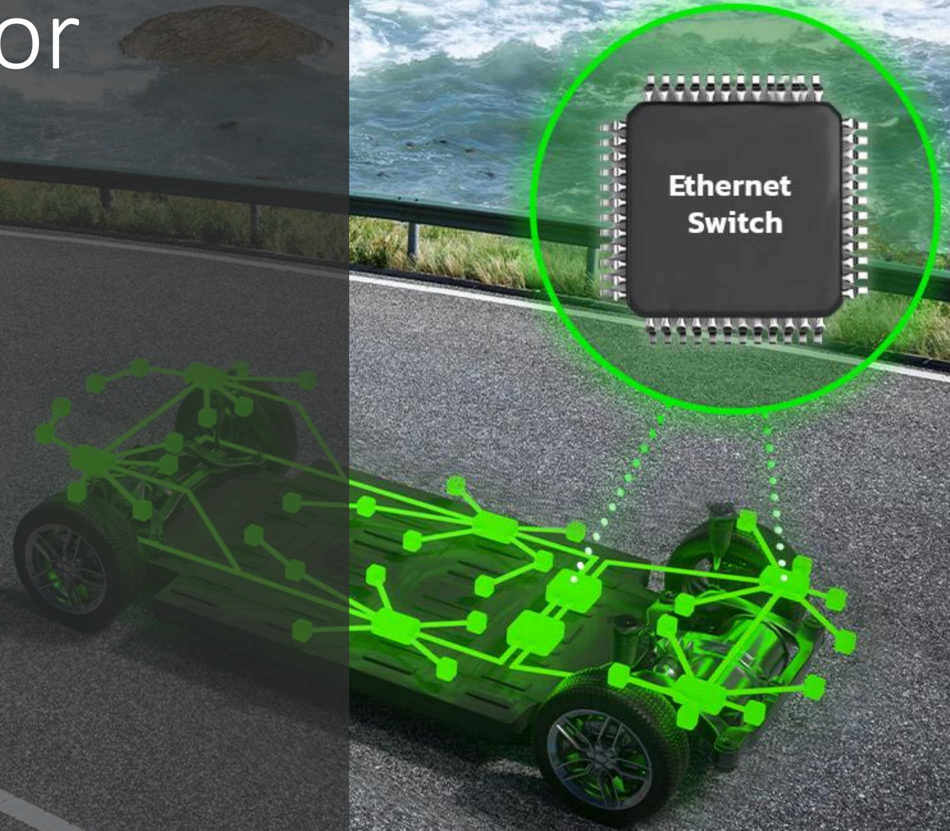
IEEE SA STANDARDS ASSOCIATION

Elektrobit

Optimized Ethernet switch HW/SW collaboration for new E/E architectures



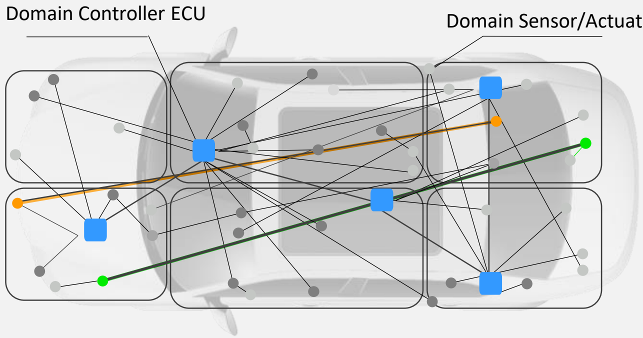
Illia Safiulin

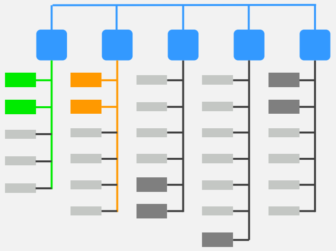
Elektrobit

Moving from domain to zonal architecture

Network demand is ever increasing...

Domain Architecture





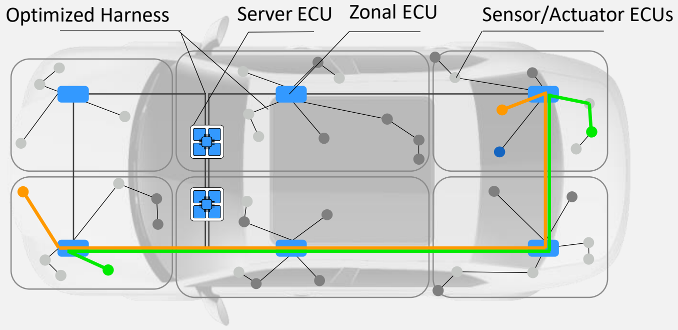
- Physical separated domain networks (CAN, LIN, FR, Ethernet)
- (loosely) coupled via domain controllers acting as network nodes

-> Basically hw-defined network

Reducing harness complexity

- Wire weight savings > 30%
- Wire length savings > 30%

Zonal Architecture



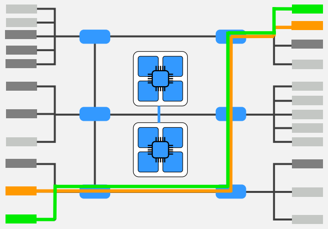
Challenges

- **Increasing network demand**
- **Re-use of HW and SW**
  - „Anything anywhere“ – adding a sensor and use it from any domain
  - „Service Oriented Architecture“ with re-usable services including signals of legacy networks

Advantages

- Cost-efficient functionality updates
- Better re-use of hardware and software
- Increased network reliability

Network Nodes are key components



- Vehicle-wide zonal network (CAN, LIN, Ethernet, PCIe...)
- Highly integrated, cross-domain via zonal ECUs and HPCs acting as network nodes

-> Basically sw-defined network (virtualized network topology)

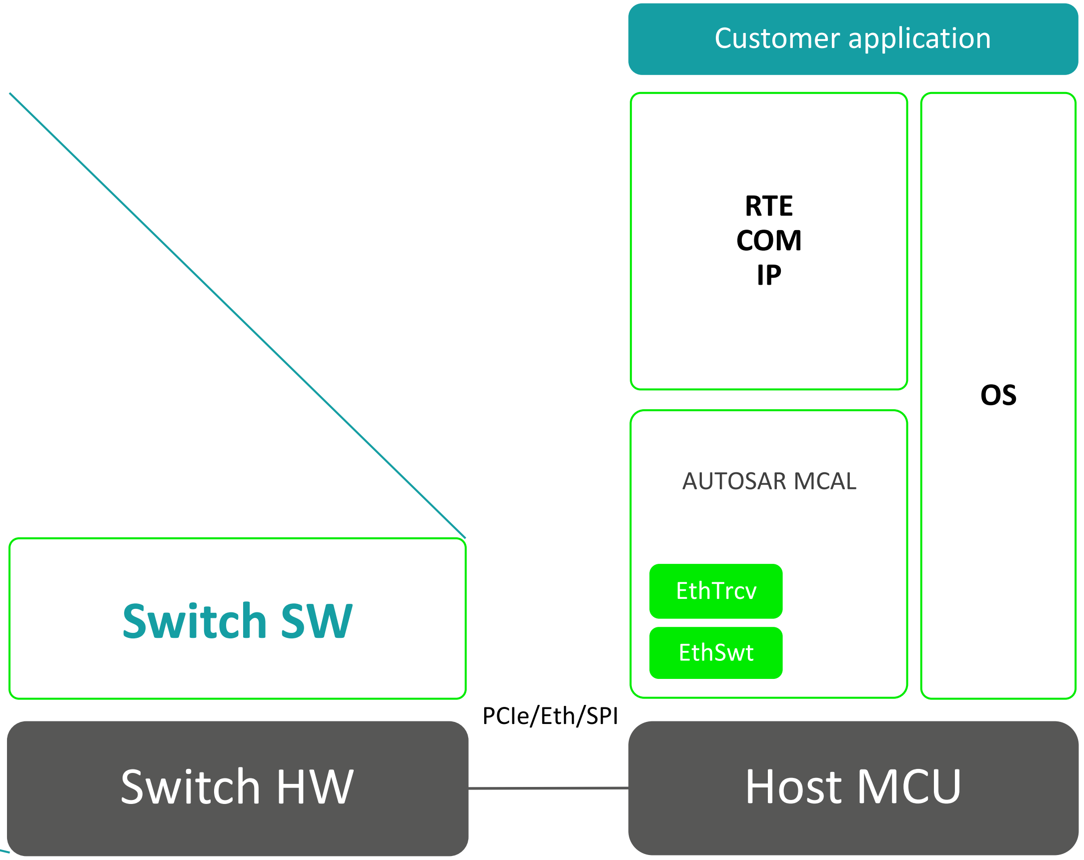
Legend: 🟦 Network node

Importance of the Ethernet switches

From a simple peripheral to an advanced network device

Ethernet switch features for new E/E architecture

- Switch with own CPU system
- TCAM support
- TSN features included
- HSM included
- Health management
- 10Base-T1S
- TC10
- MACsec
- Advanced cyber security



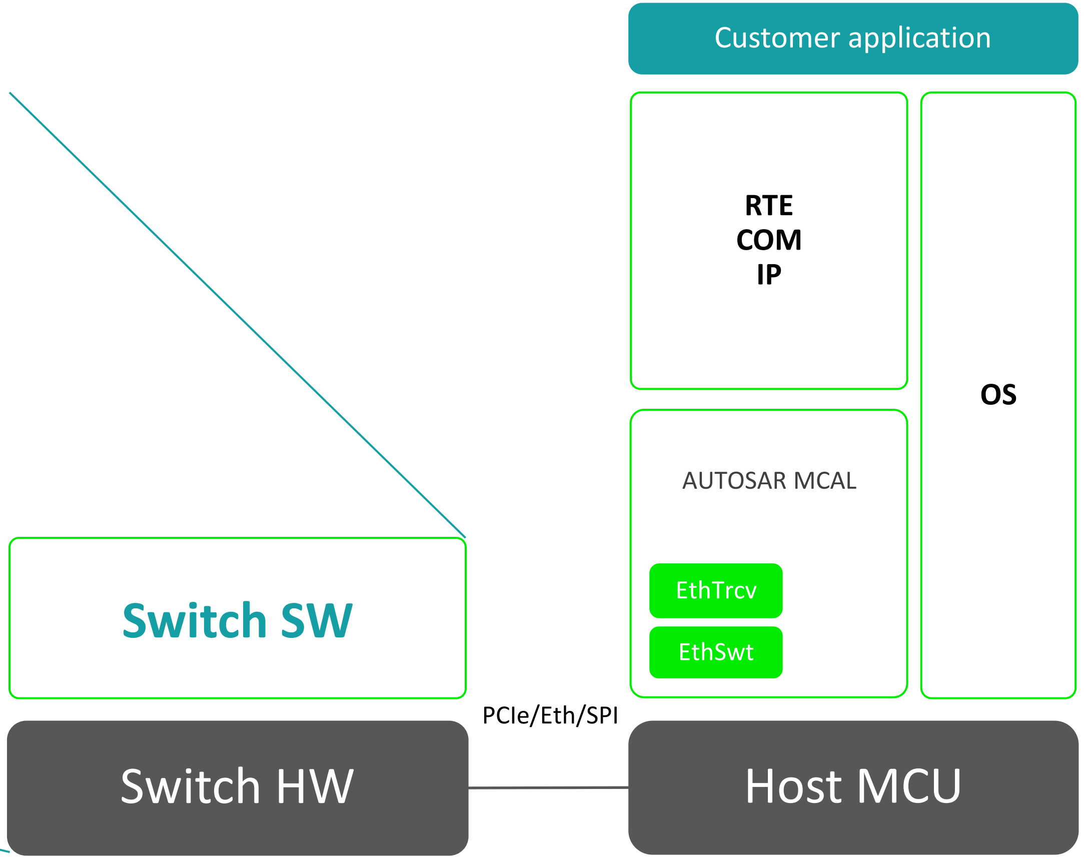
Optimized Ethernet switch HW/SW collaboration

Importance of the Ethernet switches

From a simple peripheral to an advanced network device

Ethernet switch features for new E/E architecture

- Switch with own CPU system
- TCAM support
- TSN features included
- HSM included
- Health management
- 10Base-T1S
- TC10
- MACsec
- Advanced cyber security



Optimized Ethernet switch HW/SW collaboration

What type of SW to use?

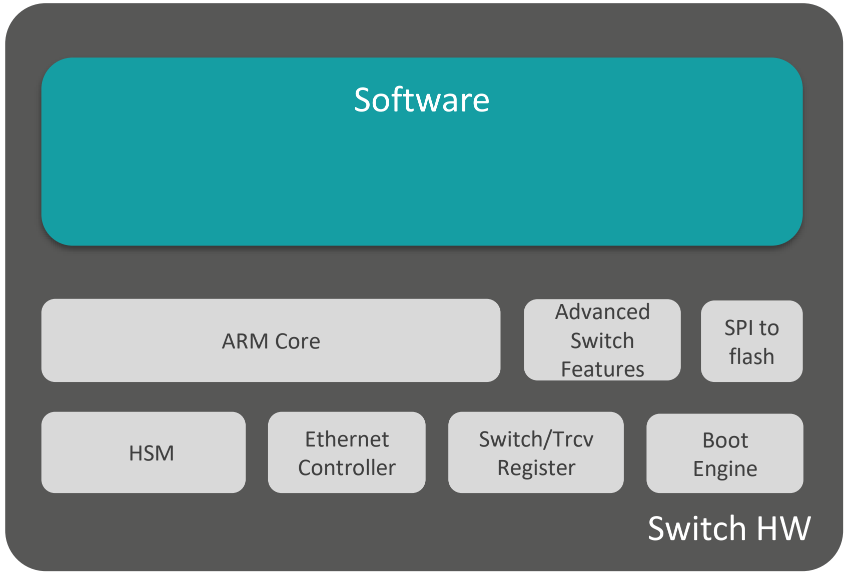
What is under the hood?

Modern switches:

- Number of ports:
  - 4 up to 16 (or more later)
- Speeds:
  - From 10BASE-T1S up to 10GBASE KR, XFI or USXGMII
- Host interface:
  - From SPI up to PCIe Gen3

However:

- CPU
  - From ARM based Real M500 with 333MHz and **816DMIPS**
  - Up to ARM Cortex-R52 with 700MHz and **3000DMIPS**
- Internal Memory
  - instruction-RAM (ITCM) of 256kB
  - **data-RAM (DTCM) from 128kB up to 256kB**



Generic SW vs Optimized SW for switches

What can be used on switches?

Building blocks to create any application
Generic BSW based on AUTOSAR as is

- **Pros**
  - Well established modules, high re-use
  - Known protocols
  - Configuration workflow
- **Cons**
  - HW-specific features are not fully supported
  - SW footprint
  - Configuration and integration efforts for integrators

Pre-integrated for specific use-case
Optimized switch SW compliant to AUTOSAR

- **Pros**
  - Optimized for switch functions
    - Max performance
    - Small SW footprint
    - Pre-integrated
  - Full usage of HW features
- **Cons**
  - SW vendor needs deep HW know-how

General SW vs Optimized SW for switches

Specialized SW can still talk to AUTOSAR

- Our recent research* showed that usage of optimized SW is quite beneficial (performance increase by factor of 100 in IP routing).
  - HW accelerators were used in a combination with distinctive SW for certain tasks
  - And it was in accordance with the standard AUTOSAR workflow

Coming back to the **switches**:

- Update
- Configuration
- Notification

AUTOSAR interfaces and protocols can be used with optimized SW for specific use-cases!

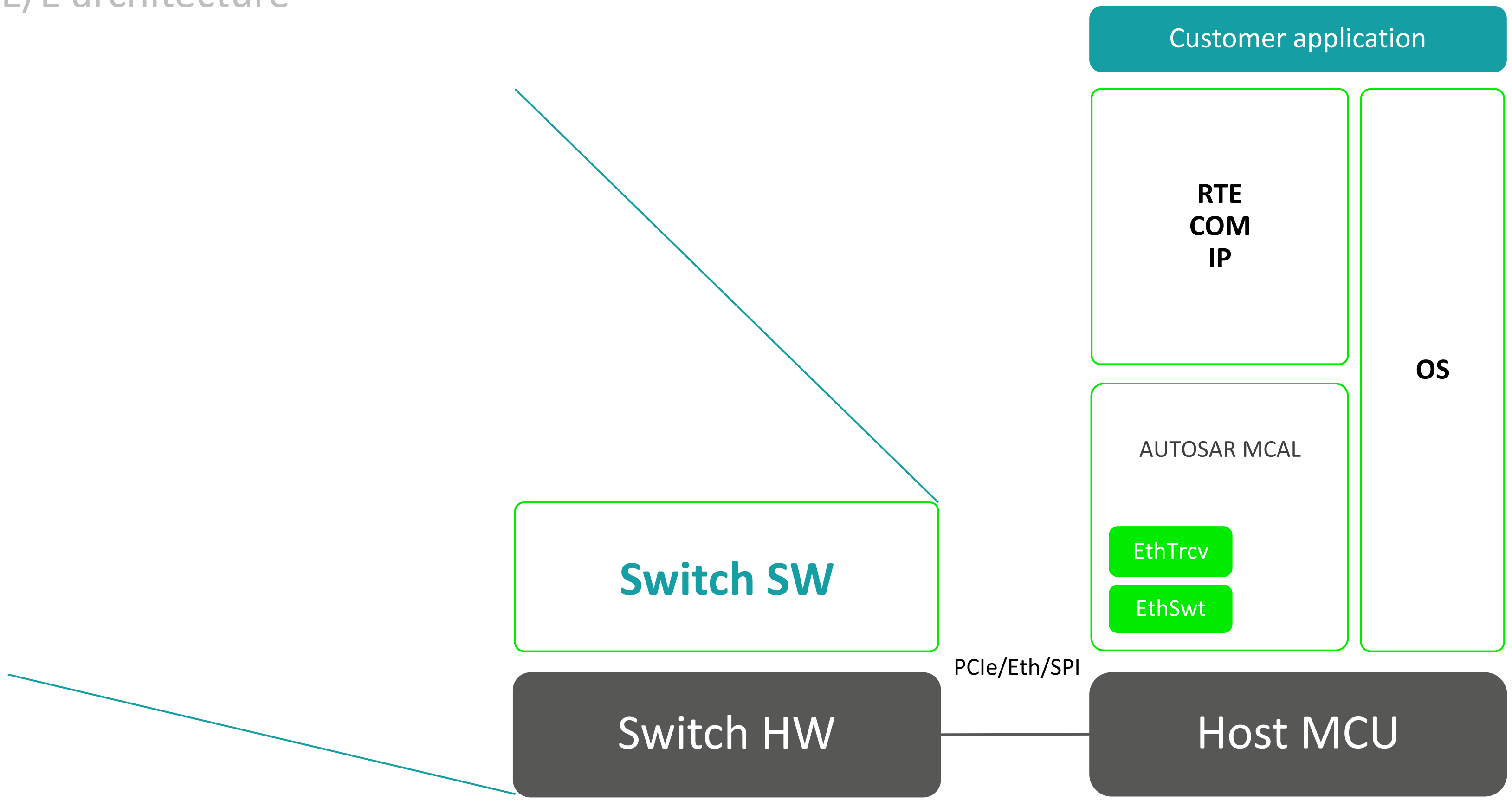
*Symbiosis of hardware and software to cope with IP routing challenges, Automotive Ethernet Congress 2022

Importance of the Ethernet switches

From a simple peripheral to an advanced network device

Ethernet switch features for new E/E architecture

- Switch with own CPU system
- TCAM support
- TSN features included
- HSM included
- **Health management**
- 10Base-T1S
- TC10
- MACsec
- Advanced cyber security



Optimized Ethernet switch HW/SW collaboration

What is health monitoring?

Problem – HW-dependent continuous monitoring of a high number of registers

In some use-cases, the Host MCU is required to retrieve the following information from the automotive Ethernet switches for diagnostic purposes:

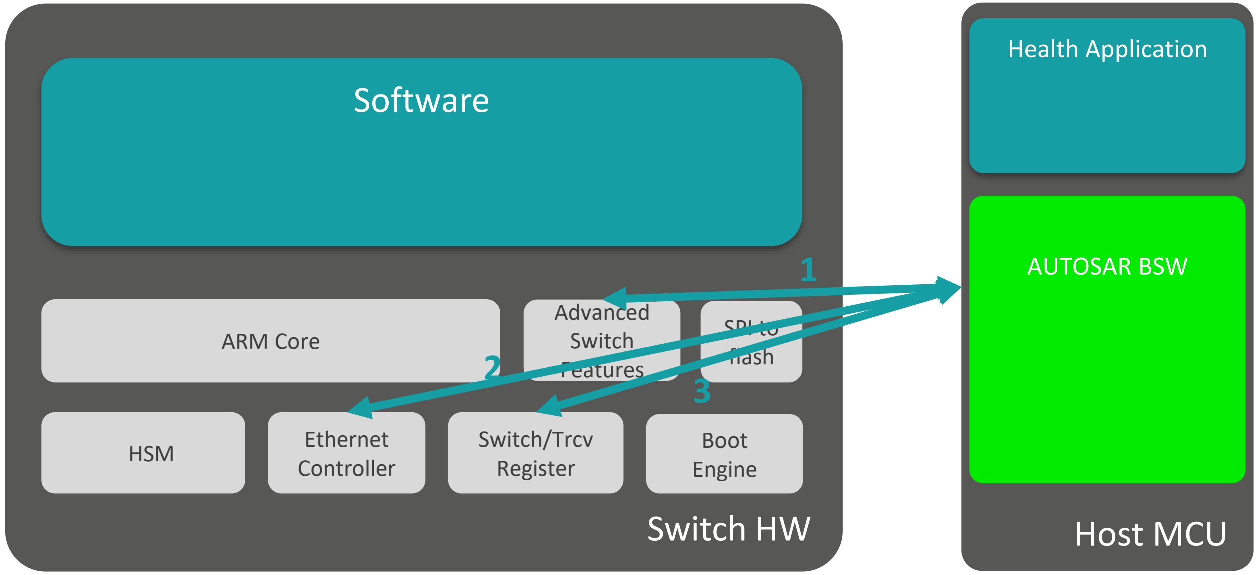
- Link states
- Bandwidth utilization
- Transceiver temperatures

Has to:

- Support remote calls and notifications
- Be reliable and restricted

Currently this operation is:

- Resource and time consuming
- HW-dependent



Link Status:

- 4 register reads per HW port
- application is blocked as the IP stack reads data permanently

Can we do better?

Potential solution: do it from switch and use AUTOSAR services for notification

To significantly offload the MCUs both in terms of runtime overhead and required bandwidth for communication with the switch hardware, this task is done **on the switch** and only notifies the MCU about the results/changes.

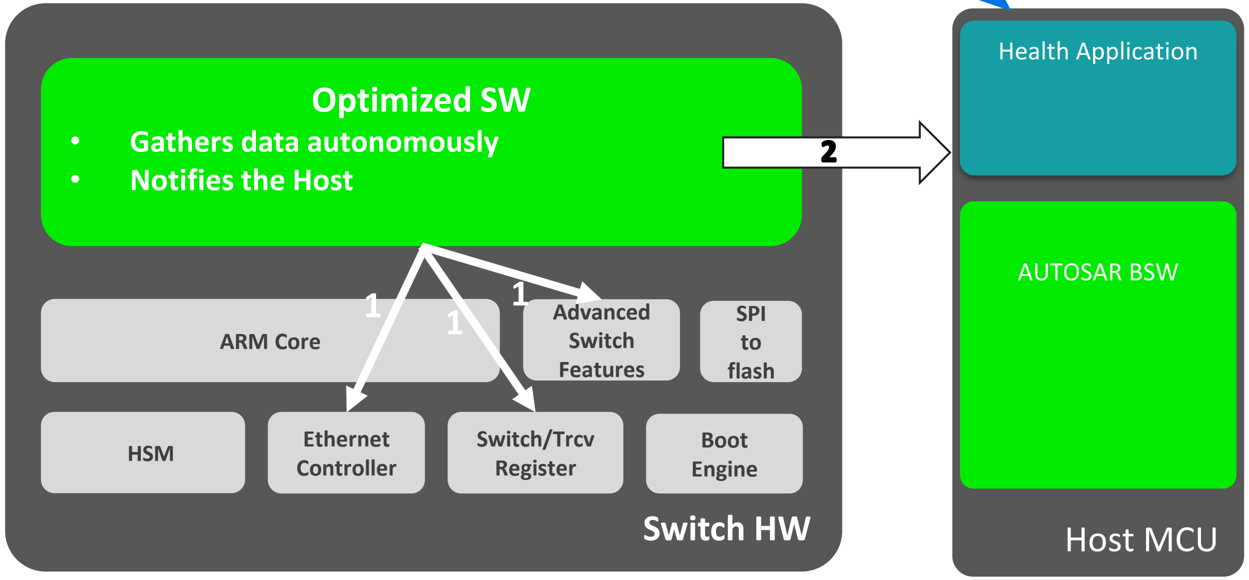
How to get? -> special HW-aware SW running on the switch

How to provide? -> over TCP/IP. TCP/IP is a very well-known, reliable and established protocol, that can take care of handling of frame loss.

How to protect? -> restrict resources for a single client, IP address and TCP client port number.

Applicable for Classic AND Adaptive AUTOSAR!

Don't micromanage – **delegate**

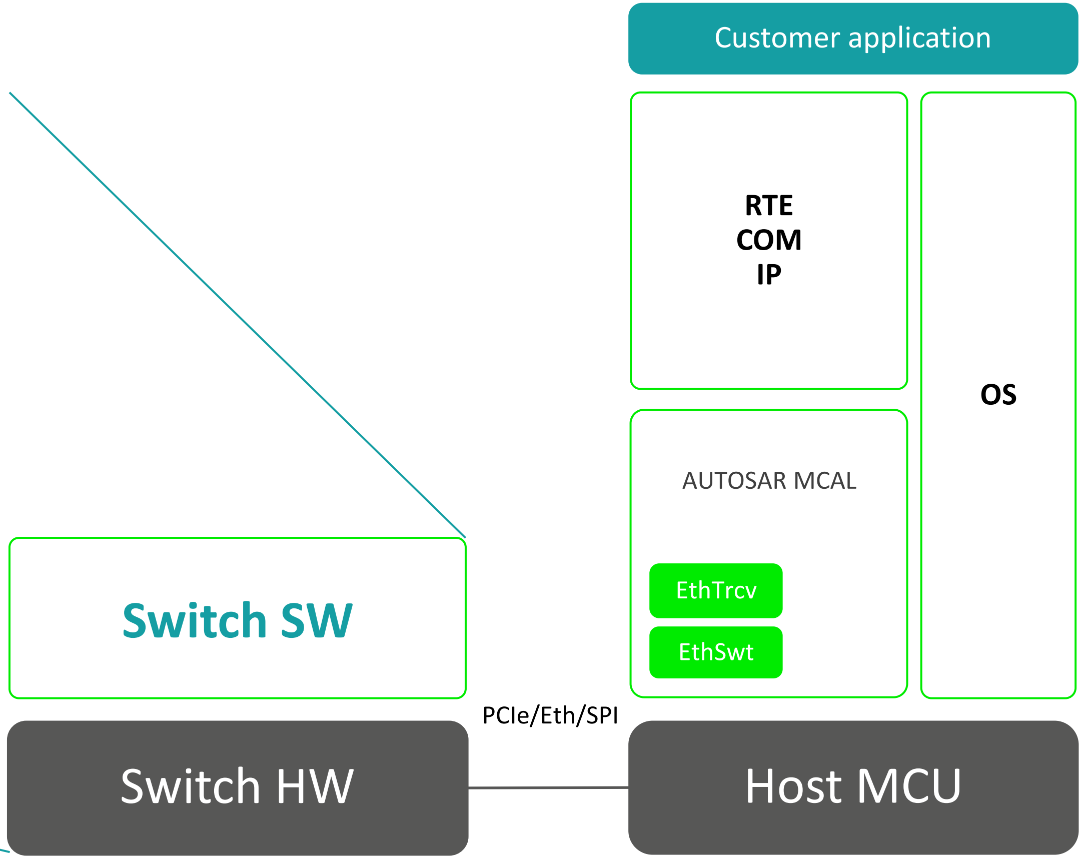


Importance of the Ethernet switches

From a simple peripheral to an advanced network device

Ethernet switch features for new E/E architecture

- Switch with own CPU system
- TCAM support
- TSN features included
- HSM included
- Health management
- 10Base-T1S
- TC10
- **MACsec**
- Advanced cyber security

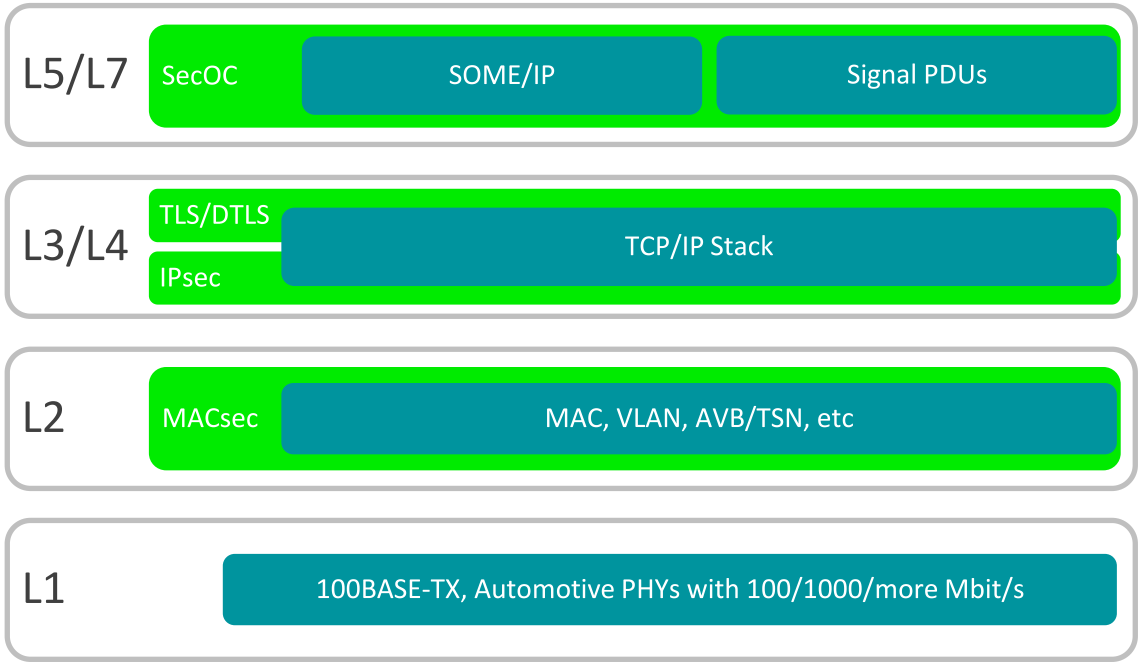


Optimized Ethernet switch HW/SW collaboration

MACsec general functions

Why and where?

- MACsec can protect all communication on Automotive Ethernet against external attackers
  - MACsec Key Agreement (MKA) + Extensible Authentication Protocol (EAP)
  - Special Keys:
    - Connectivity Association Key (CAK)
    - Key Encryption Key (KEK)
    - Integrity Check Value Key (ICK)
    - Secure Association Key (SAK)
- Support in HW:
  - Either in Microcontroller with HSM or purely in SW
  - Or in MACsec-capable Ethernet transceivers

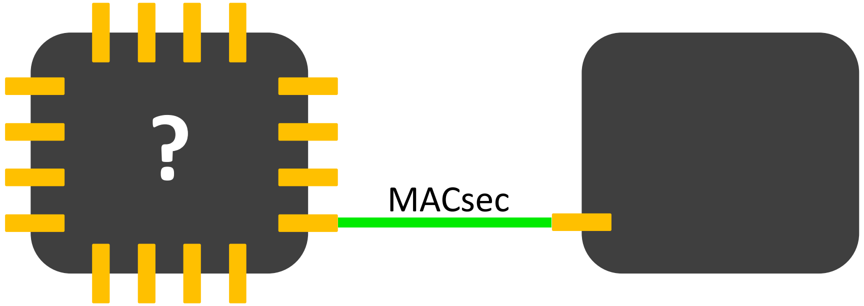


MACsec influence on the startup time

Why is it important?

- Typical startup time requirement in Automotive networks is around **200 ms**
- In order to establish a secure communication, there has to be a new SAK established
  - Done with MKA + EAP
- Recent studies* showed that
  - **With** some optimization on a relatively powerful HW the **MKA of ~23 ms** was achieved but the time was not stable.
  - It is for **ONE** direct link

How to deal with 16 links in parallel?

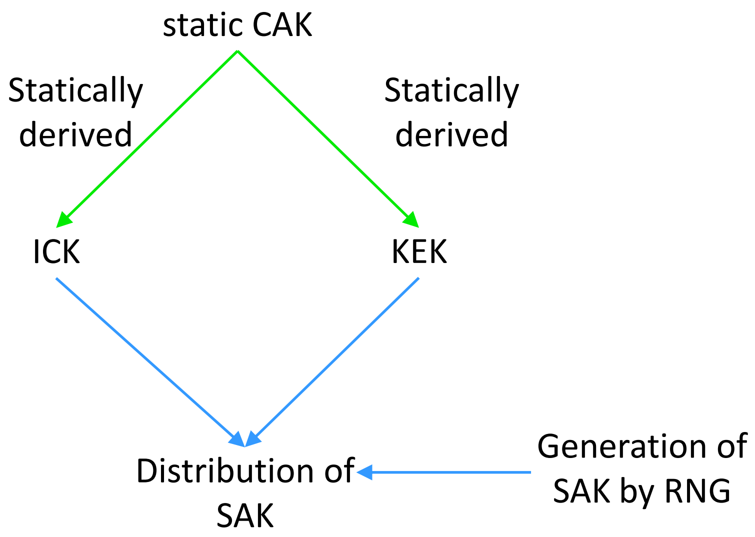


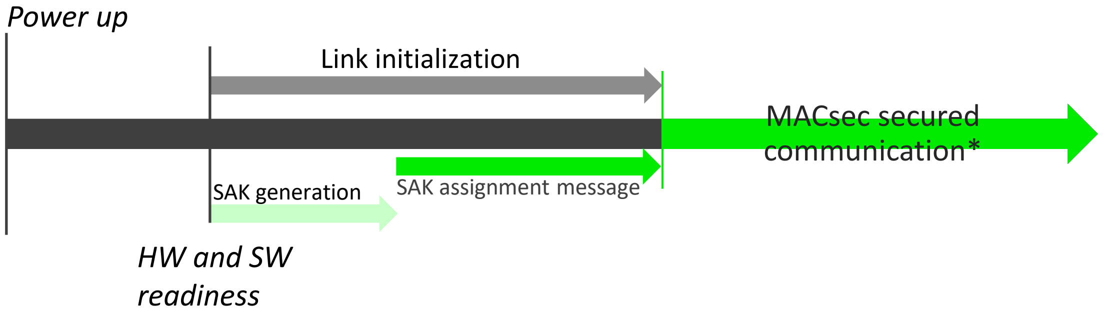
** STARTING UP MACSEC FOR AUTOMOTIVE ETHERNET, 7th International VDI Conference – Cyber Security for Vehicles, Technica Engineering*

How to reduce startup time?

One solution for switches with many ports

1. Make the switch MKA Key server by definition.
2. At the start, the KEK and the ICK must first be derived from the CAK ---> **time consuming on the switch!** These keys will be calculated at the configuration time of the CAK and stored in the secure memory.
3. Directly after the startup the switch generates the SAK for each port by using RNG from internal HSM. It is a legitimate approach according to the standard (see page 89 of 8021X-2020).
4. After the SAK is available, the EAP SAK assignment message will be calculated.
5. Step 3. and 4. are executed in parallel to the link initialization procedure which might take up to 100ms.





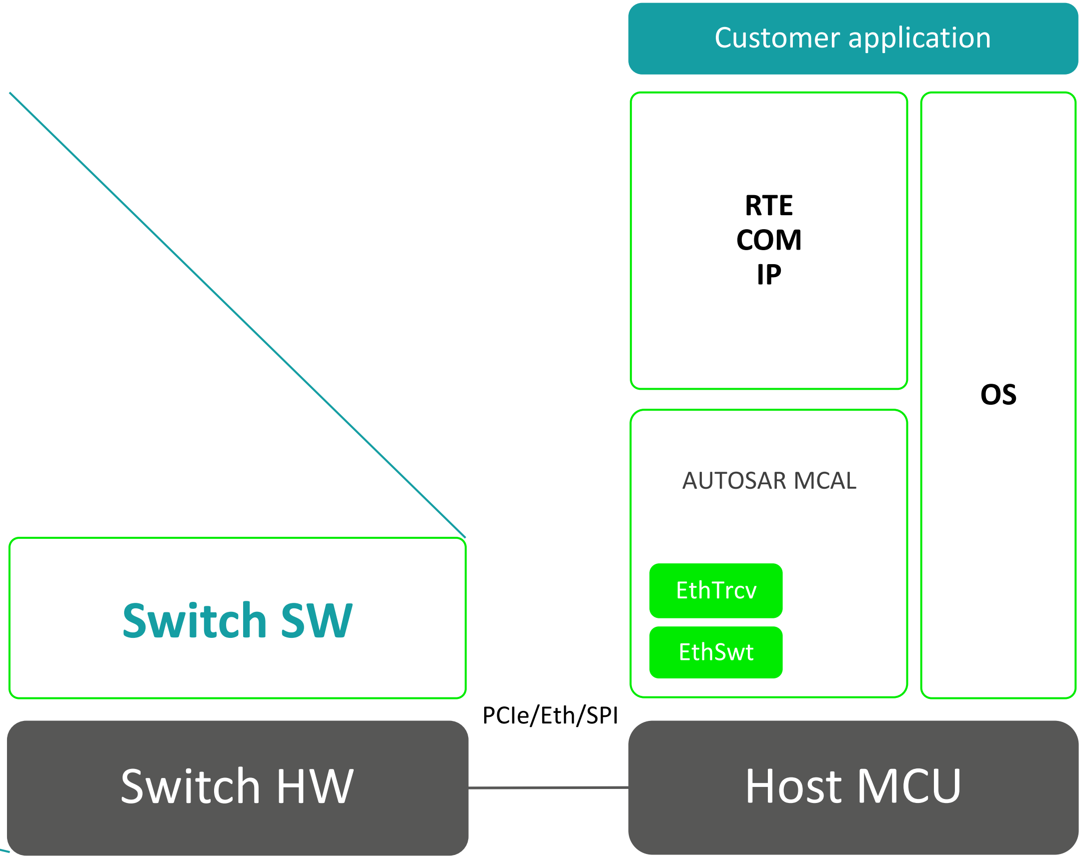
*Processing time of other protocols in not considered.

Importance of the Ethernet switches

From a simple peripheral to an advanced network device

Ethernet switch features for new E/E architecture

- Switch with own CPU system
- TCAM support
- TSN features included
- HSM included
- Health management
- 10Base-T1S
- TC10
- MACsec
- **Advanced cyber security**

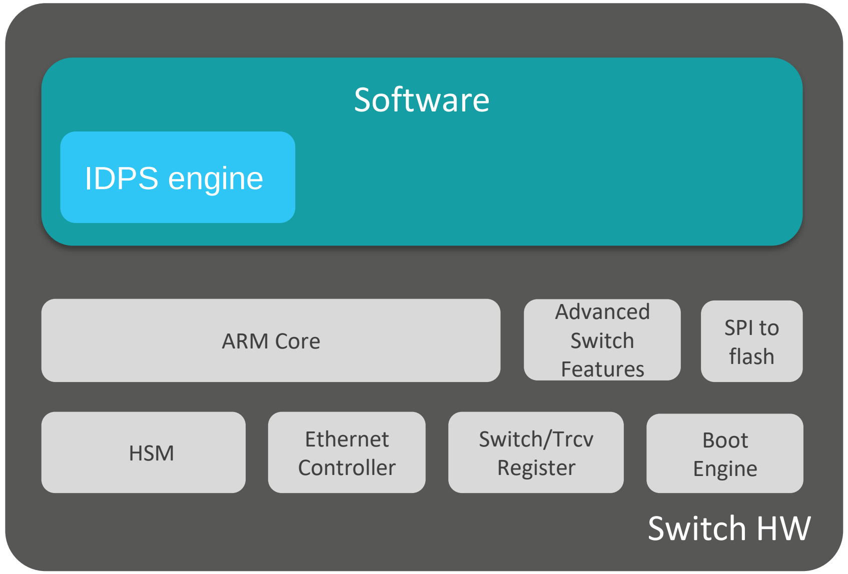


Optimized Ethernet switch HW/SW collaboration

Advanced cyber security in the switches

Why do we need it?

- Increased requirements on cyber security:
  - UN Regulation No. 156
  - GBT gateway regulation
  - Many more to come
- Implementing advanced cyber security measures in the Ethernet switch leads to
  - **Early detection and prevention** of unauthorized traffic (offloading µC resources)
  - **Reduced integration efforts** as IDPS functionality fully integrated in the Switch
  - **Efficient implementation** due to HW features of the switch



Advanced cyber security in the switches

How does it work? Where is the problem?

IDPS usage for SOME/IP whitelist

Dst MAC	Src MAC	VLAN tag	IP Src	IP Dst	IP Proto	SOME IP serv ID	SOME IP Int V	SOME IP Msg T

Checks to be done:

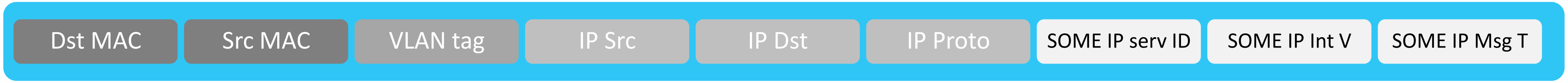
1. ETH.dst_mac==1c:ce:15:00:00:02 &&
2. ETH.src_mac==1c:ce:15:00:00:01 &&
3. ETH.ether_type== 0x8100 &&
4. VLAN.tag==20 &&
5. IP.src== 10.30.1.37 &&
6. IP.dst= 10.30.1.30 &&
7. IP.proto==0x11 &&
8. SOMEIP. service_id == 0xaaa &&
9. SOMEIP. interface_version == 0x1 &&
10. SOMEIP. msg_type == 2 &&

- Secure
- Precise
- Flexible
- Slow

Advanced cyber security in the switches

How SW can be accelerated by HW to make it more effective?

IDPS usage for SOME/IP whitelist



- Clear understanding of the traffic classes to establish
  - Check only what needs to be checked!
- TCAM rules can be used:
  - For a **single** part of the frame
  - For **multiple** parts of the frame

ETH.dst_mac==1c:ce:15:00:00:02 &&

ETH.src_mac==1c:ce:15:00:00:01 &&

ETH.ether_type== 0x8100 &&

VLAN.tag==20 &&

IP.src== 10.30.1.37 &&

IP.dst= 10.30.1.30 &&

IP.proto==0x11 &&

SOMEIP. service_id == 0xaaa &&

SOMEIP. interface_version == 0x1 &&

SOMEIP. msg_type == 2 &&

ETH.dst_mac==1c:ce:15:00:00:02 &&

ETH.src_mac==1c:ce:15:00:00:01 &&

~~ETH.ether_type== 0x8100 &&~~

~~VLAN.tag==20 &&~~

IP.src== 10.30.1.37 &&

IP.dst= 10.30.1.30 &&

IP.proto==0x11 &&

SOMEIP. service_id == 0xaaa &&

SOMEIP. interface_version == 0x1 &&

SOMEIP. msg_type == 2 &&

Summary

What to remember?

- Ethernet switches in automotive industry are:
  - playing **key** role in the in-vehicle communication
  - **complex** devices with **special** HW features inside

- With **smart** and **innovative** SW on automotive Ethernet switches:
  - **Full** HW functionality can be uncapped with support of AUTOSAR interfaces and protocols
  - **Separation** of the network from the HW can be achieved
  - **MACsec** startup issue can be defeated
    - Protocol tweaks
    - HW acceleration
  - **Cyber security** can be effectively integrated

Thank you for your attention!

Illia Safiulin

Product Manager, Elektrobit
Illia.Safiulin@elektrobit.com
elektrobit.com