Věda a perspektivy № 11(30) 2023
ISSN 2695-1584 (Print)
ISSN 2695-1592 (Online

SÉRIE "Podniková ekonomika"

https://doi.org/10.52058/2695-1592-2023-11(30)-394-402

Denys Tsvaig

Specialist- Enterprise Economics.
CEO and Co-Owner of DeHealth
Contributing Writer HackerNoon
https://hackernoon.com/u/denystsvaigDeHealth
12 Mulberry Place, Pinnell Road, London,
United Kingdom, SE9 6AR
https://orcid.org/0000-0003-3228-3765

THE SCIENT ISSUE OF CYBER SECURITY OF AUTONOMOUS SYSTEMS AND ROBOTICS

Abstract. The paper examines the safety of autonomous systems and robots. The analysis of threats related to the use of artificial intelligence in autonomous vehicles, robots, and other autonomous systems was carried out. The importance of cyber security and the imperative of close cooperation between the various disciplines involved in the development of autonomous driving systems, such as vehicle development, software development, and IT security, are emphasised. Information flows in autonomous systems and the technological component of communication are described. It is emphasised that the data generated by external sensors includes communication between various means connected to the overall system. Both cascading and cross-level control loops are defined, emphasising that they become necessary to meet the diverse requirements of all levels of the hierarchical model, such as hardware, operating system, software, server, and cloud. Security issues are outlined, emphasising that the main problem arises from autonomous systems being in the field for long periods of time, so future systems must be prepared for changes in cryptocomputing power and key length requirements, taking into account or balancing new cryptographic techniques such as post-quantum cryptography, etc. An innovative concept is proposed, which is aimed at the constant assessment and optimisation of the capabilities of autonomous driving systems in real-time is an adaptive real-time manager, taking into account the environment of the autonomous vehicle, implementation conditions, visibility, and quality of the network connection, which affect the ability of autonomous driving systems in the real-time mode It is noted that the adaptive real-time manager

offers an approach to solve the problems related to autonomous driving and cyber security.

Keywords: robotics, transportation, artificial intelligence, cyber security, cyber threat, autonomy

Introduction and problem statement. In today's environment, the transition from autonomous individual transport to unmanned mobility with an autonomous driving system (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 a variety of hardware, software, and service portfolios to meet their customers' expectations. Safety level 4 is a top priority: modern vehicles are already equipped with numerous safety and assistance systems, making driving very safe. A modern autonomous transport system needs to be extremely reliable, which is challenging not only in terms of design but also in terms of verification.

ADS-based mobility requires a secure, continuous connection between all road users. Therefore, it relies on a smooth and fast data flow 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 protected, regardless of the point of attack. At the same time, it must be ensured that the time of receipt and response of all data in the relevant information chains is reliable, deterministic, and predictable. Therefore, an appropriate computing infrastructure with cybersecurity - QoS (quality of service) and real-time IoT capabilities is required.

The ADS system must provide both cybersecurity and real-time IoT capabilities across all information chains of the entire system. It is important to conduct the necessary analysis at the design stage to develop concepts, architectures, and strategies that will resolve this tension.

Analysis of recent research and publications. The formulation of scientific thought in security of autonomous systems and robots is heterogeneous and extensive. In the modern scientific field, there are works devoted to the study of cloud services and algorithms for their implementation in intelligent automotive systems to increase the level of cybersecurity.

V. I. Malinovskyi and L. M. Kupershtein [2] analysed the security threats to microcontrollers that are part of autonomous systems and robots. The authors investigated a number of mechanisms for protecting microcontrollers, which together reduce the risks of unauthorised influences on the microcontroller system. These include the following: cyclic control of code redundancy, power monitoring, and resource monitoring, use of isolation and control of the functionality of the clocking system, control of the integrity and reliability of memory contents, control of external

physical and electrical parameters of the MC, virtualisation of the main computing process and its multi-level redundancy by copying and restoring previous states.

C. Sarkar et.al. [3] examined the trends in the development of modern industrial robotics and modern types of industrial robots, as well as the areas of their use. The author draws conclusions about the use of modern industrial robots in various industries.

Among foreign authors, it is worth noting the works of such scholars as: Kshetri Naresh [4], Wang, Yulei, Huang An, Yang Fan, Bian Ning, Zhang Jiazhi, Guo Lulu [5], Takahashi Junko [6], Elihchi Hadi, Hamid Thayer, Akpoduado Maria [7], Anda Maxwell Ekou Okine [8], Tusher Hassan Mahbub, Munim Ziaul, Nottebum Theo, Kim Tae In, Nazir Salman [9], Oreiomi Michael, Jahanhani Hamid [10], Basit Abdul, Kazi Tehmina, Aziz Abdul, Niyazi Abdul, Aziz Ifr]], Gupta Sandeep, Maple Carsten, Passerone Roberto [12], Håkansson Anne, Amberkar Mayuresh [13] and others.

However, despite the scale of scientific research, the relevance of this work is beyond doubt.

Objective. The purpose of the study is to investigate the security of autonomous systems and robots, to analyse the threats associated with the use of artificial intelligence in autonomous vehicles, robots, and other autonomous systems.

Summary of the main research material. With the increase in connectivity and communication between vehicles, traffic control systems, robots, and other infrastructure elements, the likelihood of attack and potential vulnerability also increases. 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 systems by increasing latency and slowing down the response time of autonomous systems. However, with careful planning and innovative solutions, both cybersecurity and real-time performance can be achieved without compromising the security and reliability of autonomous systems.

The importance of cybersecurity has been recognised by legislators, leading to the introduction of UNECE Regulations R.155 and R.156. These regulations set out cybersecurity requirements for 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 capabilities requires close collaboration between the various disciplines involved in the development of autonomous driving systems, such as vehicle design, 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 systems. To achieve this, the following concepts and ideas are presented to effectively combine cybersecurity and real-time capabilities to ensure the safety and functionality of autonomous driving systems.

Information flows in autonomous systems include both input variables to the ADS using a variety of external sensor-generated data, server-side environmental data, and even satellite location information. The data generated by external sensors includes the communication between the various means connected to the overall system.

The real-time requirements in the immediate vicinity of autonomous vehicles are obviously higher than in third-party environments from which, for example, spatial data is obtained. The decentralisation (edge computing) in the IoT network allows a decision on the next action to be made as close to the distributed sensors as possible. 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 several levels of interaction in an IoT network. During the software development process, it is important to consider the transitions between different levels of interaction.

Both cascading and cross-level control loops become necessary to meet the diverse requirements of all levels of the hierarchical model, such as hardware, operating system, software, server, and cloud. To calculate the continuous autonomous driving speed for all collision-free positions, the information chains require the processing of multi-sensor input information, resulting in a MIMO (multiple input, multiple output) system.

In the context of implementing autonomous systems, ensuring cybersecurity and real-time operation is crucial. The main challenge is to ensure end-to-end cybersecurity in real-time. This requires security measures to be implemented at all levels of the system, starting with sensors and extending to communications and the cloud. Examples include real-time authentication and key exchange. The typical use of asymmetric encryption methods is problematic for key updates at runtime due to their slow execution time. For efficient real-time operation, the possibility of parallel key updating at runtime is implemented. In addition, the use of parallelisable crypto algorithms can be an important building block; for example, authentication procedures, such as the message authentication code (MAC) procedure, can be parallelised to guarantee real-time operation.

Another component is edge computing, where data processing and analysis takes place in the underlying control (vehicle, robot, autonomous system) rather than in the cloud, which can help optimise latency and data transfer rates. This supports real-time assurance by reducing the amount of data transmitted over the network and increasing the speed of response to events.

The main challenge arises from the fact that autonomous systems are in the field for long periods of time, so future systems must be prepared for changes in crypto processing power and key length requirements, taking into account or balancing new crypto techniques such as post-quantum cryptography, etc. For example, the ongoing development of quantum computers poses a particular challenge, challenging the security of traditional asymmetric key exchange methods.

An innovative concept aimed at continuously evaluating and optimising the real-time capabilities of autonomous driving systems is the Adaptive Real-time Manager

Věda a perspektivy № 11(30) 2023
ISSN 2695-1584 (Print)
ISSN 2695-1592 (Online

(ARM). Factors such as the environment of the autonomous vehicle, the implementation conditions, visibility, and the quality of the network connection affect the real-time capability of autonomous driving systems. The AMRM continuously evaluates these factors and adjusts the implementation strategy accordingly (Fig. 1).

An important aspect of the AMRF concept is the round-trip time (RTT) of the closed information chain from the sensors and actuators of the autonomous system to the cloud and back. RTT varies depending on the desired cybersecurity mechanisms, which can be selectively integrated at different security levels. The AMRF assesses the real-time capability of the relevant closed information chain, taking into account the RTT and, if necessary, other system parameters. This allows the key parameters to be optimally adapted to the relevant conditions.

Compared to existing solutions, AMRF offers a more dynamic approach to real-time evaluation and optimisation of autonomous systems. Continuous analysis of influencing factors and strategy adaptation increase the security, efficiency, and flexibility of these systems. Another advantage of AMRF is the ability to selectively enable cybersecurity mechanisms at different security levels. This ensures data security and system integrity without unnecessarily compromising the real-time operation of the autonomous system.

Thus, AMRF offers an approach to addressing the challenges associated with autonomous driving and cybersecurity. Continuous real-time evaluation and optimisation, selective activation of cybersecurity mechanisms, and improved interaction with infrastructure make AMRF a unique and promising solution in this area.

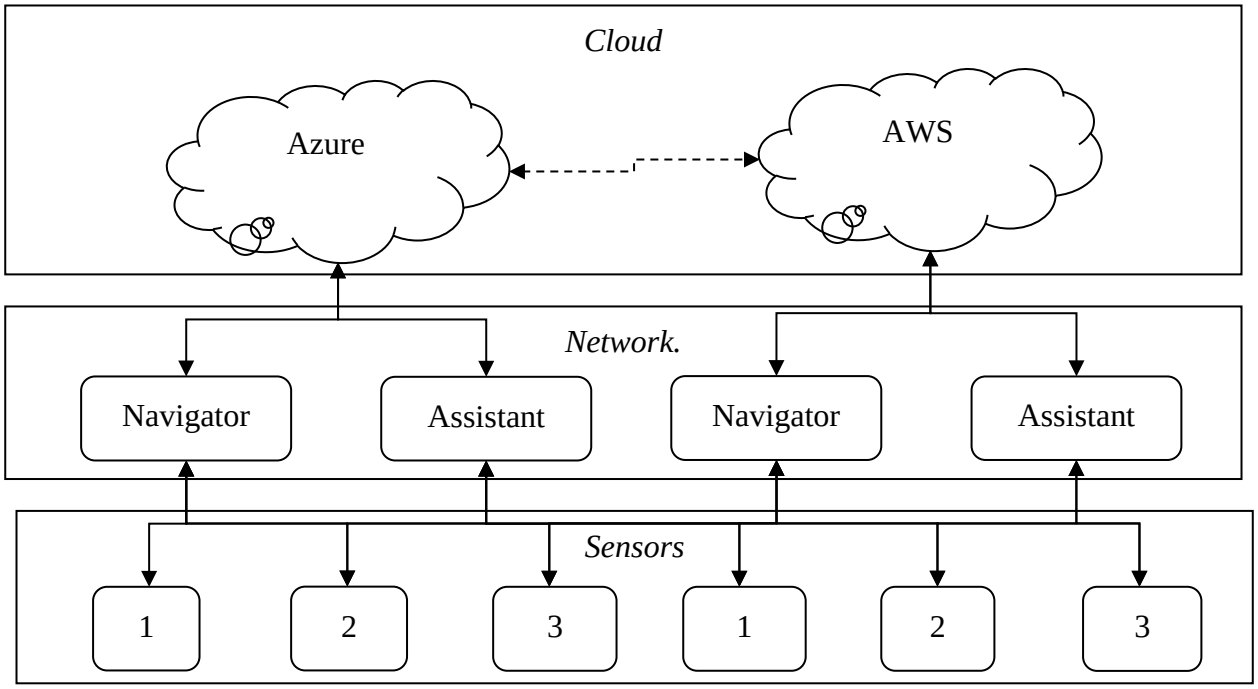

Fig.1 *Typical architecture of an autonomous system without middleware and an adaptive real-time manager*

Along with the AMRF, there are two main building blocks that can accelerate integration into an ADS system:

– Cloud-Broker concept: provides independence from the cloud provider and a single interface on the ADS side to the cloud. An important step here is the integration and management of the cloud broker interface into the ADS system (Figure 2).

– simulation of a real-time adaptive manager and a cloud broker.

By using a simulator, the effort required for field testing can be reduced, as many of the shortcomings have already been identified by the simulation.

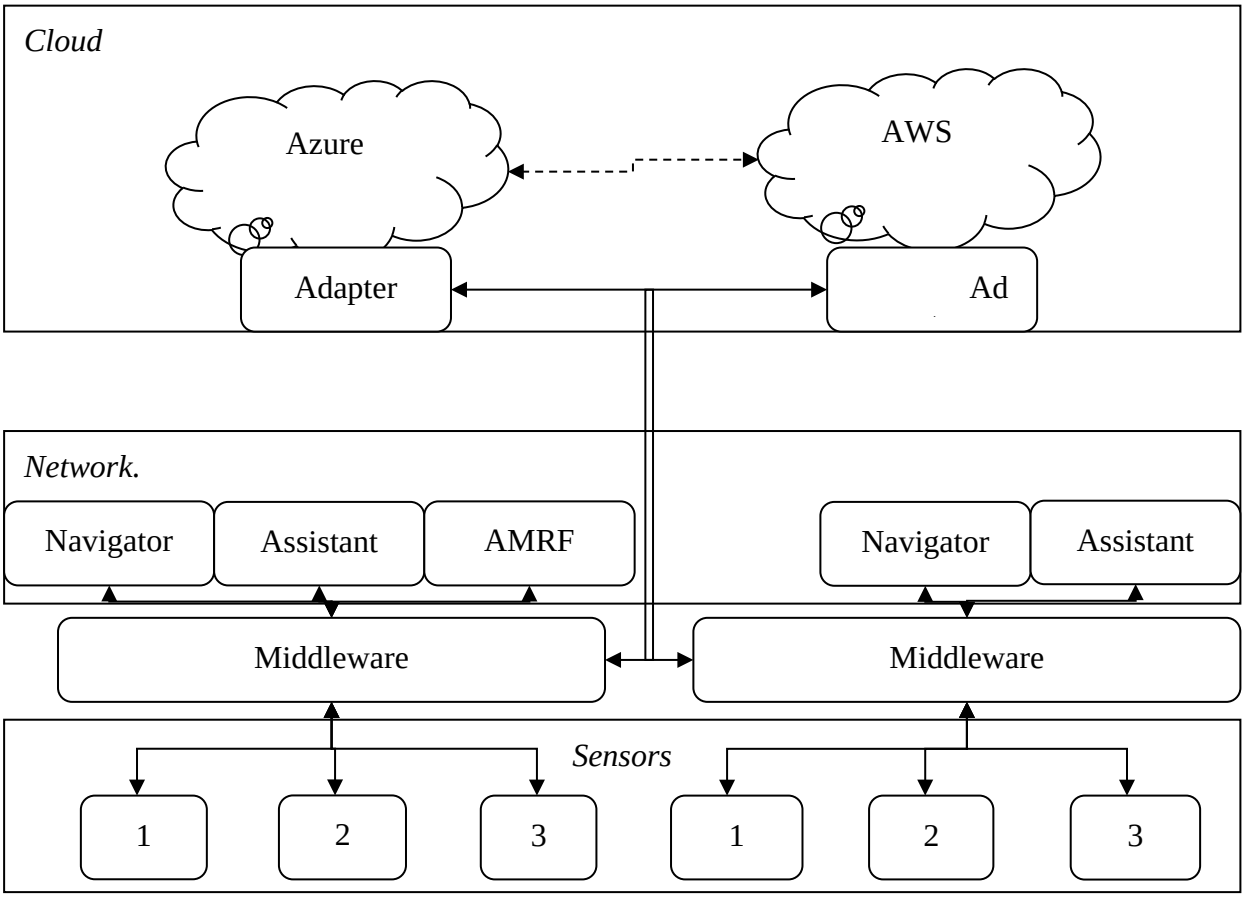

Fig.2 *Architecture of an autonomous system with middleware and adaptive real-time manager*

The data required to control an autonomous system comes from a variety of sources:

– physical measurements such as location and speed;

– external events;

– linguistic variables as a description of a state. A linguistic variable provides an imprecise description of a certain perceived value.

Physical measurements can be direct and indirect. Direct measurements are made by various sensors, while indirect measurements estimate the values of other measurements, events, and linguistic variables.

The same physical value can be measured in different ways, each characterised by different qualities:

– accuracy is the degree to which a given set of measurements (observations or readings) approximates the true value;
– accuracy: how precisely the measured values can be determined;
– confidence, the level of trust in a measurement source, quantified to some degree as a probability or possibility;
– availability of a measurement source, for example, in the case of remote services, such as satellites, cloud servers;
– delay, the time required for the measurement to become available;
– time interval and spatial location of the measurement point.

Thus, the same physical quantity can be measured by different sensors and estimated indirectly with a wide variety of accuracy, confidence, and availability. The large variety of sources must be integrated by means of plausibility checks and inferences based on the reliability and availability of the sources.

Because sources can contradict each other, the inference model must support conditional reasoning. This is necessary when the confidence level of a measurement depends on a specific event or other measurements, for example, in the case of calculated values.

A confidence measure can describe one or both types of uncertainty:

– probabilistic, which is the result of a stochastic measurement process;
– fuzzy data derived from human judgement and uncertain processes.

In addition to uncertainty, a confidence measure should also describe contradictions, which allows for the combination of erroneous sources.

In addition, the inference process is subject to real-time constraints. Therefore, it is necessary to take into account when choosing:

– support for parallelism, for example, when going through the decision tree of alternatives;
– gradual refinement of the estimate to be able to get a response, even if the deadline is reached prematurely at the cost of loss of accuracy and certainty;
– use of conditional words in reasoning and decision-making.

The delays associated with the measurement process take into account the temporal aspect, such as time stamps and time intervals of values, events, and linguistic variables.

The communication performance of a WLAN with multiple antennas is an important aspect in this context, especially as a MIMO system, to improve the channel throughput. But this is mainly a concern for the transport layer.

For existing ADSs with MIMO (multiple inputs, multiple outputs) characteristics, the multisensor input is simplistically defined as follows:

– onboard data of the autonomous system;

– near-field data generated by external sensors;
– information from the server and satellite.

Output variables:

– speed of movement and the absence of collisions;
– the current position of the autonomously controlled system.

To control the behaviour of the ADS in RTT traffic, the information chain plays a crucial role.

Methods of controller synthesis:

selection of the sampling time

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

angular sampling rate

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

where. $\omega_T$according to Shannon's theorem, is the highest angular frequency that occurs in the information chain.

However, the angular frequencies of the interference signals, the multi-sensor input variables, and the bandwidths of the controls must also be considered in this context. These considerations apply to both control variables, ADS speeds, and continuous collision-free position determination.

Conclusions. Providing cybersecurity and real-time control capabilities for autonomous systems is a complex task that requires a combination of different technologies and concepts. Integration of edge computing, parallel key updating and authentication, and adaptation to future cryptographic requirements are key elements to ensure the security and performance of autonomous vehicles in the information world.

Ensuring real-time control, end-to-end cybersecurity, and controllability are critical aspects of developing effective autonomous systems. The proposed concept of an adaptive real-time manager is a promising approach to solving these problems by continuously evaluating and optimising the capabilities of autonomous control systems in real-time, taking into account various influencing factors and selectively integrating cybersecurity mechanisms.

Future research and development will undoubtedly open up new challenges and opportunities to further improve the safety, efficiency, and acceptance of these innovative transport solutions.

References:

1. Narayanan, S., & Antoniou, C. (2023). Shared mobility services towards Mobility as a Service (MaaS): What, who and when? *Transportation Research. Part A, Policy and Practice*, *168*(103581), 103581. https://doi.org/10.1016/j.tra.2023.103581

2. Malinovskyi, V., Kupershtein, L. (2022). Security threats analysis of microcontrollers. *Information technology and computer engineering*, *55*(3), 21–32. https://doi.org/10.31649/1999-9941-2022-55-3-21-32

3. Sarkar, C., Das, B., Rawat, V. S., Wahlang, J. B., Nongpiur, A., Tiewsoh, I., ... & Sony, H. T. (2023). Artificial intelligence and machine learning technology driven modern drug discovery and development. *International Journal of Molecular Sciences*, *24*(3), 2026.

4. Kshetri, N. (2022). *The global rise of online devices, cyber crime and cyber defense: Enhancing ethical actions, counter measures, cyber strategy, and approaches*. Unpublished. https://doi.org/10.13140/RG.2.2.33257.57446

5. Wang, Y., Huang, A., Yang, F., Zhang, J., Bian, N., & Guo, L. (2023). Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles. *Security and Safety*, *2*, 2023027. https://doi.org/10.1051/sands/2023027

6. Takahashi, J. (2018). An overview of cyber security for connected vehicles. *IEICE Transactions on Information and Systems*, *E101.D*(11), 2561–2575. https://doi.org/10.1587/transinf.2017ici0001

7. Elikhchi, H. D., Hamid, T., & Akpoduado, M. (2023). Robotics Cyber Security Issues. In *Lecture Notes in Networks and Systems* (pp. 217–225). Springer Nature Switzerland.

8. Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*.

9. Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, *24*(2), 208–227. https://doi.org/10.1057/s41278-022-00214-0

10. Oreyomi, M., & Jahankhani, H. (2022). Challenges and opportunities of autonomous cyber defence (ACyD) against cyber attacks. In *Blockchain and Other Emerging Technologies for Digital Business Strategies* (pp. 239–269). Springer International Publishing.

11. Basit, A., Qazi, T. F., Niazi, A. A. K., & Niazi, I. A. K. (2023). *Structural analysis of the barriers to address cyber security challenges*. Zenodo. https://doi.org/10.5281/ ZENODO.7908753

12. Gupta, S., Maple, C., & Passerone, R. (2023). *An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles*. https://doi.org/10.36227/techrxiv.20115317.v5

13. Håkansson, A., & Amberkar, M. S. (2022). The Handie system: Hand signs interaction with autonomous, mobile cyber-physical systems. *Procedia Computer Science*, *207*, 3681–3690. https://doi.org/10.1016/j.procs.2022.09.428