PORSCHE

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Information Technology
Department of Software Engineering

SYTEM FOR SIGNAL MANIPULATION ON AUTOMOTIVE ETHERNET

Master's Thesis

Ing. Oleksandr Korotetskyi
Supervisor: Ing. Martin Štěpánek

October 17, 2024
(February 14, 2024)

Agenda

Problem Statement, Objectives & Methodology

To test automotive control units, it is mandatory to simulate all the necessary values/states of the input signals that are sent in Ethernet packets (frames). In some cases, it is easier to manipulate with data *"on-the-way"* and simulate all the states directly in the packet than to use the simulation of other control units.

1. Perform research on signals and SAE levels in Automotive Ethernet
2. Perform research on possibilities of manipulation with data in Ethernet packet and data security
3. Collect RQs for the test system
4. Design SW architecture
5. Design and implement SW for signal manipulation
6. Design a test strategy for the developed SW
7. Perform the test of implemented SW
8. Implementation should be done on Linux OS

Methodology: theoretical research, practical experimentation & statistical interpretation of results

Page(s) in thesis: 0, 2

Motivation

- Front edge of automotive technologies
- No similar publications made yet
- No devices capable of desired functionality existed *at the beginning of the work*
- Possible future practical utilization in testing of VW Group vehicles
- Personal interest & engagement in the field

Page(s) in thesis: 1-2

Preliminaries

- **Highlights of Driving Automation** → *What are the levels of driving automation?* *What is the impact of functional safety?*
- **E/E Architecture** → *What makes driving automation physically feasible?*
- **Automotive Networking** → *What are the means for in-vehicle networking?* *How Automotive Ethernet works?*
- **AUTOSAR** → *What are signals? How are they being sent & received?*
- **Security of In-vehicle Communication** → *How in-vehicle communication is protected?* *How to bypass selected security mechanisms?*
- **Existing Solutions** → *What are the analogous solutions? How do they work?*

Page(s) in thesis: 5-40

Challenges

Overall, the task of performing the *"on-the-way"* signal manipulation implies:

1. **Acquiring the information** about signal and security mechanisms within Ethernet packet (frame) **in advance**.
2. **Capturing the existing ongoing traffic** in Automotive Ethernet network.
3. **Identification of a desired signal** within the captured traffic.
4. **Modification** of signal value(s) **via direct bit substitutions** in the Ethernet packet (frame).
5. **Circumvention of security mechanisms** via direct bit substitutions of recalculated checksums & counters.
6. **Resending** the modified Ethernet packet (frame) via communication bus.

Steps **2-6** have to be accomplished with minimal processing delay and no packet losses.

All the communication parties must not be aware of any existing interference.

Page(s) in thesis: 40

Requirements Synthesis

- **Functionality Limitations (7)**
- **User Requirements**
- **Use Cases (3)**
- **Hardware Requirements**
- **Software Requirements**
  - **Functional (9)**
  - **Non-functional (1)**

L2: **The system shall not be fully autonomous.** It order to operate, it shall partially rely on the information provided by the user.

L3: **The system's applicability is limited to inter-ECU communication exclusively.** Manipulation of signals between different SWCs located in one ECU requires additional integration into AUTOSAR RTE, which is deemed to be unnecessary in terms of this work.

L4: **The Automotive Ethernet network employed shall not incorporate any specialized traffic protection protocols, such as IPsec, MACsec, TLS, gPTP or any alternative solutions, including those developed by the manufacturer.** Bypassing the protection provided by one or more of these mechanisms could be challenging and is a separate issue that goes beyond the scope of this thesis.

L5: **The system shall be compatible merely with IEEE 802.3 Ethernet standard.** Compliance with other standards (namely IEEE 1722 in context of AVB/TSN) is not a common case and requires additional efforts, theoretical background, etc.

FR1: **System has to be capable of changing the value of specified signal(s).**

FR2: **System has to be capable of automatic detection and circumvention of in-PDU Alive Mechanism.**

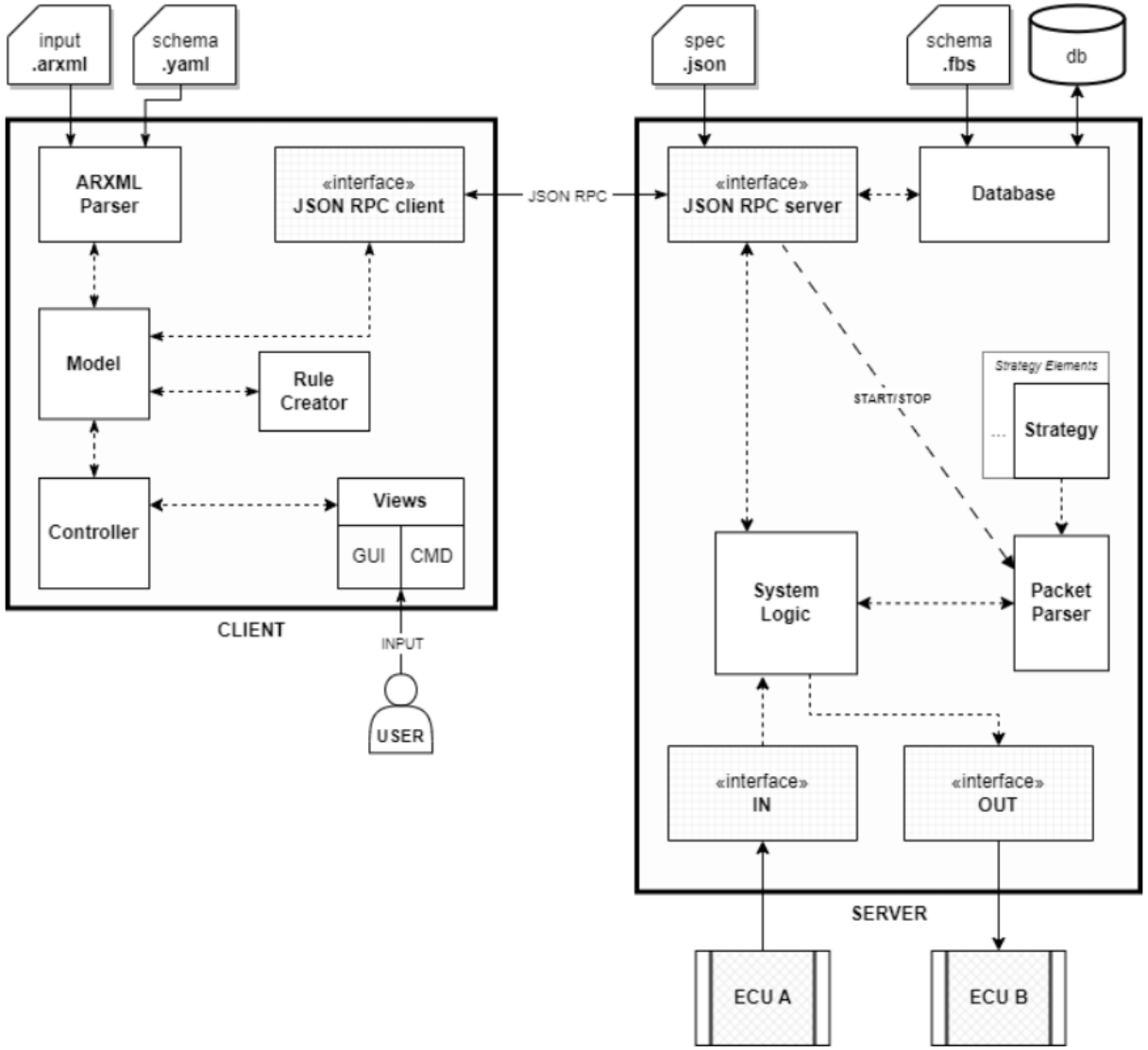
FR3: **System has to be capable of automatic detection and computation of in-PDU CRC based on provided polynomial.**

FR4: **System has to be capable of automatic recomputation of in-packet checksums.**

Page(s) in thesis: 41-45

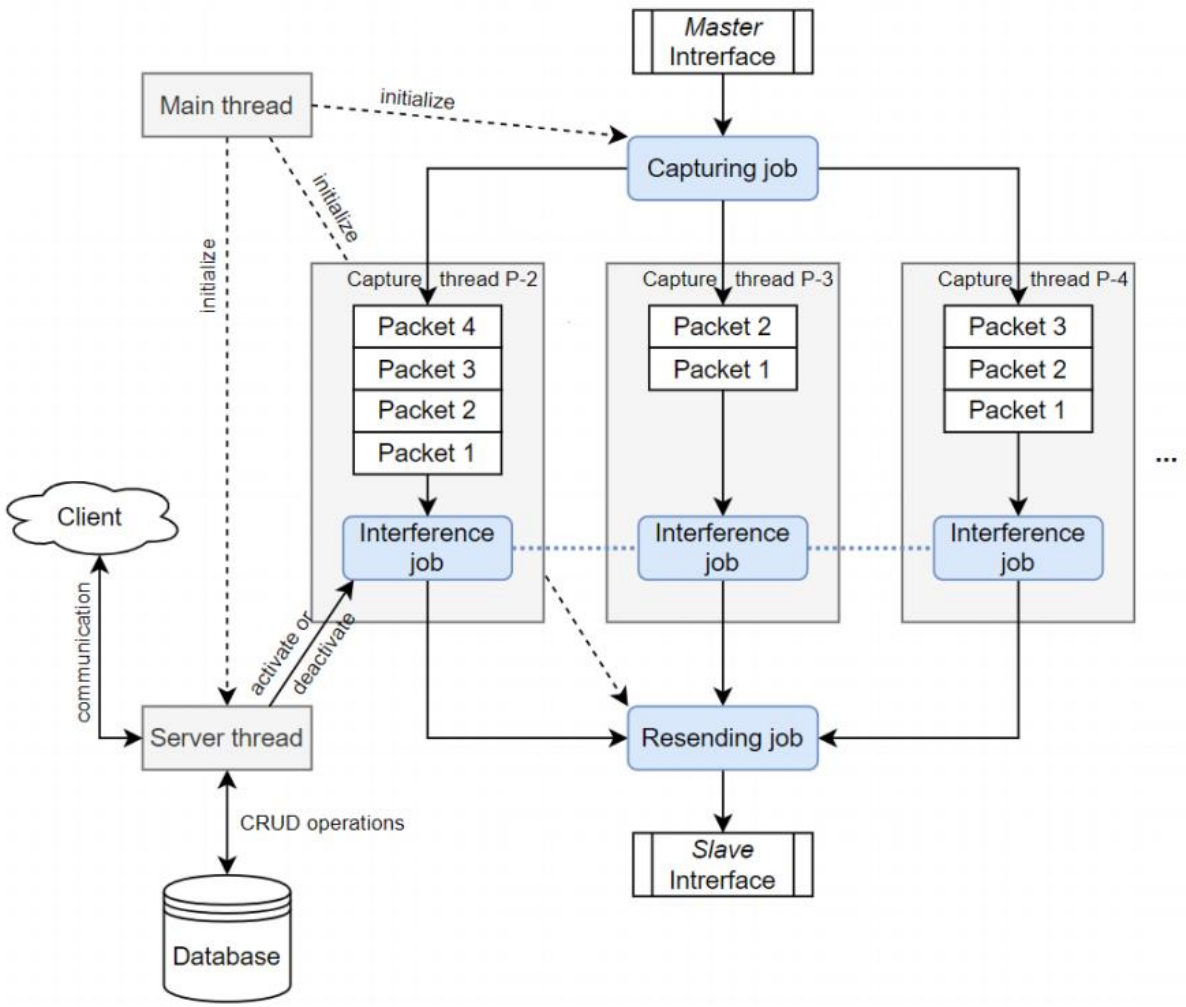
Software Design & Implementation (1)

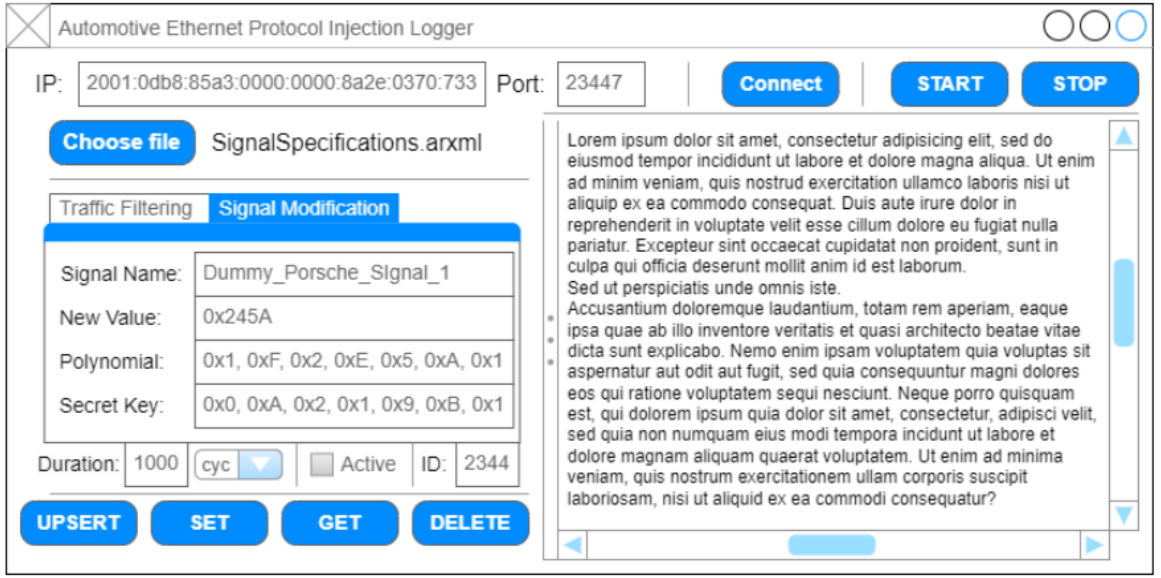
- **Architectural design:** *client-server* architecture
  - JSON-RPC interface with 7 procedures
  - Rule-based operation
- **Client:** *user interaction*
  - Schema-based customizable ARXML parsing
  - GUI, command line operation
- **Server:** *direct traffic interference*
  - Database
  - 2 operational modes (filtering/modification)
  - Multithreaded environment
  - Discrete interference strategies

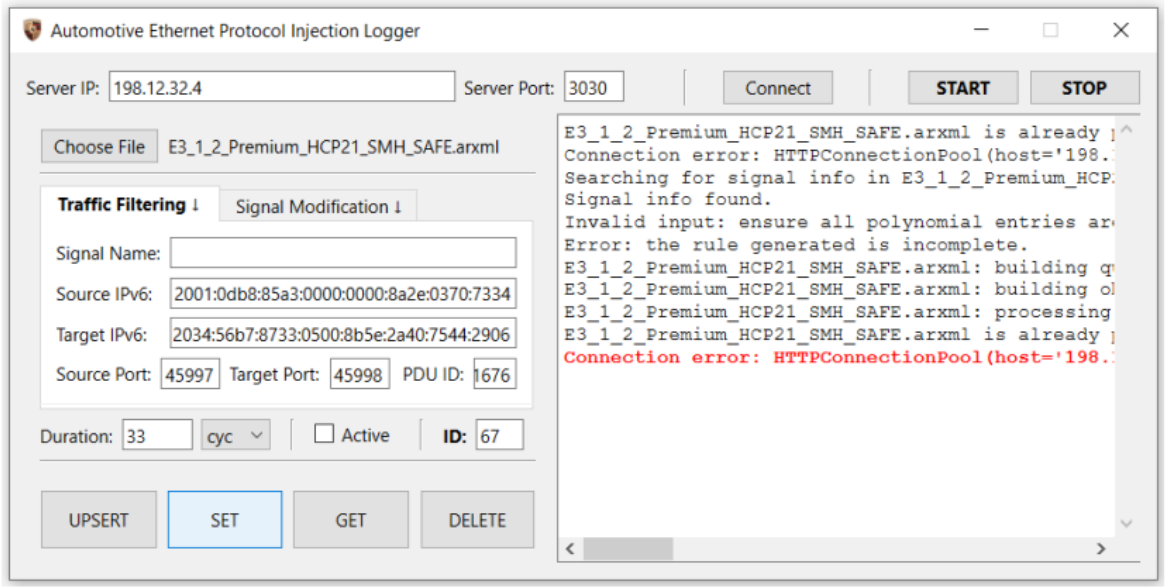


Page(s) in thesis: 47-90

Software Design & Implementation (2)



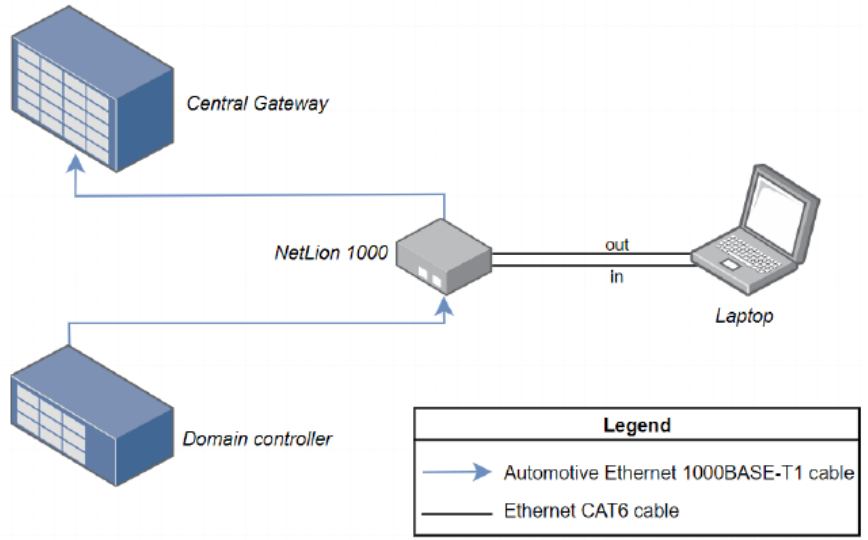




Page(s) in thesis: 53-90

Testing Setup

- Controlled laboratory environment
- Two laptop HW configurations used to compare testing results
- Car environment simulated with HiL, no mock data used
- Resulting data measured, captured & verified with CANoe
- Repetitive testing for results accuracy
- Late December 2023

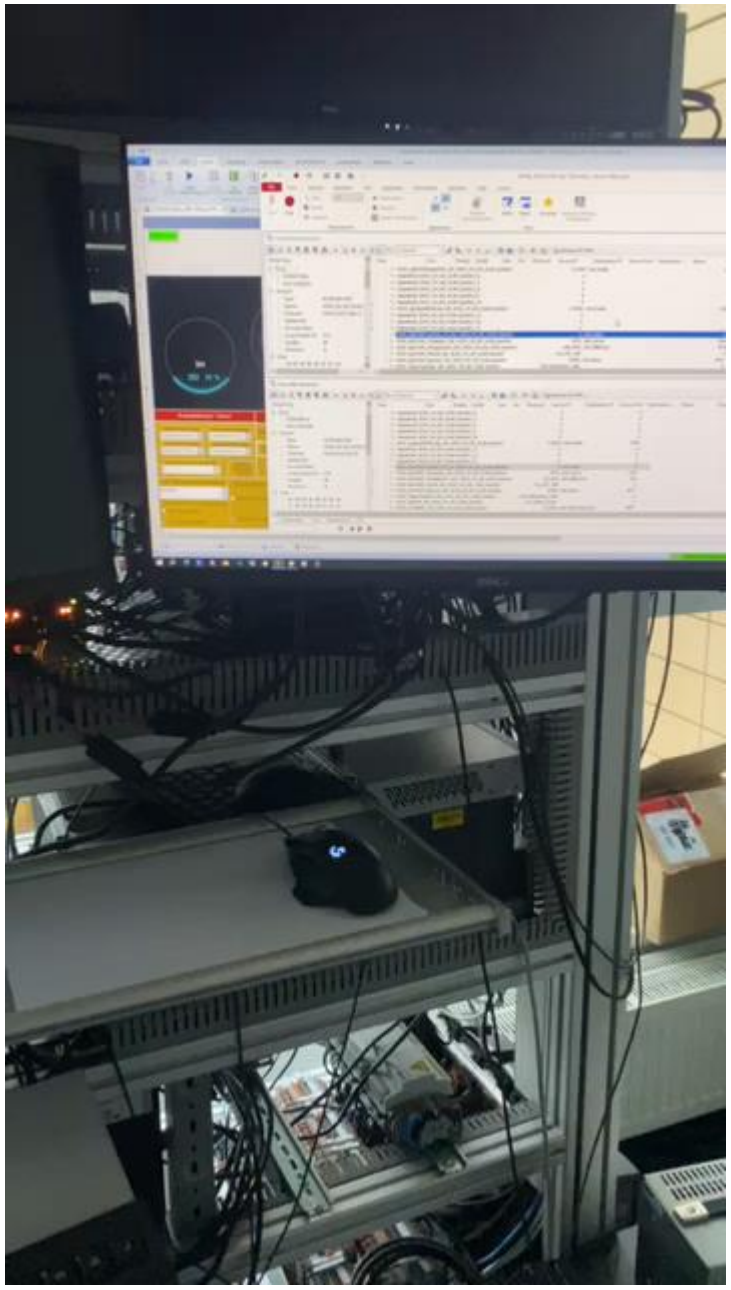


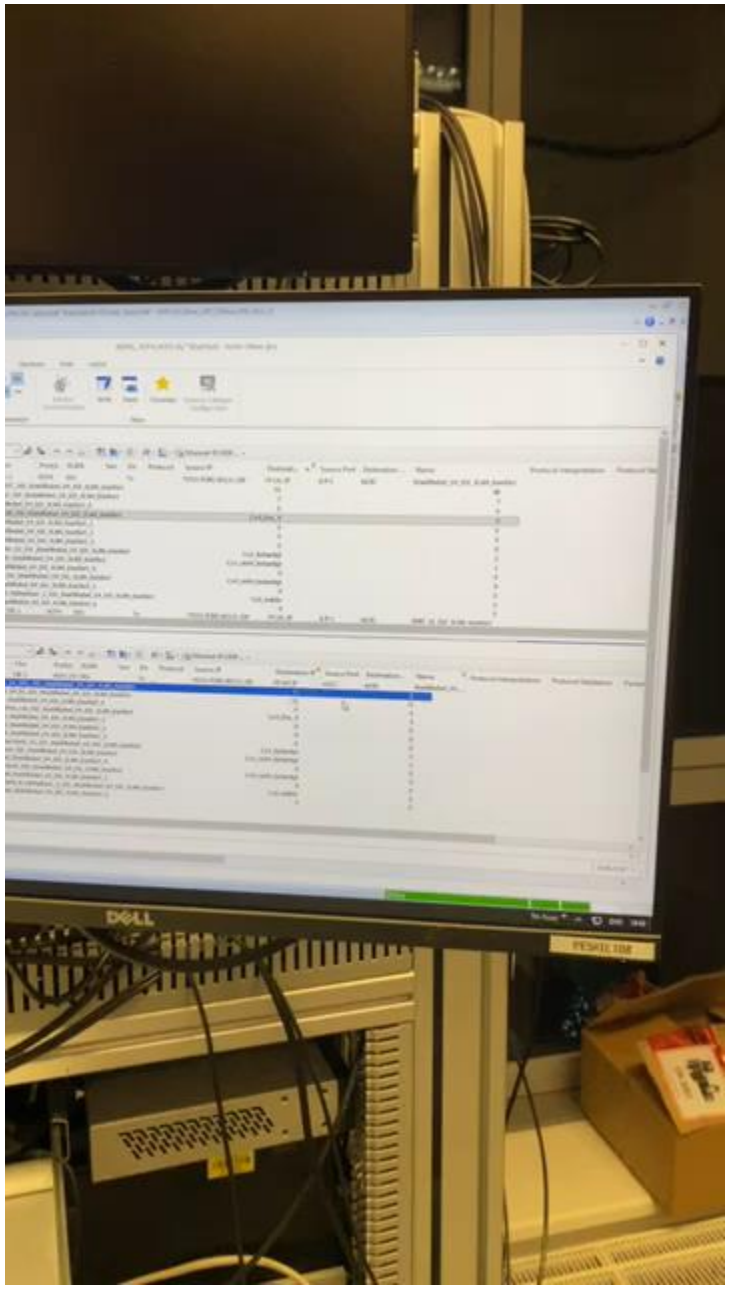
+

Page(s) in thesis: 91-113

Testing

- **Client testing:**
  - GUI:
    - Heuristics analysis
    - User-involved tests
  - ARXML Parser:
    - Component & Structural tests
    - Non-functional tests
  - System testing
- **Server:**
  - System testing (simulation-based):
    - Functional
    - Non-functional (2 HW configurations)





Page(s) in thesis: 91-113

Testing Results

- **Key Technical Achievements ✓:**
  - Successful ARXML data extraction and signal modification
  - Security bypass mechanisms proven feasible
  - Signal(s) modified within required timeframe
  - Real-time intervention capabilities confirmed
- **Identified Challenges ⚠:**
  - Performance issues with large ARXML files
  - GUI requires usability improvements
  - Some unexplained artifacts discovered -> implementation flaw?
  - Network load testing limitations
- **Final Assessment ✅:**
  - All primary requirements met
  - Core functionality (proof of concept) successfully demonstrated
  - Clear path for future improvements identified

Page(s) in thesis: 91-113

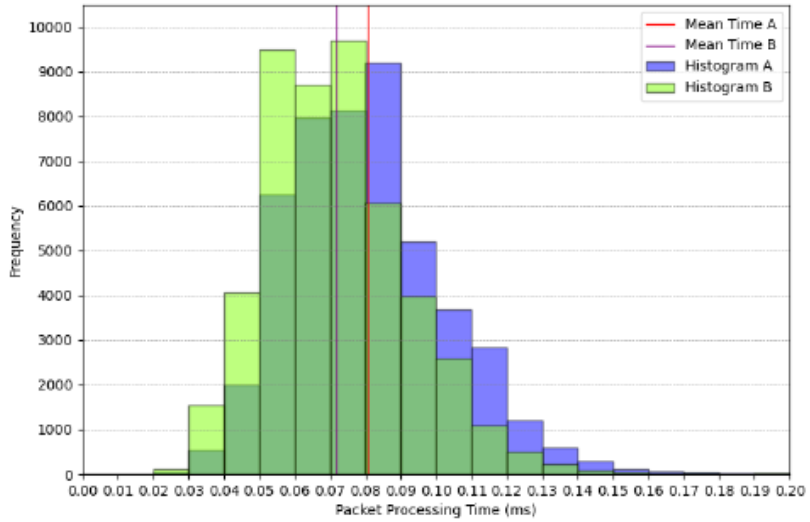


Figure 5.10 Average Ethernet packet processing time on Computers A and B in Traffic Filtering mode, one capture thread utilized.

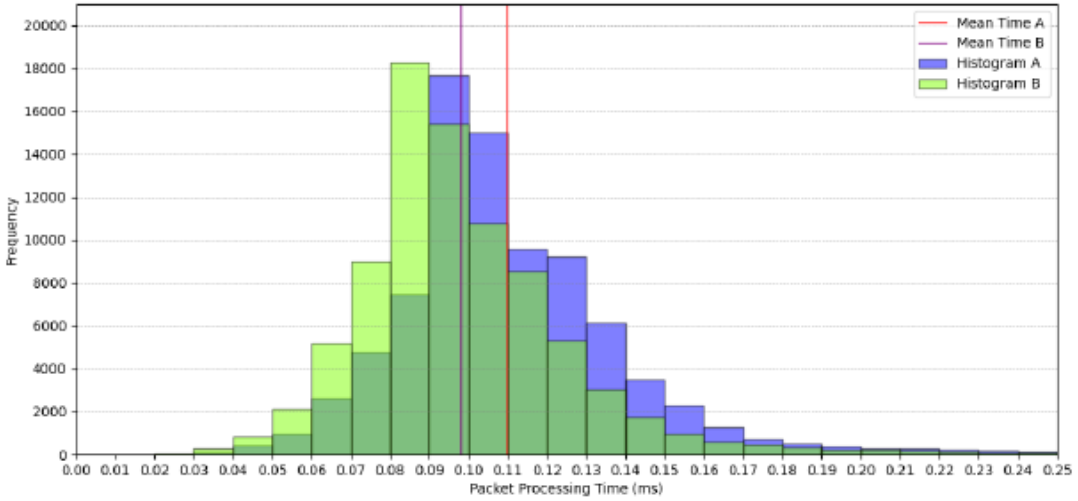


Figure 5.12 Average Ethernet packet processing time on Computers A and B in Signal Modification mode (one signal modified) with in-PDU CRC recalculated, one capture thread utilized.

Conclusion

- **Objectives achieved:** developed a prototype for testing of electronic control units on Automotive Ethernet.
- **Theoretical insights:** covered a wide spectrum of theoretical topics, delivering a solid introduction to automotive world.
- **Industry-driven requirements:** co-developed SW RQs with Porsche, ensuring the system's relevance and applicability.
- **Design and implementation:** implemented a client-server system, detailing design choices and technology use.
- **Comprehensive testing:** conducted rigorous tests, including simulation-based evaluations with industry partners, to verify system compliance and functionality.
- **Security bypass achieved:** successfully manipulated Automotive Ethernet signals, circumventing specific security measures without detection.
- **Defect identification & compliance:** detected SW issues yet confirmed the system's alignment with initial RQs and goals.

- **Significant contributions:** offered valuable theoretical and practical insights for automotive technology.
- **Future research potential:** highlighted opportunities for further exploration in field, system enhancement, and testing.
- **Innovative and relevant:** despite emerging market solutions, the thesis is in the front edge of automotive testing technologies.

Page(s) in thesis: 39, 45, 90, 112, 115

THANK YOU FOR YOUR ATTENTION

QUESTIONS?