Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

3-WP14 – Security Monitoring and Testing of Automotive Electronics

Coordinator of the WP

Czech Technical University in Prague, doc. Jiří Novák, Ph.D.

Participants of the WP

CTU FEE – Ing. Jan Sobotka, Ing. Michal Špaček, Ing. Jakub Svatoš, Bc. Peter Fučela, Bc. Lukáš Kulhánek

ŠKODA AUTO a. s. – Ing. Jiří Blecha, Ing. Jaroslav Hrbek, Ing. Adam Šťáva

TÜV Süd – Ing. Dalibor Zeman, Ing. Vladislav Kocián, Ing. Petr Lockenbauer

Main Goal of the WP

Provide a technology enabling identification of in-vehicle networks topology, network nodes and their relations. Use this knowledge to identify security critical protocols used for in-vehicle communication and implement automated test sequences focused on identified security threats.

Partial Goals for the Current Period

Test framework configuration for seamless rest-bus simulation, implementation of example test suite in CAPL scripting language. Development and implementation of framework for passive network analysis and in-vehicle network topology reconstruction. Identification of particular communication relations and threats related to protocols used for.

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

3 – WP14 – 001 - Software framework for ECU test bus simulation with realistic implementation of security protocols.

The framework provides for a realistic rest bus simulation of ECU external communication environment on all physical communication interface types (including CAN, LIN, Ethernet …) at all required OSI model protocol layers. Framework is structured in order to allow easy insertion of new security oriented layers into the communication stack. An API providing for particular layers testing is defined and predefined test cases are implemented.

R - Software (CTU FEE + Škoda Auto + TÜV Süd) Project deadline: 06.2026

3 – WP14 – 002 - **Framework for security monitoring and communication security testing.**

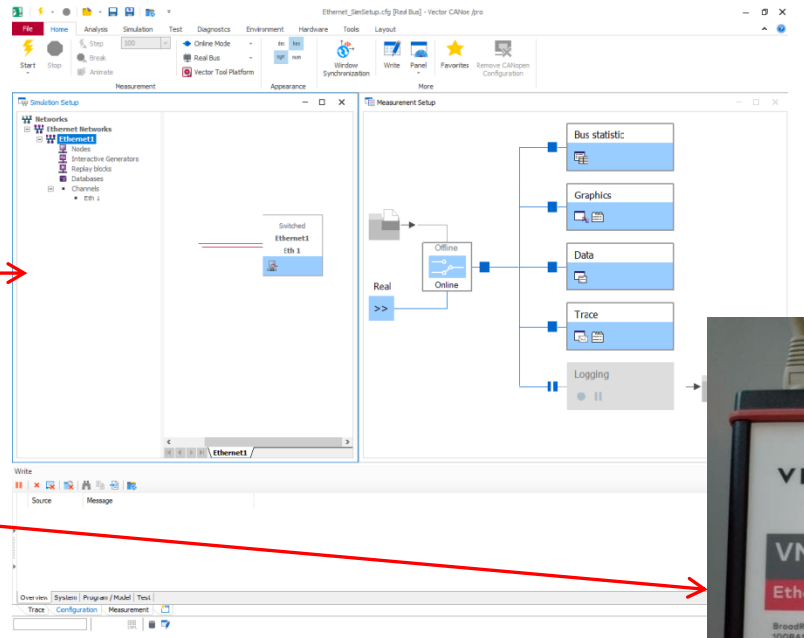
The framework provides for a communication monitoring on different physical communication interface types (including CAN, LIN, Ethernet …) at all OSI model protocol layers. It provides for filtering and logging of selected protocols (especially those security oriented) and their testing, including selected intrusive tests. For intrusive testing an API providing for message/packet injection is implemented.

R - Software (CTU FEE + Škoda Auto + TÜV Süd) Project deadline: 06.2026

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 001 - Software framework for ECU rest bus simulation with realistic implementation of security protocols.

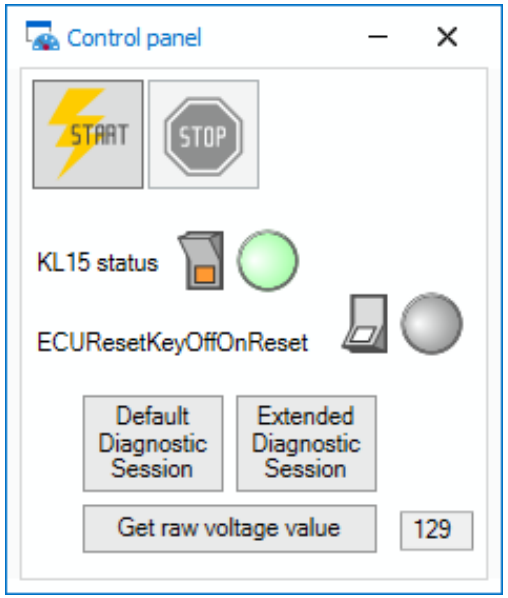
- detailed specification of result
  - application for security testing of single ECUs
  - realistic rest-bus simulation on all ECU interfaces
  - predefined set of security oriented tests at all layers
- selection of suitable tools
  - CANoe environment with suitable HW modules
  - VN56xx series hardware (support for CAN and Ethernet)
- selection of suitable programming tools for CANoe
  - Python interface – tested, but finally rejected (suits only for high-level application models)
  - CAPL (internal scripting language) and .NET were evaluated → CAPL was selected as an optimal tool



Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 001 - Software framework for ECU rest bus simulation with realistic implementation of security protocols.

- The unit MIB3 EI GP (Infotainment) was selected for initial development
  - 2 x CAN
  - 1 x Ethernet
- CANoe based simulation framework implemented
  - VAG modeling AddOn used for simulation support
  - DBC source files for CAN interface
  - ARXML source files for Ethernet interface
  - ODX data based diagnostics support
- Initial verification of the communication performed by reading diagnostic data

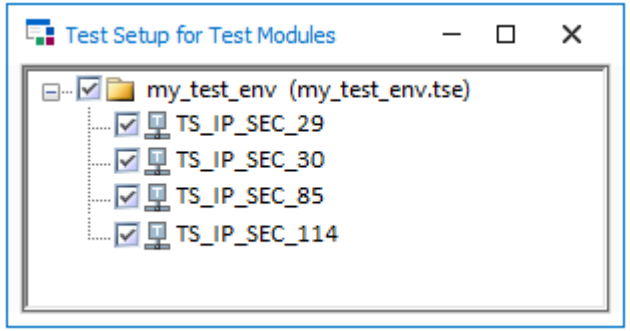


[14:03:16] - Rx	Positive response:
Record Data Identifier	ECU Serial Number
Data Record	0x53 0x4B 0x5A 0x41 0x5A 0x32 0x42 0x30 0x35 0x37 0x38 0x34
ECU Serial Number	SKZAZ2B0578480
Matching Record Data Identifier	0xF1 0x8C

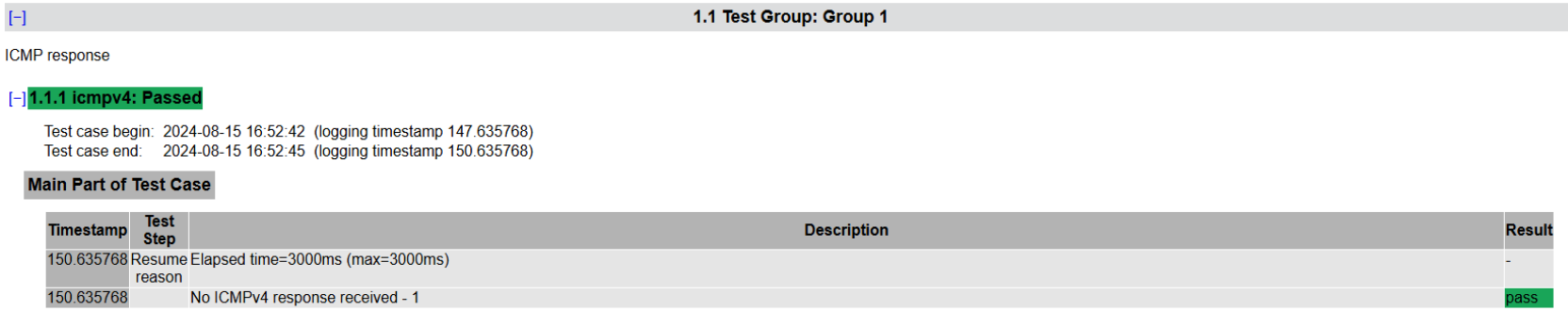
Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 001 - Software framework for ECU rest bus simulation with realistic implementation of security protocols.

- Set of 15 representative test cases was selected for initial implementation steps
- CANoe Test Modules environment is used
  - Test Modules provide a testing interface with interactive features and testing functions for an easier testing process
  - Each test case can be implemented in **CAPL** or .NET
  - The output of the testing, in the form of a test report, can be generated as an XML or HTML file



- Selection of tests is currently under implementation
  - incorrect rest-bus simulation issues are slowing down the progress



[–] **1.1 Test Group: Group 1**

ICMP response

[–] **1.1.1 icmpv4: Passed**

Test case begin: 2024-08-15 16:52:42 (logging timestamp 147.635768)
Test case end: 2024-08-15 16:52:45 (logging timestamp 150.635768)

Main Part of Test Case

Timestamp	Test Step	Description	Result
150.635768	Resume reason	Elapsed time=3000ms (max=3000ms)	-
150.635768		No ICMPv4 response received - 1	pass

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 002 - Framework for security monitoring and communication security testing.

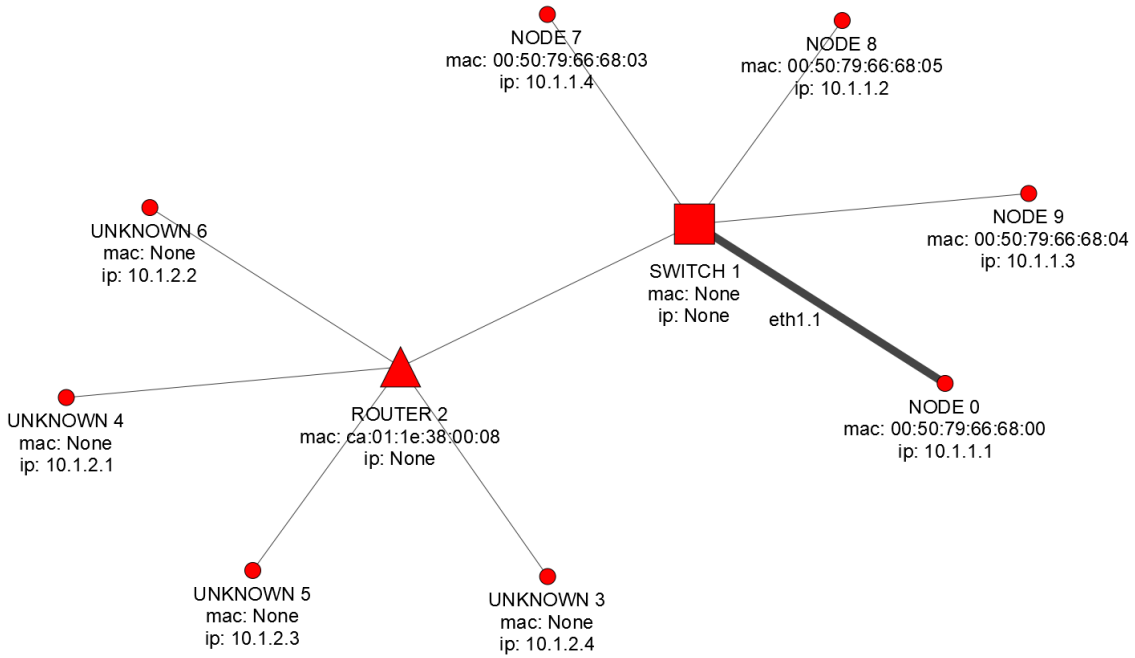
In 2023:

- detailed specification of result
  - application for vehicle certification process
  - automated analysis of in-vehicle networks topology (focused on Ethernet networks)
  - automated analysis of in-vehicle protocols (including automotive specific ones)
  - automated generation of test suite focused on security of detected in-vehicle protocols
- selection of suitable tools
  - off the shelf Ethernet switches, media converters for 100/1000Base-T1 Ethernet
  - GNU Linux + Python development chain
  - future deployment of WP01 – 007 - Programmable hardware platform is expected

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 002 - **Framework for security monitoring and communication security testing.**

- Offline topology mapping
  - Goal is information gathering for R155 testing.
  - Able to reconstruct physical and logical in vehicle network topology.
    - Rule based algorithm
  - Input is set of annotated capture files.
  - Output is network graph with node types and parameters identified.
  - Actually in stage of software prototype
    - All features implemented.
    - Tested with data from MEB platform and our own simulated topologies.
    - Needs to be tested with more data, especially from vehicles
    - UX needs to be improved.



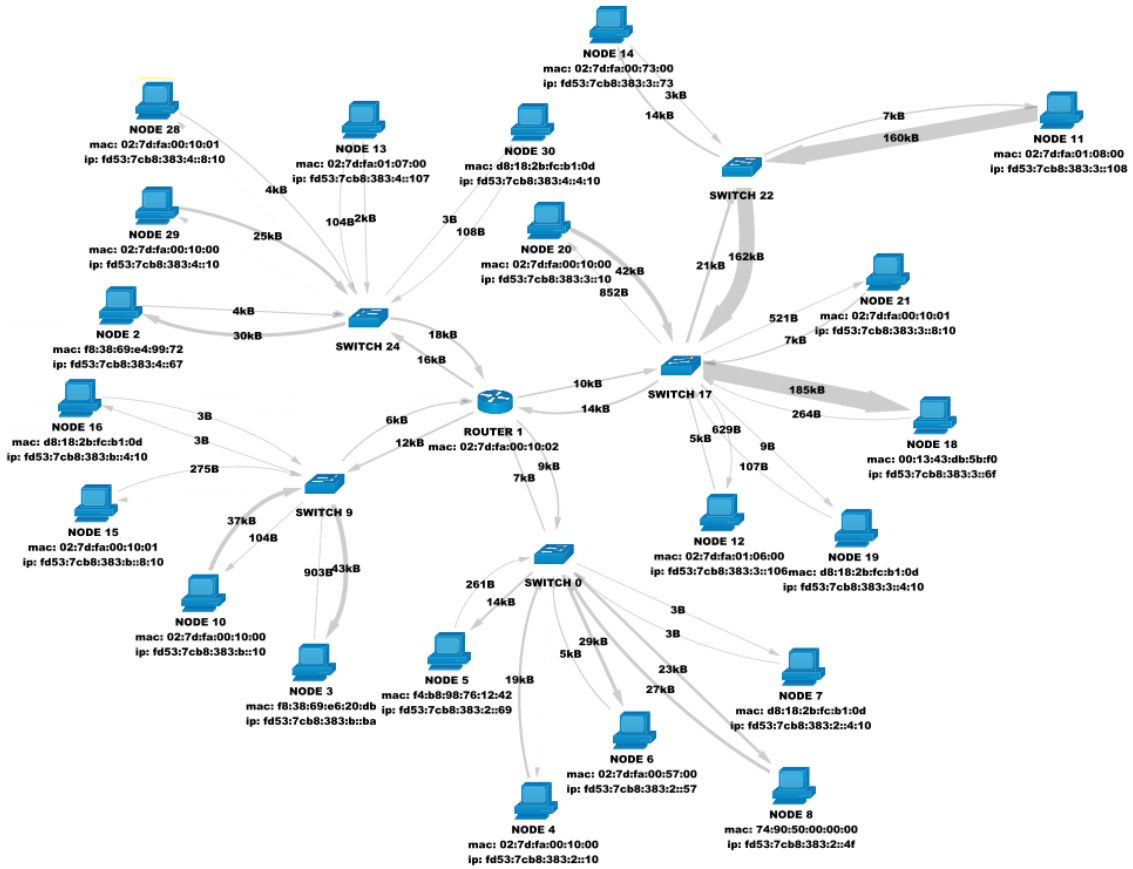
Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Activities to reach 3 – WP14 – 002 - **Framework for security monitoring and communication security testing.**

- Traffic Flow Analysis
  - On the top of identified network topology the tool is able to analyze data flows between ECUs in graph or table format.
  - from ISO/OSI Layer 4 (TCP&UDP) up (e.g. TLS, DoIP …)

UDP CONVERSATIONS

ID	Address A	Port A	Address B	Port B	Packets	Bytes	Packets A -> B	Bytes A -> B	Packets B -> A	Bytes B -> A
0	fd53:7cb8:383:3::10	42810	fd53:7cb8:383:3::73	29310	10566	1.58MB	10545	1.57MB	21	2kB
1	fd53:7cb8:383:b::10	42810	fd53:7cb8:383:b::ba	42810	10428	1.4MB	10428	1.4MB	0	0B
2	fd53:7cb8:383:3::10	42810	fd53:7cb8:383:3::108	29310	3530	589kB	3530	589kB	0	0B
3	fd53:7cb8:383:3::106	42810	fd53:7cb8:383:3::108	29310	2074	1.02MB	2074	1.02MB	0	0B
4	fd53:7cb8:383:3::8:10	42810	fd53:7cb8:383:3::73	29310	2005	249kB	2005	249kB	0	0B
5	fd53:7cb8:383:3::8:10	30490	fd53:7cb8:383:3::108	30490	1354	182kB	1145	135kB	209	47kB
6	fd53:7cb8:383:4::67	56175	fd53:7cb8:383:b::ba	42558	1100	108kB	1100	108kB	0	0B
7	fd53:7cb8:383:3::106	30490	fd53:7cb8:383:3::108	30490	1048	128kB	524	68kB	524	60kB
8	fd53:7cb8:383:3::73	30490	fd53:7cb8:383:3::10	30490	1042	197kB	521	102kB	521	95kB
9	fd53:7cb8:383:3::73	30490	fd53:7cb8:383:3::8:10	30490	624	76kB	312	42kB	312	34kB



Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Current State of Deliverables and Fulfillment of Goals

- 3-WP14-001 | Software framework for ECU rest bus simulation with realistic implementation of security protocols., R, VI./2026, CTU FEE 0.2; SA 0.6; TUV 0.2 – **in progress & no major delays:**
  - HW as well as SW platforms were selected (Vector's VN series modules and CANoe)
  - .NET API and internal CAPL (CANoe scripting language) were evaluated in order to identify platform limits in terms of communication timing accuracy, communication throughput in different scenarios – CAPL was chosen
  - Framework supporting the rest-bus simulation CAN and Ethernet) was implemented
  - Initial test suite implementation for selected set of threats has started
- 3-WP14-002 | Framework for security monitoring and communication security testing., R, VI./2026, CTU FEE 0.3; SA 0.1; TUV 0.6 – **in progress & no major delays:**
  - HW as well as SW platforms were selected (of the shelf Linux computer with Ethernet media converters, Python for SW development)
  - Algorithms for in-vehicle network topology identification were designed and implemented
  - Validation of above mentioned algorithms (based on known real as well as artificial network topologies) has successfully passed
  - In-vehicle data flows identification and related threats testing implementation is in progress

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

List of Due Deliverables and Their Added Value

- 3-WP14-001 – Software framework for ECU rest bus simulation with realistic implementation of security protocols.
  - Due date 06/26
  - Provides for fast automated testing of known security threats at tier 1 component suppliers as well as final car manufacturers.
- 3-WP14-002 – Framework for security monitoring and communication security testing
  - Due date 06/26
  - Provides for "grey box" semi-automated monitoring and testing of security threats and their mitigation during vehicle homologation process.

Assessment of the Contribution of Deliverables

Both software framework or their parts can be used within the other work-packages for in-vehicle data communication monitoring and analysis, as a (online/offline) source of information for other research tasks.

Content of Work Package DP 3-WP14 – "Security Monitoring and Testing of Automotive Electronics"

Assessment of the Formal/Administrative Goals of the Work Package

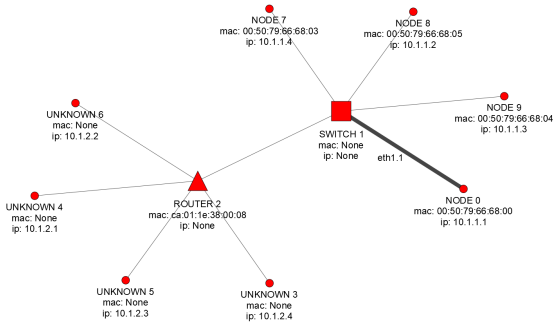
- Work-package budget at all three participating bodies is being spent according to the plan with minor changes following the TACR rules
- At CTU the income from commercial activities exceeds planned project requirements
- All the work-package deliverables due date is 06/2026; the current level of development guarantees completion on the scheduled date

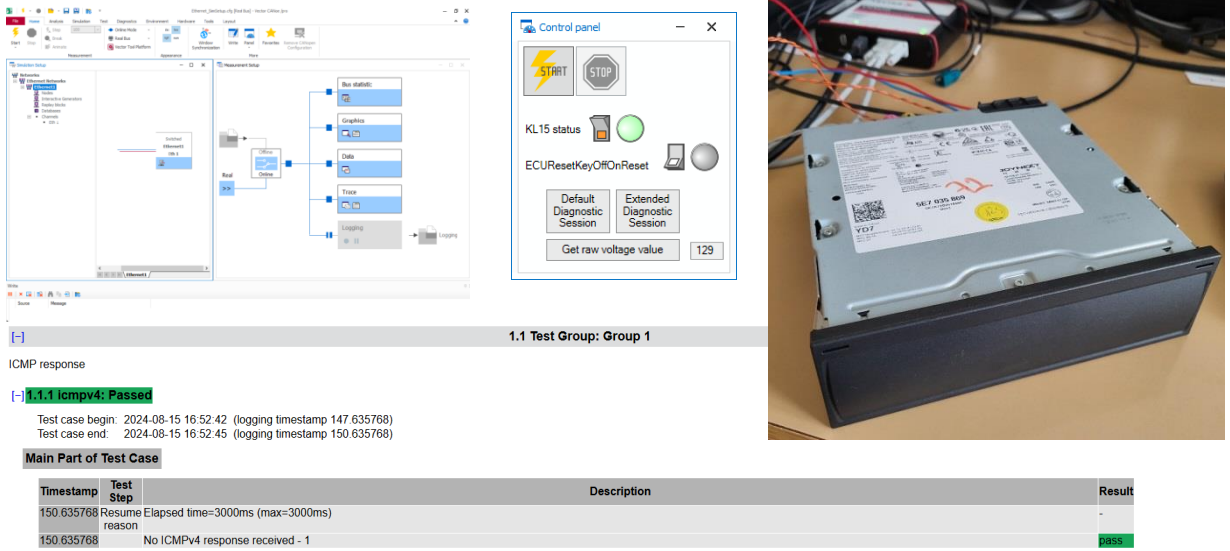
Acknowledgment

This research has been realized using the support of Technological Agency, Czech Republic, programme National Competence Centres II, project # TN02000054 Božek Vehicle Engineering National Centre of Competence (BOVENAC).

Výtah z prací 2023-2025 na 3-WP14 – "Monitoring a testování vozidlové elektroniky zaměřené na kybernetickou bezpečnost"

(ČVUT – Škoda Auto – TÜV Süd)





Framework pro bezpečnostní analýzu a testování vnitřních komunikací vozidla

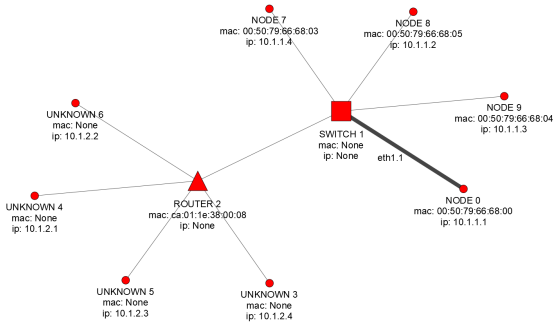
- automatizovaná analýza logů ze segmentů vnitřní sítě vozu
- rekonstrukce topologie vnitřní sítě a typů jednotlivých síťových zařízení
- identifikace datových toků a souvisejících bezpečnostních hrozeb na různých vrstvách OSI modelu

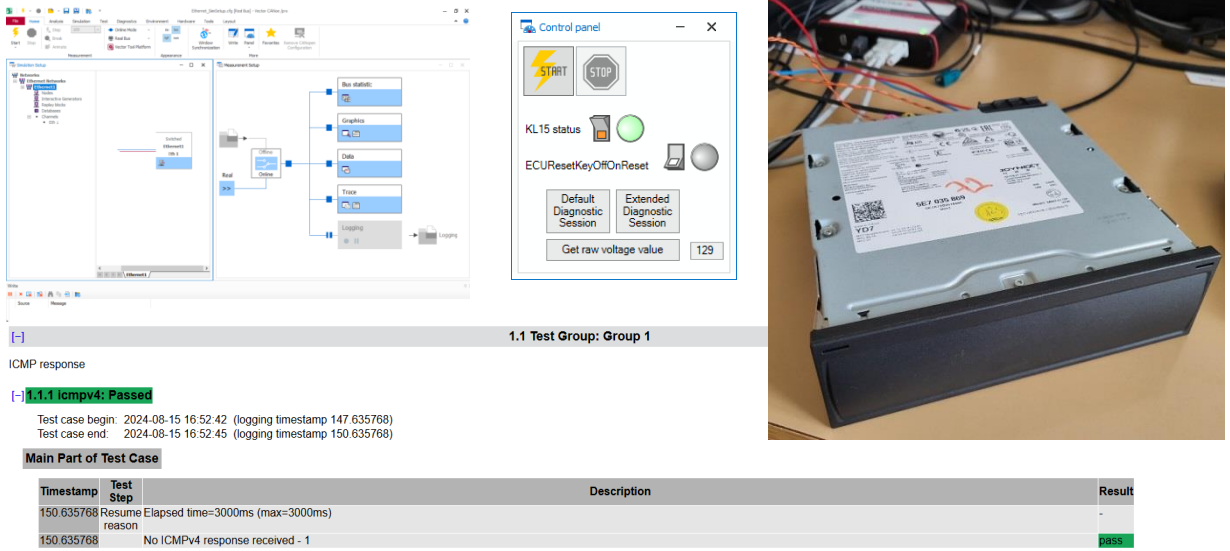
Framework pro realistickou rest-bus simulaci pro řídicí jednotky s důrazem na bezpečnostní protokoly.

- výběr platformy CANoe, volba jazyka CAPL na základě výkonnostní testů
- implementace frameworku pro rest-bus simulaci v sítích CAN a Ethernet
- probíhá implementace vybraných testů

Results of 3-WP14 – "Security Monitoring and Testing of Automotive Electronics" – Achieved 2023 - 2025

(ČVUT – Škoda Auto – TÜV Süd)





Framework for security analysis and testing of in-vehicle communication

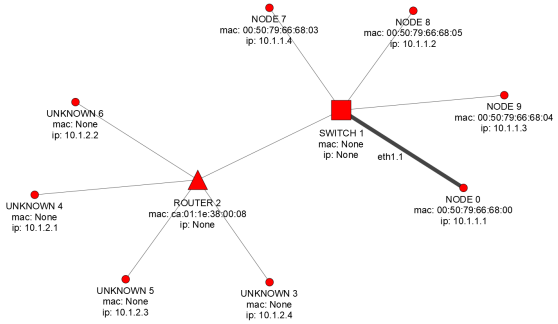
- automated internal vehicle network segments logs analysis
- reconstruction of internal network topology, particular network node types and their parameters
- particular data flows and related security threats identification at various OSI model layers

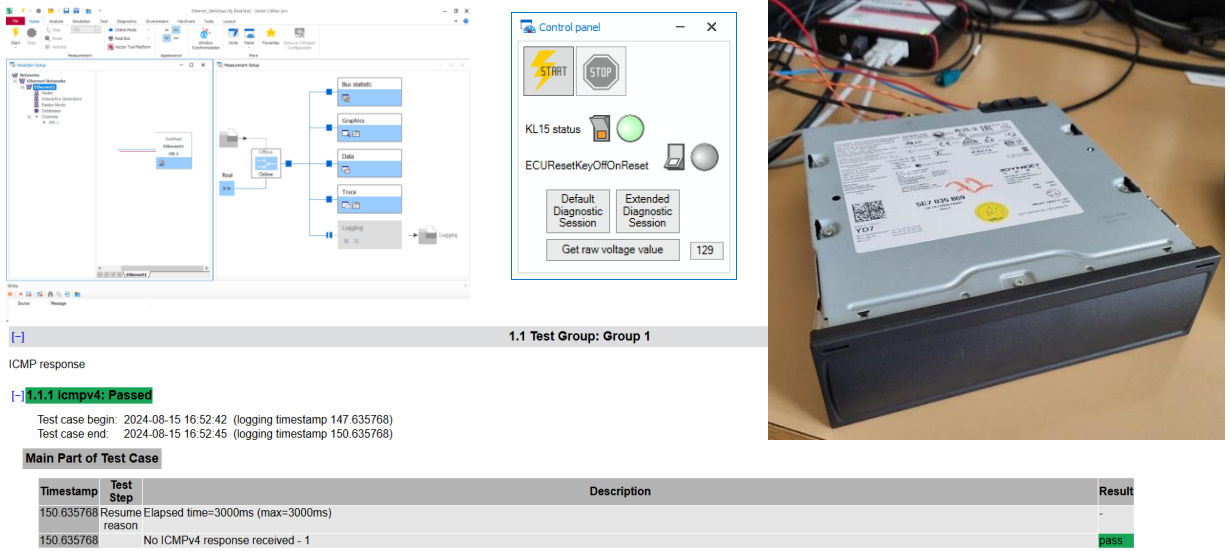
Framework for realistic rest-bus simulation for ECUs with focus on security related protocols.

- CANoe platform selection, CAPL programming language chosen based on various performance tests
- rest-bus simulation framework implemented for CAN and Ethernet networks
- suite of selected security oriented tests is under development

Výtah z prací 2024 na 3-WP14 – "Monitoring a testování vozidlové elektroniky zaměřené na kybernetickou bezpečnost"

(ČVUT – Škoda Auto – TÜV Süd)





Framework pro bezpečnostní analýzu a testování vnitřních komunikací vozidla

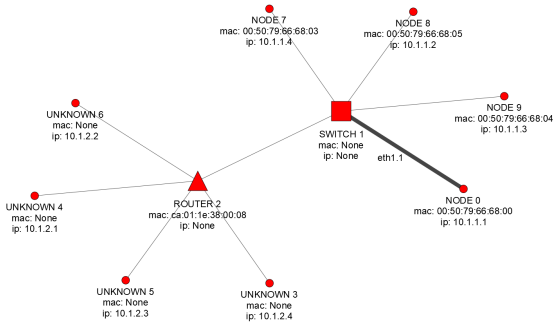
- rekonstrukce topologie vnitřní sítě a typů jednotlivých síťových zařízení
- identifikace datových toků a souvisejících bezpečnostních hrozeb na různých vrstvách OSI modelu

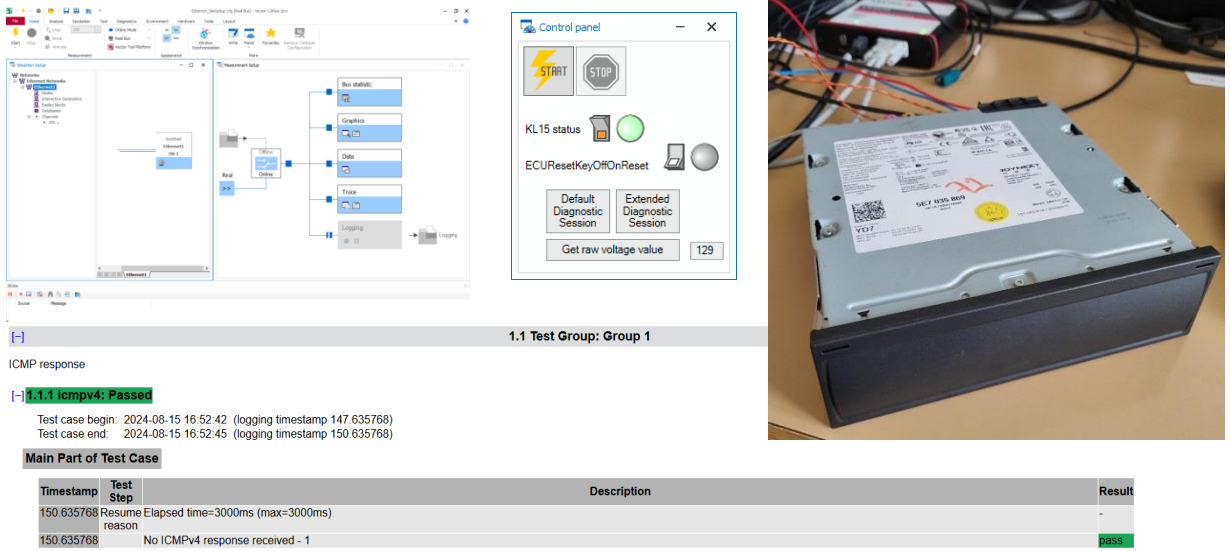
Framework pro realistickou rest-bus simulaci pro řídicí jednotky s důrazem na bezpečnostní protokoly.

- finální volba jazyka CAPL na základě výkonnostní testů
- implementace frameworku pro rest-bus simulaci v sítích CAN a Ethernet na platformě CANoe
- zahájení implementace vybraných sady testů

Results of 3-WP14 – "Security Monitoring and Testing of Automotive Electronics" – Achieved 2024

(ČVUT – Škoda Auto – TÜV Süd)





Framework for security analysis and testing of in-vehicle communication

- reconstruction of internal network topology, particular network node types and their parameters
- particular data flows and related security threats identification at various OSI model layers

Framework for realistic rest-bus simulation for ECUs with focus on security related protocols.

- CAPL language selection based on various performance tests
- rest-bus simulation framework implementation for CAN and Ethernet networks
- implementation of suite of selected security oriented tests has been started