Security areas and modular IDPS

architecture design elements protecting Automotive Ethernet Networks

2019 IEEE-SA Ethernet & IP @ Automotive Technology Day – Detroit

Dr. Georg Gaderer & Dr. Michael Ziehensack, Elektrobit

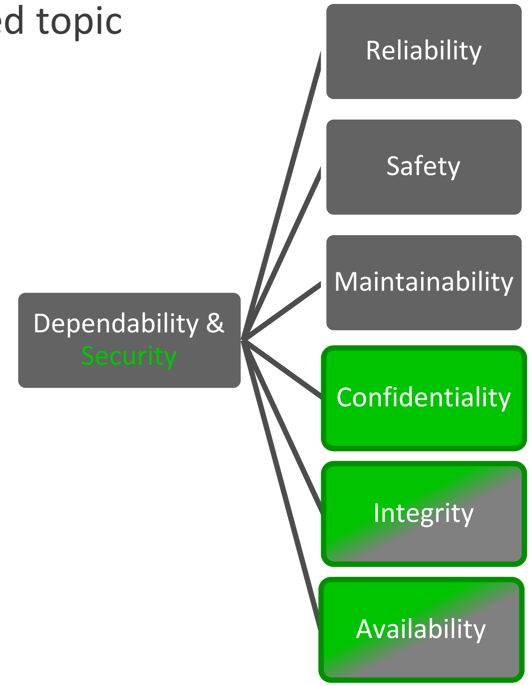
Elektrobit

Motivation

- Classical Dependability is a well known and throughout the automotive industry well mastered topic

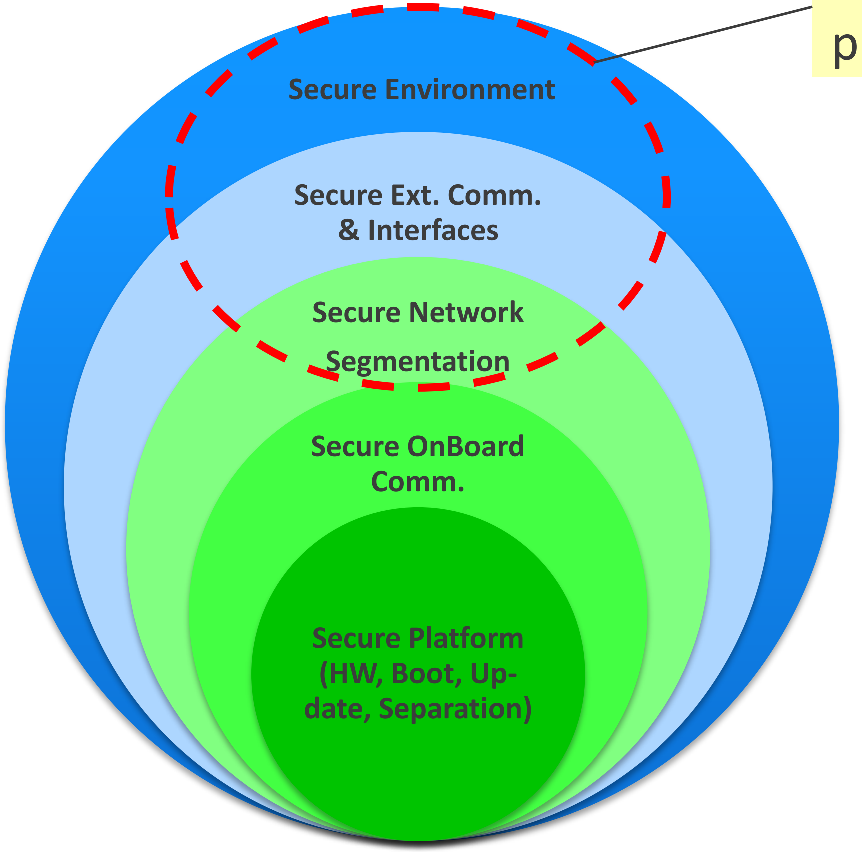
- Nowadays we see several needs raising
  - Rasing data-rate of communication (CAN, LIN, FR vs. GBit Ethernet)
  - Raising computing effort (simple logic vs. High Performance, multicore computing)
  - Raising complexity (window control vs. Piloted driving)
  - Rase of connectivity to outside world (simple OBD connector vs. Update over the air)

This increases the focus on security, yet strengthening the safety aspect (Integrity, Availability)



Protecting Automotive Ethernet Networks

Automotive System Security Layers



focus of presentation

Multi-Level Communication Security Architecture

Level 1: restrict access to the network

Level 2: secure onboard communication

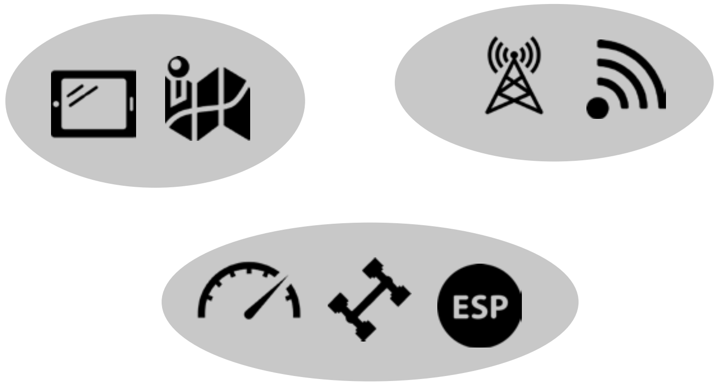
Level 3: apply data usage policies

Level 4: detect anomalies and defend

Security Areas

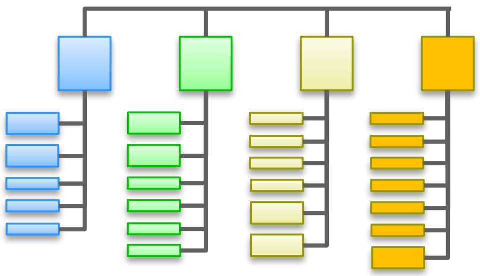
What to separate?

- **Vehicle Functions according to criticality and trust level** grouped in security areas
- For example,
  - security area with highly critical functions (breaking, steering, …)
  - security areas with HMI functions …
  - security area with functions that contain external interfaces (mobile connection, remote key, WLAN, V2G, …)

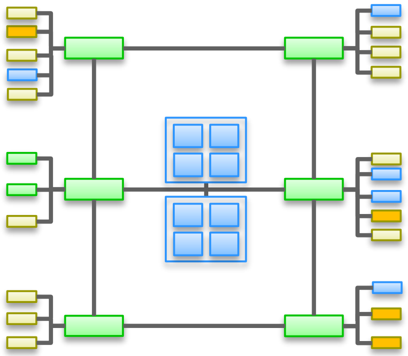


How to separate?

- **Physical**: Domain E/E Architecture (physical)
- **Logical**: VLANs, IP Subnets for new E2E architectures with mixed topology (e.g., centralized architecture with no physical separation or zonal E/E arch.)



Domain E/E Architecture
(physical separation via domains)



Zonal E/E Architecture
(logic separation required)

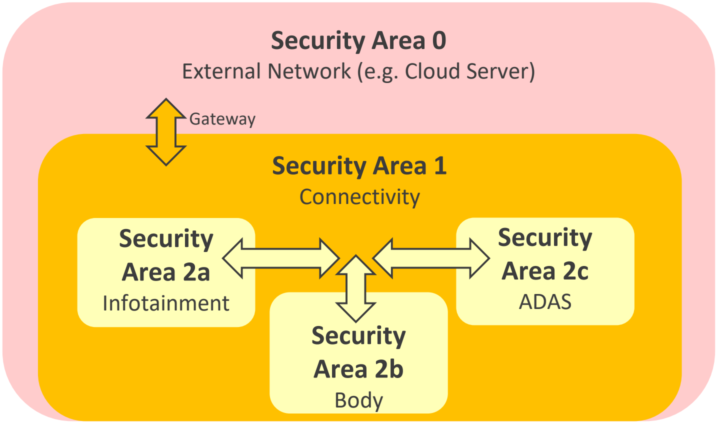
- **Gateways:** Traffic between the security areas is only possible between adjacent areas via a gateway

Security Areas

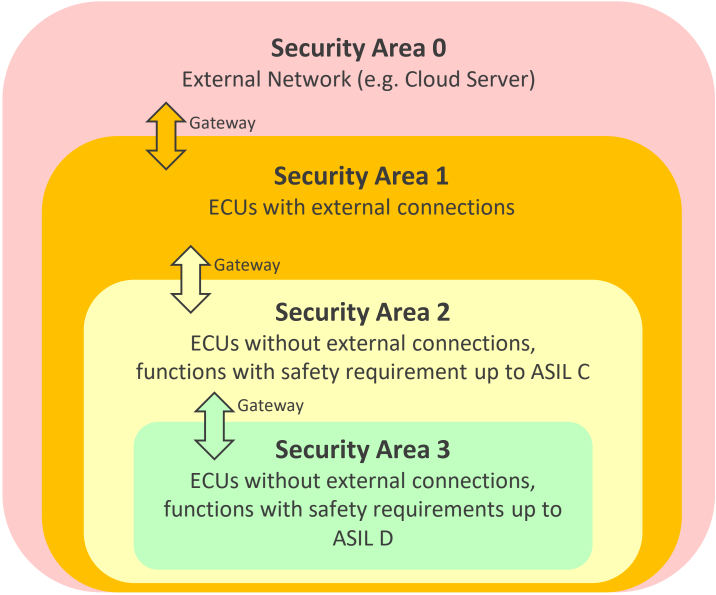
Level of Separation?

- **Goal**: increase the number of borders to cross between security areas
  - Like an onion skin, the **security areas are nested into each other**, with the innermost security area offering the highest level of protection, e.g., a frame from the cloud must never reach a breaking ECU directly.
  - End nodes can only be part of a single security area.

- **Gateways** (Security Area Crossings)
  - Communication between areas only via dedicated gateways such as, **VLAN Bridges, IP routers, Application Level Gateways**
  - Dedicated gateways shall provide a **Firewall with deep packet inspection** (e.g., check of VLAN, MAC/IP-addresses, port numbers, L5+ protocol type, …)



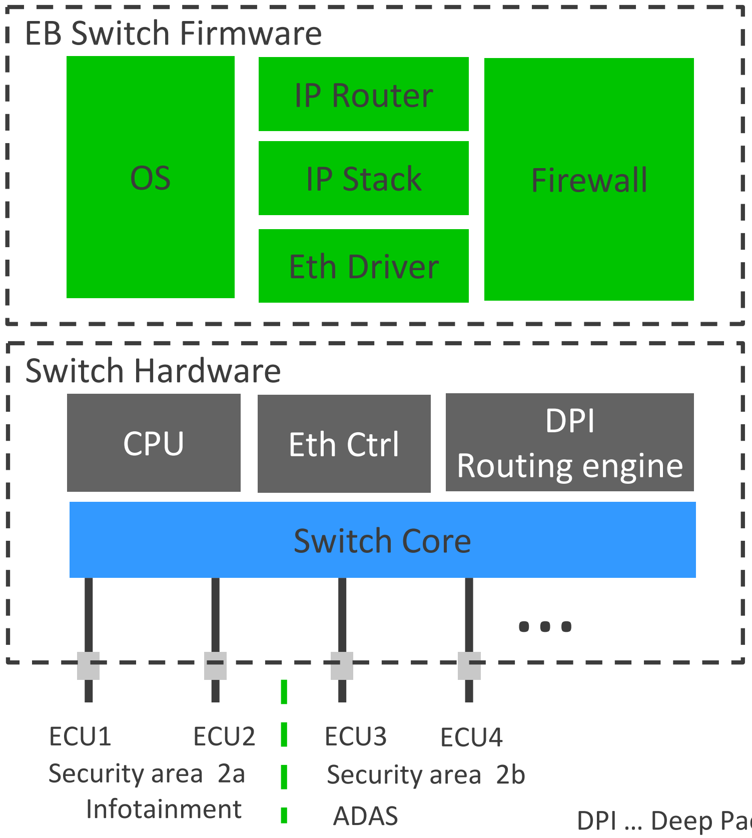
Variant A:
- Separation based on domains
- no hierarchy beside external connection
- Max. 2 borders
- Comparison with IT:
  Sec Area 0 = public network
  Sec Area 1 = DMZ
  Sec Area 2 = private network



Variant B:
- Separation based on criticality
- multiple hierarchy levels
- Max. 3 borders

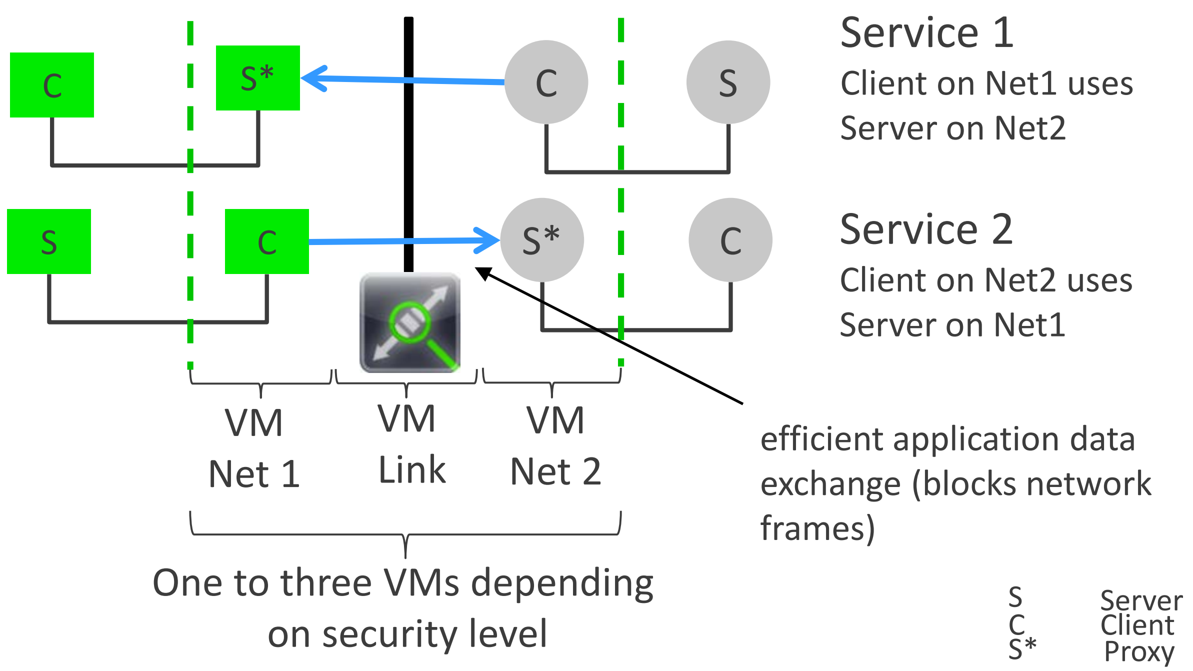
Example for a Security Area Crossing

IP Router with Firewall



DPI … Deep Packet Inspection

Service Proxy (application level gateway)



Intrusion dedection and prevention System (IDPS)

Intrusion Detection

Traffic Monitoring
- Location: Host
- Layer: Application

IP Security Events
- Location: Host
- Layer: UDP/TCPI

IP Traffic
- Location: Host, Switch, Firewall, Router
- On demand mirroring

IP Statistics
- Location: Host, Router
- Layer: IP

Port Statistics
- Location: Switch
- Layer: MAC, Phy

Network Stack

Data

TCP/UDP Header | TCP/UDP Header

IP Header | IP Data

Frame Header | Frame Data

Intrusion prevention

Plausibilisatoin in Application
- Location: Host
- Layer: context aware Application

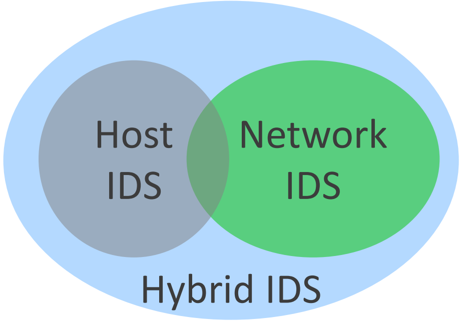
Firewall, stateful firewall
- Location: Host
- Layer: UDP/TCP

IP Traffic limitation, whitelists
- Location: Host, Switch, Firewall, Router
- Layer: all, network setup

VLANs, Port Whitelists
- Location: Host, Router
- Layer: IP

Port Checking, VLANs
- Location: Switch
- Layer: MAC, Switch Config

IDS types



	Host IDS	Network IDS	Hybrid IDS
Analyzes	• internals of a computing system and • Host network interfaces on a ingress packet level	• Packets in the network to detect suspicous activities • Can be on a packet or packet statistics level	• Both, Host based sensor data and network sensor data
Pros	One can instrument on every layer • Can monitor encrypted communication if directed to the host	• Independent from target system	• Combination of both principles • Higher coverage
Cons	• Depends on protocol stack of the host • Cannot detect anomalies in t he whole network	• A full coverage would require mirroring of all packets • Unefficient, thus usually not done • Cannot monitor encrypted packets	• Needs a management and data collection system (IDPS Vehicle Controller)

Elektrobit

Attack Patterns and detection mechanisms

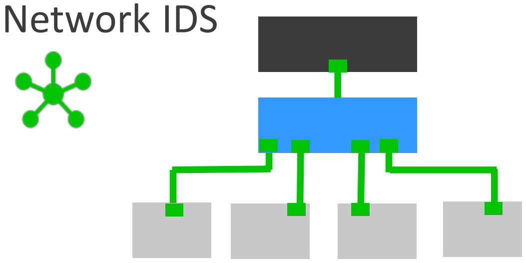
Attack Pattern	Host IDS	Network IDS	Hybrid IDS
Port Scan from one host	Most cases detectable	Difficult to detect but possible	Additional data from Network IDS may improve Host IDS
Distributed port scan	Difficult to detect	Many cases detectable	Additional data from Host IDS may improve Network IDS
Buffer overflow attack	Many techniques for detection exist	undetectable	Same as Host IDS
Denial of service attack (non distributed)	Detectable	Detectable and easy to isolate	Additional Data from Host IDS may improve Network IDS
Denial of service attack (distributed, e.g., gateway)	Detectable, difficult to isolate	Difficult to detect	Detectable, difficult to isolate
Man in the middle	Difficult to detect	May be detected	May be detected

IDS Sensor Examples

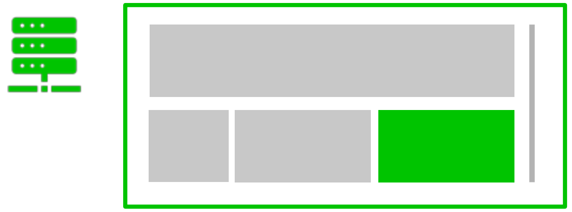
Where, what and How

Location	Data	Type*	Implementation	Remark
Network IDS (Switch)	Port Statistics	(M)	Traffic statistics per port	Hardware supported ingress sampling needed
Host IDS (Host Ethernet Interface, Switch firmware, router)	IP Statistics	(M)	Table statistics per flow (Layer 4) Sampling of configuration interface data	Hardware supported ingress sampling needed
Network IDS(Switch, Switch Firmware, Router)	IP Traffic duplication	(D)	Duplicate matching packets acc. To a filter	Layer 2 filtering support needed
Host IDS (Host Ethernet Interface, Firewall)	IP security Events	(D)	Forward dropped frames (or metadata)	e.g., frames out of spec (comm. Matrix)

Network IDS



Host IDS



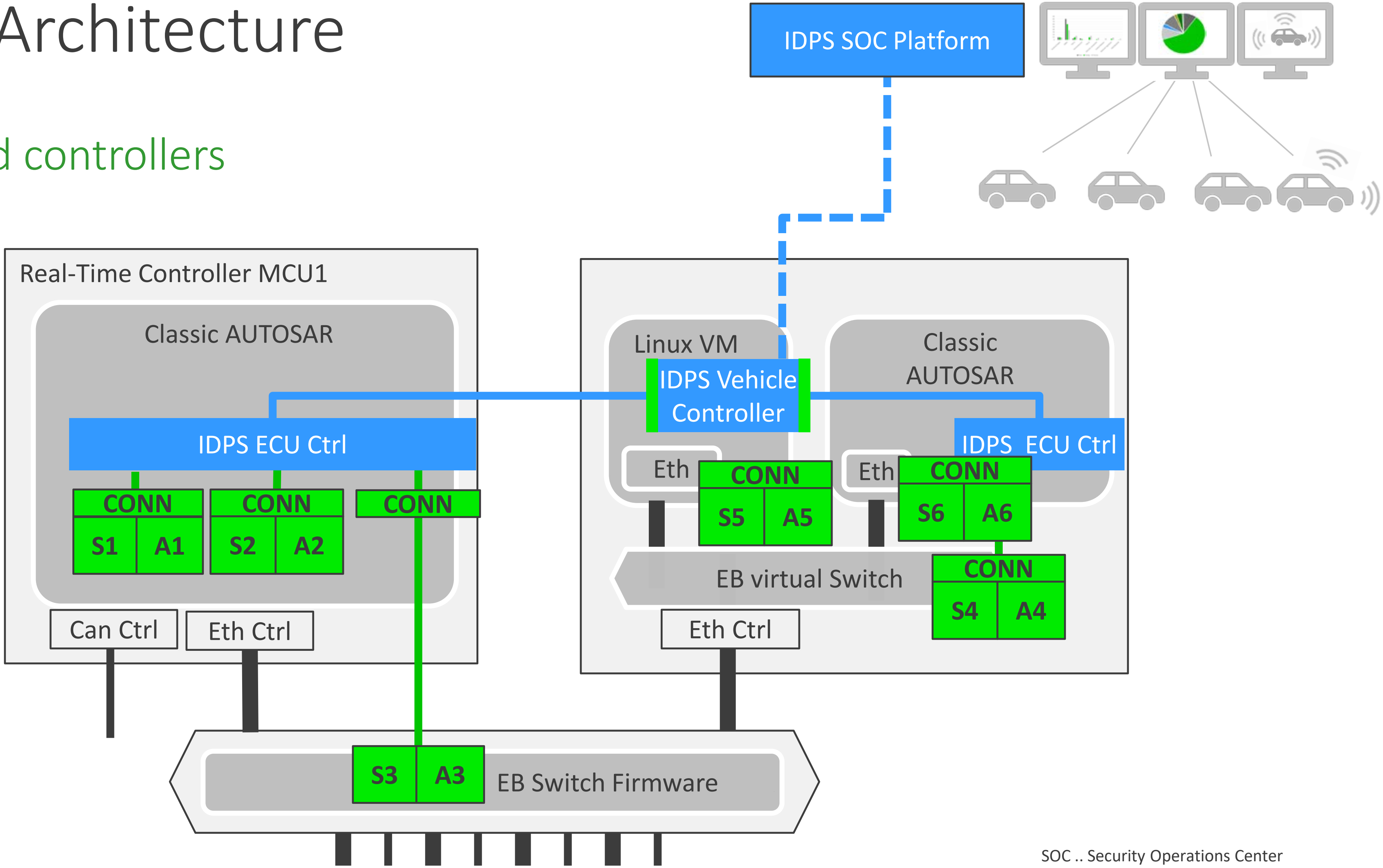
*Sensor Type:
- (M)etadata (Port, protocol statistics)
- (D)eep Packet Inspection (Frame by frame inspection, flow analysis)

Elektrobit

Modular IDPS Architecture

Sensors, actuators and controllers

- Sensors and actuators are usually paired
- Each sensor/actuator needs unified interface (CONN)
- Sensors and actuators for VM internal parts are not shown
- SOC* Platform is connected via gateway
- Controller do an anomaly detection based on sensor data



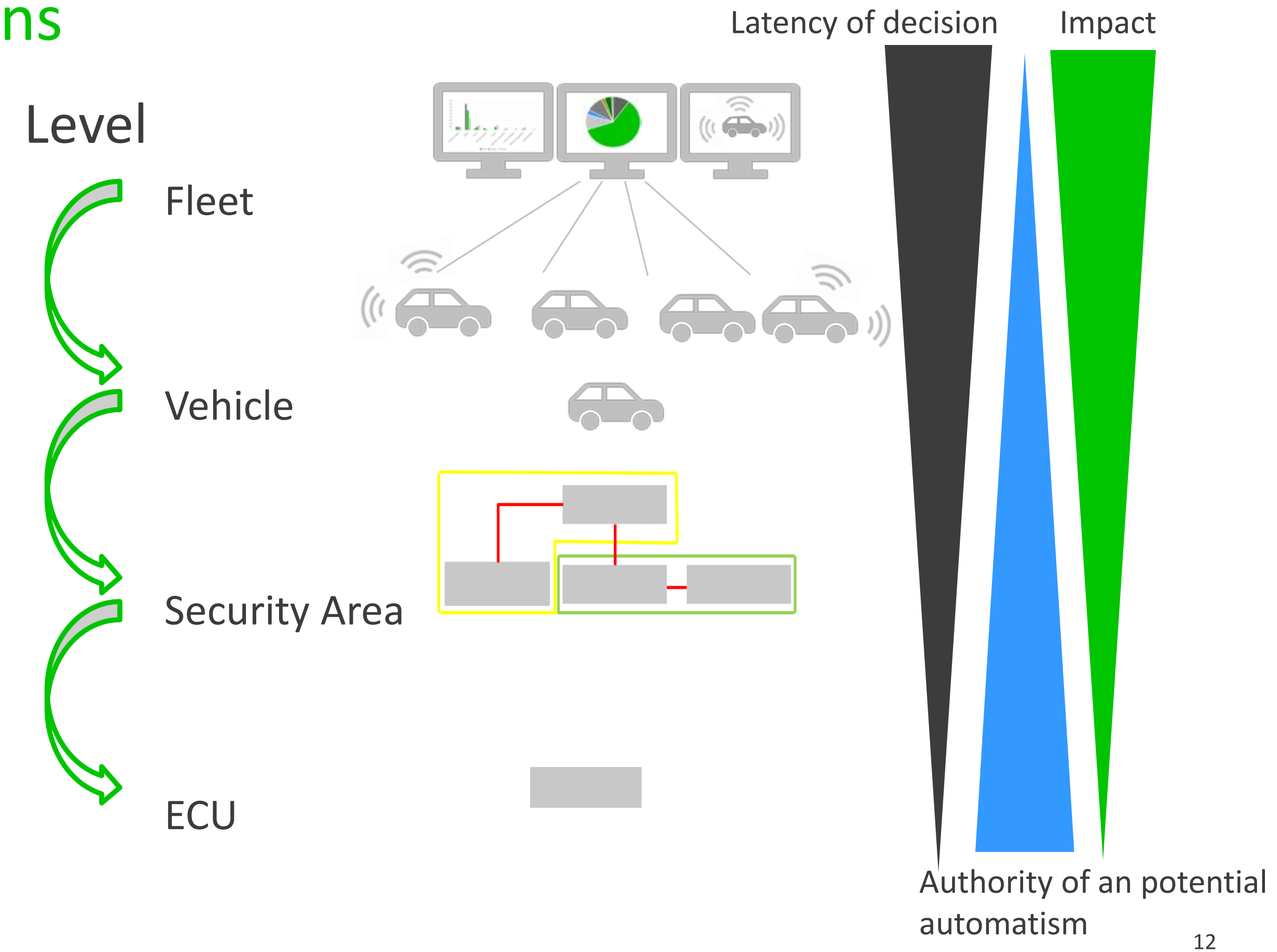
SOC .. Security Operations Center

The Impact-Automatism-Latency tradeoff

Influencing factors of IDSPs reactions

Intrusion detection might end up in extensive decisions. Those are dependent on level

- The Latency of decision: from a certain level on one might want to have human in the loop (e.g., grounding of a whole fleet)
- The Authority of an automatism: on a low level decisions can be taken easier (e.g., discard packets with security violation)
- The Impact: on a higher level decisions influence a bigger portion of the system



Summary

- Protect automotive networks is important, because of safety, legal and commercial requirements
- Security areas have been defined to restrict the attack surface
- Crossing Security areas are limited to gateways with firewalls and deep packet inspection
- EB’s modular IDPS consists of sensors, actuators and controllers for efficient intrusion detection
- Anomaly detection is done on different levels considering latency, automation level and impact

Thank you for your attention!

Author information

Dr. Georg Gaderer, Elektrobit
Senior Manager, Car Infrastructure Software
georg.gaderer@elektrobit.com

Dr. Michael Ziehensack, Elektrobit
VP, Car Infrastructure Software
michael.ziehensack@elektrobit.com

Get in touch!

Elektrobit

sales@elektrobit.com
www.elektrobit.com