HW/SW CO-DESIGN OF AN AUTOMOTIVE EMBEDDED FIREWALL

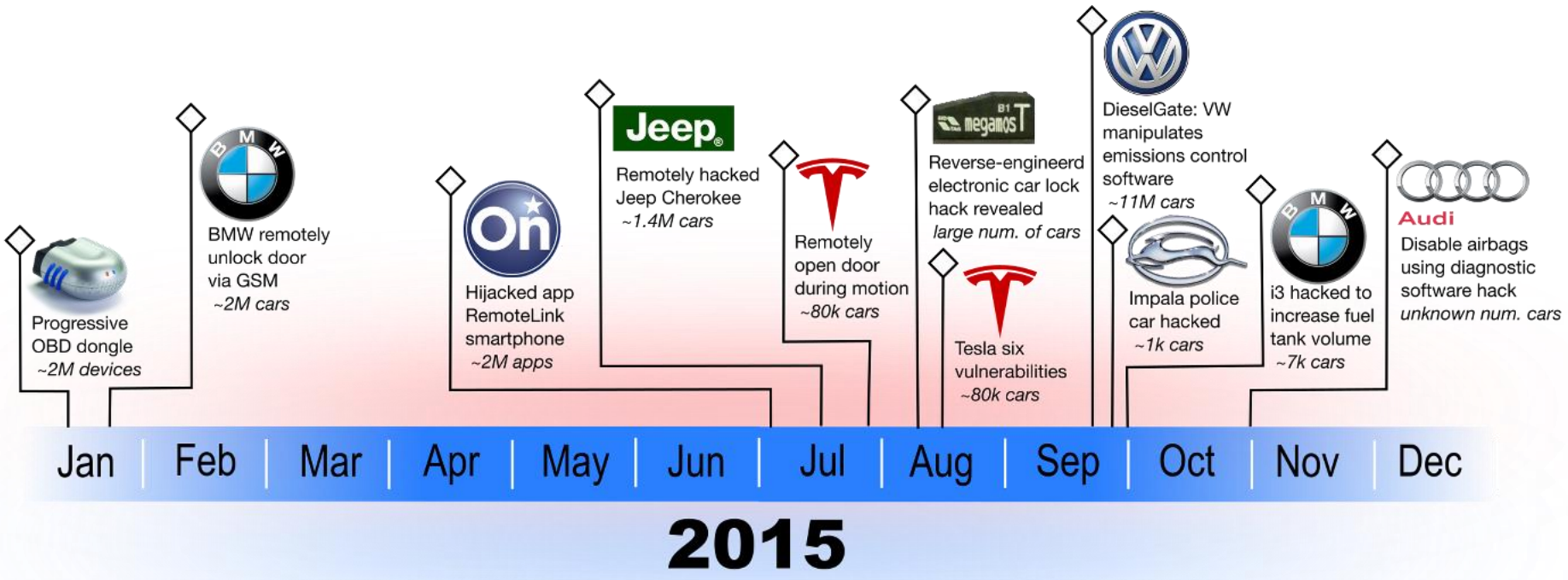
Mert D. Pesé, Karsten Schmidt
Audi Electronics Venture GmbH
Harald Zweck
Infineon Technologies AG

Agenda

Introduction
Concept
Implementation
Results
Outlook

Introduction

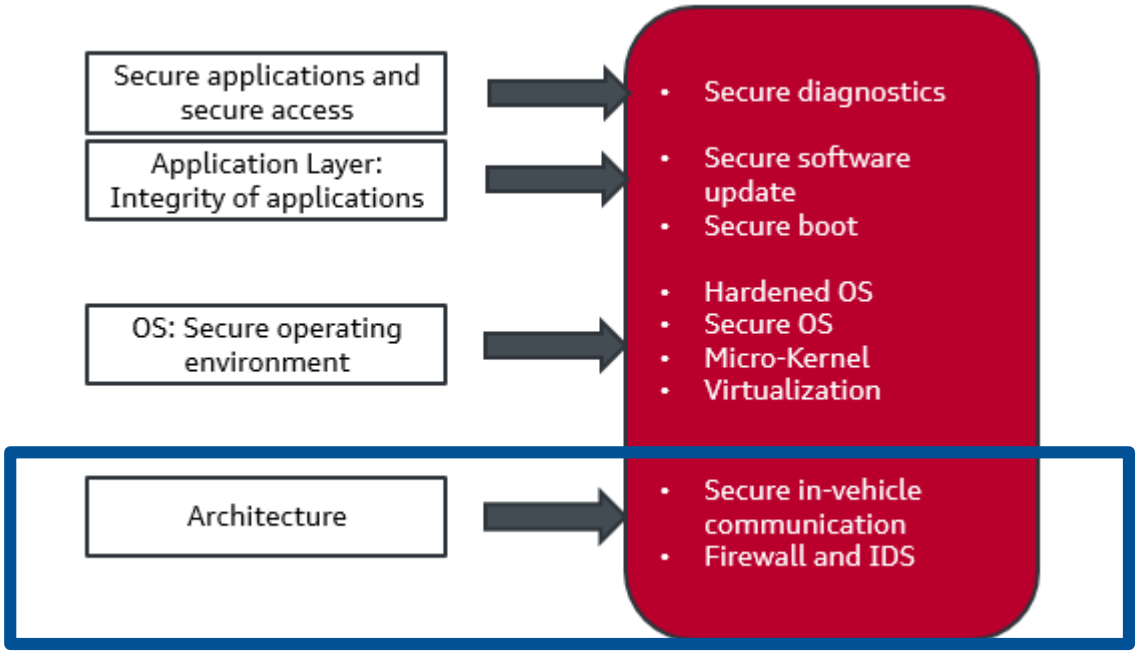
Automotive cybersecurity is an emerging field



Introduction

Definition of countermeasures

- based on a holistic security concept for vehicles



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

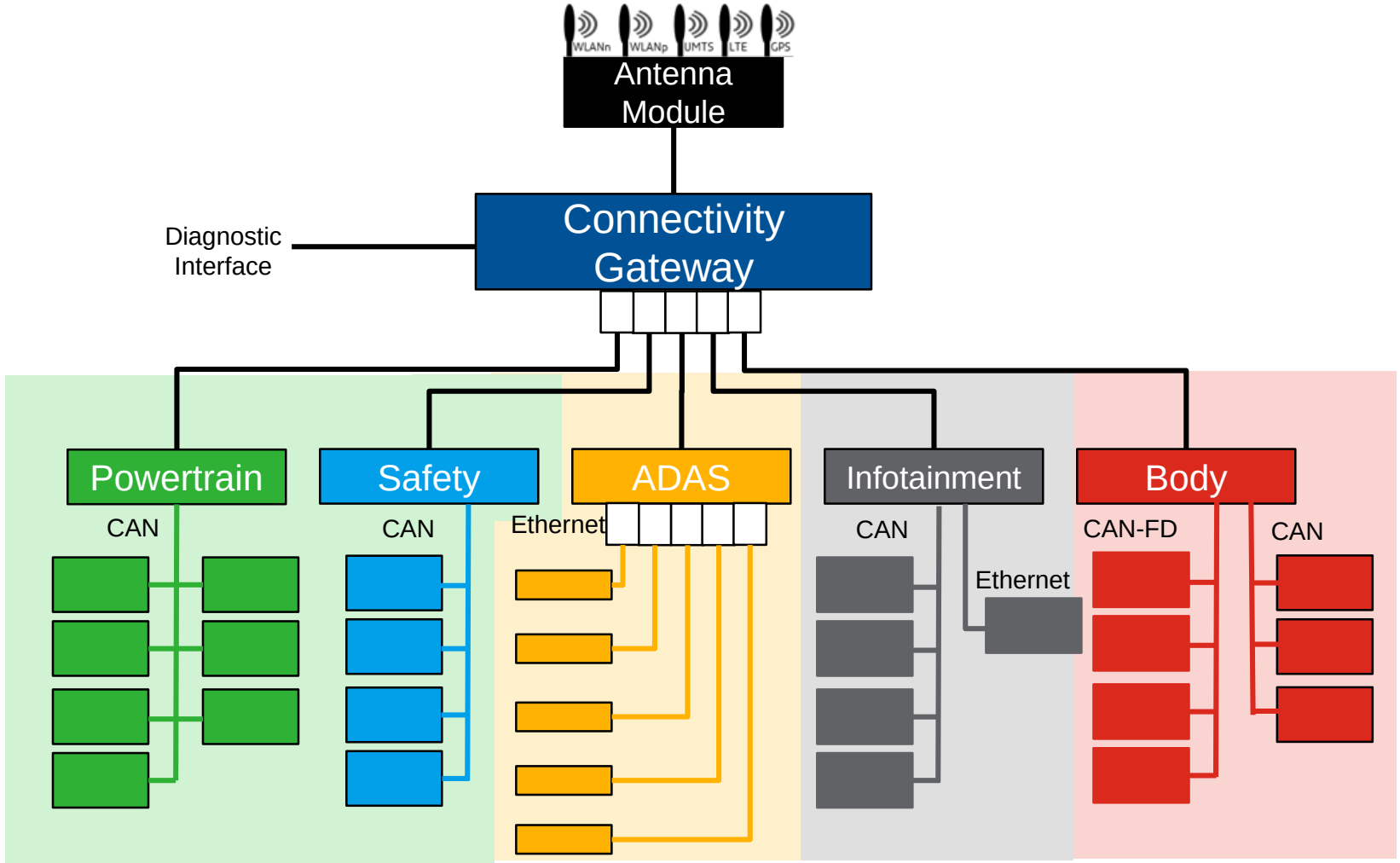
Holistic network security concept consisting of four barriers

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

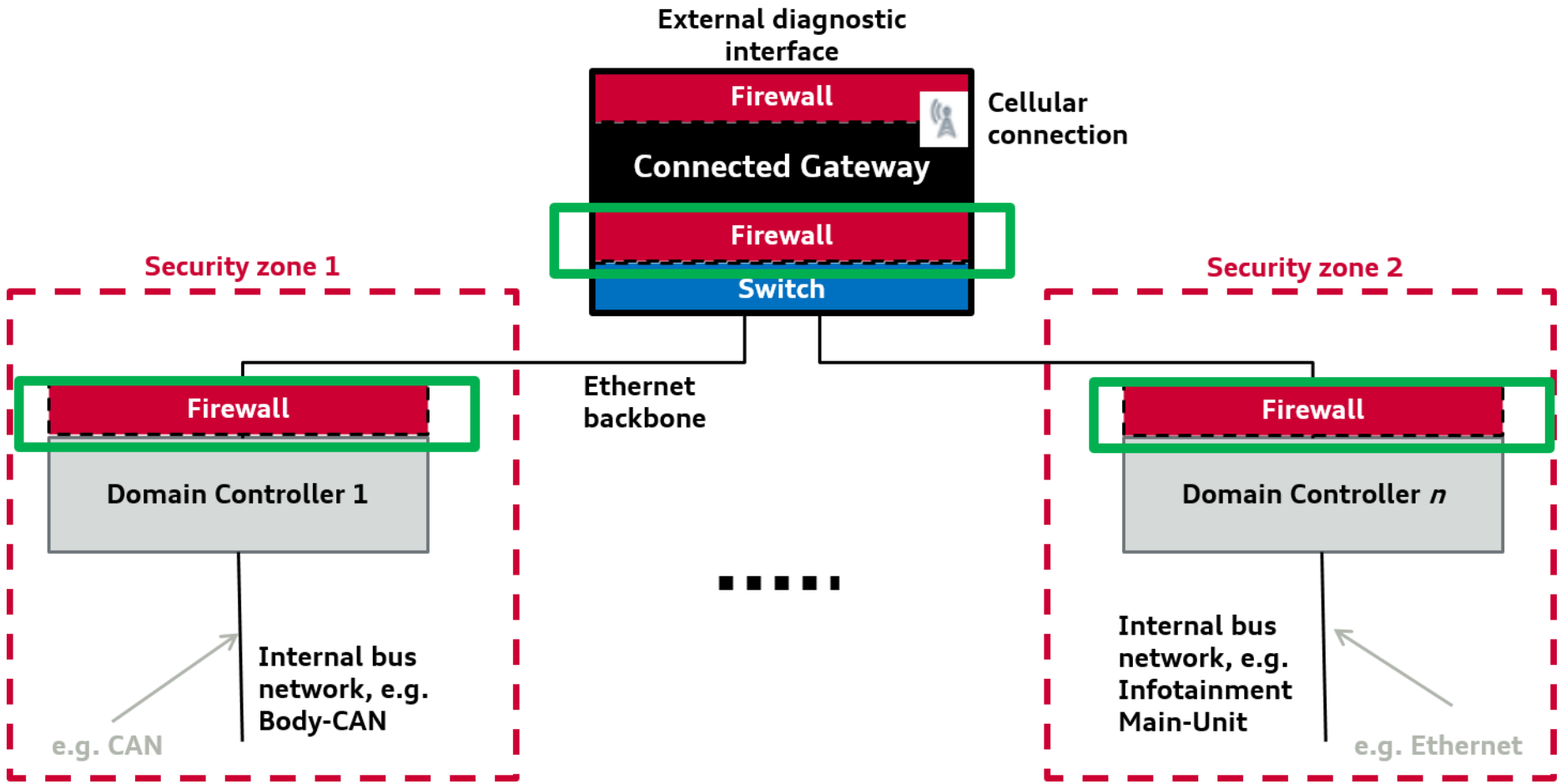
Agenda

Introduction
Concept
Implementation
Results
Outlook

E/E Architecture: Next-Generation Domain Architecture



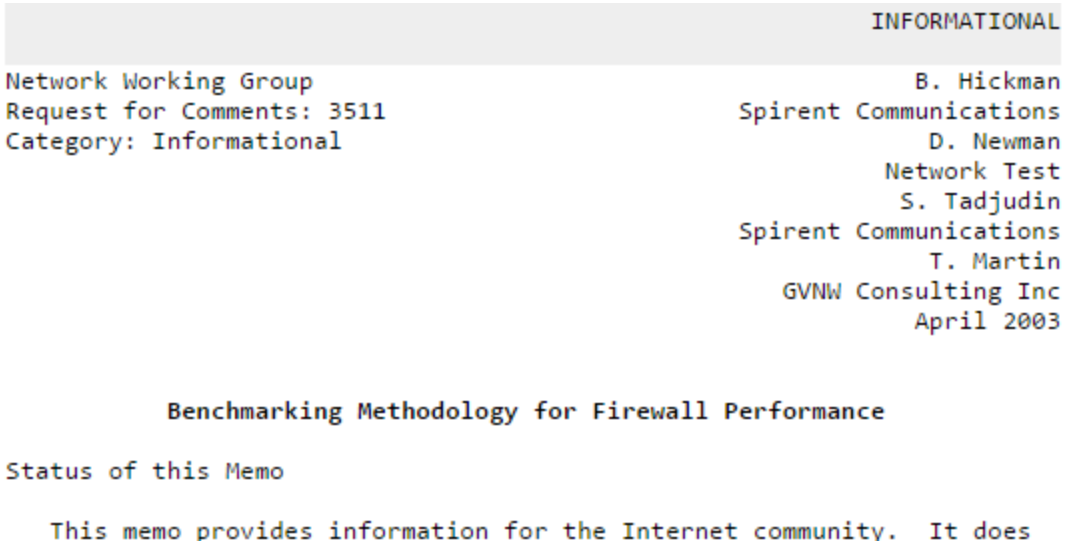
Abstract system model



Concept

Evaluation of firewall performance based on automotive requirements

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



INFORMATIONAL

Network Working Group
Request for Comments: 3511
Category: Informational

B. Hickman
Spirent Communications
D. Newman
Network Test
S. Tadjudin
Spirent Communications
T. Martin
GVNW Consulting Inc
April 2003

Benchmarking Methodology for Firewall Performance

Status of this Memo

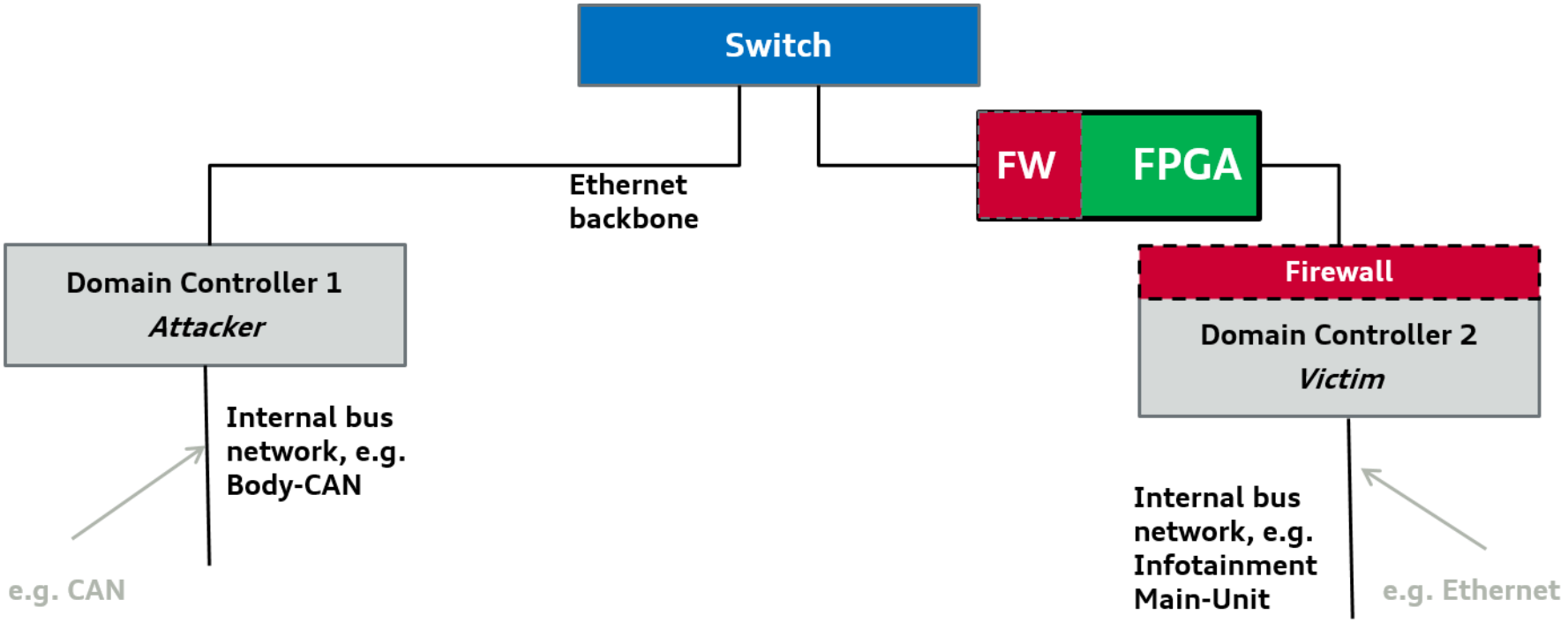
This memo provides information for the Internet community. It does

Latency and throughput requirements in in-vehicle networks

Traffic Type	Throughput	Max. End-to-End Delay [ms]
Control Data	1.6 - 16 kbit/s	≤ 10
Driver Assistance Camera Data	25.1 Mbit/s	≤ 45
Multimedia Audio Data	1.4 Mbit/s	≤ 150
Multimedia Video Data	11.8 Mbit/s	≤ 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

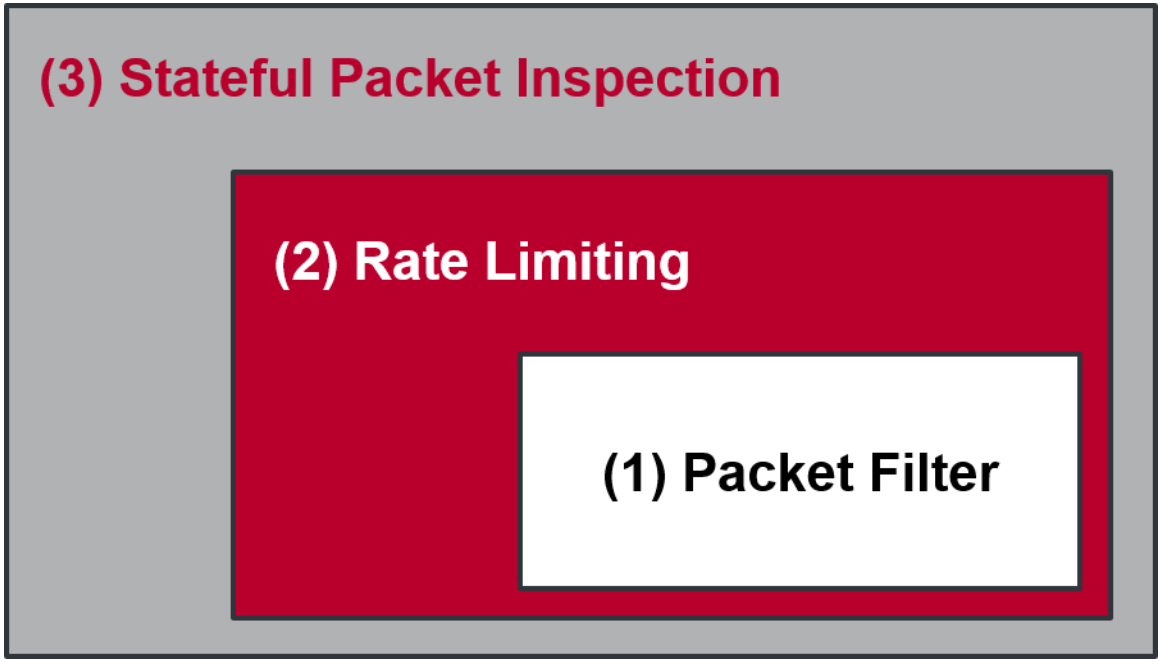
Experimental setup



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			

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

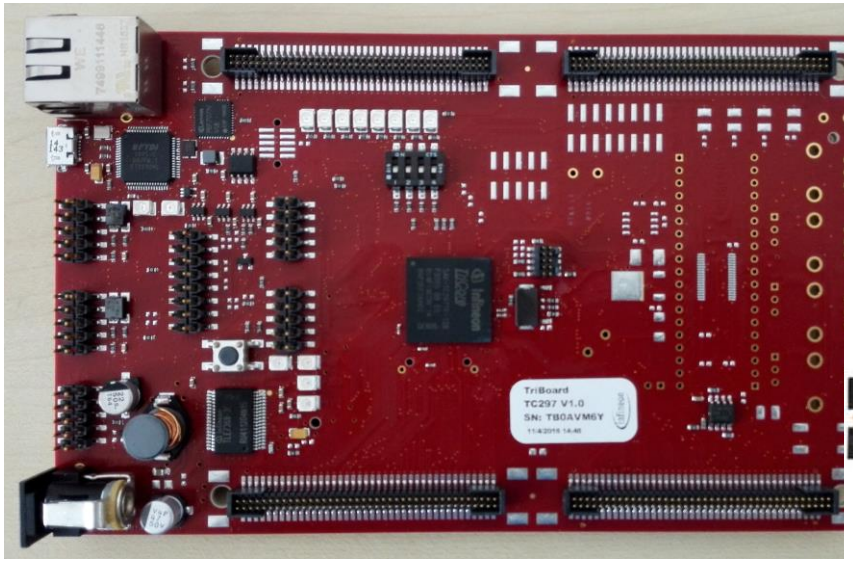
Snoop the content of traffic on the network to extract information

Source: Broadcom

Agenda

Introduction
Concept
Implementation
Results
Outlook

Implementation



Infineon AURIX TriCore TC297-TF

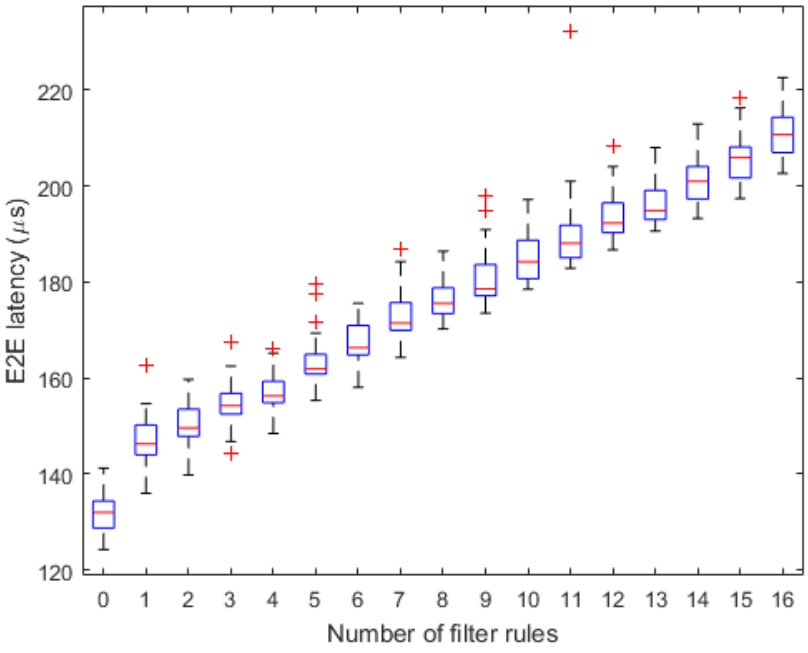
Altera Cyclone V SoC Development Kit

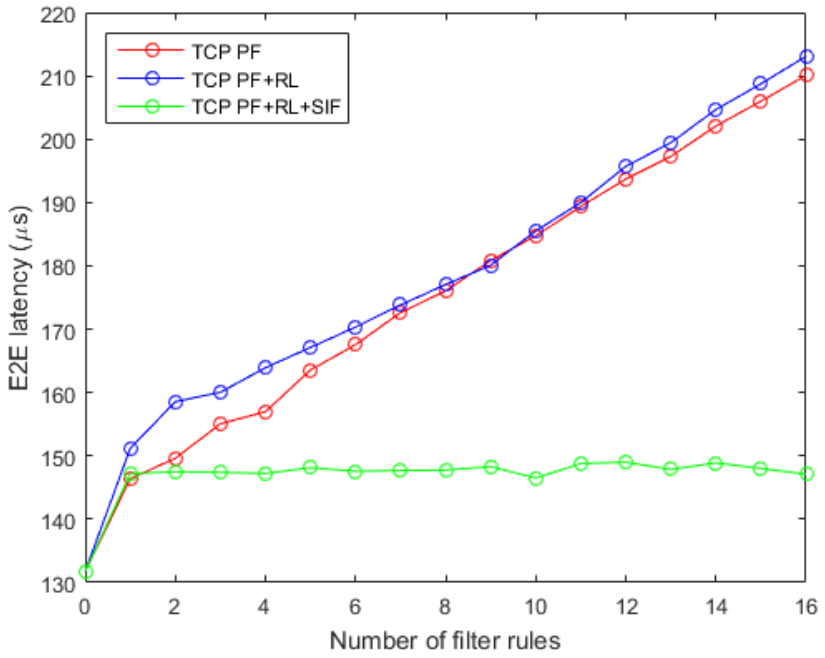
Agenda

Introduction
Concept
Implementation
Results
Outlook

Results

E2E latency MCU

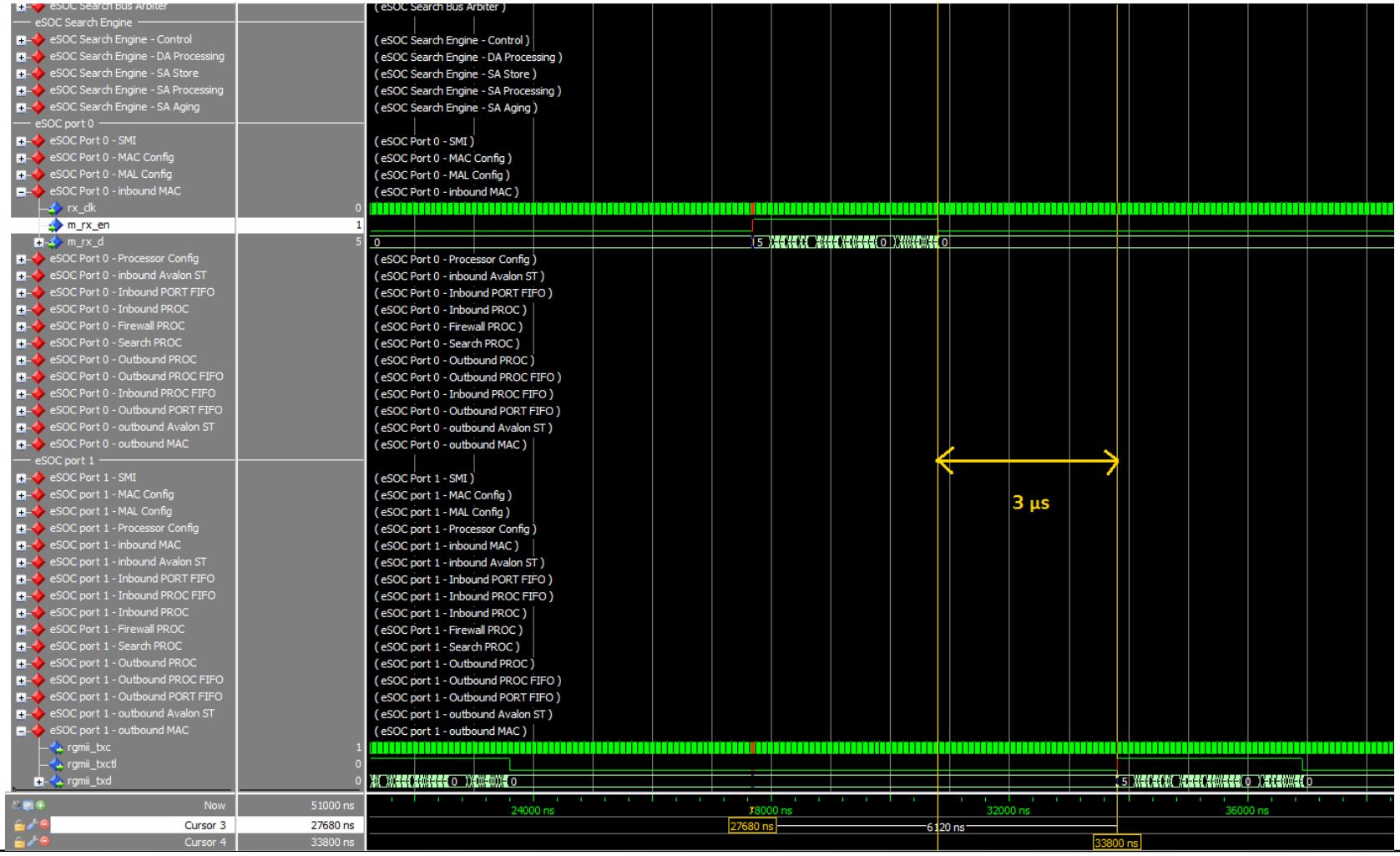




500 rules: 2.3 ms → 2.2 ms overhead

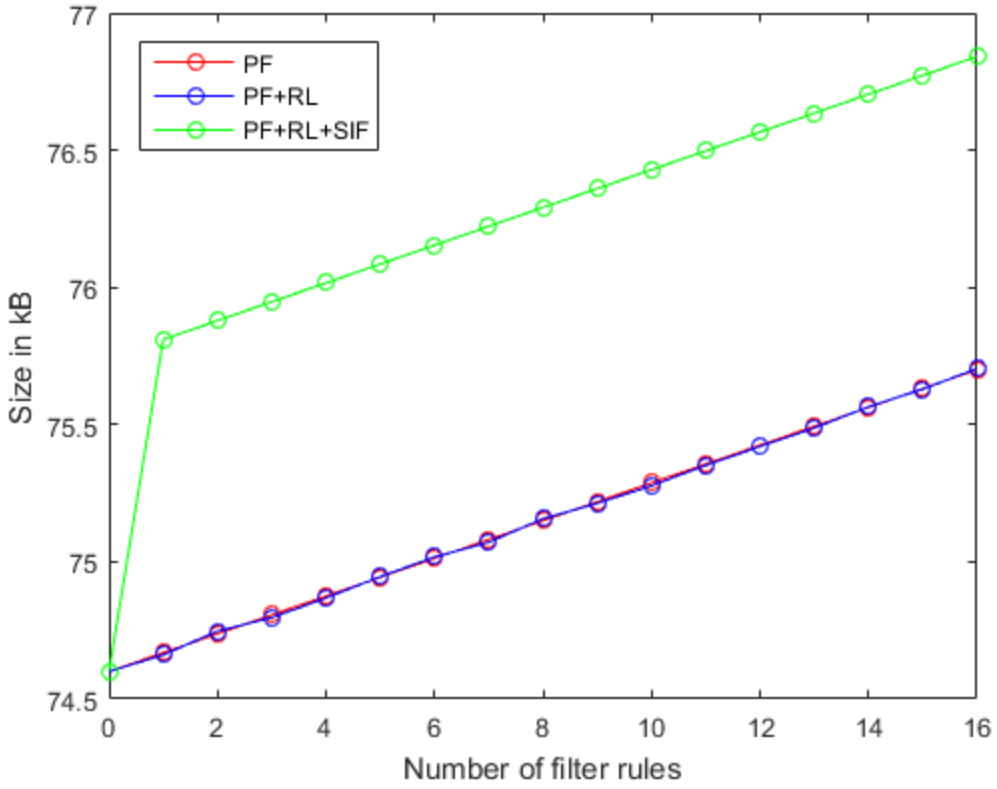
Results

E2E latency FPGA



Results

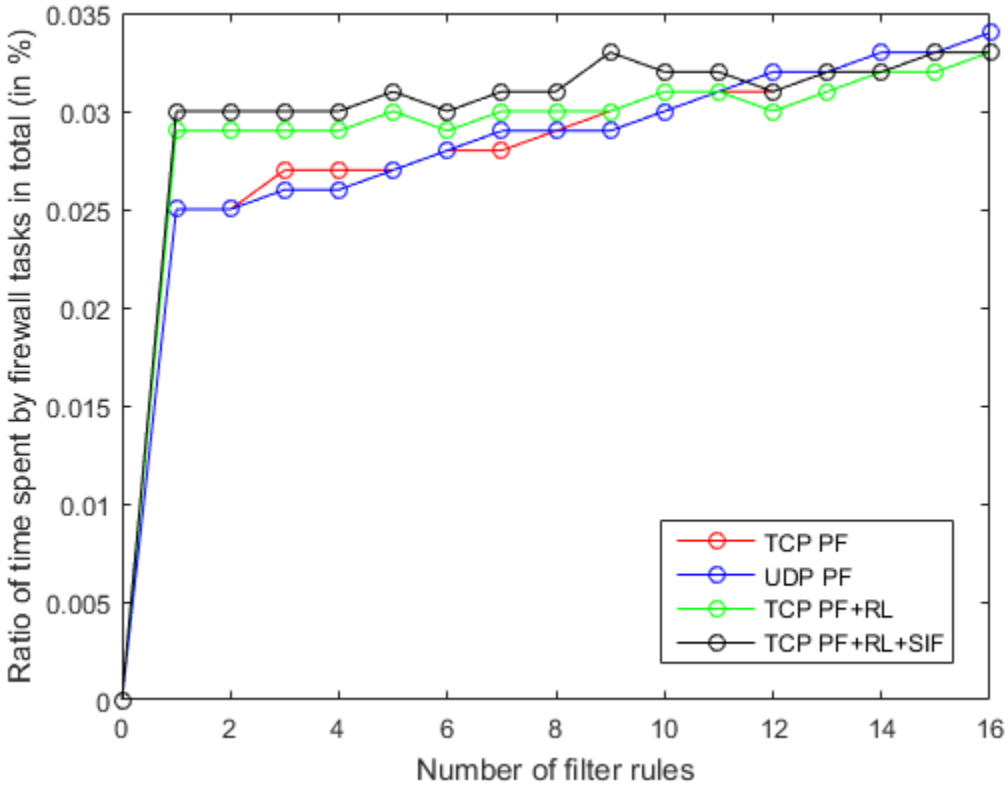
RAM consumption MCU



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