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

33

CYBERSECURITY VULNERABILITIES IN ELECTRIC VEHICLE OPERATING SYSTEMS: A GLOBAL AWARENESS ANALYSIS

DOI: 10.37199/c41001033

Aleksa RADEVIĆ
University of Donja Gorica, Montenegro
aleksa.radevic@udg.edu.me

Luka FILIPOVIC
University of Donja Gorica, Montenegro

Abstract

Modern electric vehicles run up to 150 million lines of code across approximately 100 electronic control units. This complexity creates cybersecurity vulnerabilities that threaten vehicle safety, user data, and charging infrastructure. This paper examines real-world security incidents and documented vulnerabilities across major automotive operating systems including BlackBerry QNX, Android Automotive OS, and Automotive Grade Linux to raise awareness about the current state of electric vehicle cybersecurity.

This paper analyzes cybersecurity incidents and vulnerabilities documented between 2019 and 2024. Data sources include Common Vulnerabilities and Exposures databases, Pwn2Own Automotive competition results, and security research from Asia, Europe, and North America. The analysis focused on three primary operating systems used in electric vehicles and examined attack vectors including charging infrastructure vulnerabilities, wireless connectivity exploits, and software update mechanisms.

At Pwn2Own Automotive 2024, researchers discovered 49 zero-day vulnerabilities and compromised Tesla modems, infotainment systems, and charging stations. Analysis of Android Automotive bulletins shows ongoing high-severity flaws, with approximately 80% of automotive apps containing security vulnerabilities. Major incidents include the 2022 Ukrainian hack of Russian charging stations, the December 2024 Volkswagen breach affecting 800,000 vehicles, and the June 2024 CDK Global ransomware attack causing over $1 billion in losses.

Electric vehicle operating systems face significant security gaps. Manufacturers add connected features faster than they secure them, creating risks for vehicle owners and critical infrastructure. While manufacturers work with security researchers, new connected features are deployed faster

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

than they can be properly tested. These vulnerabilities threaten not just individual vehicles but also charging networks and power grids. Solutions must include security-by-design, mandatory security standards for charging protocols, and faster patch deployment across the industry.

Keywords: electric vehicles, cybersecurity, operating systems, vulnerability assessment, automotive security

I. INTRODUCTION

Electric vehicles are fundamentally different from traditional cars. A modern EV runs approximately 150 million lines of code across 100 electronic control units. This software complexity creates cybersecurity risks that did not exist in conventional vehicles. As governments push electrification mandates, more connected vehicles create more attack opportunities. EVs connect to charging stations, vehicle-to-grid (V2G) systems, cloud services, and receive over-the-air (OTA) updates. Each connection is a potential attack vector. The consequences of successful exploits range from vehicle theft and privacy breaches to critical infrastructure disruption.

Three primary operating systems dominate the EV market. BlackBerry QNX, designed specifically for safety-critical applications, operates in over 275 million vehicles globally. Android Automotive OS has gained adoption among 16 major automotive manufacturers as of 2023. Automotive Grade Linux provides an open-source alternative that enables code transparency and community review. According to Upstream Security (2025), automotive cybersecurity incidents reached 409 in 2024, representing a 39 percent increase over the previous year. This analysis follows the ISO/SAE 21434 framework for automotive cybersecurity risk assessment and lifecycle management.

This paper examines vulnerabilities in three major EV operating systems and analyzes security incidents from 2019 to 2024. The research draws on data from Asia, Europe, and North America to assess risks across different manufacturers.

II. METHODS

This research covers EV cybersecurity incidents and vulnerabilities from January 2019 to December 2024. During this period, the global EV market grew from about 2.1 million vehicles sold in 2019 to over 14 million in 2023, significantly expanding the attack surface.

1. Data collection

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

The main data came from the National Vulnerability Database for Common Vulnerabilities and Exposures (CVE) affecting QNX, Android Automotive, and AGL. Security bulletins from Google and BlackBerry were useful. The Pwn2Own Automotive competitions in Tokyo provided real-world examples of what hackers can actually do when they put their minds to it. Upstream Security's annual reports provided quantitative data on overall trends.

Incidents were selected for inclusion in Tables 1 and 2 based on three criteria: confirmed attribution through official reports or security research publications, documented technical details or CVSS scores, and impact affecting multiple vehicles or significant financial or operational consequences. Security bulletins and CVE entries were validated against at least two independent sources to ensure accuracy.

2. Analysis framework

Vulnerabilities were scored using Common Vulnerability Scoring System (CVSS) 3.1 to maintain consistency. The three operating systems were compared based on their architecture, update mechanisms, and security features. For the incidents, the analysis looked at timing, location, attack method, and impact.

III. RESULTS

1. Operating System Vulnerabilities

Each of the three operating systems has its own issues. BlackBerry QNX is generally considered secure, though vulnerabilities exist. CVE-2021-22156 had a CVSS score of 9.0 (Critical) and allowed remote code execution through an integer overflow bug (CISA, 2021). Given that QNX operates in 275 million vehicles, even patched vulnerabilities demonstrate the critical importance of automotive cybersecurity.

Android Automotive is different. Google (2024) releases monthly security bulletins, and some of them have included privilege escalation bugs. A significant concern is all the third-party apps. Studies suggest that approximately 80 percent of automotive apps contain security vulnerabilities. This indicates that the threat surface extends beyond the OS itself.

Automotive Grade Linux being open-source sounds like it would be good for security since anyone can review the code. In practice, implementation varies considerably. Researchers have found access control issues and privilege escalation bugs. A significant concern is that different

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

manufacturers implement AGL differently, so two vehicles running the same base system might have very different security levels.

Table 1 summarizes the key security characteristics of each operating system platform.

Table 1

Characteristic	**BlackBerry QNX**	**Android Automotive**	**Automotive Grade Linux**
Architecture	Microkernel RTOS	Linux-based monolithic	Linux-based open source
Market Share	275+ million vehicles	16+ major brands	Toyota, Mercedes, others
Update Mechanism	Vendor-managed OTA	Monthly security bulletins	Varies by manufacturer
Key Vulnerability	CVE-2021-22156 (9.0)	Privilege escalation bugs	Access control issues
Primary Strength	Safety certifications	Regular patching cycle	Open source transparency
Primary Weakness	Closed source code	Third-party app risks	Inconsistent implementation

While a quantitative comparison of documented vulnerabilities across operating systems would provide additional insight, precise vulnerability counts specific to automotive implementations were not consistently available across all three platforms in public databases during the study period.

2. Real-World Security Incidents

Pwn2Own Automotive 2024 in Tokyo was the first major hacking competition focused specifically on cars. Over three days in January, 17 teams from 9 countries tried to hack vehicles and chargers. Tesla sponsored the event. The results were eye-opening: 49 previously unknown vulnerabilities and $1,323,750 in prize money (Zero Day Initiative, 2024). A French team called Synacktiv walked away with $450,000, including rewards for hacking a Tesla modem and breaking out of the Tesla infotainment sandbox to access vehicle controls.

EV chargers demonstrated the most vulnerabilities at the competition. Researchers found 29 vulnerabilities across just six charger models. The ChargePoint Home Flex was sufficiently vulnerable that six different teams successfully exploited it. The Autel MaxiCharger had a stack-based buffer overflow, hard-coded credentials, and more overflow bugs. Phoenix Contact CHARX SEC-3100 fell to multiple exploit chains (Zero Day Initiative, 2024).

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 Volkswagen breach in December 2024 showed what can go wrong with cloud security. Cariad, VW's software subsidiary, left terabytes of data sitting on misconfigured Amazon Web Services (AWS) storage (Scherschel, 2024). The breach affected 800,000 EVs across VW, Audi, Seat, and Skoda. The exposed data included Global Positioning System (GPS) locations accurate to 10 centimeters, logged every time the car was turned on or off. Names, emails, phone numbers, and home addresses were also leaked. About 300,000 of those cars were in Germany, 80,000 in Norway. The list of affected people included German politicians, business executives, and even police vehicles. The Chaos Computer Club found the vulnerability and reported it. Cariad fixed it quickly, but the damage was already done.

In early 2022, a Ukrainian company disabled Russian EV charging stations on the M11 motorway between Moscow and St. Petersburg (Franceschi-Bicchierai, 2022). They had built the controller components and left themselves backdoor access. They used it to shut down the stations and display political messages. The actual damage was just service disruption, but it raised bigger questions about supply chain security in charging infrastructure.

3. Additional Global Incidents

Security incidents have popped up all over the world. In January 2022, a 19-year-old German researcher named David Colombo found a vulnerability in TeslaMate, a third-party logging tool. He managed to access 25 Teslas across 13 countries, unlocking doors, flashing headlights, and tracking locations (Colombo, 2022). The vulnerability got a CVSS score of 9.8. In 2023, researchers in Berlin jailbroke Tesla's infotainment system using voltage glitching to extract encryption keys. Ferrari got hit by ransomware that leaked client data. The UK suspended sales of certain Spanish EV chargers over security concerns in 2024. In November 2024, a breach exposed 116,000 records from global charging networks.

The biggest financial hit came from the CDK Global ransomware attack in June 2024. CDK provides software to about 15,000 car dealerships in North America. The BlackSuit ransomware gang encrypted their systems, and dealerships could not process sales, manage financing, or even schedule repairs for almost three weeks. Anderson Economic Group estimated the losses at over $1 billion. CDK reportedly paid around $25 million in ransom to get things running again. It showed how one software vendor can become a single point of failure for an entire industry.

Table 2 provides a summary of significant global EV cybersecurity incidents documented between 2021 and 2024.

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

Table 2

Year	Location	Target	Attack Type	Impact
2022	13 countries	Tesla vehicles	Third-party app exploit	25+vehicles accessed
2022	Russia	M11 EV chargers	Backdoor access	Service disruption
2023	Germany	Tesla infotainment	Voltage glitching	Encryption keys extracted
2023	Italy	Ferrari SPA	Ransomware	Client data exposed
2024	Japan (Tokyo)	Multiple EV systems	Pwn2Own competition	49 zero-days found
2024	Europe(8 countries)	VW Group vehicles	Cloud misconfiguration	800,000 vehicles exposed
2024	United Kingdom	Spanish EV chargers	Security concerns	Sales suspended
2024	USA/Canada	CDK Global (15,000 dealerships)	Ransomware (BlackSuit)	$1 billion+ losses

4. Attack Vectors

Wireless connections represent the primary vector for remote vehicle attacks. Researchers have exploited Bluetooth to gain access, then moved to the Controller Area Network (CAN) bus where critical safety systems operate. Cellular modems present additional vulnerabilities. At Pwn2Own, the Synacktiv team hacked a Tesla modem by setting up a fake cell tower. WiFi poses risks as vehicle access points often run outdated firmware. Even Near Field Communication (NFC) for keyless entry has been exploited with relay attacks that work from far away.

Charging infrastructure is a big target. Many charging stations still use Open Charge Point Protocol (OCPP) 1.6, which has some serious gaps: no mandatory authentication, no encryption, and unverified firmware updates. OCPP 2.0.1 is better with Transport Layer Security (TLS) and certificates, but upgrading costs money so adoption is slow. Over-the-air updates are necessary to patch vulnerabilities; however, when improperly implemented, they can also serve as an attack vector. A compromised update server could push malicious firmware to thousands of cars at once.

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

IV. DISCUSSION

1. Current State Assessment

The overall picture reveals significant security gaps. When 49 previously unknown vulnerabilities get discovered in a single competition and incidents are up 39 percent year over year, there is a demonstrable gap between how fast new features are being added and how much attention security is getting.

None of the three operating systems is perfect. BlackBerry QNX has good isolation but is closed source. Android Automotive gets regular updates but has app ecosystem risks. Automotive Grade Linux is transparent but inconsistently implemented.

2. Infrastructure and Cloud Security Concerns

Charging stations are particularly concerning because a compromised charger could potentially infect vehicles or even attack the power grid. The Volkswagen breach demonstrates what happens when cloud security is neglected.

3. Regulatory Landscape

Regulations are beginning to address these issues, though progress remains gradual. The United Nations Economic Commission for Europe WP.29 R155 and R156 regulations now require manufacturers to have cybersecurity management systems covering the entire vehicle lifecycle. Since July 2024, this applies to all new vehicles in the European Union, Japan, and South Korea. Interestingly, Porsche decided to discontinue some models in certain markets partly because of compliance challenges. ISO/SAE 21434 provides additional standards. This standard establishes requirements for cybersecurity risk management throughout the vehicle lifecycle, from concept through decommissioning, and mandates threat analysis and risk assessment (TARA) processes for automotive systems. The United States has proposed banning connected vehicle components from China and Russia. However, regulations consistently lag behind both technology deployment and emerging threats.

4. Industry Recommendations

Car makers need to build security in from the start rather than adding it later. The industry would benefit from more standardization so different manufacturers are not all doing their own thing.

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

Regular security updates and fast patch deployment are essential. Consumers should be more aware that their electric vehicle has cybersecurity risks like any other connected device.

Going forward, defense in depth with multiple security layers makes more sense than relying on any single protection. Regulators should establish minimum security requirements for connected cars and charging infrastructure before a major incident force their hand.

V. CONCLUSIONS

Electric vehicles benefit the environment, but software complexity has created security problems the industry struggles to address. The incidents covered here, from the $1 billion CDK Global attack to 800,000 exposed Volkswagen owners, demonstrate inadequate security measures. With 409 incidents in 2024 representing a 39% increase, the industry must choose: implement comprehensive security now, or wait for a catastrophic event to force action.

REFERENCES

Colombo, D. (2022, January 25). How I got access to 25+ Teslas around the world. By accident. And curiosity. Medium. https://medium.com/@david_colombo/how-i-got-access-to25-teslas-around-theworld-by-accident-and-curiosity-8b9ef040a028

Cybersecurity and Infrastructure Security Agency. (2021, August 17). BadAlloc vulnerability affecting BlackBerry QNX RTOS (Alert AA21-229A). U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-229a

Franceschi-Bicchierai, L. (2022, February 28). Russian electric vehicle chargers hacked, tell users 'Putin is a dickhead.' Vice. https://www.vice.com/en/article/russian-electric-vehiclechargers-hacked-tell-usersputin-is-a-dickhead/

International Organization for Standardization. (2021). ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering. https://www.iso.org/standard/70918.html

Google. (2024). Android Automotive OS security bulletins. Android Open Source Project. https://source.android.com/docs/security/bulletin/aaos

National Institute of Standards and Technology. (2021). CVE-2021-22156 detail. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2021-22156

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

Scherschel, F. A. (2024, December 27). Volkswagen leak exposed location data for 800,000 electric cars. Der Spiegel. https://www.spiegel.de/netzwelt/web/volkswagen-leak-exposedlocation-data-for-800000-electric-cars-a-e564f223-1407-44ac-be68-8e4af95731b0

Upstream Security. (2025). 2025 global automotive and smart mobility cybersecurity report. https://upstream.auto/reports/global-automotive-cybersecurity-report/

Zero Day Initiative. (2024, January 26). Pwn2Own Automotive 2024 – Day three results. Trend Micro. https://www.zerodayinitiative.com/blog/2024/1/26/pwn2own-automotive-2024day-three-results

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