INTEC

Co-funded by the European Union

UNIVERSITETI POLIS

BOOK OF PROCEEDINGS

INTERNATIONAL CONFERENCE

SUSTAINABLE MOBILITY

5-6 MARCH

2026

The INTEC International Conference brings together academics, researchers, policymakers and industry experts to discuss innovative approaches and collaborative solutions for a sustainable future in engineering and mobility. The conference will be hosted by POLIS University in Tirana, Albania, and co-organized by partners from across the EU as part of the Erasmus+ CBHE Project 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2.

INTEC International Engineering Competence Centres to push sustainable mobility development in Albania and Montenegro
Project Reference: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project Partners:

FH JOANNEUM University of Applied Sciences · Frankfurt University of Applied Sciences · UPT · UCG · UDG · AVL · GAMA-AUTO · ALFA Centar

ISBN 9789928347268

DOI: 10.37199/c41001000

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

Partner Universities

Project Coordinator: FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Frankfurt University of Applied Sciences (FRA-UAS), Germany
University of Split (US), Croatia
POLIS University (POLIS), Albania
Polytechnic University of Tirana (PUT), Albania
University of Vlore "Ismail Qemali" (UV), Albania
University of Montenegro (UOM), Montenegro
Adriatic University Bar (FSKL), Montenegro
University of Donja Gorica (UDG), Montenegro
AVL List GmbH (AVL), Austria
Gama Auto d.o.o. (GA), Montenegro
NVO Alfa Centar (AC), Montenegro

Conference Chair

DI Daniela Wenzl
Dr. Elona Karafili
Dr. Flora Krasniqi

Conference Keynote Speaker

DI Horst Pflügl, AVL List GmbH (AVL), Austria
MSc. Mine Bushi, General Directorate of Road Transport Services in Albania

Scientific Committee

Prof. Emeritus Dr. Nataša Gospić, Adriatic University Bar (FSKL), Montenegro
Prof. Dr. Bhavin Kapadia, FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Assoc. Prof. Dr. Ivan Tolj, University of Split (US), Croatia
Prof. Dr. Kristofor Lapa, University of Vlore "Ismail Qemali" (UV), Albania
Prof. Dr. Damir Sedlar, University of Split (US), Croatia
Prof. Dr. Boško Ilija Matović, University of Montenegro (UOM), Montenegro
MA Adrian Millward-Sadler, FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Dr. Anis Sulejmani, Polytechnic University of Tirana (PUT), Albania
Dr. Enkelejd Mëhilli, University of Vlore "Ismail Qemali" (UV), Albania
Dr. Blenard Xhaferraj, Polytechnic University of Tirana (PUT), Albania
Dr. Elona Karafili, POLIS University (POLIS), Albania
Dr. Flora Krasniqi, POLIS University (POLIS), Albania
Dr. Ivana Ognjanović, University of Donja Gorica (UDG), Montenegro

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

Organizing Committee

DI Daniela Wenzl
Dr. Keti Hoxha
Dr. Flora Krasniqi
Dr. Elona Karafili
MSc. Sadmira Malaj
MSc. Sindi Doce
MSc. Glejdi Fejza

TABLE OF CONTENTS

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

34

CYBERSECURITY CHALLENGES IN MODERN VEHICULAR COMMUNICATION NETWORKS

DOI: 10.37199/c41001034

Aleksandar GRGUREVIĆ
Faculty for Traffic, Communication and Logistics, Budva, Montenegro
alexandargrgurevic@gmail.com

Nataša GOSPIĆ
Faculty for Traffic, Communication and Logistics, Budva, Montenegro

Oliver POPOVIĆ
Faculty for Traffic, Communication and Logistics, Budva, Montenegro

Abstract

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. With the development of concepts such as smart cities and autonomous vehicles, these networks are becoming increasingly complex and dynamic, but simultaneously more vulnerable to cyberattacks that can jeopardise their functionality, data accuracy, and the safety of traffic participants. Due to the large number of nodes, wireless communication methods, and limited computational resources of the sensors, these networks are exposed to risks such as communication interception, unauthorised data modification, DoS attacks, node compromise, injection of false information, and device identity spoofing.

This paper analyses the fundamental security challenges that accompany the operation of traffic sensor networks, as well as the potential consequences that a successful attack can have on the transport system, including improper traffic light management, creation of artificial congestion, disruption of autonomous driving algorithms, and endangering the physical safety of drivers.

The aim is to provide a comprehensive overview of the most significant threats, standards, and recommended security mechanisms, as well as to highlight the importance of a systemic approach to protecting traffic sensor networks as a critical component of the future transportation ecosystem.

Keywords: cybersecurity, threats, vehicular networks

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

I. INTRODUCTION

Electric vehicles (EVs) represent one of the key technological trends in the development of the modern automotive industry and play a significant role in the transition to sustainable and energy-efficient transport systems. In addition to reducing harmful gas emissions, electric vehicles introduce a high degree of digitisation and automation, which transforms the classic vehicle into a complex cyber-physical system that integrates hardware, software and communication technologies.

Modern electric vehicles rely heavily on sensor systems and communication networks to ensure efficient operation of the drive system, battery health monitoring, safe braking, driver assistance and interaction with the environment. These systems collect and process large amounts of data in real time, which enables advanced functionalities, but at the same time increases the complexity and vulnerability of the overall vehicle architecture.

The development of wireless communication technologies has enabled electric vehicles to connect with other vehicles, traffic infrastructure and remote server systems. Functionalities such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, as well as remote software updates (OTA - Over-the-Air), contribute to increased security and comfort, but at the same time open up new vectors of cyber-attacks. Attacks on these communication channels can have serious consequences for the safety of vehicles and passengers.

Sensor networks represent the basis of the functioning of electric vehicles, as they provide a reliable collection of information about the condition of the battery, electric motor, control system and vehicle environment. If the integrity or availability of sensor data is compromised, the vehicle may make wrong decisions, which may lead to reduced performance or a direct threat to safety. Therefore, the cybersecurity of sensor networks becomes one of the key challenges in the development of electric vehicles.

The aim of this paper is to provide an overview of sensor networks in electric vehicles, identify the most important cybersecurity risks related to these systems and analyse the role of IEEE standards in ensuring secure communication. Special emphasis is placed on the IEEE 1609 standard as the basic security framework for connected vehicles, while other relevant standards are discussed in a brief overview [1–7].

1. Sensor networks in electric vehicles

Sensor networks in electric vehicles represent a distributed system composed of different types of sensors, communication buses and electronic control units (ECU). Their basic function is to collect, process and exchange data in real time in order to enable stable and safe driving of the vehicle [4].

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

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 [5]

1.1. 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 [6].
Based on the collected sensor data, the BMS regulates the charging and discharging processes of the battery, as well as cell balancing. Compromising sensor data in this system can have serious consequences, including reduced battery efficiency, accelerated cell degradation, and potential security incidents [7].

1.2. Communication networks in the vehicle

Communication between sensors and electronic control units in electric vehicles is most often realised via the Controller Area Network (CAN) bus. The CAN protocol enables reliable and efficient data exchange between different vehicle components, which makes it a standard in the automotive industry [8].
However, the CAN protocol was designed without built-in security mechanisms, such as message authentication and encryption. This shortcoming makes the CAN network vulnerable to unauthorised access and data manipulation, especially in the context of modern connected vehicles [9].

2. Cyber security risks

The increasing connectivity of electric vehicles is leading to the emergence of new cybersecurity threats. Attacks on sensor networks can have a direct impact on the safety of vehicles and passengers, as well as on the integrity and reliability of data.

2.1. Attacks on the integrity of sensor data

Attacks on the integrity of sensor data represent one of the most dangerous threats to electric vehicles. These attacks are based on the modification or falsification of the data that the sensors send to the control units. As a result, the vehicle may receive incorrect information about speed,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

battery temperature or brake system status. Such attacks can be carried out through compromised ECU units, wireless communication or diagnostic ports [12,13].

2.2. Unauthorised access to the vehicle's communication network

Unauthorised access to the vehicle's internal communication network represents another significant security risk. An attacker can gain access to the network through compromised ECUs, diagnostic ports, or wireless interfaces, such as Bluetooth and Wi-Fi. This type of attack can allow interception, modification or blocking of communication messages between sensors and ECU units [14,15].

2.3. 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 [16,17].

3. IEEE standards for cybersecurity of sensor networks in electric vehicles

IEEE standards represent the basis for secure communication in modern electric 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 [18].

3.1. IEEE 1609 – the basic security standard for connected vehicles

IEEE 1609 represents a set of protocols known as WAVE (Wireless Access in Vehicular Environments), which are intended for secure data exchange in the environment of connected and autonomous vehicles. Of particular importance is the IEEE 1609.2 standard, which defines security services for communication between vehicles and infrastructure [21,22].
The core security functions of the IEEE 1609 standard include authentication of communication participants, protection of message integrity, and management of digital certificates. Each vehicle and infrastructure element has cryptographic keys that enable verification of the identity of the sender, which significantly reduces the possibility of sending false or malicious messages [21,22].

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

In the context of electric vehicle sensor networks, IEEE 1609 enables the secure exchange of critical data, such as traffic condition information, safety warnings, and sensor data shared between vehicles [22].

3.2. The role of IEEE 1609 in the protection of sensor networks

The application of the IEEE 1609 standard is of particular importance for the protection of sensor networks because it allows the data originating from the sensors to be cryptographically protected during transmission. The standard also foresees mechanisms for preserving user privacy through the use of temporary certificates, thus preventing long-term tracking of vehicles [21,22].

3.3. Other IEEE standards (brief overview)

In addition to IEEE 1609, other IEEE standards are also applied in the field of electric vehicle communication. The IEEE 802.11p standard defines the physical and MAC communication layers for vehicles and represents the basis on which WAVE protocols are implemented. Its role is primarily technical and does not include complete security mechanisms [19,20].
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. Comparative review and application of safety standards

The first two ISO standards are process-oriented and cover the internal functioning of the vehicle system during its life cycle, while the third standard (IEEE 1609) is a technical protocol for safe vehicle communication with the external environment. [23,25]
ISO 26262 focuses on functional safety and mitigation of risks arising from accidental system failures. ISO/SAE 21434 represents the basic framework for managing cyber threats through the TARA methodology, while IEEE 1609 provides cryptographically protected V2X communication. [10,17]

Threat	**Description**	**ISO 26262**	**ISO/SAE 21434**	**IEEE 1609**
Attacks on sensor data integrity	Modification or falsification of sensor data	Partially (fault detection and functional safety mechanisms)	Yes (TARA-based risk management and integrity	Yes (cryptographic protection of transmitted messages)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

Threat	Description	ISO 26262	ISO/SAE 21434	IEEE 1609
	transmitted to control units		protection measures)	
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)

5. Discussion and implications of the application of standards

Based on the above, it can be concluded that the integrated application of ISO/SAE 21434, ISO 26262 and IEEE 1609 enables a balanced and efficient approach to the protection of sensor networks in electric vehicles, with clearly defined roles of each standard.

ISO 26262, although primarily oriented towards functional safety, contributes to the overall resilience of the system through the identification of critical components and the analysis of the consequences of their failure. IEEE 1609 standards provide technical mechanisms for secure V2X communication, thus protecting data exchanged between vehicles and infrastructure.

ISO/SAE 21434 represents the central framework for cyber risk management, as it enables the systematic identification and assessment of threats through the TARA methodology, as well as the definition of appropriate protection measures throughout the entire life cycle of the vehicle. This standard directly addresses sensor data integrity attacks, unauthorised network access, and DoS attacks. [23,25]

The comparative analysis of the standards presented in the table confirms that the safety of sensor networks in electric vehicles requires the combined application of several complementary approaches. Different types of threats cannot be effectively addressed by a single standard, but it is necessary to connect procedural and technical security mechanisms.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

II. CONCLUSION

Sensor networks form the core of the functioning of modern electric vehicles, as they enable precise monitoring of the state of the battery, electric motor, control system and vehicle environment in real time. However, precisely because of their critical role, these networks represent one of the most vulnerable components from the aspect of cybersecurity. Compromising the integrity, availability or confidentiality of data can have serious consequences for vehicle performance, passenger safety and the reliability of driver assistance or autonomous driving functions.

Vulnerabilities in communication protocols, the lack of standardised security measures and the presence of various attack vectors make sensor networks a tempting target for malicious actors. Therefore, implementing robust cybersecurity frameworks is critical. The application of IEEE safety standards, especially IEEE 1609, in combination with other industrial standards such as ISO/SAE 21434 and AUTOSAR recommendations, represents a fundamental step towards increasing the resistance and reliability of these systems [21–25].

Further development and standardisation of security protocols, including improvements in authentication, encryption and privacy protection, will be crucial to ensuring that electric vehicles can operate safely in an increasingly complex and interconnected traffic environment. In addition, continuous monitoring of new threats and implementation of innovative solutions in real time will ensure that sensor networks remain reliable and resistant to attacks, thus directly contributing to overall security and acceptance of electric vehicles as a safe and reliable alternative in global transportation.

In conclusion, the integration of advanced safety standards into the design and operational functionality of electric vehicle sensor networks is not an option, but a necessity. Only through a systematic and standardised approach to cybersecurity is it possible to ensure long-term success and trust in electric vehicle technology [21–25].

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

LITERATURE

[1] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA, 2011.

[2] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile," IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010.

[3] J. Petit and S. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546–556, 2015.

[4] R. Bosch GmbH, Automotive Handbook, 10th ed., Wiley, 2018.

[5] N. Navet and F. Simonot-Lion, Automotive Embedded Systems Handbook, CRC Press, Boca Raton, FL, USA, 2009.

[6] 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.

[7] 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.

[8] ISO 11898-1, Road vehicles – Controller Area Network (CAN), International Organisation for Standardization, 2015.

[9] 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.

[10] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," Workshop on Embedded Security in Cars (ESCAR), 2004.

[11] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway," Wired Magazine, 2015.

[12] H. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, and M. Nixon, "WirelessHART: Applying wireless technology in real-time industrial process control," IEEE Real-Time and Embedded Technology and Applications Symposium, 2008.

[13] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," Proceedings of the First Workshop on Secure Control Systems, 2010.

[14] 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.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

[15] C. Miller and C. Valasek, “A Survey of Remote Automotive Attack Surfaces,” Black Hat USA, 2014.

[16] R. Mitchell and I. R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” ACM Computing Surveys, vol. 46, no. 4, 2014.

[17] M. Wolf and T. Gendrullis, “Design, implementation, and evaluation of secure in-vehicle communication,” Information Security Journal: A Global Perspective, 2012.

[18] IEEE Standards Association, IEEE Standards for Intelligent Transportation Systems, IEEE, New York, USA.

[19] IEEE Std 802.11p-2010, Wireless Access in Vehicular Environments (WAVE).

[20] H. Hartenstein and K. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008.

[21] IEEE Std 1609.2-2016, Standard for Wireless Access in Vehicular Environments – Security Services.

[22] J. Harding et al., “Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application,” National Highway Traffic Safety Administration (NHTSA), 2014.

[23] ISO/SAE 21434, Road Vehicles – Cybersecurity Engineering, International Organization for Standardization, 2021.

[24] AUTOSAR Consortium, Specification of Secure Onboard Communication, Release 4.x.

[25] ENISA, Cybersecurity and Resilience of Smart Cars, European Union Agency for Cybersecurity, 2019.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

INTEC

Co-funded by the European Union

International conference on sustainable mobility

Agenda

Project title: International Engineering Competence Centres to push Sustainable Mobility Development in Albania and Montenegro
Acronym: INTEC

Work package	
WP11	**International conference**
TASK	
11.4	Coummunity Building Events

Dates	05.03.-06.03.2026
City	Tirana
Meeting venue	POLIS University Entrance Hall
Address	Rr. Bylis 12, Kodi Postar 1051, Kutia Postare 2995, Tirana, Albania

05.03.2026	
Entrance Hall, POLIS University	
8:30 – 9:00	**Registration**
9:00 – 9:30	**Opening Performance**
Welcome session – Auditorium A5 (Ground floor)	
9:30 – 10:00	**Opening Remarks** **Dr. Elona Karafili** (Vice Rector, POLIS University) **Dr. Flora Krasniqi** (Head of Office of Projects and Internationalization, POLIS University) **DI Daniela Wenzl** (INTEC Project Coordinator)
Auditorium A5 (Ground floor)	
10:00 –11:00	**Keynote speakers** **DI Horst Pflügl AVL** Collaborative Research for sustainable Mobility **DPSHTRR Representative** – (General Directorate of Road Transport Services in Albania)
11:15 – 11:30	**Coffee break (Moving into parallel sessions)**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

11:30	SESSION 1: POLITICAL AND REGULATORY FRAMEWORK AULA B1	SESSION 2: TECHNOLOGICAL INNOVATION AULA B4
11:30 – 11:45	**Opening Session:** Prof. Emeritus dr Nataša Gospić (FSKL)	**Opening Session:** Associate Prof. Ivan Tolj (US)
11:45 – 12:00	**Integrating Event Data Recorder (EDR) Technology into Sustainable Road Safety Frameworks within the European Green Deal** Eriselda Alimeti, Parid Milo, Mentor Çejku, Anis Sulejmani, Odhisea Koça	**Empirical Comparative Study of Structural CFRP Sandwich Structure Inserts for Out-of-Plane loads** Imre Kovács
12:00 – 12:15	**Infrastructure Readiness for Sustainable Mobility: EU Frameworks and the Case of Albania** Ervin Kalemaj, Parid Milo, Mentor Çejku, Anis Sulejmani, Odhisea Koça	**The Role of Intermodal Transportation for the Sustainable Mobility** Márton Kovács
12:15 – 12:30	**Review of the Evolution of International Ship Energy Efficiency Regulations and the Albanian context** Dr. Blenard Xhaferaj, Doklejda Hodaj	**Impact of Heat Pump Systems on Winter Energy Use and Driving Range in Battery Electric Vehicles** Luis Henrique Pereira Martins
12:30 – 12:45	**Renewable Energy Procurement (CPPA) and Transport Electrification: European Perspectives and Albanian Challenge** Antonio Ndoci, Anis Sulejmani, Odhisea Koça, Mentor Çejku, Parid Milo	**Liquid Cooling Systems for Electric Vehicle Batteries: Improving Safety, Performance and Sustainability** João Miguel de Almeida Ribeiro Silva
12:45 – 13:00	**The Current Status of Autonomous Vehicle**	**Analysis of Battery Charging and Discharging Behavior for Electric Vehicle Applications** Leona Markic, Luka Filipović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

	Technology Adoption in the Balkan Region Darjana Lopičić, Oliver Popović, Miloš Ilić, Bojan Kocić	
13:00 – 14:00	**Lunch**	
14:00 – 14:15	**Reviewing the European Green Deal in Energy, Mobility and Industry** Veselinka Calasan, Ivana Ognjanovic	**Automotive Cooling Systems Sustainability: A Focus on the Expansion Tank** Ana Inês Barbeiro Casimiro
14:15 – 14:30	**The European Green Deal and its National Implementation: From Strategy to Practice** Blerina Bektashi, Andi Bektashi	**Design and Development of a Constant-Volume Combustion Chamber for Optical Investigation of Hydrogen and Water Injection Under Engine-like Conditions** Julius Hollerith, Prof. Dr. Bhavin Kapadia
14:30 – 14:45	**From Prediction to Regulation: Evidence Production Approaches in Autonomous Mobility Research and Their Policy Implications** Sadmira Malaj	**Emission Reduction of Marine Propulsion Systems in SECA Zones Through the Integration of Hydrogen Technologies** Motalleb Miri, Ivan Radaš, Marija Mandić, Ivan Tolj
14:45 – 15:00	**Questions and Discussion**	**A Comprehensive Analysis of Ventilation System for Enhanced Energy Efficiency in Marine Propulsion Applications** Sara Blašković, Gojmir Radica, Jakov Šimunović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

15:00 – 15:15		**Design and Topology Optimization of a Lightweight Chain Sprocket for Electric Motorcycle Applications** Teo Čolović, Ivo Marinić-Kragić
15:15 – 15:30	**SESSION 3: ECONOMIC AND BUSINESS PRESPECTIVES + CASE STUDIES AND GOOD PRACTICES** Aula B1	**Questions and Discussion**
	Opening Session: Dr. Anis Sulejmani (PUT)	
15:30 – 15:45	**Managing Renewable Energy Resources as a Foundation for Sustainable Mobility Transitions** Deivi Sinanaliaj, Martin Bektashi	
15:45 – 16:00	**Feasibility of Electric Bus deployment in Montenegro: A Case Study of Budva (Erasmus+ INTEC / IECC Context)** Anastasija Mrkajic, Vinko Nikic.	
16:00 -16:15	**Children Paths as an Urban Regeneration Strategy: Naim Frasheri Study Case** Dejvi Dauti	
16:15 – 16:45	**Questions and Discussion**	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

INTEC

Co-funded by the European Union

International conference on sustainable mobility

Agenda

Project title: International Engineering Competence Centres to push Sustainable Mobility Development in Albania and Montenegro
Acronym: INTEC

Work package	
WP11	International conference
TASK	
11.4	Coummunity Building Events

Dates	05.03.-06.03.2026
City	Tirana
Meeting venue	POLIS University Entrance Hall
Address	Rr. Bylis 12, Kodi Postar 1051, Kutia Postare 2995, Tirana, Albania

06.03.2026		
First Floor Hall, POLIS University		
8:30 – 9:00	Registration	
9:00– 9:15	**SESSION 4: SOCIAL AND ENVIRONMENTAL IMPACT** AULA B1	**SESSION 5: FUTURE SCENARIOS** AULA B4
9:00 – 9:15	**Opening Session:** Prof. Dr. Bhavin Kapadia (FHF)	**Opening Session:** MA Adrian Millward-Sadler (FHJ)
9:15 – 9:30	**Comparison of Lifecycle Emissions of a SUV with Fuel Cell and Battery Electric Powertrains** - Bhavin Kapadia, Alper Sayin, Sandra Eisenträger	**GENAI Literacy as a Transversal Skill for Emerging Professionals: Implications for Sustainability-Critical Knowledge Work** – Adrian Millward-Sadler
9:30 – 9:45	**Smart Mobility Technologies and their Impact on Urban Sustainability: Insights from**	**Effects of Technical Traffic Calming Measures** – Filip Perović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

	European and Western Balkan Cities – Alma Gjonaj, Vjola Ziu	
9:45 – 10:00	**The Disappearing Squares: Social and Environmental Impacts of Urban Mobility Planning in Durres –** Arjola Sava	**Cybersecurity Vulnerabilities in Electric Vehicle Operating Systems: A Global Awareness Analysis -** Aleksa Radević
10:00 – 10:15	**The City that Demands Continuous Movement: The Disappearance of the Right not to Move within the Framework of Sustainable Mobility –** Avrili Meshi	**Development of a risk assessment model for the transport of hazardous materials using ALOHA and GIS software tools –** Marko Radetić
10:15 – 10:30	**Between Rhetoric and Reality: Discursive Framings, Greenwashing and Outcomes in Sustainable Mobility –** Kejsi Veselagu	**Mapping Distance and Time Leveraging Isochrone Intelligence in Emerging Cities** - Andia Vllamasi, Erjon Cobani
10:30 – 10:45	**Reimagining the City Through Green Mobility Strategies: The Case of Tirana** - Vjola Ziu, Alma Gjonaj	**Can AI develop its Own "Taste" Automotive Design?** - Gregor Andoni, Kristjana Meço
	Coffee Break	
11:00 – 11:15	**Linking Morphology, Perceived Safety, and Sustainable Mobility in Post-Socialist Urban Contexts-** Sindi Doce	**Optimizing Public Transport Corridors Using AI-Based Scenario Modelling: A case Study on Tirana's Ring Road** - Erjon Çobani, Julian Beqiri, Merita Guri
11:15 – 11:30	**Towards Sustainable Transport: A Comparative Analysis of Electric Vehicle Adoption in Montenegro and Albania -** Radmila Milić	**Threat Landscape and Multi-Layered Protection Mechanisms for Autonomous and Electric Vehicle Systems** - Marko Asanovic, Oliver Popović, Zoran Avramović, Nataša Gospić

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

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

11:30 – 11:45	Questions and Discussion	**Cybersecurity Challenges in Modern Vehicular Communication Networks** - Aleksandar Grgurević, Nataša Gospić, Oliver Popović
11:45 – 12:00		**Green Transition in Albania: Challenges and Future Actions** - Erik Kushta, Andi Hyka, Enea Nasto
12:00 – 12:15	**SESSION 6: CONTROVERSIES AND CHALLENGES** Aula B1 **Opening Session:** Prof. Kristofor Lapa (UV)	**Use of AI in the Process of Green Transformation and Impact on Public Health** - Esmeralda Hamiti, Federika Alliaj, Kristi Metushi
12:15-12:30	**The Adoption of Electric Vehicles in Albania: A Comparative Study with Other Western Balkan Countries** - Doklejda Hodaj, Andrea Lapa	**Development of an Automatic Traffic Sign Detection System Using YOLOv8** - Valentina Vojinović, Luka Filipović
12:30-12:45	**Application of Quality Tools in the Analysis of Factors Influencing the Development of Electromobility in Montenegro** - Jelena Šaković Jovanović, Draško Jovanović, Mirjana Grdinić Rakonjac, Marko Lučić, Miloš Perović, Aleksandar Vujović, Gordana Radulović	**The Historical Development of Artificial Intelligence and Its Influence on the job market in Automotive Engineering** - David Josef Pilgram
12:45 – 13:45	**Questions and Discussion**	**Questions and Discussion**
13:45	**Lunch**	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2