Chapter

Autonomous Driving and Cybersecurity by Design

Cecil Bruce-Boye, Moritz Krebbel, Andreas Fechner, Robert Luyken and Telse David

Abstract

So far, real-time requirements for the overall autonomous driving (AD) have been addressed only in a few cases. Cybersecurity and real-time capability are usually addressed separately. However, with regard to a justifiable mobility quality, these requirements are in direct interaction with each other. Therefore, as suggested here, it makes sense to consider the provision of a suitable IT infrastructure with cybersecurity, QoS (Quality of Service) and simultaneous real-time IoT capabilities. The early integration of security and real-time by design, as well as the architecture concepts mentioned, are measures that limit development costs, make the solution modular, scalable and thus sustainable. We introduce the adaptive-real-time-manager (ARM), an innovative concept for continuous assessment and optimization of the real-time capability of autonomous driving systems. The paper also proposes a cloud-broker-concept and simulation as essential building blocks to accelerate the integration of the ARM into an autonomous driving system (ADS). Furthermore, we discuss aspects of multisensory data acquisition and processing, addressing the integration of various data sources and their qualities. Finally, we highlight the importance of driveability for autonomous vehicles, emphasizing its role in comfort, safety, and user acceptance.

Keywords: autonomous driving, cybersecurity, real-time, adaptive real-time, real-time management multisensory data, driveability

1. Introduction

1.1 General thoughts about autonomous driving

The transition from self-driving individual transport to driverless on-demand mobility with ADS is a major challenge for both people and technology. Innovative mobility concepts such as Mobility-as-a-Service (MaaS) and Transport-as-a-Service (TaaS) are being developed to bring safe, environmentally friendly, cost-effective and convenient solutions to the market [1].

As the mobility market evolves, companies will need to offer diverse hardware, software, and services portfolios to meet the expectations of their customers. Among the top priorities is Level 4 safety: Today’s vehicles are already equipped with numerous safety and assistance systems, making driving very safe. On average, a human driver causes a fatal accident every 600 million kilometers [2]. Self-driving systems are expected to further reduce the number of accidents. To achieve this, the system needs to be extremely robust, which is not only challenging in terms of design, but also in terms of verification.

1.2 A new approach: real-time IoT and cybersecurity

ADS-based mobility requires a secure, uninterrupted connection between all traffic participants. It therefore relies on a smooth and fast flow of data for each individual information chain between all relevant participants. This also means that these chains must be protected from attack. All possible attack vectors must be secured, regardless of the point of attack. At the same time, it must be ensured that the acquisition and response times of all data in the relevant information chains are reliable, deterministic and predictable. A suitable computing infrastructure with cybersecurity—QoS (Quality of Service) and real-time IoT capabilities—is therefore required [3].

The ADS system must ensure both cybersecurity and real-time IoT capabilities across all information chains of the entire system. While these requirements may seem contradictory at first, it is essential to perform the necessary analysis during the design phase to develop concepts, architectures and strategies that resolve this contradiction. By doing so, we can avoid the costly and often unattainable process of implementing security and real-time capabilities in an ADS after the fact.

1.3 Cybersecurity for autonomous driving system

With the increase in connectivity and communication between vehicles, traffic management systems and other elements of the transport infrastructure, the attack surface and potential vulnerabilities are also increasing. One of the main challenges in implementing cybersecurity in autonomous systems is that security mechanisms such as encryption, authentication and integrity checks require time and computing resources. These additional requirements can potentially impact the real-time capabilities of the systems by increasing latency and slowing the response time of autonomous vehicles. However, with careful planning and innovative solutions, it is possible to achieve both cybersecurity and real-time performance without compromising the safety and reliability of autonomous driving systems.

The importance of cybersecurity has been acknowledged by lawmakers, leading to the introduction of UNECE Regulations R.155 and R.156 [4, 5]. These regulations establish requirements for the cybersecurity of vehicles and their systems, and require the automotive industry to take appropriate security measures to ensure the cyber resilience of their vehicles.

The combination of cybersecurity and real-time capability requires close collaboration between the various disciplines involved in the development of autonomous driving systems, such as vehicle engineering, software development and IT security. An appropriate IT infrastructure that provides both cybersecurity QoS and real-time IoT capabilities is crucial for the safety and reliability of autonomous vehicles. To achieve this, the following concepts and ideas are presented, which enable an efficient combination of cybersecurity and real-time capability to ensure the safety and functionality of autonomous driving systems.

1.4 Multisensory input information

In addition to vehicle data, a variety of external sensor-generated data, server-based environmental data and even satellite-based positioning information are used as input variables in the ADS. External sensor-generated data includes Car2Car communication. This ensures that the speed and distance of autonomous road users in the vicinity are monitored.

The real-time requirements in the immediate vicinity of autonomous vehicles are obviously higher than those in the superimposed environments, from which, for example, spatial or environmental data are obtained. Decentralization (edge computing) in the IoT network allows the next action decision to be made as close as possible to the distributed sensors. This decision is then made available to higher-level intelligent instances for further coordination and regulation of the overall process. As a result, there are multiple levels of interaction in the IoT network. During the software development process, it is important to consider the transitions between the different interaction levels.

In Section 6, we will consider velocity and position control. It is important to note that the time to acquire data, calculate the next action and provide instructions must be at least twice as fast as the process speed or constant to control the current process in real-time [6]. In addition, certain safety requirements for the ADS can only be ensured by guaranteeing real-time conditions in the information chain. It is obvious that there is some interplay between cybersecurity and safety in terms of real-time requirements. However, this issue is not addressed in this article.

We assume that both cascaded and cross-layer control loops are likely to become necessary to meet the varying requirements of the different layers of the hierarchical model, e.g. hardware, operating system, software, Car2Car, server and cloud. In order to calculate the continuous autonomous driving speed for all collision-free positions, the information chains require the processing of multisensory input information, resulting in a MIMO (multiple input, multiple output) system [7, 8]. We consider the multiple antenna approach on the transport level as given. We also want to evaluate the driving behavior of the AD, and for this purpose we introduce the term “ADS driveability” in Section 7. We want to encourage an objective evaluation of the driving experience of an AD, as this can ultimately be a decisive factor in the competitive use of ADS services.

2. Information chain according to the shell model

In order to achieve real-time control, it is essential that the data acquisition, computation, and provision of the next instruction occur at a speed that is at least twice as fast as the process being controlled [6].

Accordingly, all interaction levels in IoT must be measured for their QoS (Quality of Service) in addition to Round-Trip Times (RTT). Only then can a reliable decision be made as to which processes can be controlled in real-time. Alternatively, the process speeds can be adjusted to the determined real-time characteristics (or real-time limits) of the respective interaction levels. The speed at which the autonomous vehicle performs over the measured interaction level should not exceed half of its real-time capability.

Figure 1 gives a rough overview of the information flow to the IoT interaction levels and back.

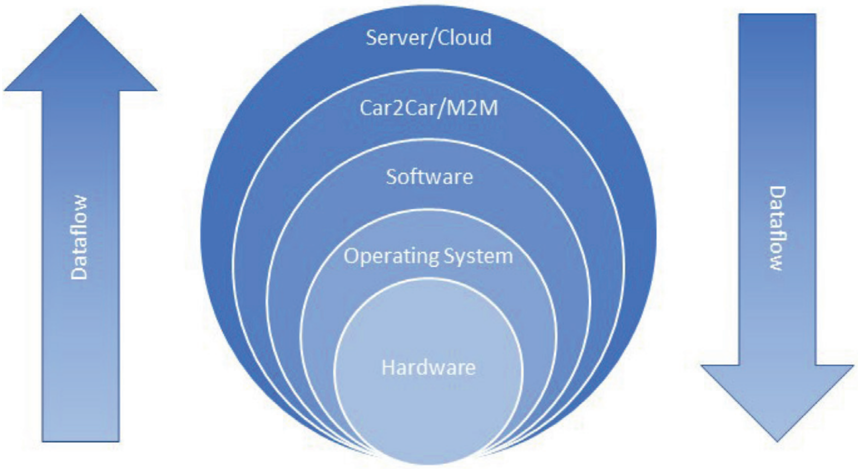

Figure 1.
Shell model for the IoT interaction levels [9].

Our objective is to propose a software development methodology for real-time IoT interactions. The term “propose” implies that this is a sketch that does not claim to be complete, but rather represents one of many possible solutions. Given the enormous complexity of the subject, it cannot be fully represented within the scope of this framework.

3. Cybersecurity und real-time

In the context of autonomous driving, ensuring cybersecurity and real-time capability is crucial. With the increasing networking and automation of vehicles, new challenges and questions arise that will be discussed in this section.

A central problem is ensuring end-to-end cybersecurity under real-time conditions. To do this, security measures must be implemented at all levels of the system, starting with the sensors and extending to communications and the cloud.

Examples include authentication and key exchange under real-time conditions. The typical use of asymmetric crypto methods is problematic for key renewal during

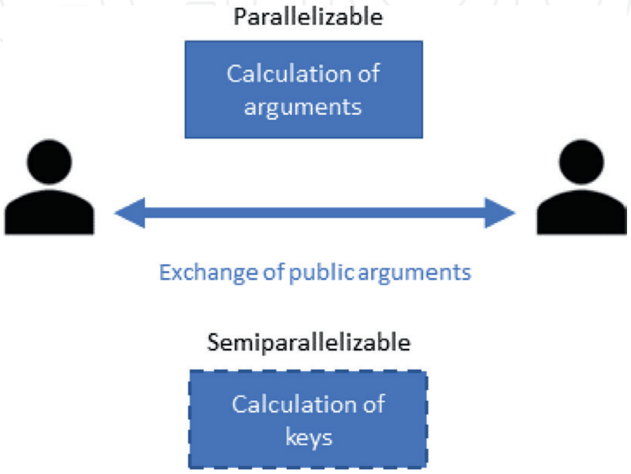

Figure 2.
Challenges of parallelizability in key exchange with asymmetric cryptography.

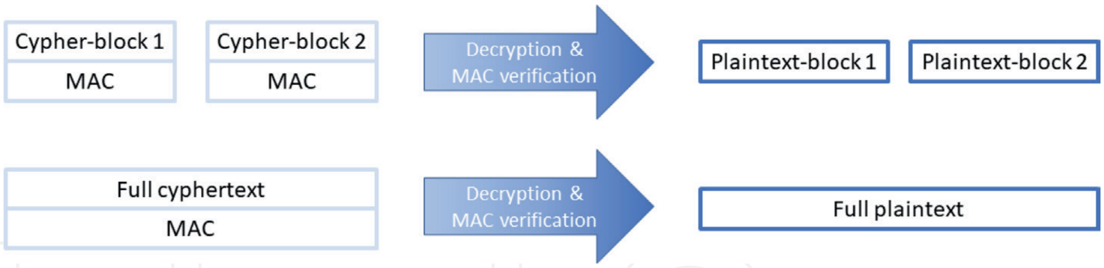

Figure 3.
Example of parallelizing a MAC calculation.

runtime due to their slow runtime. So, if you want to still have real-time capability, you must consider parallel key renewal during runtime (**Figure 2**). In addition, the use of parallelizable crypto algorithms can be an important building block; for example, authentication procedures, such as the Message Authentication Code (MAC) procedure, can be parallelized to guarantee real-time capability (**Figure 3**).

Another component is edge computing, where data processing and analysis take place in the vehicle instead of in the cloud, which can help optimize latency and data rates. This supports real-time guarantees by reducing the amount of data transmitted over the network and increasing the speed of response to events.

A major challenge arises from the fact that vehicles are in the field for a long period of time, so future systems should be prepared for changing crypto computing power and key length requirements by considering or balancing newer crypto techniques such as post-quantum cryptography etc. For example, the ongoing development of quantum computers poses a particular challenge by challenging the security of traditional asymmetric key exchange methods [10].

In summary, ensuring cybersecurity and real-time capability in autonomous driving is a challenging task that requires a combination of different technologies and concepts. The integration of edge computing, parallel key renewal and authentication, as well as the adaptation to future crypto requirements are key elements to ensure the security and performance of autonomous vehicles in the connected world.

4. Real-time management

Our adaptive-real-time-manager (ARM) is an innovative concept that aims continuously assessing and optimizing the real-time capability of autonomous driving systems. This section discusses the basic design of the ARM and its advantages compared to existing solutions.

Factors such as vehicle environment, traffic conditions, visibility, and network connection quality influence the real-time capability of autonomous driving systems. The ARM constantly evaluates these factors and adjusts driving speed and strategy accordingly (**Figure 4**).

A crucial aspect of the ARM concept is the Round Trip Time (RTT) of the closed information chain from the vehicle's sensors and actuators to the cloud and back. The RTT varies depending on the preferred cybersecurity mechanisms, which can be selectively integrated at different security levels.

The ARM assesses the real-time capability of the respective closed information chain by considering the RTT and, if necessary, other system parameters. This enables optimal adjustment of driving speed and strategy to the respective conditions.

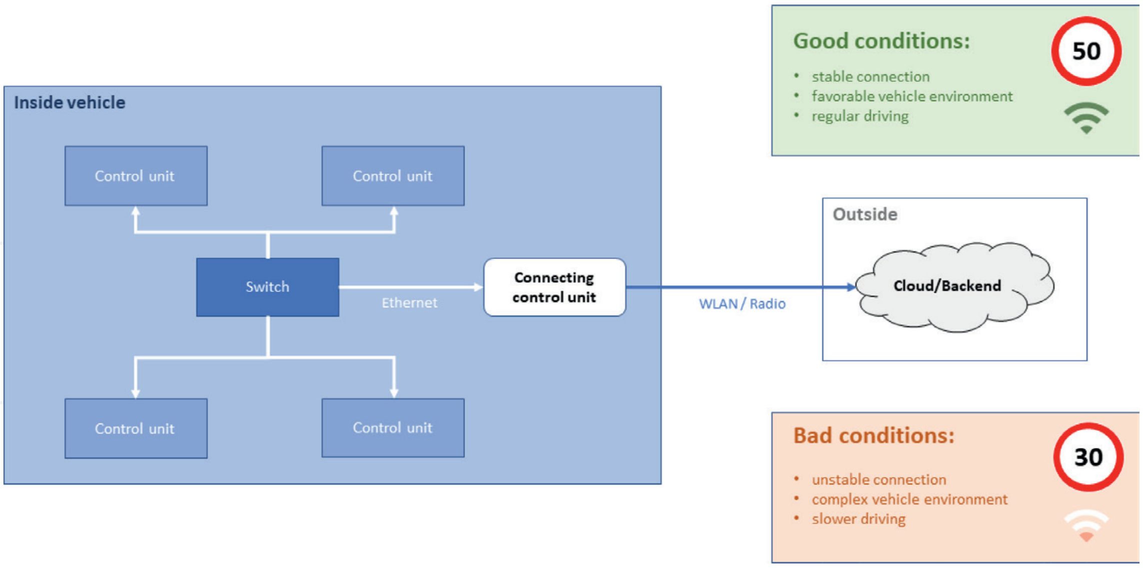

Figure 4.
The ARM might suggest a speed of 50 km/h when the connection quality is good and the vehicle environment is favorable, but only 30 km/h when the connection quality is poor or the vehicle environment is more complex.

The ARM can reduce the impact of traffic control systems on the real-time capability of autonomous driving systems. This is achieved by continuously adapting driving strategies and speeds to the current conditions and, if necessary, to the information provided by traffic control systems.

A real-world scenario illustrates this benefit of ARM: An autonomous vehicle stops before a green light at an intersection. One possible explanation for this behavior is that the intelligent traffic light has informed the autonomous driving system of the time remaining in the green phase. However, the ARM has suggested a driving speed that is not sufficient to cross the intersection without a collision, so in this case the vehicle waits for the next full green phase.

Compared to existing solutions, the ARM offers a more dynamic approach to real-time assessment and optimization of autonomous driving systems. The continuous analysis of influencing factors and the adaptation of driving speed and strategy increase the safety, efficiency and flexibility of these systems.

Another advantage of the ARM is the ability to selectively incorporate cybersecurity mechanisms at different security levels. This ensures data security and system integrity without unnecessarily compromising the real-time capability of the autonomous driving system.

In summary, the automITe Adaptive Real-time Manager offers a promising approach for addressing the challenges related to autonomous driving and cybersecurity. Continuous real-time assessment and optimization, selective incorporation of cybersecurity mechanisms, and enhanced interaction with infrastructure make the ARM a unique and forward-looking solution in this field. It remains to be seen how the ARM will prove itself in real application scenarios and what further developments and optimizations are possible in the future (**Figure 5**).

Together with the ARM there are two essential building blocks that can accelerate the integration into an ADS system:

- Cloud-Broker-Concept: This ensures independence from the cloud provider and a uniform interface on the ADS side to the cloud. An essential step here is the

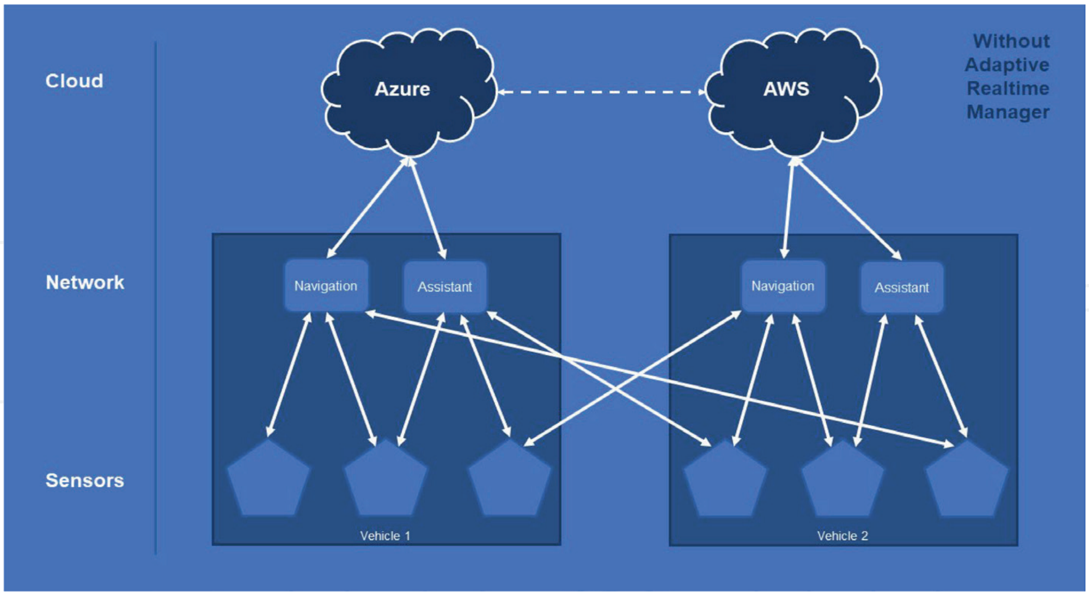

Figure 5.
Typical vehicle architecture without middleware and adaptive-real-time-manager.

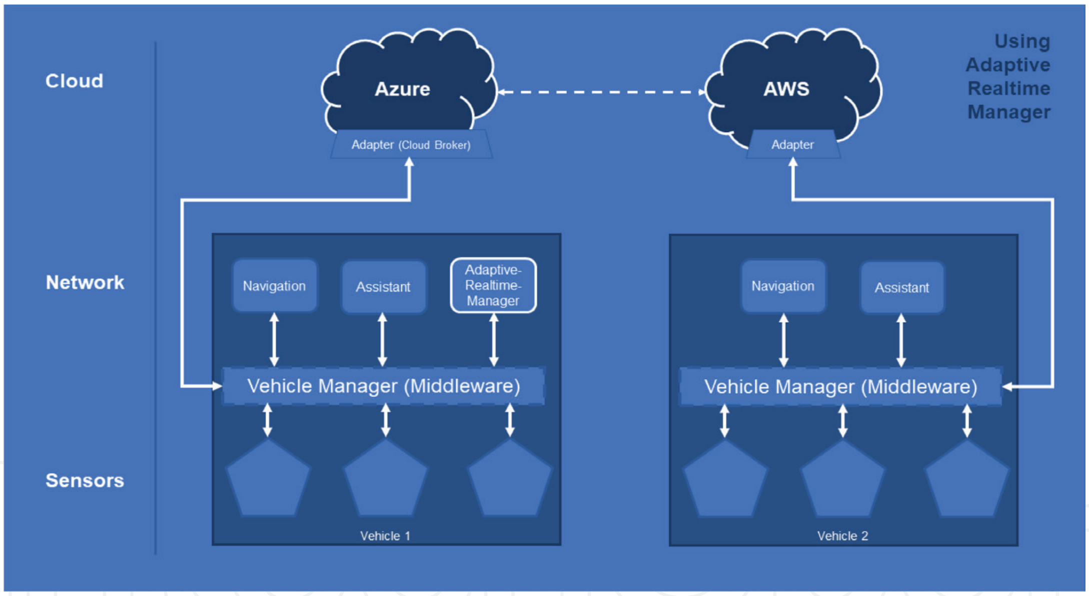
Cloud
Network
Sensors
Azure
AWS
Using Adaptive Realtime Manager
Adapter (Cloud Broker)
Adapter
Navigation
Assistant
Adaptive-Realtime-Manager
Navigation
Assistant
Vehicle Manager (Middleware)
Vehicle Manager (Middleware)
Vehicle 1
Vehicle 2

Figure 6.
Vehicle architecture with middleware and adaptive-real-time-manager in place.

integration and the interface management of the cloud broker into the system of the ARM (see **Figure 6**).

- Simulation of the Adaptive Real-time Manager and the Cloud Broker: For this purpose, we are currently designing a driving simulator that can be used and extended to simulate the driving of a vehicle in a city, with all driving information obtained from the cloud. By using the simulator, the effort required for testing in the field can be reduced, as many shortcomings are already revealed by simulations.

5. Aspects of multisensory data acquisition and processing

Data necessary for driving a car comprised of various sources:

- Physical measurements such as location and speed;
- Events like states of traffic lights
- Linguistic variables like human descriptions of traffic congestion. A linguistic variable gives an imprecise description of some perceived value like high, medium, low.

Physical measurements can be direct and indirect. The direct measurements are performed by various sensors while indirect measurements estimate values from other measurements, events, linguistic variables. The same physical value can be measured by different ways each characterized by different qualities of:

- Accuracy, how close a given set of measurements (observations or readings) are to their true value;
- Precision, how fine measured values can be specified;
- Confidence, the level of trust in the measurement source quantified in some measure like probability or possibility;
- Availability of the measurement source, e.g. in the cases of remote services like satellites, cloud servers, neighbor traffic participants;
- Latency, the time needed for the measurement to become accessible;
- Time span and spatial location of the measurement point.

The events and linguistic variables are characterized by:

- Confidence
- Availability
- Latency
- Time span and spatial location.

Thus the same physical value can be measured by different sensors and estimated indirectly with a great variety in accuracy, confidence, availability. For example, the car speed can be estimated using the car wheels with high availability and low precision; or from the GPS system with low availability, precision and high latency; or from a radar with high precision; or queried from other traffic participants with low confidence etc.

The wide variety of sources must be integrated using plausibility checks and inference based on the reliability and availability of the sources.

Since the sources may contradict each other, the inference model must support conditional reasoning. This is necessary when the confidence measure of a measurement is conditional on some event or other measurements, such as in the case of computed values. At the same time driving has mission critical aspect. Therefore it should allow reasoning under contradiction when different events and measurements contradict each other since so that contradictions be resolved using information from other sources available.

The confidence measure may describe either or both kind of uncertainty:

- Probabilistic resulting from a stochastic measurement process;
- Fuzzy incoming from human estimations and processes of ill-defined nature.

In addition to uncertainty the confidence measure also needs to describe contradiction allowing combination of erroneous sources.

Furthermore, the inference process is a subject of real-time constraints. Therefore the choice of must consider:

- Support of fine-grained parallelism, e.g. when walking down a decision tree of alternatives;
- Gradual refinement of the estimation in order to be able to get an answer even if the deadline was prematurely reached at the cost of accuracy and certainty loss;
- Using conditionals in reasoning and decision making.

The latencies imposed on the measurement process consideration of the time aspect, such as the time stamps and time intervals of the values, events and linguistic variables.

6. AD-velocity and position control

The performance of WLAN communication of multiple antennas is an important aspect in this context, especially as a MIMO system, to improve the channel capacities [11]. However, it essentially concerns the transport level. We consider it as a given [12]. And on the other hand we focus on the MIMO concepts for the control of the driving behavior of an ADS via the information chain [9]. For the present ADS with MIMO (multiple input, multiple output) characteristics [7, 8], we define the multisensory input information in a simplified way as follows:

- Vehicle board data
- External sensor-generated near-field data
- Server and satellite-based information.

The following should be considered as output variables:

- Driving speed and the collision-free
- Current position of the autonomously driving vehicle.

To control the driving behavior of the ADS, the RTT of the information chain plays a crucial role.

Suitable methods for controller synthesis are available according to (Ackermann). For digitization, the choice of sampling time is

$$T = \frac{RTT}{2} \tag{1}$$

or sampling angular frequency is

$$\omega_T = \frac{2\pi}{T} \tag{2}$$

where ω_T, according to the Shannon theorem, is the largest angular frequency occurring in the information chain. However, the angular frequencies of the disturbance signals, the multisensory input variables, and the bandwidths of the controls must also be considered in this context. These considerations apply to both control variables, ADS velocities and the continuous determination of collision-free positions.

7. AD-driveability

Initially, driveability refers to a vehicle's driving dynamics, particularly in terms of power, throttle response, engine, transmission, braking and steering control. It is an important aspect of the overall ride quality of a vehicle and has a significant impact on driver experience and customer satisfaction.

Good driveability means that the vehicle responds smoothly and predictably in all driving situations. Driveability is particularly important in modern vehicles with electronic controls, as it ensures precise and responsive control of the engine and other systems.

Driveability is of high importance for both comfort and safety. For example, in critical situations such as emergency braking or quick evasive maneuvers, good driveability can help the vehicle remain stable and the driver to maintain control.

Autonomous vehicles are not driven by human drivers. Therefore, the term driveability should be redefined as AD-driveability. This creates a basis for objectively evaluating different MaaS and TaaS concepts in terms of driving style and experience.

As far as comfort is concerned, passengers should not be impaired in their activities (working, reading, sleeping…) during the journey. For example, by braking too hard, accelerating too fast or driving in a jerky manner.

Good and safe driving behavior "AD-driveability" will become a competitive factor for autonomous vehicles, as the purchase decision will essentially depend on it. It is expected that the MaaS, TaaS concept, which reaches the destination faster with smooth driving comfort, will achieve a higher acceptance in the MaaS and TaaS service market.

The solutions outlined here, for the correlation of real-time and cybersecurity and adaptive real-time managers can make a decisive contribution to this.

8. Conclusion

This paper has presented a comprehensive overview of various challenges and potential solutions related to autonomous driving and cybersecurity by design.

Ensuring real-time control, end-to-end cybersecurity, and driveability are critical aspects of developing successful autonomous driving systems. The proposed adaptive-real-time-manager (ARM) concept is a promising approach to addressing these challenges by continuously assessing and optimizing the real-time capability of autonomous driving systems while considering various influencing factors and selectively integrating cybersecurity mechanisms.

The integration of edge computing, parallel key renewal, and authentication, as well as the adaptation to future crypto requirements, are essential elements for ensuring the security and performance of autonomous vehicles in the connected world. The Cloud-Broker-Concept and simulation of the Adaptive Real-time Manager and the Cloud Broker further support these efforts by facilitating the integration into an ADS system and allowing for more effective testing and optimization.

Aspects of multisensory data acquisition and processing have also been explored, emphasizing the importance of integrating a variety of data sources and managing uncertainties and contradictions in the inference process. Speed and position control have been addressed as crucial aspects of autonomous driving, highlighting the significance of considering the round trip time of the information chain in controller synthesis.

Finally, the concept of driveability has been discussed in the context of autonomous vehicles, underlining its importance for passenger comfort, safety, and overall user experience. As the field of autonomous driving continues to evolve, the strategies and concepts presented in this paper serve as valuable building blocks for developing secure, efficient, and adaptable autonomous driving systems that meet the demands of an increasingly connected world. Future research and development efforts will undoubtedly reveal new challenges and opportunities for further enhancing the safety, performance, and acceptance of these innovative transportation solutions.

Conflict of interest

The authors declare no conflict of interest.

Author details

Cecil Bruce-Boye[1*], Moritz Krebbel[2], Andreas Fechner[2], Robert Luyken[3]
and Telse David[4]

1 International Project Consultant (iPcon), Lübeck, Germany

2 AutomITe-Engineering GmbH, Lübeck, Germany

3 Hochschule Flensburg, Flensburg, Germany

4 Technische Hochschule Lübeck, Lübeck, Germany

*Address all correspondence to: cecil@bruce-boye.com

References

[1] The Transformation has Begun. Available from: https://www.moia.io/de-DE/innovation. [Accessed: May 9, 2023]

[2] Volkswagen Plans to Make Autonomous Driving Market-ready, 2019. Available from: https://www.volkswagenag.com/en/news/2019/10/autonomous_driving.html. [Accessed: May 9, 2023]

[3] Bruce-Boye C, Kazakov DA. Quality of uni- and multicast services in a middleware LabMap study case? In: Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, Dordrecht: Springer; 2007. pp. 89-94

[4] UN Regulation No. 155 - Cyber Security and Cyber Security Management System. Available from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. [Accessed: May 9, 2023]

[5] UN Regulation No. 156 - Software Update and Software Update Management System. Available from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update. [Accessed: May 9, 2023]

[6] Shannon RV. A model of safe levels for electrical stimulation. IEEE Transactions on Biomedical Engineering. 1992;**39**:424-426

[7] O. Nelles, Regelungstechnik. Siegen: University of Siegen. Available from: https://www.mb.uni-siegen.de/mrt/lehre/rt/rt_skript.pdf. [Accessed: May 9, 2023]

[8] Weiss GHM. Repetitive control of MIMO systems using H∞ design. Automatica. 1999;**35**(7):1185-1199

[9] Bruce-Boye CLDRM. Echtzeit-IoT im 5G-Umfeld. Vol. 39. Wiesbaden: Springer Fachmedien Wiesbaden; DOI: 10.1007/978-3-658-28307-0_14

[10] Shor PW. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Washington, DC Annual Symposium on Foundations of Computer Science, Washington, DC; 1996

[11] Ghayoula ABRG-YE. Capacity and performance of MIMO systems for wireless communications. Journal of Engineering Science and Technology Review. 2014;**7**(3):108-111

[12] Ackermann JPTMAHGFRWT. A robust digital predistortion algorithm for 5G MIMO: Modeling a MIMO scenario with two nonlinear MIMO transmitters including a cross-coupling effect. IEEE Microwave Magazine. 2020;**21**(7):54-62