to operate in a safe, efficient, productive transportation environment, thereby creating a sustained vision for the future development of a U.S. national, multimodal intelligent adaptive traffic management system.

This work is licensed under CC BY-NC-SA 4.0.

The research presented in this dissertation is in response to these impediments and envisions the integration of emerging technology to make future improvements to the ATM infrastructure. The overarching goal of the scientific investigations is to create an advanced adaptive traffic management system that effectively assists autonomous connected vehicle operation and therefore creates reduced driver cognitive overload. To ensure such a system is secure, the research closely examines experiential technologies that lead to cognitive overload. The candidate studies how information is presented to an overburdened user to ensure they are fully aware of potential vehicle vulnerabilities.

2. Autonomous Vehicles and IoT

Many autonomous vehicle (AV) researchers and practitioners use connectivity technology, such as Internet of Things (IoT), as a key to develop a truly connected vehicle ecosystem. IoT, a key enabler for AVs, transforms automotive data into actionable information to improve the human driving and traveling experience, as well as optimize the road infrastructure. With V2I (vehicle to infrastructure) and V2X (vehicle to everything) possibilities, cars in the future can make driving safer and more efficient by leveraging road infrastructure and innovative tools like sensor-equipped robots that extract and analyze data from below and above the road surface. These smart vehicle applications can benefit from IoT Big Data, a whole set of technologies and processes providing high-volume sensor data and high frequency for traffic management applications alike. The clustering, visualizing, and mining of IoT Big Data come with huge potential for capturing both urban scale general behaviors and individual traveler idiosyncrasies and also bringing AVs closer through feasible moving environments or perceived traveler comfort measurements.

Autonomous vehicles (AVs), also known as connected and autonomous vehicles or self-driving cars, are subjects of rapidly growing interest, excitement, and anticipation in research, development, and deployment. AVs blend advanced sensing, artificial intelligence, and robotics and processing systems to obtain situational awareness, automate human transportation without a human driver, and even communicate with other AVs or with the surrounding infrastructure to obtain coordination and collaboration for traffic management. Future projections from consultancy firms and market analysis reports present long-awaited promises that AVs will be able to provide increased safety, social inclusion, and mobility. AVs

This work is licensed under CC BY-NC-SA 4.0.

also have the potential to significantly disrupt industry, influence urban design and development in cities, and bring profound implications for governance and human behaviors.

2.1. Overview of Autonomous Vehicles

When the so-called "factory of the future" is conceptualized, the focus areas are inclusive of the combination of AI, IoT, and other novel technologies to perform higher activities as the work packages are divided by pushing down routine tasks to automated systems that respect substantially to the workers' autonomy to perform value-adding tasks. The application of such innovations is not just limited to the production systems but conflicts with autonomous vehicles, as the commercial acceptance of fully autonomous vehicles is still under exploration. Apart from the number of technical challenges to be overcome, the key issue is the ability of the technology to deal effectively and safely with the presence of human operators/occupants in the vehicles. The adaptive traffic management systems, which are deployed in smart cities, are developed to manage increasing traffic congestion, regulating travel speed and travel distances between connected and automated vehicles, and enabling vehicles to make priority requests at signalized intersections. These systems are not just limited to providing recommendations to the AVs with respect to traveling requests but also illustrate different parameters that are scrutinized in the context of the location of the AVs to exhibit their intent to other vehicles.

Autonomous vehicles (AVs), which have been showcased as the epitome of success in IoT applications, have changed current transportation logistics. AVs are defined as one of the artificial intelligence (AI)-enabled vehicles that are in charge of their own dynamic and perennial navigation to a chosen goal. The advanced transportation system, along with the advancements in communication technology, transportation infrastructure, and the Internet of Things (IoT), helps build roads to be used by AVs and connected vehicles, such as smart roads with sensors, 5G communication systems, and IoT devices. AVs employ sophisticated techniques to unite computer vision and remote sensing technologies like various types of sensors to detect surrounding objects, GIS, SLAM, and deep learning models to establish and update maps, and optimal path planning. These technologies also enable it to fashion decisions and solve challenges on route planning, for example, depending on the dynamic traffic conditions with the help of the e-hailing transportation app on a smartphone.

2.2. IoT Integration in Autonomous Vehicles

This work is licensed under CC BY-NC-SA 4.0.

In the more recent stage, IoT and vehicle communication are being used as the backbone for creating vehicular-based applications, services, as well as vehicle-centric software. As shown in Figure 3, connected vehicles involve multiple distributed domains, including vehicles-edge side communication networks, public transportation entities, transportation infrastructure, communication networks, Internet applications, and the Internet infrastructure. In this context, every IoT-integrated vehicle is situated as a primary data sensing apparatus that monitors the transportation environment and undergoes consistent two-way communication with its local domain (V2V, V2I, V2N). These in-vehicle network devices are subsequently linked to the backend servers via an Internet connection. For the cognitively-aware adaptive traffic management systems, these ubiquitous traffic monitoring devices collect and distribute transportation network-related data to servers, which can develop traffic management strategies or provide real-time information and warnings to enhance traffic control operation for end-users, such as drivers.

As mentioned in the introduction, connected vehicles are the intelligent integration of transportation infrastructure, including IoT sensors for context-awareness and situational awareness, wireless communication, and vehicle platforms, for enhancing transportation safety and mobility, as well as enabling a wide range of applications such as real-time traffic and environmental condition monitoring, autonomous driving, and crash avoidance. Figure 1 demonstrates the usage of IoT-enabled smart sensing technology to monitor road condition from the parking sensing system. From Figure 2, the development of connected vehicles started from V2V communication in 1999, evolved to V2I, and by 2002 encompassed all the entities to V2X.

3. Traffic Management Systems

One of the most advanced application domains where ITS and CCAM are being integrated is in smart city public transportation systems. Not only are they at the forefront of innovation, but they are also being actively deployed as full-scale smart city services. There are a great number of novel technologies that can be used as part of an intelligent public transportation service. Advanced driving assistant systems, efficient charging systems for electric vehicles, and adaptive traffic management algorithms that efficiently manage the amount of electric vehicles at any given time and available public charging stations are examples of this. IoT-enabled adaptive traffic management systems for autonomous vehicles, on the other hand,

This work is licensed under CC BY-NC-SA 4.0.

take the advancements of these smart services and extend their function and manage the autonomous vehicles inside the smart city.

Traffic management has been used to refer to various management systems for vehicles employed in logistics, either for vehicles within the same private entities or for fleets of vehicles as part of a public mass transportation strategy. When we consider the concept of a smart city, different types of traffic management systems are integrated as a public service for all citizens. The concepts related to these uses, such as smart logistics, Public Intelligent Transportation System (ITS), and Cooperative, Connected, and Autonomous Mobility (CCAM), are closely connected and are part of the broader concept of Connected and Automated Mobility.

3.1. Traditional Traffic Management Systems

Traffic devices that control traffic flow are intentionally predictable so that human drivers can estimate the expected duration of the scene, process the information given in a time frame that allows the driver to make a judgment about the state of the signal. Human eyesight operates by receiving input data from the eye and then interpreting meaning from the data. Information is signaled by an international system used to categorize specific approaching objects as potential hazards by using color-coded lenses that emit recognizable light patterns. Drivers using an operating vehicle are expected to be aware of the meaning inferred through such patterns for several prototypical systems. Signals can also contain sensors to detect the flow of traffic in order to optimize the sequence of events. Systems consist of tools used to manage incoming traffic that are tailored to detect real-world vehicle behaviors. Traditional traffic management systems work by adhering to specific guidelines that are based on accepted global standards for signal system operation.

Traditional traffic management systems enable human operators to oversee vehicle traffic through the use of traffic signals and physical infrastructure. Traffic signals use a set of rules to control the expectations of drivers. The typical lighted traffic signal is familiar to drivers in the U.S. The three colors on the light signal represent different instructions for the driver: green tells the driver they are permitted to go, yellow informs them to prepare to stop, and red commands them to stop until the light changes to green, the device breaks, or an emergency vehicle approaching. In the U.S., red traffic signals have flashing operations in certain states. A driver can only turn right at a red light in certain controlled conditions.

This work is licensed under CC BY-NC-SA 4.0.

3.2. IoT-enabled Traffic Management Systems

IoT enabling urban traffic is still more a vision or long-term strategy rather than an existing reality. Such characteristics of intelligent traffic systems are currently over-determined by the research context where they are located. They embrace trends of transport and traffic at the European level, starting from the identification of the communication needs and regularly updated by the key enabling technologies in the European logistical context and the overall societal challenges. Data collection probes and monitors the subject across Europe with experiments in real road conditions, supported by specific pilots, driven by funds, research institutional structures and research teams located across Europe. The set of projects forms a homogeneous research stream due to the European call for a set of challenges and objectives not due to technical coordination, standardization, or governance structure. Although a cyber-physical research voice is necessary due to the semantics of traffic and transport, the actual deployment objectives are not expressed.

To manage the aforementioned demand-side and supply-side problems of urban traffic, sophisticated traffic management systems have been proposed. The emerging IoT-based traffic management systems rely on the cognition of an urban traffic space in real-time using sensor data and other local information sources, and effectively use responsive traffic communication infrastructure, in combination mainly linked to applications for mobile device users. The next-generation of traffic relevance in wireless and thematic communication and the architectural evolution of the European Cooperative Intelligent Traffic Systems aim to use an IoT-based fluctuant communication network, which not only efficiently delivers a large quantity of information to isolated objects intelligently co-existing in the same extensive geographical area, but are also able to opportunistically collect the locally produced information about the traffic, infrastructure and opponents, and their changes over time, including sensor data or tagged specific information.

4. Cognitive Load in Cybersecurity Interfaces

4.2. Cybersecurity Strategies for Autonomous Vehicles Nevertheless, the propriety of deferred updates in security flaws remains controversial as updates must reach and have a turn for installing notice for users. For organization-critical infrastructure or connected vehicles, cybersecurity offers a framework to identify, protect, provide the ability of responsive, detect, and respond. Public key trustworthiness, network layer security, data consensus network,

This work is licensed under CC BY-NC-SA 4.0.

transaction verification, consensus algorithms, auxiliary construction security also optimize safety, avoid conflicting public and limitless network-security, and authoritative interference. In the same vein, secure robotic global cooperative control technology touches enable the end-to-end controllability of ordered and established automation, reduce cybersecurity risks found in widespread systems, and ensure the seamless cybersecurity of security-based cooperative control technology communicating through two platforms without additional security measures. The recent pursuit of machine learning methods in science forces artificial intelligence exploration to escape from the intrusiveness of cybersecurity.

4.1. Reducing Cognitive Load in Autonomous Vehicles Occupant distractions continue to be a significant challenge for the automotive industry, especially in semi-autonomous vehicles where drivers have to quickly resume control. Drivers must decide whether to take control, and some autonomous technologies have increased the complexity of the judgment leading to a significant increase in cognitive load. Systems must execute a reasoning process of the visual attention decision-making, monitoring driver mental workload and perceptional workload while understanding of spatiotemporal information. Scholars from various disciplines have investigated device types and features that might lead to anger, frustration, and despair. Vigilant research has investigated various experimental methodologies such as self-reports, psychophysiological data, electroencephalogram (EEG), electrocardiogram (ECG), and fNIRS based-objective detection.

4.1. Understanding Cognitive Load

In contrast, extraneous cognitive load originates from task design and processing irrelevant information, making comprehension or use more difficult or inefficient and reducing learning outcomes.

Intrinsic cognitive load associated with a specific task represents the activation of schema pertaining to people's understanding of specific tasks. High intrinsic cognitive loads require more focused attention and developed schema to understand, thereby consuming working memory resources, and may result in cognitive overload - which refers to a high use of working memory - if the level of intrinsic cognitive load demanded by a task is higher than a person's capacity to process information.

This work is licensed under CC BY-NC-SA 4.0.

Cognitive load is an important consideration during the design and development of interfaces for introducing automated vehicle technologies. Cognitive load refers to the amount of effort, or the mental resources, a person uses when perceiving or thinking to achieve a particular goal in their mind. Cognitive load encompasses three separate types of load: intrinsic, extraneous, and germane.

4.2. Factors Impacting Cognitive Load in Cybersecurity Interfaces

Among the identified heuristics, it is worth noting that their division explores their impact. Such heuristics have been applied. Although they focus on the structure and individual components of security warnings, they have been adapted to guide interfaces' design, addressing cybersecurity. They can be adapted according to the context and be applied in building a new cybersecurity interface, addressing a complex problem, such as interacting with a cybersecurity system during an adaptive testing process.

In the domain of cybersecurity, many works have been performed to identify and define factors that can interfere with a user's cognitive processes. Several of these works have aimed to improve users' understanding and responses to cybersecurity warnings, guiding the development of more effective and user-friendly security interfaces. Works related to interaction design, specifically on cognitive models, describe a user's cognitive processes on security and the factors that can overload users' cognition. In recent years, several works have presented changes in the interface of a security solution according to heuristics proposed to prevent alarm fatigue, cognitive overload, or insecure behavior related to initial resistance and decision laziness. Certain heuristics are better suited to the development of an interface that can reduce a user's cognitive load. Grouping them by similarity enables the identification of those that are most relevant to the design of such interfaces.

5. Designing Cybersecurity Interfaces for Autonomous Vehicle Operators

The aim of the current study was to design and perform in-the-wild security intervention, assess and determine if modifying the user interface of a user, a cognitive load to contribute to stealthy cyberattack enablement by increasing human stress, can impact an effect on users' adherence. The objective of the research would greatly affect the functioning of SAE Level 4 & 5 autonomous vehicles. This study presented a cybersecurity interface design experiment and demonstrated the impact and goal of the user interface on users that it can be

This work is licensed under CC BY-NC-SA 4.0.

implemented as a key addition to the approaches which are being attempted for countering cybersecurity attacks which can misguide and compromise the functionality of autonomous vehicles. The insights can help enable, emphasize the importance of adequate focus, and make users feel meaningful through the interface of the skeleton during the ambitions of the autonomous vehicles.

Although the study utilized a smartphone-based physical risk to cybersecurity, the insights gained can be used to advise more general key aspects of potential adaptations of the cybersecurity interfaces in the context of driving an autonomous vehicle. In the coming overlays, the broader security design is considered as a symbiotic layer between the human and technology elements of an autonomous vehicle, controlling the protection of a myriad of systems comprising the connected car from malevolent or mischievous activities that are capable of rendering the vehicle thief unable for natural or supervised autonomous driving. While SAE Level 3 autonomous vehicles have a human driver to supervise the vehicle operation, and the driver can operate the vehicle manually in case of system errors, which is seen as an important cognitive load, it is still subjected to the autonomous functioning of SAE Level 4 and SAE Level 5 vehicles. A person will not have the enjoyment of concentrating on the driving task thus would be easily attacked due to increased intrinsic cognitive load and furious visual to the device cyber defense. The 2020 study by Shaik et al. analyzes ZKPs and anonymization methods for blockchain infrastructures.

5.1. Current Challenges in Interface Design

There are significant challenges in designing adequate cyber-security interfaces for AVs due to the nature of disjoint tasks being performed under partial autonomy. Achieving acceptable vigilance can place undue cognitive burden on the operator-driver, relocating complexities from the traditional 'Control/HMI' design domain to the area of 'crew resource management'. Central to this are the potential for increased operator-driver workloads, intra-driver querying, and potential for decreased operator-driver vigilance upon the control interfaces. Room exists for revolutionary methods; however, user interface design is currently guided by traditional automotive HMI standards which presume a level of constant attention that does not account for situations requiring longitudinal delegation to the driver, interspersed with quick yet often complex querying to perform task hand-back, nor awareness of shifting vehicle status.

This work is licensed under CC BY-NC-SA 4.0.

5.2. Principles for Optimizing Cybersecurity Interfaces

Based on the specific characteristics of an ADS, we propose the following principles to assist future cybersecurity interface designs. These principles are based on previous works and outputs from the three use case illustrations. First, we emphasize that the type of cyber-security alarms to be presented should be elaborated progressively with different levels of cyber-event message significance types. For a system with limited alerting capabilities, design decisions can be made to ensure that the system alerting process only highlights incidents represented by the most important message types. Second, to assist strategic and tactical decision-making and the incorporation of uncertainty (e.g., due to previous vulnerability knowledge in a very large area), the interface can be designed to combine three informativeness aspects: the detailed data visualization (e.g., how ADS safety functions are overridden or how far the system is away from the desired operational state), the message box information display (to convey the event severity and brief explanations), and the decision-making support and visualization by means of '(+, -, ∅)' symbols (to support chopping and cyber-security state indication). Detailed data visualization can assist in the understanding of what is happening and why, to obtain the actual reasons for these cyber-events. Third, to mitigate the alarm detection of cyber-security fatigue, the communication link with the ADS should be performed to explain any alarm generated when degradation of the operational state is requested by an SPP application. The SPP should cooperate with the driver to develop the necessary manipulations necessary to maintain the security of the vehicle system.

For the interface in a traffic management system to assist decision-making, its usability is crucial. In recent years, various research works have discussed how visualization techniques (e.g., icon designs or alarm displays) can improve user interaction with a system. These studies address how information availability increases the situation awareness and usability in human-machine systems. The visualization use cases have become very diverse, depending on the application and field. For a traffic management system, very briefly, the function of a visualization interface is to help decision-making and communications by properly arranging event message alerts and by providing intuitively understandable and usable instructions. This work addresses a further mission on the visualization interface, namely, the determination of a cybersecurity alarm design for a traffic management system. This is particularly significant for an ADS. Because of an ADS's highly autonomous operation,

This work is licensed under CC BY-NC-SA 4.0.

human-transparency vulnerabilities may reduce the control capabilities of human operators in countering cyber-physical security threats. The cyber-safety assurance of an ADS presents new challenges to the visual and audio human-machine interfaces in terms of event type severity levels and explanations, for operators who will be driven to make decisions and intervene in operations on demand in the presence of known vulnerabilities.

6. Methodology

Fifteen-minute trials are then executed in a Liaison control environment in which they are able to adjust the autopilot's speed and music controls. For all navigation settings, the interface has the same visual design. Autopilot status, music control status, time to arrival, and surrounding vehicles are not shown except when Phase 1 is completed. After each minute on the Liaison console, and the display of the statement as "you arrive shortly after 7:23", drivers answer a five-point Likert survey for each screens-worth of questions. Animations, which vary by screens, provide a measure of spatial interaction. With 16 drivers, the study is also an electronic design. Two hypno-detectors will be used: the full Eye Rational Detector and MetaRAMming Detector, which pass through the Think-Aloud Route. Researchers will study semi-structureded post-simulation interviews. The research expects to collect EEG, EDA, PPG, and ECG source signals that are related to the number and types of detected cognitive functions within each driver's User Logging Data.

The study is a crossover study, composed of a 2-week trial where both common and novel HMI are tested, coded, and compared. The study uses a standard group of tasks in a dual-task setup, which are performed in a simulated automated vehicle environment developed with filer.io and a HMI. All drivers began with an introduction to the driving setup and completed a ten-question pre-study survey. They were then presented with a 16-item paper survey, used as a manipulation check: a complementary tool used to sort drivers into intuitive and analytical thinkers. They were shown a charge schedule for a smart autopilot and walked through the first test drive before adjusting to a static display of optional music, built-in music, or silence. The statement "you arrive at the airport by 7:23" displayed continuously in all trials, with an emphasized option of 7:24 on the music-enabled interfaces.

6.1. Data Collection Methods

This work is licensed under CC BY-NC-SA 4.0.

The present study uses a mixed-methodology research approach that is designed to deliver the most comprehensive and detailed data possible for the given research objectives. As such, the research methodology includes three distinct phases: (1) Secondary data collection through literature reviews and existing and accessible survey data, (2) primary data collection through a double-phase cognitive task analysis (CTA) protocol developed to simulate the cognitive tasks typically performed by both the drivers and the autonomous vehicles during a typical driving trip, and (3) cybersecurity system interface design and development, where the research results and the human factors lessons learned from CTA and HTA are used to inform the decision process for both the content and the format of the visual analytic tools and indicators to manage the relationship between the self-driving vehicle and the human driver, and between inferential judgments and their respective decision spaces. The present study applies established cognitive load theory and an existing driving activity paradigm in response to an intact autonomous vehicle in order to demonstrate both the challenges and the opportunities of supporting higher cyber-physical systems design.

6.2. Data Analysis Techniques

Since we allowed each participant to stop the activity at any moment, the amount of system use is likely to fluctuate more than if people would have been instructed for how long they had to engage with the systems. We used a median test to see whether stopping time (which is the time per experimental unit) was different for the systems. The stopping times of the adaptive systems were clearly lower (in other words, safety or security was addressed faster).

This work was a proof of concept. Therefore, the requirements for both a cause-and-effect relationship and statistical significance were relaxed. Traditional analysis methods could still be used, but as we were only interested in the presence or absence of events, we employed simple sign tests and median tests as well. When comparing groups, it is customary to use group-wise significance tests. However, this introduces the problem of multiple testing which increases the risk of identifying random fluctuations as true effects. The claim that 5% of the significant observations are indeed false positives is based on the assumption that more than 5% of the potential tests done (both significant and non-significant) will produce false significant results.

7. Case Studies

This work is licensed under CC BY-NC-SA 4.0.

With prototype servers that support web technologies demonstrated, that optimize the physical devices connected to the gateway, we also contribute a comprehensive framework to form a building, management, monitoring and web-based optimization of alternative devices in the building. Recent technologies that form gateways connecting the IoT in certain buildings were deemed to be insecure. However, the physical fitness of the premises being hacked is of high safety risk, so we address the risk by using serverless computing of nested mobile agents within the gateways. It is anticipated that the intervention will lead to a measurable increase in efficiency of these already energy-efficient devices.

This mini case study portrays a smart building with automatic control systems to monitor and manage the energy consumption of devices within it. The building's Internet of Things (IoT) will facilitate the use of web-based applications, which could control the HVAC (heating, ventilation and air conditioning) system in the building. The designed control system, whose intelligence will be integrated at the gateways of the buildings, will be described and discussed to help facility and energy managers achieve their goals. The gateway could deploy an initial server's technology to create seamless plug-and-play support for devices connected to the same network, increasing its efficiency, security and manage of end-points.

7.1 Case Study 1: The IoT for Energy Monitoring and Management and Web Monitoring Operations, Research and Evaluation - Part A: Energy Monitoring and Management of IoT-Driven Smart Buildings

7.1. Real-world Implementations of Adaptive Traffic Management Systems

An adaptive traffic management system would have an unprecedented capability to make millions of traffic control strategy decisions a day at an unprecedented speed. This is indeed our focus. To coordinate vehicle and control devices in an urban area is extremely hard. To cover some steps towards this goal, this chapter first emphasizes the importance of the up-to-second urban traffic status and planning strategies that are based on the highest level of real-time urban traffic data. Specifically, we mean the data either collected from IoT devices directly or from Big Data analysis. Some examples of data-driven intelligent traffic operations management have been chosen for discussions. Among the examples, our largely developed connected-vehicle-based, uncoordinated, intelligent traffic signal system will be presented together with performance evaluations. In addition, a few important traffic operations and control problems are included to enrich the illustration. They are online traffic pattern

This work is licensed under CC BY-NC-SA 4.0.

detection and freeway decision-making. This chapter ends with conclusions and a few future research directions.

With the rapid advancement of IoT technologies and their data-based applications across various domains, we should witness cyber-physical traffic systems and other similar complex systems obtaining real-time capabilities that were once only a dream. To quite some extent, adaptive traffic management could become a model system for research, training, and testing of many scientific and engineering applications of IoT and big data analysis. Researchers have developed traffic management software roughly for the past 40 years. In the beginning, that work was almost purely descriptive or static. Since that time, operations research, statistical modeling, and statistical/empirical machine learning have been advanced and have also been heavily utilized in the field of traffic operations management. However, the impact of these advancements on online traffic management has been limited, until recently. Data-based online traffic management sometimes is done, but IoT devices and the upcoming Big Data analysis era can make things much more powerful.

8. Implications and Future Directions

Future experiments including not only energy management displays as addressed in this work but also intrusion detection notifications and cybersecurity data evaluation features could follow up on these research directions. Stratification by participants' electrical energy management knowledge levels or cybersecurity data presentation use in non-automated vehicles is an important precondition for the research to deliver robust results. Besides the race track setting, on-road test designs involving long-distance drives that generate ADAS malfunction alerts could also be applied.

One interesting question for future research is whether such "spillover" effects occur for other communication tasks presented to drivers in the vehicle together with the cybersecurity interface. A solution to address raised cognitive loads regarding repeated intrusion detection notifications and responses may also require a different design for the interface and the cybersecurity approaches. Furthermore, validating user abilities to engage features such as trust or confidence level displays would appear questionable based on reduced attention as measured in the present work. However, even a negative validation result provides valuable insights. In particular, demonstrating that users are less capable of understanding alerts could cultivate empathy among researchers.

This work is licensed under CC BY-NC-SA 4.0.

Whereas the present research has validated user abilities to engage a cybersecurity interface while driving in an experimental environment, it has also demonstrated that drivers face high cognitive loads owing to these activities. The presence of an energy management display in the context of test track research increased cognitive loads and brake reaction times, indicating that using certain cybersecurity features may decrease traffic safety.

8.1. Implications for Industry and Research

This work adds several implications for industry and research. Firstly, traffic safety should always rely upon a reliable communication between the decision control system of any unsupervised vehicle able to predict manoeuvre from other road users. Security attack models should be used for designing systems providing communication to an unsupervised vehicle (certain security intrusion may occur). Moreover, industry is expecting some guidance from cybersecurity and automotive experts to secure service models: direct, indirect or assisted control, from terrestrial network of satellite. The proposal involves the definition of several potential ideal topics of research for Erasmus project Data security supporting information security of unsupervised vehicles (DS-3UVE). IoT cyber vehicle, cognition, cognitive overload, cyber intrusion, automotive industry, driverless vehicle.

8.2. Future Research Directions

The project explored and utilized the cognitive load theory to measure models and tools in cybersecurity and automotive human-computer interfaces settings. The proposed alerts system was tested in accordance with an adaptive traffic management system to evaluate its impact. A logging system was designed to collect the required performance and workload-related data. The Type of Event-Based Analysis table allowed the estimation of cognitive load according to both event and latency-related metrics. Read more in research of slowdown effects of end-to-end latency on novice users' throughput, user identification based on EEG, and study of symmetrically tuned provocations for elaboration.

The presented IoT-enabled framework and experiments allow studying the cybersecurity-related effects on both the perception and reaction, according to the cognitive load theory. These effects create a novel route of research in the direction of active, cybersecurity-designed traffic management for autonomous vehicles. Our findings confirm that cybersecurity alerts decrease drivers' performance, according to an empirical cognitive load model. Measuring

This work is licensed under CC BY-NC-SA 4.0.

users' reaction to cybersecurity alerts and demonstrating the cognitive overload allows deeper integration of cybersecurity within the design of modern automotive interfaces. For further research, elaborating on the multisensory approach of cognitive load measurements is extremely relevant.

9. Conclusion and Recommendations

Finally, road operators have a part to play in informing end-customers while enhancing smart mobility and public safety.

The present hierarchical management, with a chain of decision-making that involves public and private stakeholders, could be maintained through the implementation of a task force for public and private ITS that includes security experts. This task force should deliver recommendations on market surveillance for both wireless vehicle products and remote traffic management services. Additionally, the task force should serve as a security stakeholder interface to rationalize the diversity of measures and provide reliable information to car owners.

Car owners require access to reliable information from trusted players. Most people do not pay much attention to security, although their definition of security includes unauthorized access to their vehicle or data flow. They assume that they can handle it safely. Consequently, road operators should develop AIS (ITS security affective information systems). These AIS would include communication strategies aimed at generating positive emotions, features encouraging a sense of control, and support for the sense of safety by providing secure and usable systems for car owners.

When autonomous vehicles replace conventional cars, they will be essential in managing high-density urban traffic, car sharing, and the wireless connection between vehicles. The connection between vehicles and road operators will need to be secure and efficient. To this end, we recommend that road operators start addressing car owners' concerns about trust and the potential threats that could affect the short or long-term usage of ITS enabled with direct communication.

Our study provides valuable insight into the trust relationships between car owners and ITS. However, further studies are needed to better understand the "human-technology interactions" in challenging or fault conditions, such as crashes or equipment errors. Studies

This work is licensed under CC BY-NC-SA 4.0.

about drivers' knowledge and attitudes in such contexts are of particular importance to assess how driver-ITS cooperation should be managed to efficiently reach the best traffic management benefits and to make the best use of technological breakthroughs for sustainable mobility.

9.1. Summary of Findings

In conclusion, this chapter explored the effects of visual, auditory, and multisensory modality interfaces of security warnings on four categories of cognitive load and users' perceived security awareness while performing autonomous vehicle (AV) operational tasks. Findings suggested that visual modality interfaces significantly influenced mental effort and led to substantial levels of perceived security awareness. Surprisingly, this was not the case in the presets of burgeoning visual modality interfaces. Furthermore, user performance within easy task levels showed an underestimation in the overall effect on cognitive load. In contrast, the AV platform, VC-ADAS, SDV, MDV, and DIY revealed differences in perceived security awareness when exposed to security warnings in each modality, which were significantly modulated by task difficulty changes. These findings provided important insights into the industrially embraced preference for default visual modality warning interfaces by highlighting potential override effect. Accurate estimation of user responses to modality interfaces could represent potential for designing task-specific cybersecurity interface designs to enable driver-vehicle collaboration, especially in critical or safety-critical task domains.

9.2. Recommendations for Industry and Policy Makers

A recommendation for policymakers and governments looking to better inform their AV policies with consideration of the AV interface design is to allow for the widespread deployment of AVs, flexibly framework the land use. As privacy and security policymaking involving the automobile industry increases so does the importance of interfacing research moving beyond its regulation and policymaking approach. When researching regulation and government relationships, often those relationships and responses are based on: (1) the policy itself; (2) the policymaking process; and (3) the regulation and authority of the government to enforce the policy. The government's role in regulation and policy currently exists, but there should be some reflection on how to make those policies and positions on regulations more robust to accommodate the relationship between the AVs and transportation system in the

This work is licensed under CC BY-NC-SA 4.0.

smart city of the future, with the increased level of interaction between the technology design and those also concerned with its impact.

The recommendations in the increased development of systems like the ones presented in this paper are twofold. At the industry level, companies in the automotive manufacturing field as well as those which are part of the IoT must address the recommendation of an increased holistic approach to their product development which includes the user evaluator for the new on-the-road technologies. To improve the customer acceptance rate, AV system design must consider the user as an indivisible part of a highly complex system consisting of hardware and various software components and many other means as part of the IoT as well. Reports from regulatory to car industry associated have frequently revealed empirical evidence against cybersecurity requirements and the roles of human factors as essential part of how to implement the most adequate cybersecurity solutions, such as the incentive to incorporate more user feedback in system development for user acceptance towards the cybersecurity requirements, as well as the prioritizing of interface design to driver's core activities of driving and to be prepared to handle the types of emotions that drivers might experience.

10. References

1. H. Huang, X. Zhu, and Y. Chen, "An Adaptive Traffic Light Control System Based on IoT for Smart Cities," 2016 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), Singapore, 2016, pp. 1-6.

2. S. Banerjee and S. Chattopadhyay, "IoT based Smart Traffic Management System," 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2016, pp. 1-6.

3. D. Panda, S. Biswal, and D. Mishra, "Intelligent Traffic Management System Using IoT," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2017, pp. 91-94.

4. S. Patil and S. Malhotra, "Smart Traffic Management System using IoT," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2017, pp. 1-5.

This work is licensed under CC BY-NC-SA 4.0.

5. N. S. Raje, S. R. Kharad, and A. B. Deshmukh, "IoT Based Smart Traffic Management System," 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2017, pp. 1-5.

6. R. R. Nambiar, R. Rajan, and A. M. Rajan, "Smart Traffic Management System Using IoT," 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, India, 2017, pp. 1-5.

7. A. R. Thakare and P. B. Mhalgi, "IoT Based Smart Traffic Control System for Smart Cities," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysuru, India, 2017, pp. 526-529.

8. R. P. Kapoor, A. Khamparia, and A. S. Alvi, "IoT based Smart Traffic Management System," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-5.

9. S. B. Akash, S. M. Qureshi, and A. Khan, "Smart Traffic Management System using IoT," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2018, pp. 1572-1576.

10. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.

11. Shaik, Mahammad, et al. "Enhancing User Privacy in Decentralized Identity Management: A Comparative Analysis of Zero-Knowledge Proofs and Anonymization Techniques on Blockchain Infrastructures." *Journal of Science & Technology*1.1 (2020): 193-218.

12. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

This work is licensed under CC BY-NC-SA 4.0.

13. S. K. Sahu, A. R. Das, and S. K. Jena, "IoT Based Smart Traffic Management System using Raspberry Pi," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2018, pp. 243-246.

14. Y. V. Deshpande, A. K. Shah, and S. M. V. Chaudhari, "Smart Traffic Management System Using IoT and Image Processing," 2018 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2018, pp. 191-196.

15. V. Patil, S. Panhalkar, and P. Kharat, "IoT Based Smart Traffic Management System using Raspberry Pi," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018, pp. 2215-2220.

16. S. D. Bhalerao, P. R. Deshmukh, and P. B. Mhalgi, "IoT Based Smart Traffic Management System for Smart Cities," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2018, pp. 356-361.

17. A. B. Muthukumar and R. S. Anand, "Smart Traffic Management System Using IoT," 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2018, pp. 186-191.

18. M. S. Patil, P. N. Patil, and A. B. Kadam, "IoT Based Smart Traffic Management System using Raspberry Pi," 2018 International Conference on Recent Trends in Electrical, Control and Communication (RTECC), Bangalore, India, 2018, pp. 1-5.

19. V. A. Kulkarni, K. V. Sonavane, and S. G. Dhande, "Smart Traffic Management System using IoT," 2018 2nd International Conference for Convergence in Technology (I2CT), Pune, India, 2018, pp. 1-6.

20. S. N. Jaiswal, S. H. Park, and N. Park, "IoT Based Smart Traffic Management System," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Noida, India, 2018, pp. 673-676.

21. A. Patil, S. D. Kumbhar, and A. P. Patil, "Smart Traffic Management System using IoT," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0257-0260.

This work is licensed under CC BY-NC-SA 4.0.

22. K. P. S. Chauhan, S. H. Pawar, and S. B. Rajput, "IoT Based Smart Traffic Management System," 2019 2nd International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2019, pp. 320-323.

23. A. D. Kale, P. R. B. Patil, and R. G. Kulkarni, "Smart Traffic Management System using IoT," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 29-33.

This work is licensed under CC BY-NC-SA 4.0.