HW/SW CO-DESIGN OF AN AUTOMOTIVE EMBEDDED FIREWALL

Mert D. Pesé, Karsten Schmidt
Audi Electronics Venture GmbH
Harald Zweck
Infineon Technologies AG

SAE INTERNATIONAL

Agenda

Introduction

Concept

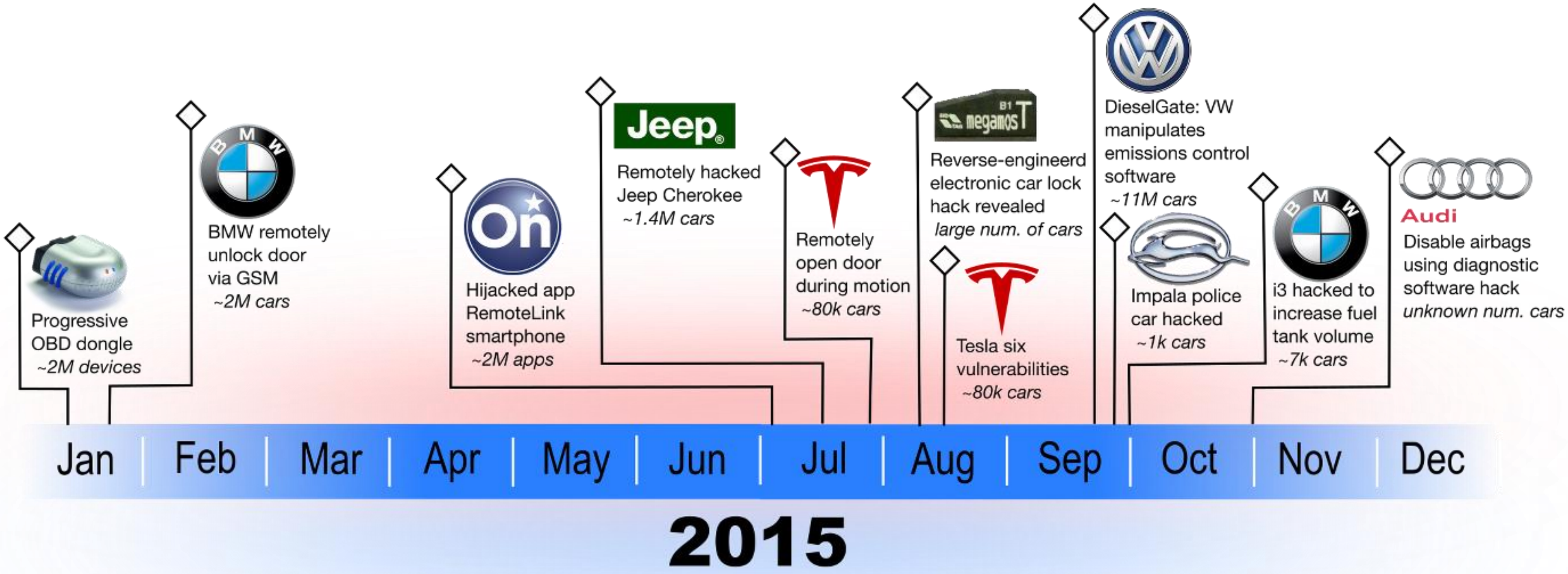
Implementation

Results

Outlook

Introduction

Automotive cybersecurity is an emerging field



Progressive OBD dongle
~2M devices

BMW remotely unlock door via GSM
~2M cars

Hijacked app RemoteLink smartphone
~2M apps

Remotely hacked Jeep Cherokee
~1.4M cars

Remotely open door during motion
~80k cars

Reverse-engineerd electronic car lock hack revealed
large num. of cars

Tesla six vulnerabilities
~80k cars

DieselGate: VW manipulates emissions control software
~11M cars

Impala police car hacked
~1k cars

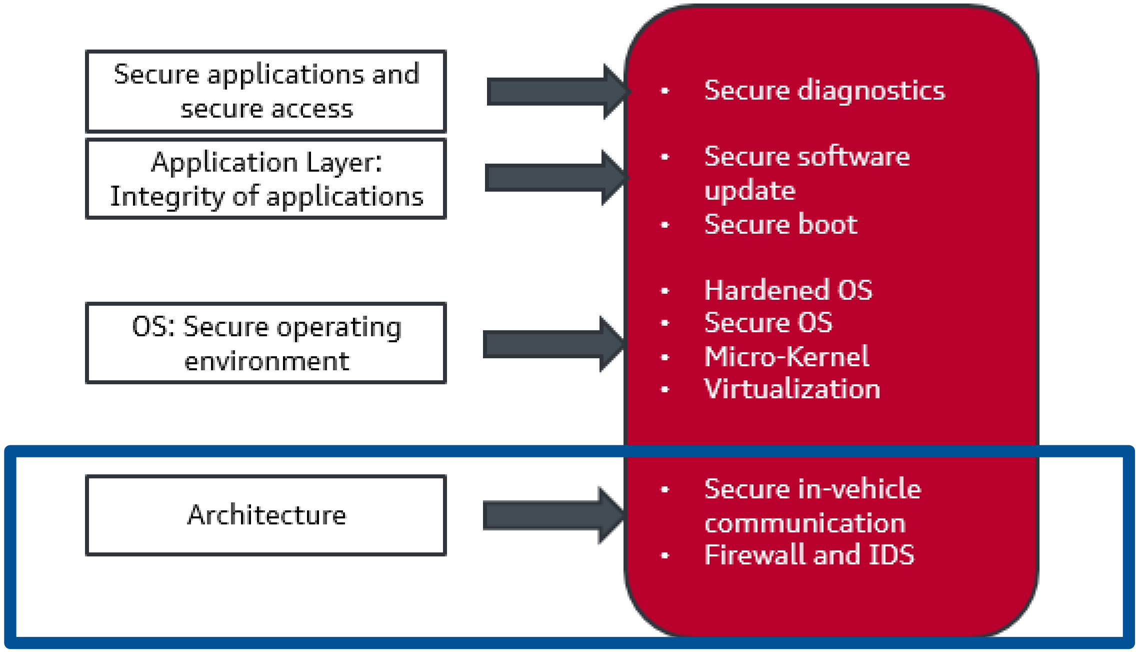
i3 hacked to increase fuel tank volume
~7k cars

Disable airbags using diagnostic software hack
unknown num. cars

Introduction

Definition of countermeasures

- based on a holistic security concept for vehicles



Secure applications and secure access

Application Layer: Integrity of applications

OS: Secure operating environment

Architecture

- Secure diagnostics
- Secure software update
- Secure boot
- Hardened OS
- Secure OS
- Micro-Kernel
- Virtualization
- Secure in-vehicle communication
- Firewall and IDS

Introduction

Holistic network security concept consisting of four barriers

- Access control to network
- Secure on-board communication
- Data usage policies
- Anomaly detection and defense

Introduction

Holistic network security concept consisting of four barriers

- Access control to network ➔ Firewall
- Secure on-board communication
- Data usage policies
- Anomaly detection and defense

Agenda

Introduction

Concept

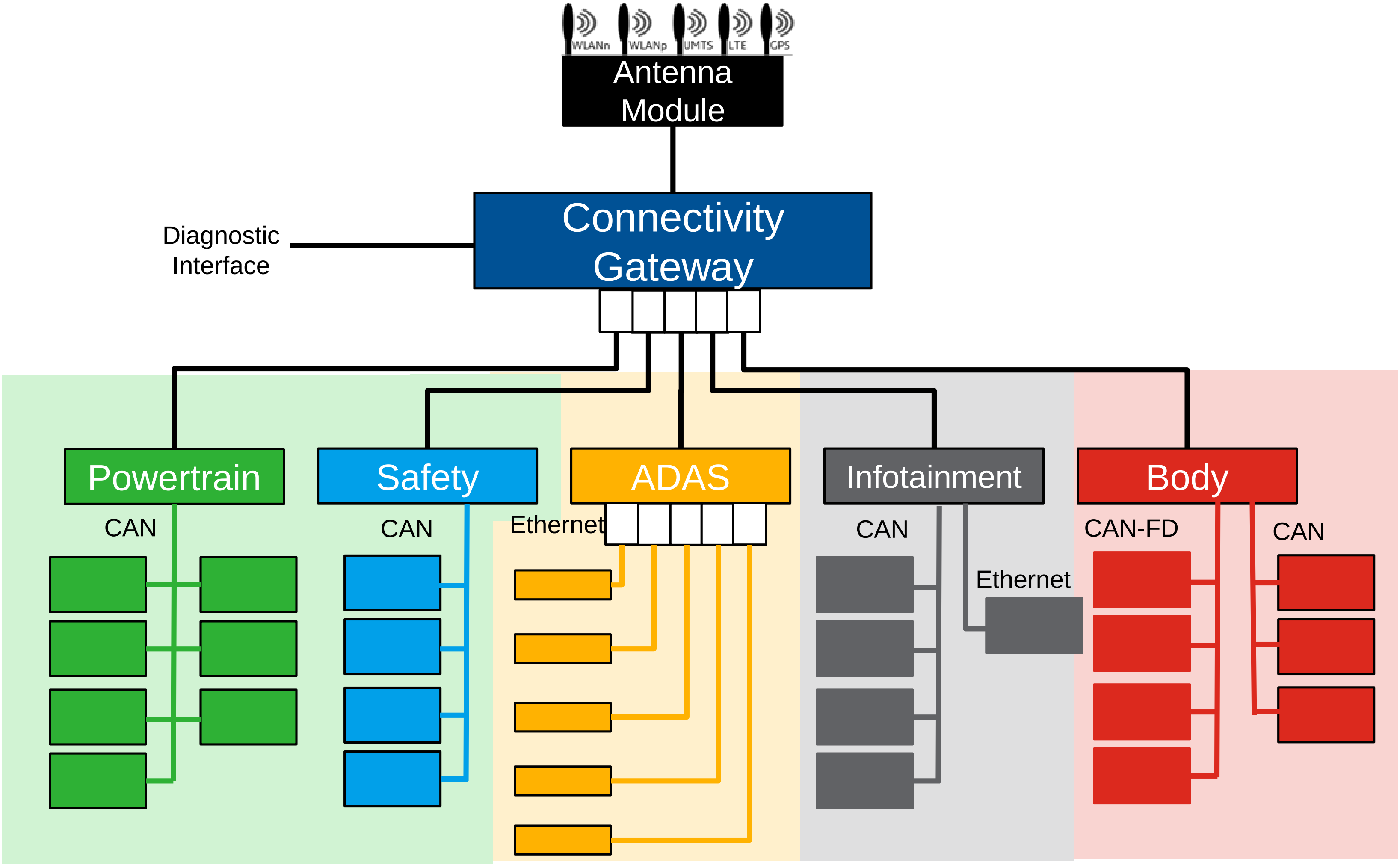
Implementation

Results

Outlook

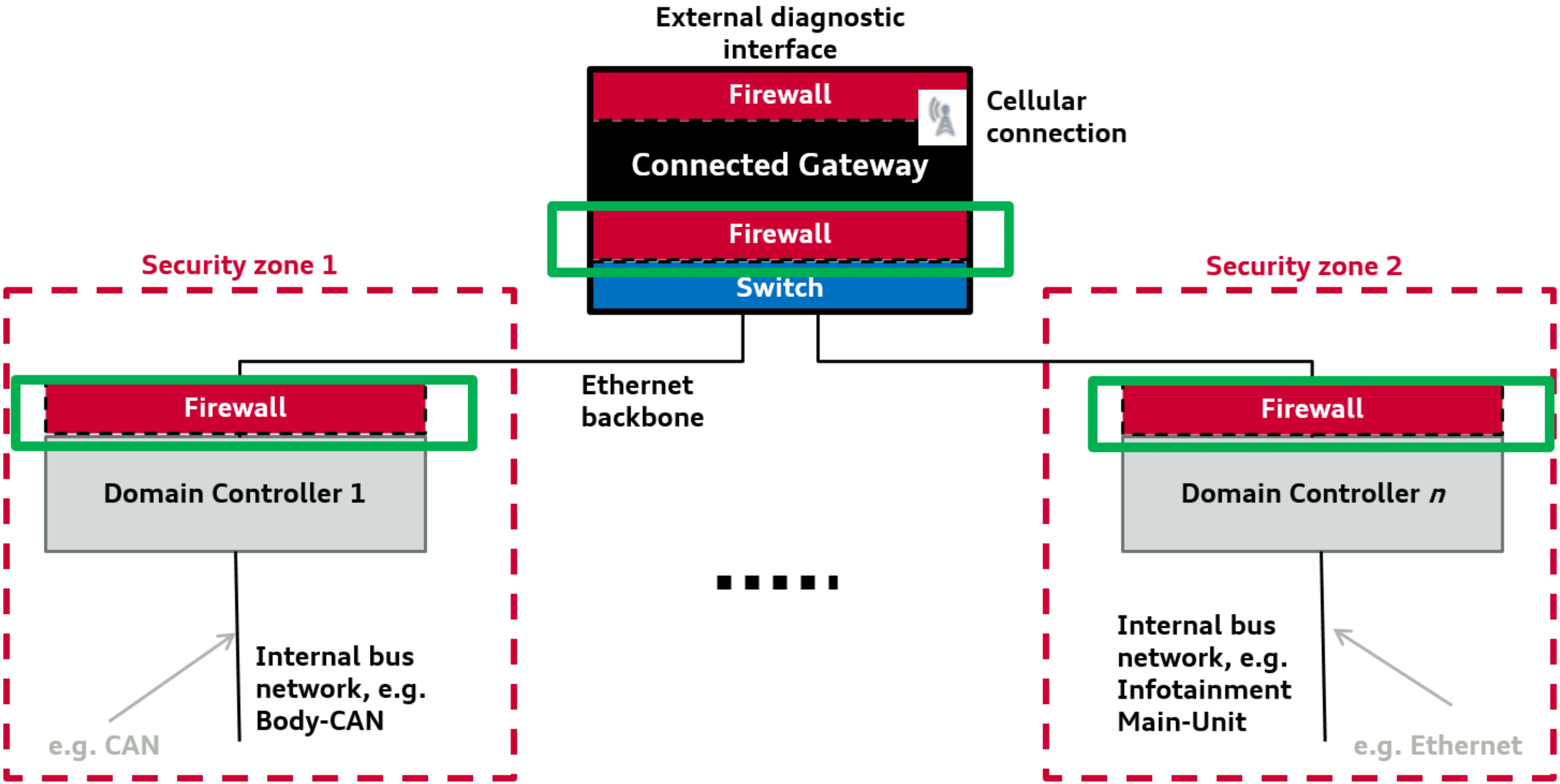
Concept

E/E Architecture: Next-Generation Domain Architecture



Concept

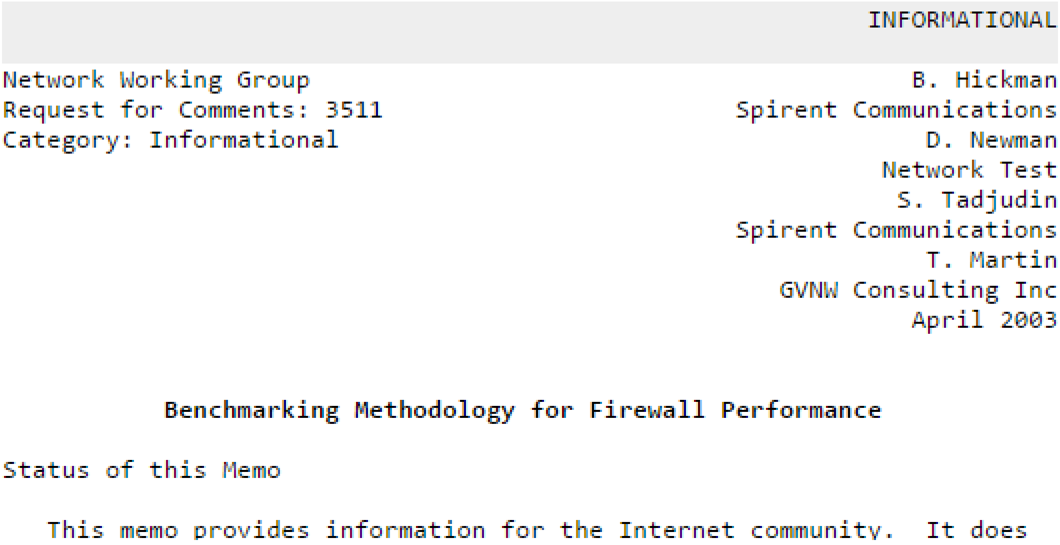
Abstract system model



Concept

Evaluation of firewall performance based on automotive requirements

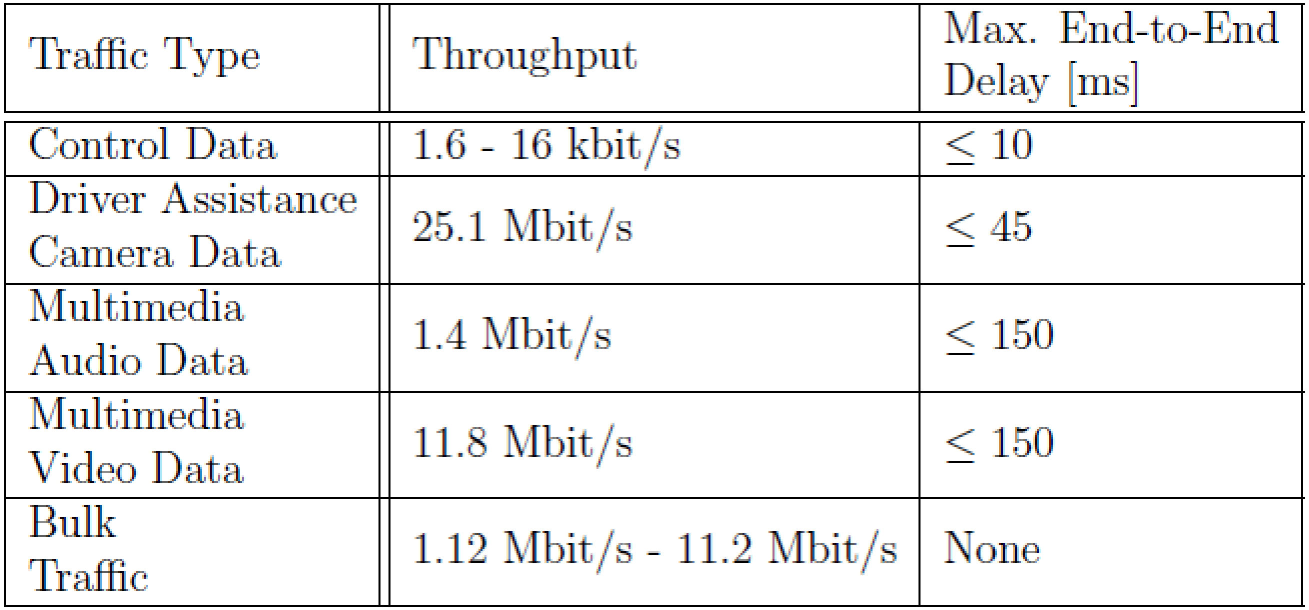
- E2E latency
- Jitter
- Throughput
- Memory/RAM consumption
- CPU utilization



```
                                                          INFORMATIONAL
Network Working Group                                        B. Hickman
Request for Comments: 3511                       Spirent Communications
Category: Informational                                      D. Newman
                                                           Network Test
                                                            S. Tadjudin
                                                 Spirent Communications
                                                              T. Martin
                                                    GVNW Consulting Inc
                                                             April 2003


           Benchmarking Methodology for Firewall Performance

Status of this Memo

   This memo provides information for the Internet community.  It does
```

Concept

Latency and throughput requirements in in-vehicle networks

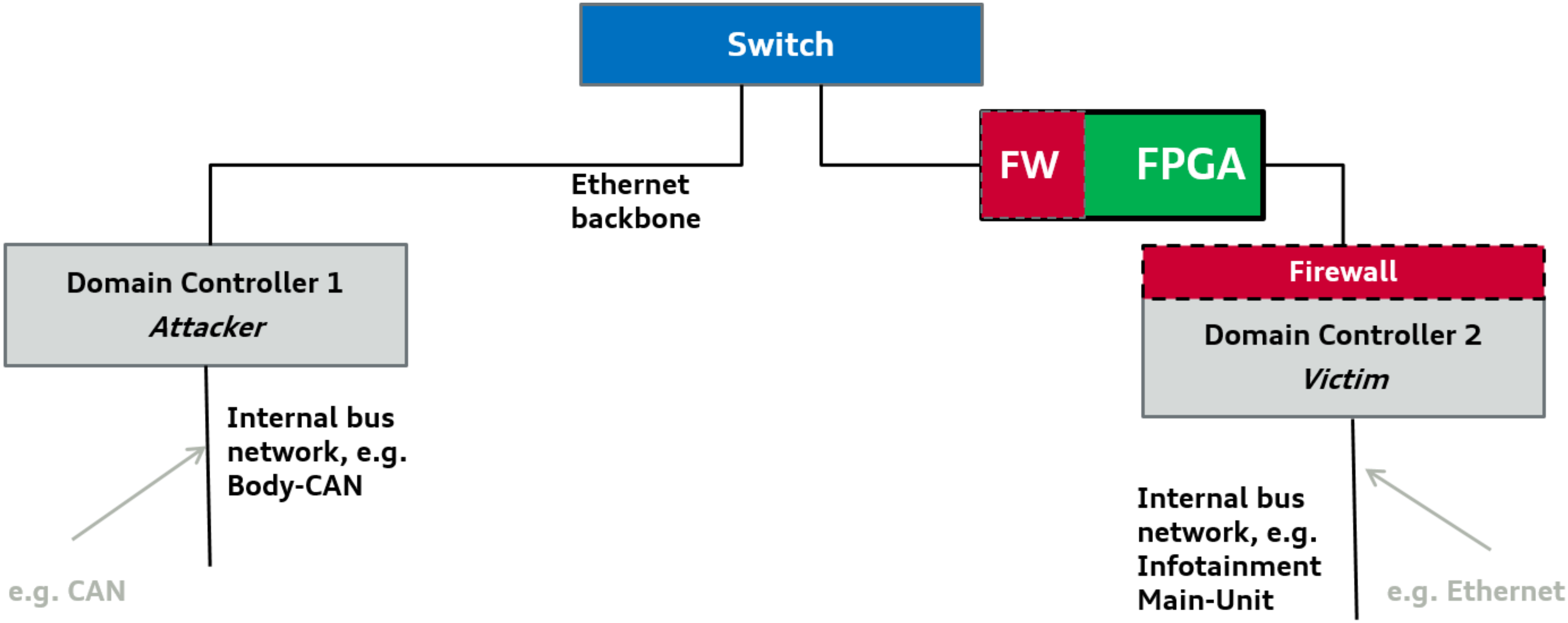


Traffic Type	Throughput	Max. End-to-End Delay [ms]
Control Data	1.6 - 16 kbit/s	$\leq$ 10
Driver Assistance Camera Data	25.1 Mbit/s	$\leq$ 45
Multimedia Audio Data	1.4 Mbit/s	$\leq$ 150
Multimedia Video Data	11.8 Mbit/s	$\leq$ 150
Bulk Traffic	1.12 Mbit/s - 11.2 Mbit/s	None

Source: Y. Lee and K. Park. Meeting the real-time constraints with standard Ethernet in an in-vehicle network

Concept

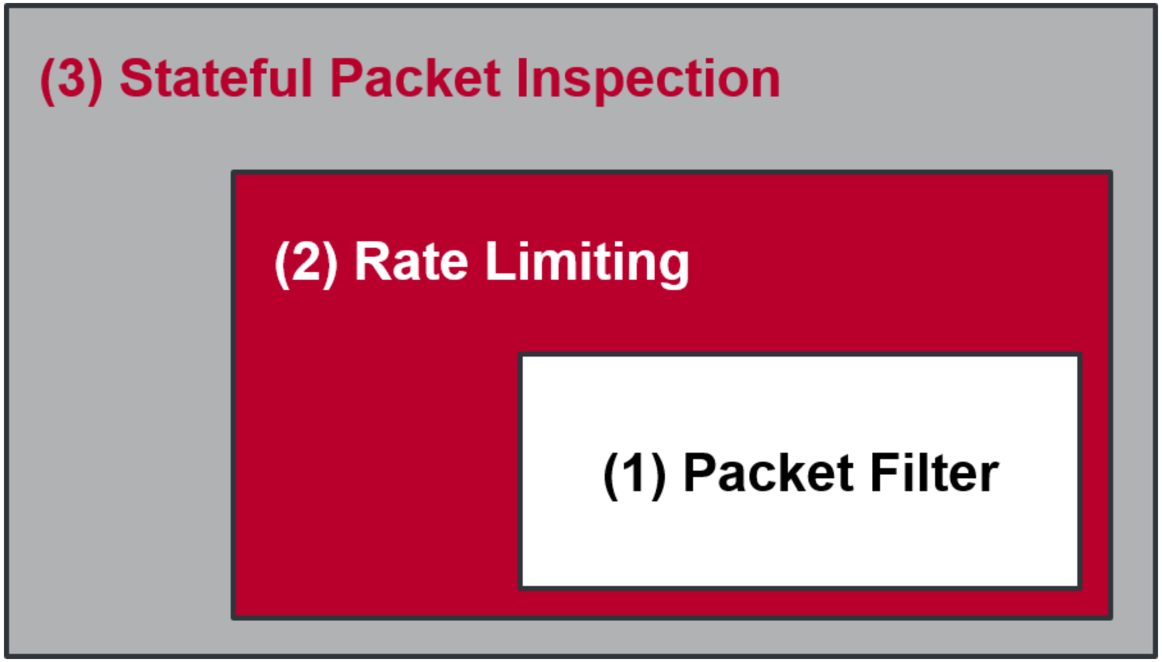
Experimental setup



Concept

Firewall features

- Successive analysis stages on MCU



Concept

Definition of assessment matrix based on requirements

- (N)PF: (No) Packet Filter
- SIF: Stateful Inspection Firewall

	CPU load (% MCU)	RAM consumption (% MCU)	E2E latency Worst Case (µs)
MCU NPF			
MCU PF			
MCU PF+SIF			
FPGA PF			
MCU+FPGA combined			

Concept

Adversary model

Network Control

Install or corrupt a device on the network to control the operation of other devices

Denial of Service

Deny access to network resources to other devices on the network

Snooping or Information Theft

Snoop the content of traffic on the network to extract information

Source: Broadcom

Agenda

Introduction

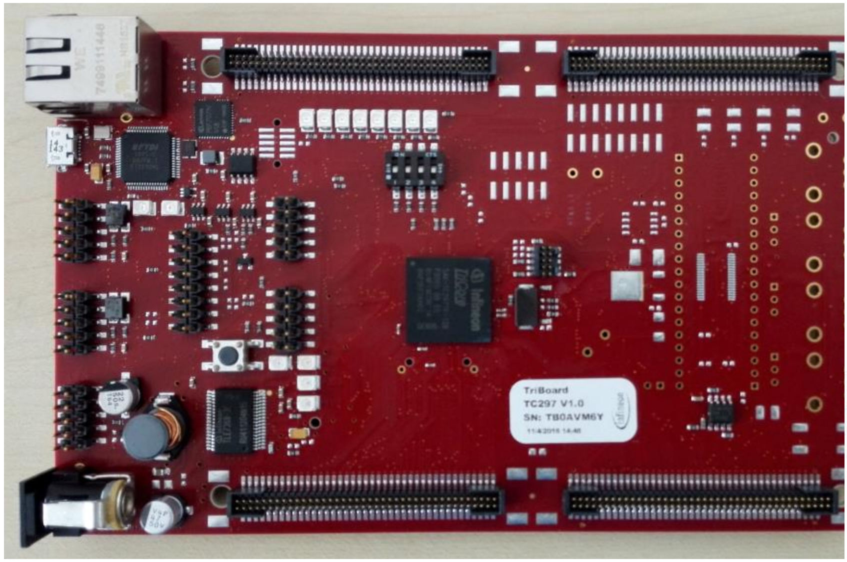
Concept

Implementation

Results

Outlook

Implementation



Infineon AURIX TriCore TC297-TF

Altera Cyclone V SoC Development Kit

Agenda

Introduction

Concept

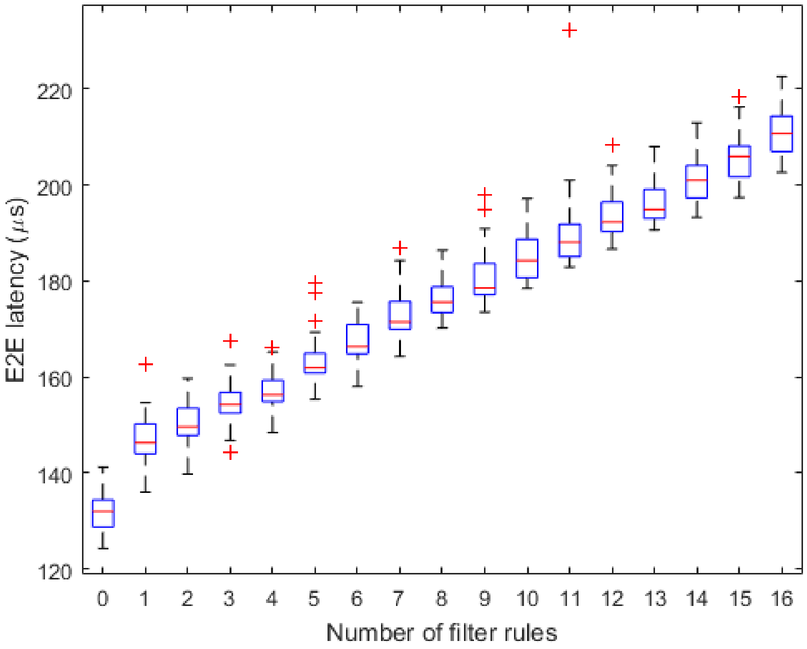
Implementation

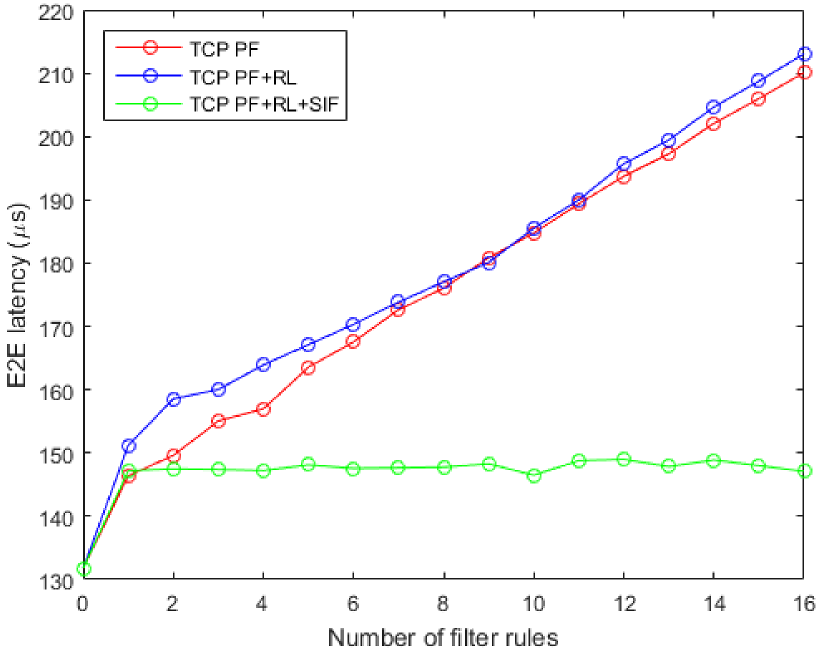
Results

Outlook

Results

E2E latency MCU

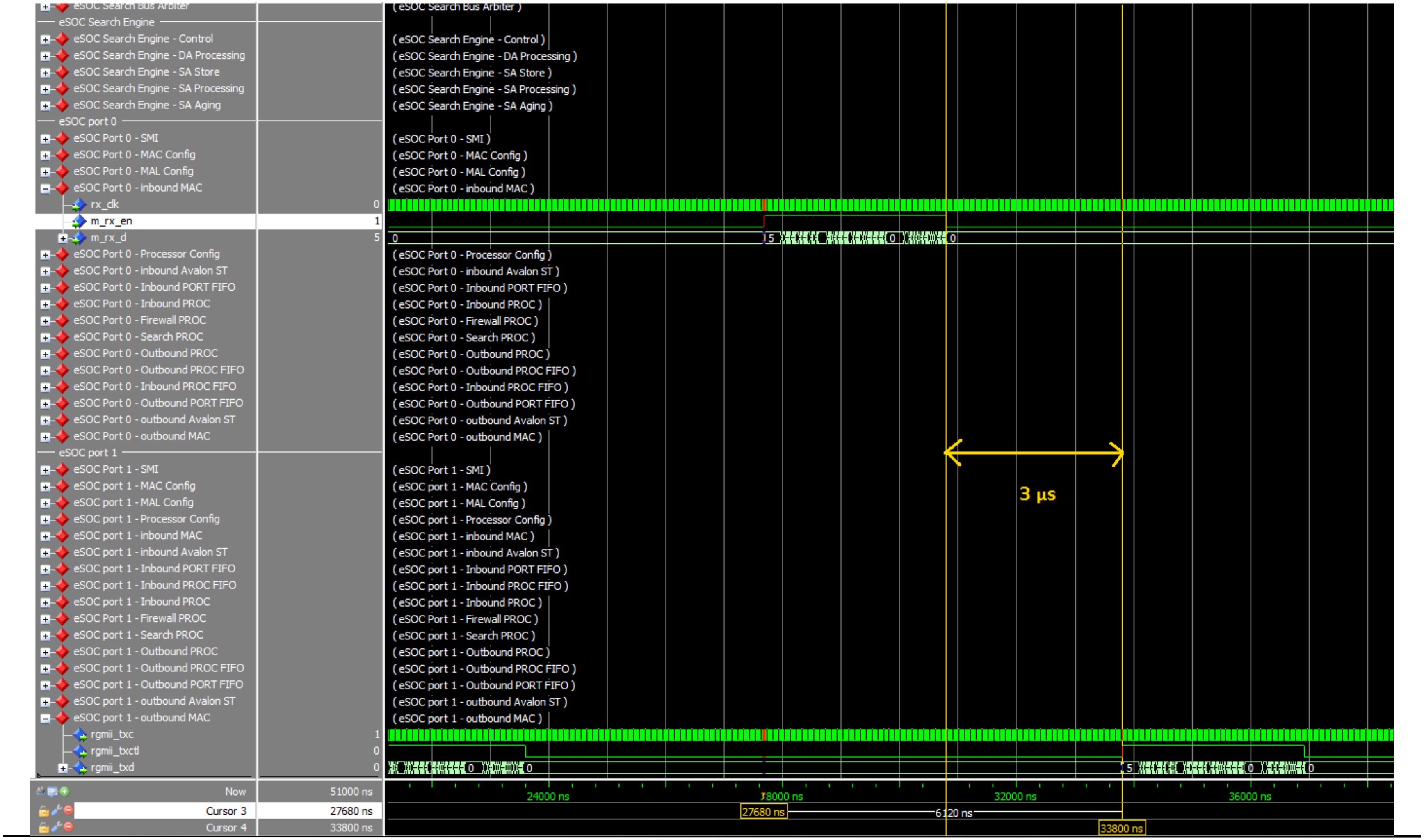




500 rules: 2.3 ms → 2.2 ms overhead

Results

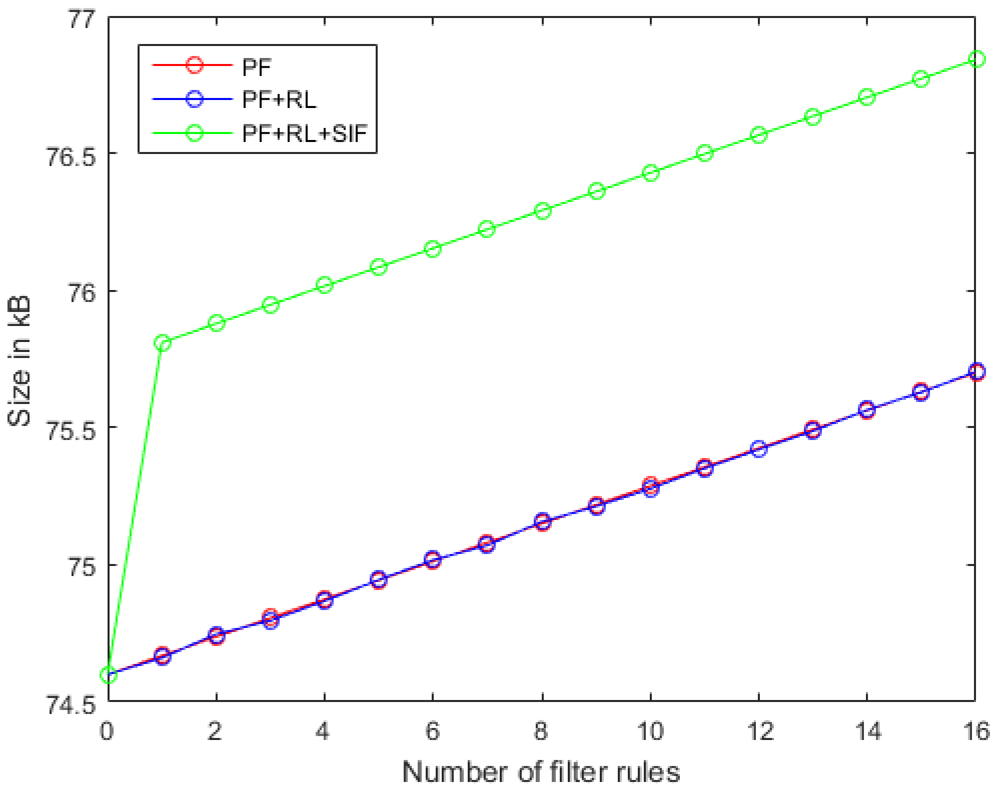
E2E latency FPGA


eSOC Search Bus Arbiter
eSOC Search Engine
eSOC Search Engine - Control
eSOC Search Engine - DA Processing
eSOC Search Engine - SA Store
eSOC Search Engine - SA Processing
eSOC Search Engine - SA Aging
eSOC port 0
eSOC Port 0 - SMI
eSOC Port 0 - MAC Config
eSOC Port 0 - MAL Config
eSOC Port 0 - inbound MAC
rx_clk
m_rx_en
m_rx_d
eSOC Port 0 - Processor Config
eSOC Port 0 - inbound Avalon ST
eSOC Port 0 - Inbound PORT FIFO
eSOC Port 0 - Inbound PROC
eSOC Port 0 - Firewall PROC
eSOC Port 0 - Search PROC
eSOC Port 0 - Outbound PROC
eSOC Port 0 - Outbound PROC FIFO
eSOC Port 0 - Inbound PROC FIFO
eSOC Port 0 - Outbound PORT FIFO
eSOC Port 0 - outbound Avalon ST
eSOC Port 0 - outbound MAC
eSOC port 1
eSOC Port 1 - SMI
eSOC port 1 - MAC Config
eSOC port 1 - MAL Config
eSOC port 1 - Processor Config
eSOC port 1 - inbound MAC
eSOC port 1 - inbound Avalon ST
eSOC port 1 - Inbound PORT FIFO
eSOC port 1 - Inbound PROC FIFO
eSOC port 1 - Inbound PROC
eSOC Port 1 - Firewall PROC
eSOC port 1 - Search PROC
eSOC port 1 - Outbound PROC
eSOC port 1 - Outbound PROC FIFO
eSOC port 1 - Outbound PORT FIFO
eSOC port 1 - outbound Avalon ST
eSOC port 1 - outbound MAC
rgmii_txc
rgmii_txctl
rgmii_txd
3 µs
24000 ns
28000 ns
32000 ns
36000 ns
27680 ns
6120 ns
33800 ns

Now	51000 ns
Cursor 3	27680 ns
Cursor 4	33800 ns

Results

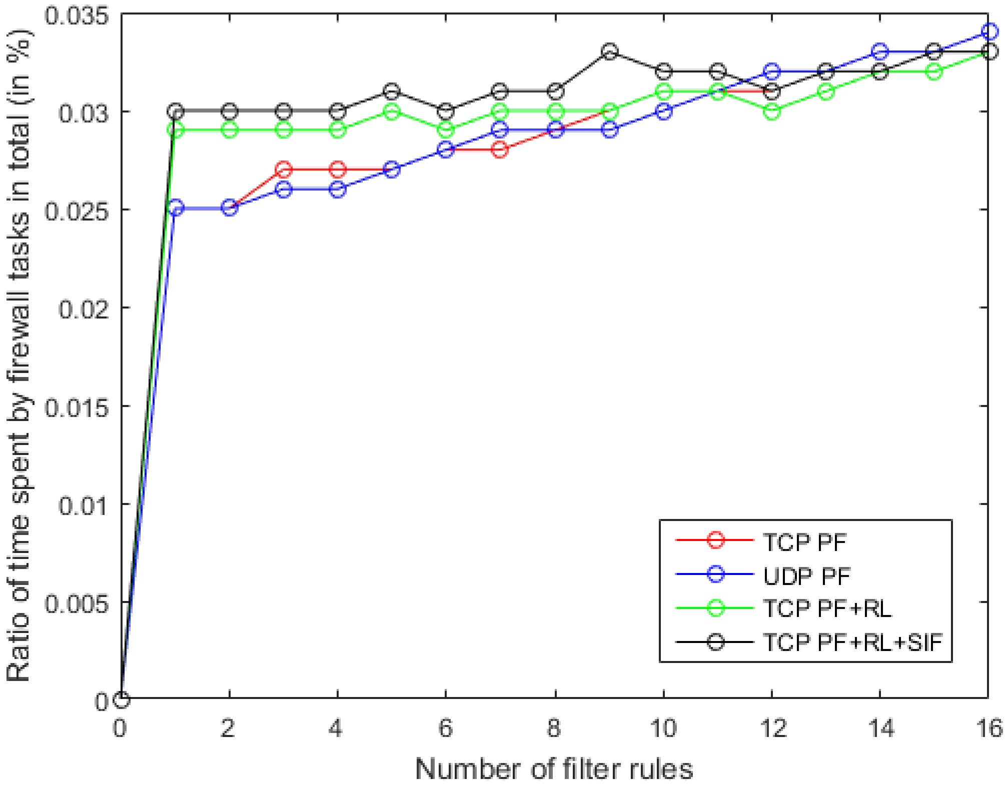
RAM consumption MCU



500 rules: 107 kB → 33 kB overhead

Results

CPU utilization



Results

Assessment matrix

- TCP traffic

	CPU load (% MCU)	RAM consumption (% MCU)	E2E latency Worst Case (µs)
MCU NPF	8.8	9.7	132
MCU PF	8.835	9.9	210
MCU PF+SIF	8.83	10	147
FPGA PF	n/a	n/a	3
MCU+FPGA combined	8.83	9.8	150

Agenda

Introduction

Concept

Implementation

Results

Conclusion and Outlook

Conclusion and Outlook

Distributed approach: HW firewall in GW, SW firewall on DCs

Trade-off SW ↔ HW regarding latency and RAM

Future Work

- Content-addressable memory (CAM)
- Application Layer filtering (DoIP, SOME/IP)
- Deep Packet Inspection in HW
- Consideration of external traffic model

Contact

Mert D. Pesé
2260 Hayward Street
Ann Arbor, MI 48109-2121

mpese@umich.edu
(734) - 489 - 2825