CSupMNE
Straightening Up Cybersecurity Posture of Montenegrin Higher Education system

Co-funded by the Erasmus+ Programme of the European Union

*issue# 4, June 2026*

# newsletter

## WORD OF THE EDITOR

**Welcome to this edition of the CSupMNE newsletter! We are pleased to introduce the project's efforts to strengthen cybersecurity resilience in Montenegro's higher education system. The initiative represents an important step toward modernising institutional frameworks, improving digital education, and addressing the growing challenges of cyber threats.**

**In this and future editions, we will share key updates, project activities, and insights contributing to a more secure and cyber-aware academic environment. Thank you to all project partners for your valuable contributions and collaboration in shaping this issue.**

**Editor**: Laura Horvat, University of Maribor; **Featured**: Oliver Popović, Nataša Gospić, Aleksandar Grgurević, Faculty for traffic, communication and logistics; **Shorts**: Slavko Gajin, University of Belgrade; ...., Ministry of Education of Montenegro; **Upcoming events & Announcements**: Milena Ljutica, Institute of Modern Technologies Montenegro; **Project Highlights**: Laura Horvat, University of Maribor; **QA:** Ministry of Education of Montenegro; **Graphical design:** Mediterranean University; **Coordinator**: Assoc. Prof. Dr. Ines Kožuh, University of Maribor, University of Ljubljana.

## Contents:



Subscribe for CSupMNE newsletters: https://csupmne.me/newsletters.php

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

# Cybersecurity Challenges in Vehicular Communication Networks

*Oliver Popović, Nataša Gospić, Aleksandar Grgurević*

*Faculty for traffic, communication and logistics, Budva, Montenegro*

**Traffic sensor networks represent one of the key elements of modern Intelligent Transportation Systems (ITS), enabling real-time data collection, traffic flow analysis, signal management, and support for vehicle-to-infrastructure (V2I) communication. While they have become highly advanced and dynamic to meet modern demands, their growing complexity has simultaneously broadened their attack surface. Today, these systems are highly susceptible to cyber threats that can compromise system functionality, distort data integrity, and directly endanger the physical safety of commuters and road users. Some of the cyber threats include communication interception, unauthorised data modification, DoS attacks, node compromise, injection of false information, and device identity spoofing..**

## 1. Introduction

Electric vehicles (EVs) are among the most important technological advancements shaping today's automotive industry and are essential for the shift toward sustainable and energy-efficient transportation. Besides lowering harmful emissions, EVs bring a high level of digitalisation and automation, turning traditional vehicles into sophisticated cyber-physical systems that combine hardware, software, and communication technologies.

Modern electric vehicles depend extensively on sensor technologies and communication networks to support efficient powertrain performance, battery condition monitoring, reliable braking systems, driver-assistance features, and interaction with the surrounding environment. These technologies continuously gather and process large volumes of real-time data, enabling advanced vehicle capabilities while simultaneously increasing the complexity and potential vulnerabilities of the vehicle's overall architecture.

The advancement of wireless communication technologies has allowed electric vehicles to interact with other vehicles, traffic infrastructure, and remote server platforms. Features such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, together with over-the-air (OTA) software updates, improve both safety and user convenience. However, these technologies also introduce new opportunities for cyber-attacks. Security breaches targeting communication channels may lead to serious risks affecting both vehicle operation and passenger safety.

Sensor networks form the basis of electric vehicle operation, as they enable reliable acquisition of data related to the battery status, electric motor, control systems, and the vehicle's surroundings. If the integrity or availability of this sensor data is compromised, the vehicle may respond incorrectly, potentially resulting in reduced performance or even direct safety risks. For this reason, ensuring the cybersecurity of sensor networks has become one of the major challenges in the development of modern electric vehicles.

## 2. Sensor networks in electric vehicles

Sensor networks in electric vehicles constitute a distributed system made up of various types of sensors, communication buses, and electronic control units (ECUs). Their primary role is to collect, process, and exchange data in real time in order to ensure stable, efficient, and safe vehicle operation (R. Bosch, 2019).

The most commonly used sensors in electric vehicles include temperature, voltage, current, pressure and position sensors. These sensors are connected to key vehicle systems, such as the drive system, braking system and battery management system. Errors or manipulations in sensor data can lead to wrong decisions of control systems and endanger vehicle safety (N. Navet and F. Simonot-Lion, 2009).

### 2.1. Battery Management System (BMS)

The Battery Management System (BMS) is one of the most critical subsystems of electric vehicles. Its basic role is to monitor the state of the battery pack by monitoring the voltage, temperature and state of charge of each individual cell (L. Lu, X. Han, J. Li, J. Hua, and M. Ouyang, 2013).

Based on the acquired sensor data, the Battery Management System (BMS) controls the battery charging and discharging processes, as well as cell balancing operations. Any compromise of sensor data within this system may lead to serious consequences, including decreased battery performance, accelerated battery cell degradation, and possible safety-related incidents (M. A. Hannan, M. M. Hoque, A. Mohamed, and A. Ayob, 2017).

### 2.2. Communication networks in the vehicle

Communication between sensors and electronic control units (ECUs) in electric

vehicles is most commonly established through the Controller Area Network (CAN) bus. The CAN protocol provides reliable and efficient data exchange among various vehicle components, which is why it has become a widely adopted standard in the automotive industry (ISO 11898-1, 2015).

However, the CAN protocol was originally developed without integrated security features such as message authentication and encryption. As a result, CAN networks are vulnerable to unauthorised access and data manipulation, particularly in the case of modern connected vehicles (T. Hoppe, S. Kiltz, and J. Dittmann, 2008).

## 3. Cybersecurity risks

The growing connectivity of electric vehicles has resulted in the emergence of new cybersecurity challenges. Attacks targeting sensor networks may directly affect vehicle and passenger safety, while also compromising the integrity and reliability of critical data.

### 3.1. Attacks on the integrity of sensor data

Attacks targeting the integrity of sensor data are considered among the most serious threats to electric vehicles. These attacks involve altering or falsifying the information transmitted from sensors to control units. Consequently, the vehicle may process incorrect data related to speed, battery temperature, or brake system status. Such attacks can be executed through compromised ECU units, wireless communication channels, or diagnostic interfaces (Y. Mo and B. Sinopoli, 2010).

### 3.2. Unauthorised access to the vehicle's communication network

Unauthorised access to a vehicle's internal communication network represents another major cybersecurity threat. Attackers may gain access through compromised ECUs, diagnostic interfaces, or wireless connections such as Bluetooth and Wi-Fi. This type of intrusion can enable the interception, modification, or blocking of communication messages exchanged between sensors and ECU units (M. Conti, N. Dragoni, and V. Lesyk, 2016).

### 3.3. Denial of Service (DoS) attacks

Denial of Service (DoS) attacks aim to prevent the normal functioning of the system by overloading the communication network. Overloading the CAN bus with a large number of messages can cause delays in communication between sensors and control units, which directly threatens the safety and reliability of the vehicle (R. Mitchell and I. R. Chen, 2014).

## 4. IEEE standards for cybersecurity of sensor networks in modern vehicles

IEEE standards represent the basis for secure communication in modern vehicles, especially in the context of intelligent transportation systems and connected vehicles. Their goal is to provide reliable, authenticated and integrity-protected data exchange between sensors, control units, other vehicles and traffic infrastructure (IEEE Standards for Intelligent Transportation Systems).

### 4.1. IEEE 1609 – the basic security standard for connected vehicles

IEEE 1609 represents a family of protocols known as WAVE (Wireless Access in Vehicular Environments), designed to enable secure data exchange within connected and autonomous vehicle ecosystems. Of particular importance is the IEEE 1609.2 standard, which specifies security services for communication between vehicles and transportation infrastructure (IEEE Std 1609.2-2016).

The main security functions defined by the IEEE 1609 standard include authentication of communication participants, protection of message integrity, and digital certificate management. Each vehicle and infrastructure component is assigned cryptographic keys that enable verification of the sender's identity, thereby significantly reducing the risk of transmitting false or malicious messages (J. Harding et al, 2014).

In the context of electric vehicle sensor networks, IEEE 1609 enables the secure exchange of critical data, including traffic condition data, safety alerts, and sensor data shared among vehicles.

### 4.2. The role of IEEE 1609 in the protection of sensor networks

The implementation of the IEEE 1609 standard is particularly important for protecting sensor networks, as it enables cryptographic protection of sensor-generated data during transmission. In addition, the standard includes mechanisms for preserving user privacy through the use of temporary certificates, thereby reducing the possibility of long-term vehicle tracking.

### 4.3. Other IEEE standards (brief overview)

In addition to IEEE 1609, several other IEEE standards are used in the field of electric vehicle communications. The IEEE 802.11p standard defines the physical and MAC communication layers for vehicular networks and serves as the foundation for the implementation of WAVE protocols. Its function is primarily technical (IEEE Std 802.11p-2010).

Other IEEE standards and recommendations are used to supplement the basic safety framework, but do not represent central safety standards for sensor networks in electric vehicles.

### 4.4 Comparative review and application of safety standards

The first two ISO standards are process-oriented and address the internal operation of vehicle systems throughout their entire life cycle, whereas the third standard (IEEE 1609) is a technical protocol intended for secure communication between vehicles and the external environment.

ISO 26262 is focused on functional safety and the mitigation of risks caused by unintended system failures. ISO/SAE 21434 provides the fundamental framework for

| Threat | Description | ISO 26262 | ISO/SAE 21434 | IEEE 1609 |
|---|---|---|---|---|
| Attacks on sensor data integrity | Modification or falsification of sensor data transmitted to control units | Partially (fault detection and functional safety mechanisms) | Yes (TARA-based risk management and integrity protection measures) | Yes (cryptographic protection of transmitted messages) |
| Unauthorised access to vehicular networks | Unauthorised access to in-vehicle or V2X communication networks | No | Yes (access control, authentication, and cybersecurity controls) | Yes (certificate-based authentication and secure communication) |
| Denial-of-Service (DoS) attacks | Disruption of communication availability through network overload | No | Partially (system resilience and risk mitigation measures) | Yes (communication control and message handling mechanisms) |

Table 1. Comparative review of safety standards in vehicular networks

managing cybersecurity threats through the TARA methodology, while IEEE 1609 enables cryptographically secured V2X communication.

## Conclusion

The combined implementation of ISO/SAE 21434, ISO 26262, and IEEE 1609 provides a balanced and effective approach to securing sensor networks in electric vehicles, with each standard having a clearly defined role.

Although ISO 26262 is primarily focused on functional safety, it contributes to the overall resilience of the system through the identification of critical components and the assessment of the consequences of their potential failures. IEEE 1609 standards, on the other hand, provide technical mechanisms for secure V2X communication, thereby protecting the data exchanged between vehicles and infrastructure.

ISO/SAE 21434 represents the central framework for cybersecurity risk management, as it enables the systematic identification and assessment of threats through the TARA methodology, along with the definition of appropriate protection measures throughout the entire vehicle life cycle. This standard directly addresses threats such as sensor data integrity attacks, unauthorised network access, and DoS attacks (ENISA, 2019).

The comparative analysis of the standards presented in the table confirms that ensuring the security of sensor networks in electric vehicles requires the integrated application of multiple complementary approaches. Various types of threats cannot be effectively mitigated by a single standard alone; instead, it is necessary to combine both procedural and technical security mechanisms.

Modern electric vehicles are no longer just mechanical devices, but complex cyber-physical systems in which the violation of the integrity of sensors or communication networks directly threatens the physical safety of passengers and the stability of the entire traffic flow. Given that the implementation of key standards requires a deep understanding of risks in V2X communication and vehicle internal systems, the study of cyber security is becoming an indispensable topic in the education of traffic engineers. Without this integrated knowledge, future experts will not be able to adequately design, manage and ensure the safety of modern e-mobility and intelligent transport systems.


Literature

1. R. Bosch GmbH, Automotive Handbook, 10th ed., Wiley, 2018.
2. N. Navet and F. Simonot-Lion, Automotive Embedded Systems Handbook, CRC Press, Boca Raton, FL, USA, 2009.
3. L. Lu, X. Han, J. Li, J. Hua, and M. Ouyang, "A review on the key issues for lithium-ion battery management in electric vehicles," Journal of Power Sources, vol. 226, pp. 272–288, 2013.
4. M. A. Hannan, M. M. Hoque, A. Mohamed, and A. Ayob, "Review of energy storage systems for electric vehicle applications," Renewable and Sustainable Energy Reviews, vol. 69, pp. 771–789, 2017.
5. ISO 11898-1, Road vehicles – Controller Area Network (CAN), International Organisation for Standardization, 2015.
6. T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks – Practical examples and selected short-term countermeasures," International Conference on Computer Safety, Reliability and Security, 2008.
7. M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," Workshop on Embedded Security in Cars (ESCAR), 2004.
8. A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway," Wired Magazine, 2015.
9. Y. Mo and B. Sinopoli, "False data injection attacks in control systems," Proceedings of the First Workshop on Secure Control Systems, 2010.
10. M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.
11. R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," ACM Computing Surveys, vol. 46, no. 4, 2014.
12. IEEE Standards Association, IEEE Standards for Intelligent Transportation Systems, IEEE, New York, USA.
13. IEEE Std 802.11p-2010, Wireless Access in Vehicular Environments (WAVE).
14. H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008.
15. IEEE Std 1609.2-2016, Standard for Wireless Access in Vehicular Environments – Security Services.
16. J. Harding et al., "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," National Highway Traffic Safety Administration (NHTSA), 2014.
17. ISO/SAE 21434, Road Vehicles – Cybersecurity Engineering, International Organization for Standardization, 2021.
18. AUTOSAR Consortium, Specification of Secure Onboard Communication, Release 4.x.
19. ENISA, Cybersecurity and Resilience of Smart Cars, European Union Agency for Cybersecurity, 2019.

# Bridging Theory and Practice: Advanced Cybersecurity Programme in Belgrade

*Addressing the growing interest among students in complementing their primarily theoretical cybersecurity knowledge with practical skills, Professor Slavko Gajin from the University of Belgrade delivered a series of training sessions from February to May within the Palo Alto Networks Academy programme, organised by the American Resource Centre Belgrade. The programme gathered 25 carefully selected final-year students from several universities across Serbia.*

The training programme consisted of two courses: Cybersecurity Foundations and Network Cybersecurity Fundamentals.

- In the Cybersecurity Foundations course, students gained insight into the current cybersecurity landscape and the fundamental concepts required to recognise and mitigate attacks targeting enterprise networks and critical infrastructure. Participants also learned the basics of configuring security zones, authentication mechanisms, and policies on next-generation firewalls. Special attention was devoted to the growing role of artificial intelligence in modern cybersecurity
- he Network Cybersecurity Fundamentals course focused on more advanced technical topics related to securing modern network environments. Students explored endpoint and network security technologies, encryption algorithms, key management concepts, and the role of digital certificates in secure communications. The course also covered practical applications of traffic encryption and certificate verification mechanisms.

Each lecture was accompanied by hands-on laboratory exercises performed on virtual firewall platforms. Through these practical sessions, students developed valuable technical skills and gained experience in configuring modern security technologies and solving real-world cybersecurity challenges.

At the end of the training programme, several companies presented their business activities and service portfolios, as well as opportunities for early-career professionals to begin and develop their careers in the cybersecurity industry.

## UPCOMING EVENTS & ANNOUNCEMENTS

As part of the project's upcoming capacity-building activities, two online trainings and one onsite workshop will be organised in **June and July 2026** for representatives of **Montenegrin higher education institutions**. The activities are coordinated by Hochschule Furtwangen and aim to strengthen institutional preparedness, resilience, and cybersecurity awareness across the higher education sector.

The first online training, **"Technology Infrastructure Resilience for Montenegrin Higher Education Institutions" (June 8, 2026)**, will focus on resilience planning, network and access protection, environmental safeguards, redundancy mechanisms, and capacity management. Through practical exercises and case studies, participants will work on developing institutional resilience action plans tailored to higher education environments.

The second online training, **"Awareness and Training for Montenegrin Higher Education Institutions" (June 9, 2026)**, will address cybersecurity awareness and institutional training practices. Topics will include user awareness, phishing prevention, role-based training approaches, onboarding processes, and methods for measuring the effectiveness of awareness programmes.

In addition, a three-day onsite training will take place from **8–10 July 2026** at the **Schwenningen Campus of Hochschule Furtwangen**, bringing together project partners and participants for collaborative discussions, practical sessions, and further knowledge exchange.

# 2nd Consortium Meeting: Project Coordination and Progress Overview

*The **2nd Project Coordination (Consortium) Meeting** was held on **26 November 2025** at the **University of Montenegro (Rectorate building, Podgorica)**, bringing together members of the Project Management Board to review progress and coordinate upcoming project activities.*

The meeting opened with an overview of the overall project progress, including key updates from Work Package 1 and planning activities for Work Package 5, with a focus on ensuring alignment between strategic objectives and implementation timelines. Special attention was given to the coordination of ongoing and upcoming project deliverables. A detailed progress review of Work Package 3 was presented by the project coordinator, outlining achievements and next steps in strengthening cybersecurity capabilities across partner institutions. This was followed by updates from Work Package 4, where partners presented developments in key deliverables, including contributions from the **University of Maribor**, **AGH University of Krakow**, and **University Mediterranean**. These activities are central to the development of technical and operational cybersecurity solutions within the project. The meeting concluded with a comprehensive overview of Work Package 10, dedicated to dissemination and visibility activities. Partners shared progress on the organisation of the **first annual project conference**, **networking event**, and **roundtable discussions**, alongside measurable indicators related to project visibility and outreach.

Overall, the Consortium Meeting reinforced coordination among partners and ensured a shared understanding of progress, challenges, and priorities, contributing to the continued advancement of cybersecurity capacity-building within the project.

# National Meeting with Montenegrin Partners in Podgorica

From **25 to 27 November 2025**, a **National Meeting combined with hands-on training** was held at the **University of Donja Gorica**, bringing together Montenegrin project partners. The event focused on coordination and practical implementation of cybersecurity activities within the project.

Participants discussed the **submission of deliverables within WP4**, the **development of cybersecurity-related documents**, and the **operational challenges faced by institutions**. The hands-on format enabled exchange of experiences and alignment of approaches to strengthening cybersecurity practices at the national level.

# Quality Control Board Meeting: Ensuring Quality and Continuous Improvement

*The **2nd Quality Control Board (QCB) Meeting** took place on **27 November 2025** at the **University of Montenegro**, focusing on the development and implementation of quality assurance mechanisms across project activities.*

The meeting began with an overview of quality control progress, highlighting the importance of systematic evaluation in achieving project objectives and maintaining high standards in cybersecurity training and outputs. The discussion emphasised the need for consistent monitoring and documentation of quality indicators throughout the project lifecycle.

A significant part of the meeting was dedicated to the **quality control of training activities**. Participants reviewed existing quality assurance instruments and discussed the introduction of structured **evaluation mechanisms following each training event**, as well as comprehensive assessment approaches for entire training sets. These mechanisms are essential for ensuring that training activities effectively build cybersecurity competencies across participating institutions.

The final session addressed **dissemination and sustainability (WP10)**, where partners explored quality control measures for improving communication and outreach activities. Participants contributed suggestions for enhancing dissemination impact, strengthening stakeholder engagement, and ensuring the long-term sustainability of project results.

The QCB Meeting highlighted the critical role of quality assurance in cybersecurity capacity-building projects, ensuring that all activities—from training delivery to dissemination—are continuously evaluated, improved, and aligned with project goals and stakeholder needs.

# In-person Training in Podgorica: Development of a Cybersecurity Strategy

*The threeday handson training "Development of a Cybersecurity Strategy for Higher Education Institutions in Montenegro" took place from **25 to 27 November 2025** at the **University of Donja Gorica**. The event was organized and coordinated by the University of Donja Gorica. The training opened with a welcome address by **Prof. dr. Milica Vukotić**, followed by an introduction by **Prof. dr. Ramo Šendelj**, the project coordinator. Throughout the first day, participants engaged in sessions led by experts from AGH University (**Prof. dr. Jerzy Duda**), the University of Maribor (**Prof. dr. Ines Kožuh**, **asist. Irena Lovrenčič Držanič**, and **Laura Horvat**), and the University of Belgrade (**Prof. dr. Slavko Gajin**), covering topics such as cybersecurity strategy development, security awareness and training policies, and acceptable use of IT resources.*

The second day continued with an indepth exploration of security awareness and training policies delivered by the **Prof. dr.**

**Ines Kožuh**, **Irena Lovrenčič Držanič**, and **Laura Horvat**. This was followed by a session on information security risk management presented by **Niels Schneider** from the University Furtwangen. In the afternoon, **Prof. dr. Slavko Gajin** introduced the Identification and Authentication Policy, offering practical insights into secure access management within higher education institutions.

On the final day, the training focused on advanced policy development. **Prof. dr. Jerzy Duda** delivered a comprehensive session on Information Security Policy, followed by a detailed presentation on Risk Assessment Policy by **Niels Schneider**. In the afternoon, all EU partners jointly conducted a mentoring session dedicated to supporting Montenegrin higher education institutions in drafting cybersecurityrelated documents.

The training was successfully completed, contributing significantly to the project's objective of enhancing cybersecurity frameworks across Montenegro's higher education sector.

# In-person Training in Maribor: Cybersecurity Identify Function: From Assets to Risk

The training **"Developing Organisational Understanding to Manage Cybersecurity Risk"** was held in person in **Maribor, Slovenia**, from **17 to 19 February 2026**, and was organised by the **University of Maribor**. Bringing together cybersecurity experts and representatives of higher education institutions, the event provided an intensive, practice-oriented learning environment focused on strengthening institutional cybersecurity capabilities. The training guided participants from establishing organisational context and ownership mapping toward the prioritisation of institutional assets based on mission impact.

# Building the Foundation: Assets and Organisational Context

The training began with a structured exploration of the Identify Function, forming the basis for riskdriven cybersecurity management in higher education institutions. Under the guidance of **Dr. Ines Kožuh** (University of Maribor and University of Ljubljana), participants examined the organisational context necessary for effective cybersecurity governance, including systems, processes, and institutional responsibilities. The session also introduced the development of Information Security Policies aligned with international standards. Building on this foundation, **Dr. Iryna Bashynska** (AGH University of Krakow) led participants through asset management fundamentals, helping them categorise institutional assets and draft tailored Acceptable Use Policies to reduce humanrelated risks. The practical dimension continued with **Dr. Jerzy Duda** (AGH University of Krakow), who guided participants in creating structured asset inventories and linking them to Access Control Policies. The first thematic block concluded with a missionbased prioritisation approach delivered by **Dr. Jerzy Duda** and **Dr. Joanna Duda**, enabling institutions to classify assets by operational importance and develop Identification and Authentication Policies incorporating MFA, privileged access management, and recovery mechanisms.


# Risk Assessment in Practice and Operational Capabilities

The second thematic block focused on translating asset knowledge into structured risk assessment and operational readiness. **Gorazd Božič** (SICERT, Slovenia) opened the day with a comprehensive session on establishing a CSIRT, covering legal foundations, organisational models, and coordination with national cybersecurity structures. The programme then shifted to understanding cybersecurity risks in HEIs, with **Dr. Ines Kožuh** guiding participants through threat–vulnerability relationships and realistic academicsector scenarios such as ransomware and insider misuse. **Irena Lovrenčič Držanič** (University of Maribor) expanded this foundation by introducing practical risk assessment methodologies, including likelihood–impact scoring and heatmap visualisation, while also addressing formal Security Assessment and Authorization Policies. The block continued with **Dr. Iryna Bashynska**, who led participants in developing structured risk registers and connecting them to Incident Response Policies through standardised documentation and severity classification. Finally, **Irena Lovrenčič Držanič** returned to guide participants through prioritising risk responses using mitigation, transfer, avoidance, and acceptance strategies, ensuring alignment with institutional risk tolerance and regulatory requirements.

# Continuous Improvement and Cybersecurity Maturity


The final thematic block addressed the longterm sustainability of cybersecurity practices through continuous improvement. **Niels Schneider** (Hochschule Furtwangen University) introduced contingency planning principles, emphasising business impact analysis, recovery strategies, and alignment with NIST guidance. He continued with a session on cybersecurity testing and exercises, where participants designed and evaluated tabletop simulations of realworld incidents to assess organisational readiness and response coordination. The capstone sessions, led by **Dr. Slavko Gajin** (University of Belgrade), integrated all previous learning into a comprehensive institutional improvement cycle, covering vulnerability management, security logging, and information classification. Participants then presented their Identifybased cybersecurity foundation plans, combining asset inventories, risk registers, and improvement frameworks. Peer review and expert feedback ensured that the outputs were robust, actionable, and adaptable to diverse higher education environments.

## Overall Training Outcome

The Maribor training successfully guided participants through the full lifecycle of the **Identify Function**, from asset discovery and classification to risk assessment, response planning, and continuous improvement. By combining theoretical frameworks with hands-on exercises, participants developed practical outputs, including asset inventories, risk registers, and institutional cybersecurity foundation plans, providing a strong basis for further implementation of the NIST Cybersecurity Framework in higher education environments.