High Performance Compute Architecture supporting revolutionary requirements

Stefan Singer

Technical Fellow & Director, EMEA FAE Automotive

November 2017

SECURE CONNECTIONS FOR A SMARTER WORLD

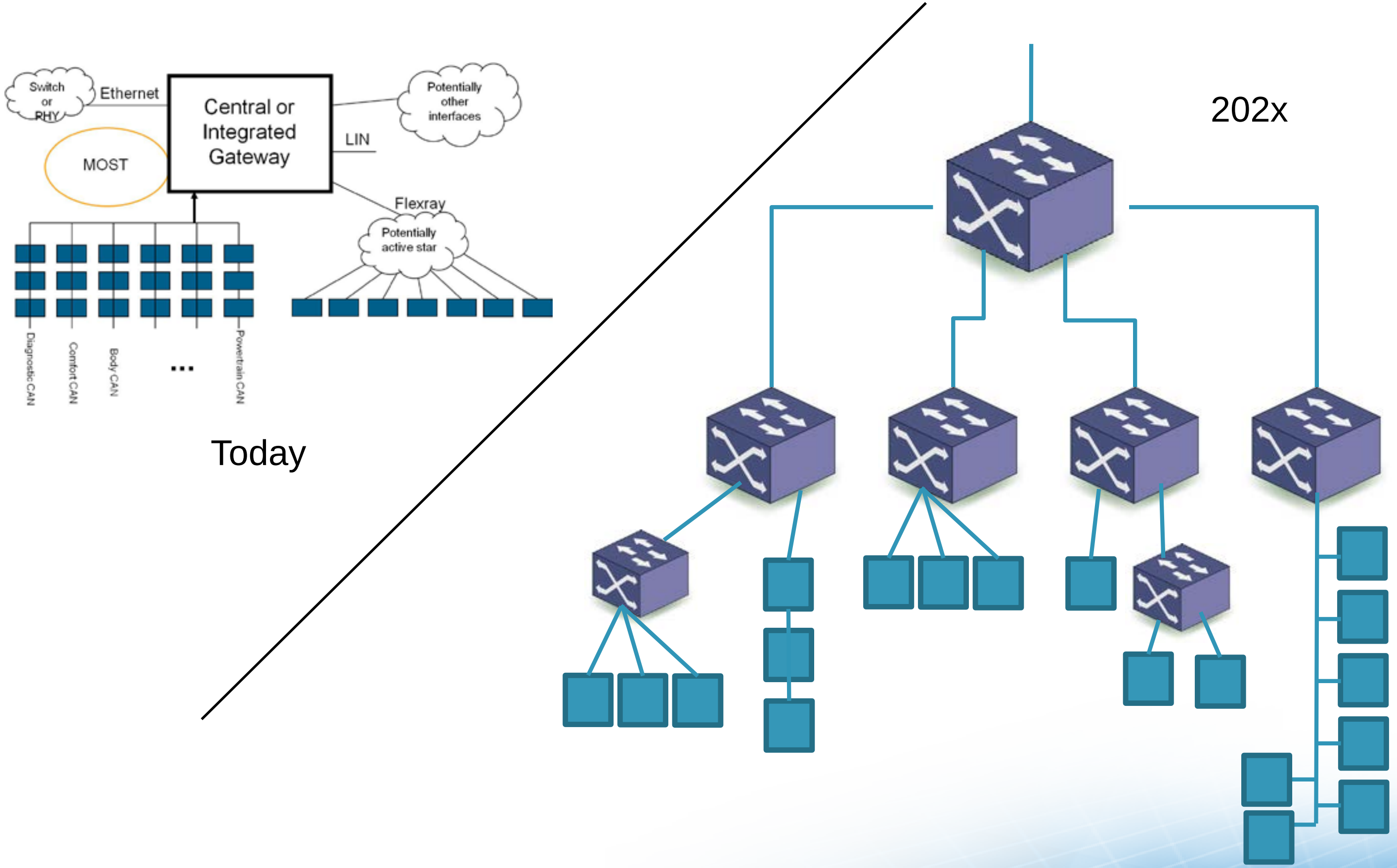
Agenda

- Motivation for Change
- E/E architecture evolution
- Network Redundancy Scenario
- 3+1 Compute elements
- Ethernet Network Security
- High Performance Compute Architecture
- Summary

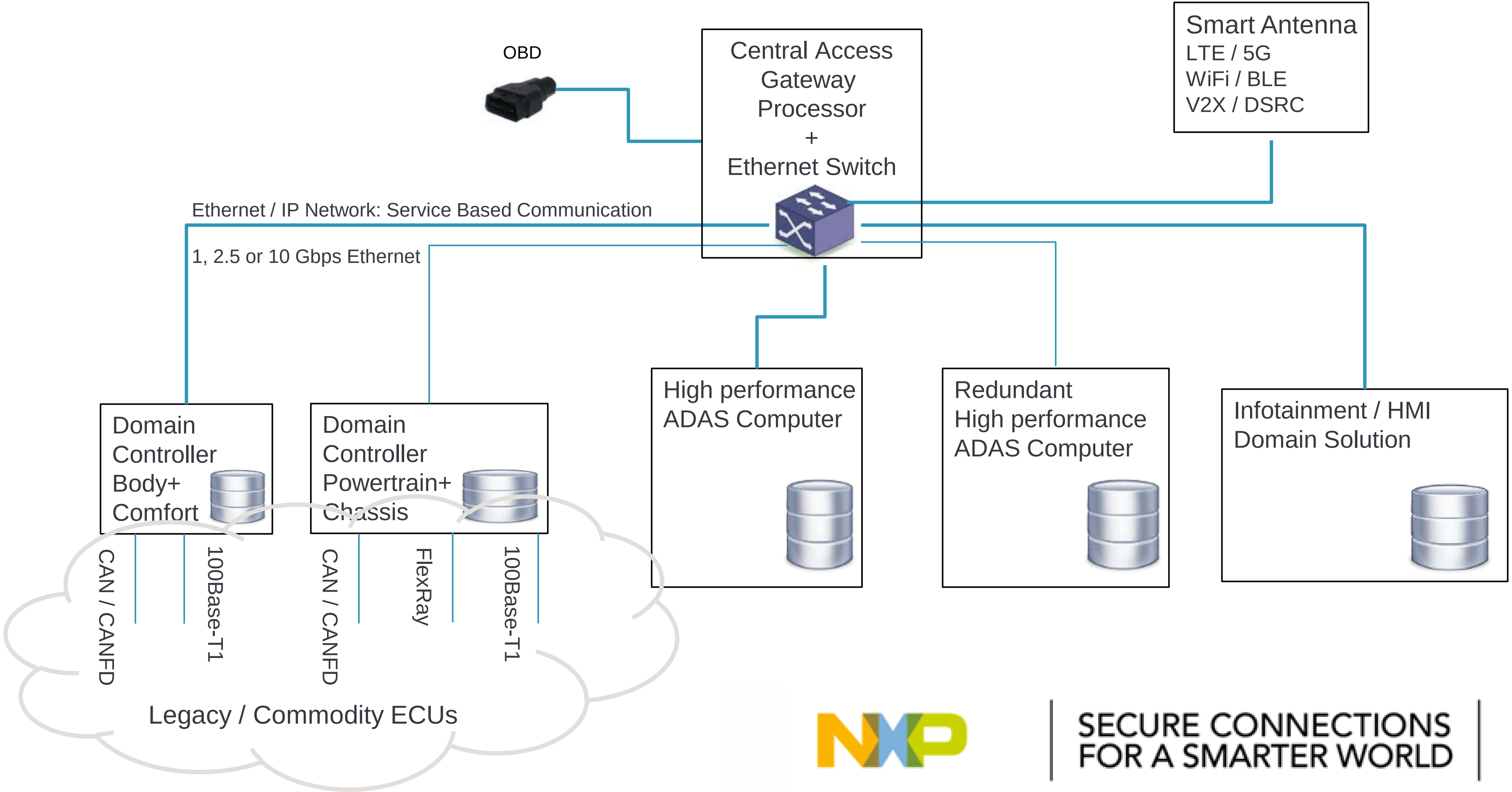
Motivation for new EE architecture

- Vehicles are becoming always connected and part of the internet
  - New services evolve, e.g. Natural Speach recognition (Amazon Alexa), Cloud based services, …
  - „Open“ connectivity into the vehicle will drive new levels of security requirements
- Drive trains evolve from combustion engines to mixtures of hybrid and electric vehicles with new challenges (e.g. for reach)
- Trend to higher levels of assisted driving up to future level 3-5 automated vehicles
  - Triggers the need for high bandwidth networking for sensor data, meta data, …
  - Also requires filtering and upstreaming of use case information into the cloud to better understand vehicle operation
- Traditional automotive development approach (i.e. one function, one box and statically defined) cannot deal with the speed of changes
- However there is no benefit in redeveloping traditional legacy functions, so therefore integration of existing ECUs will conserve existing investment

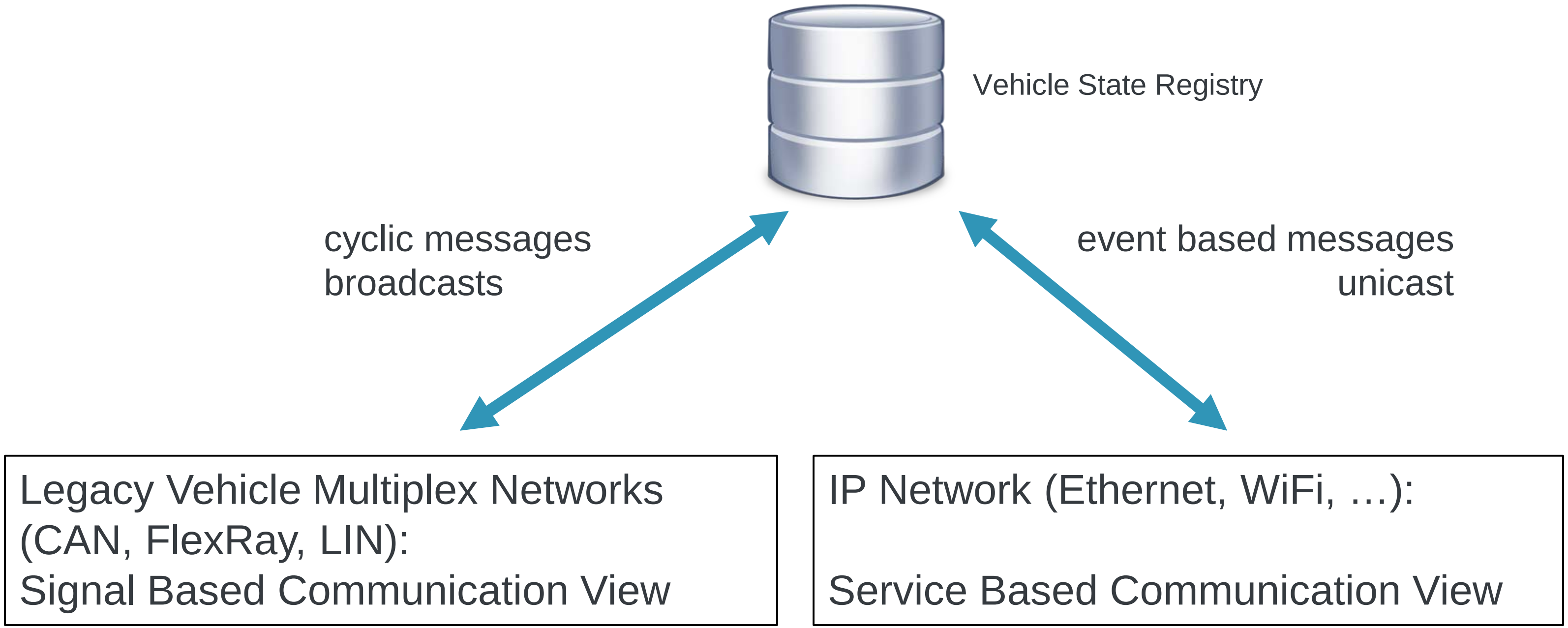
Evolution from Central Gateway to Domain Architecture



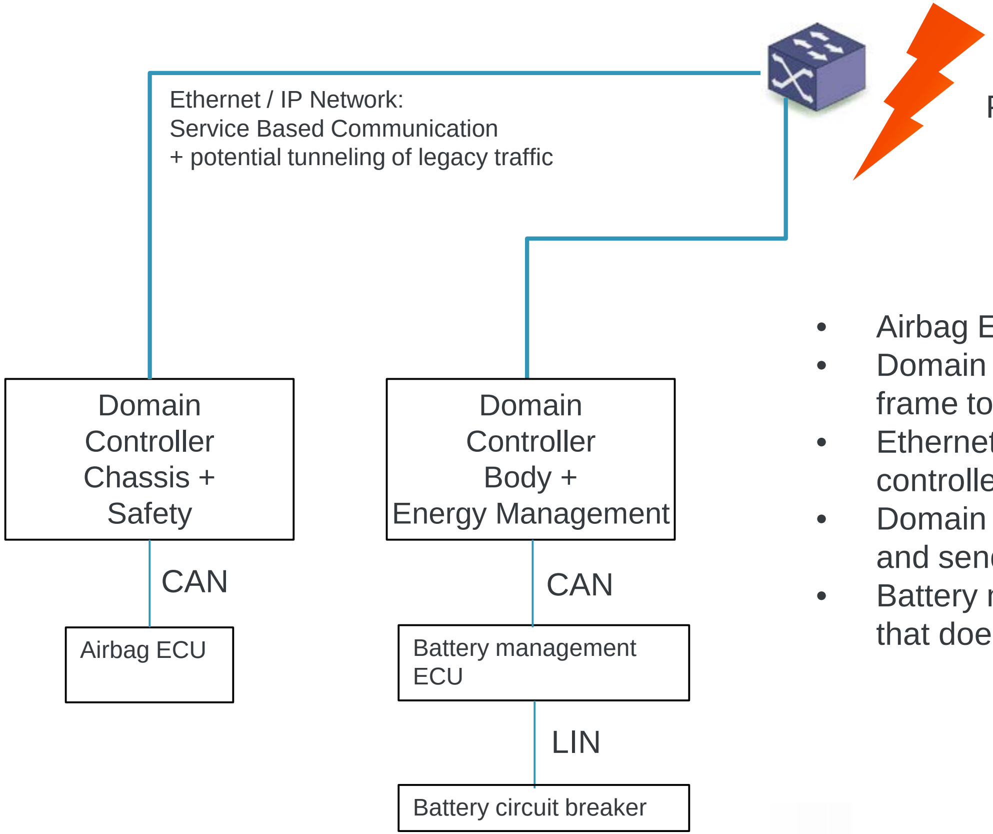
Future Vehicle E/E architecture



Coexistence of Signal Based and Service based Communication



Network Redundancy Scenario Example

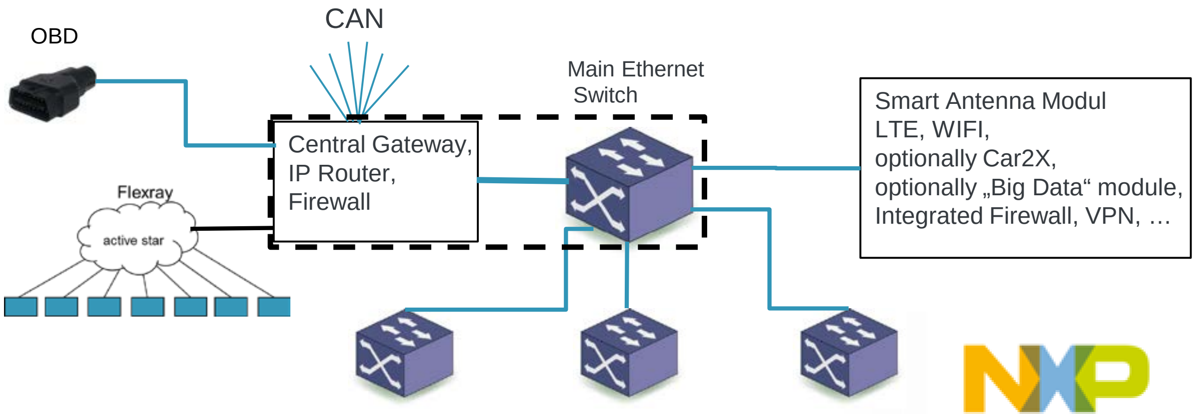


Potential single point of failure

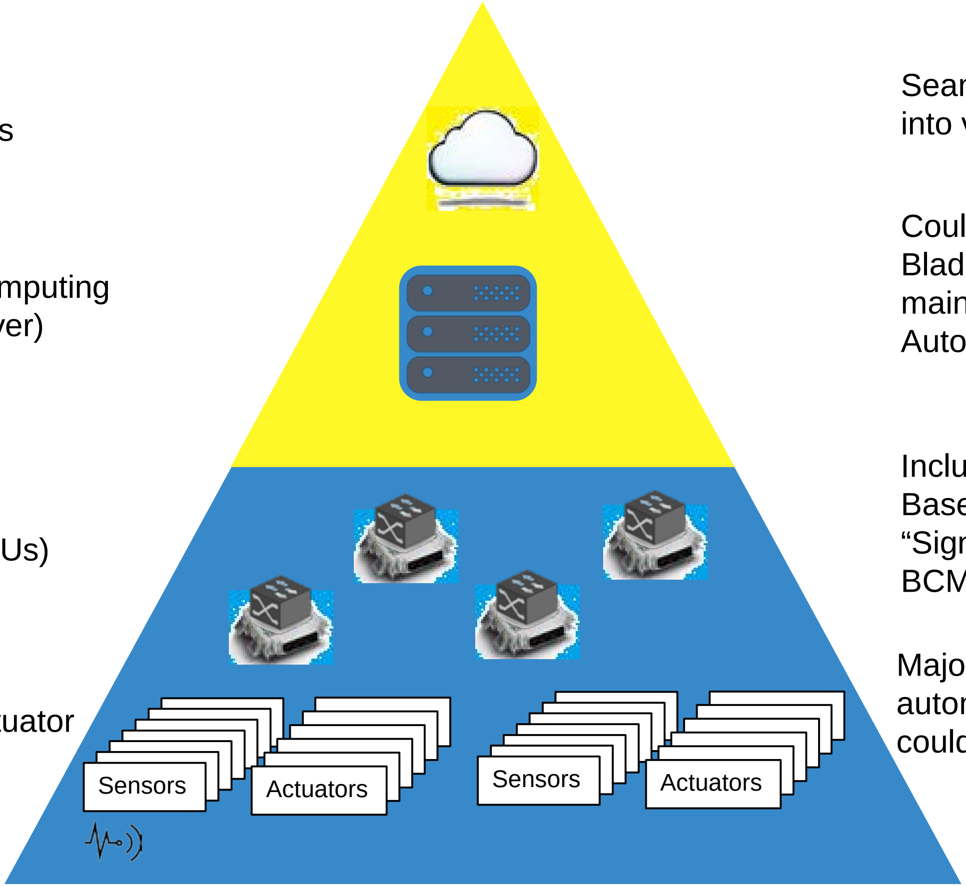
- Airbag ECU sends CAN message to domain controller
- Domain controller converts message and sends Ethernet frame to Ethernet switch
- Ethernet Switch sends Ethernet frame to different domain controller
- Domain controller converts message to CAN message and sends it to Battery management ECU
- Battery management generates LIN message to ECU, that does finally cut the energy with a circuite breaker

Alternative Legacy Automotive Overlay Network

- To simplify migration from existing vehicle network architecture an overlay network of the existing automotive interfaces (CAN, FlexRay, LIN) in the central Gateway could be a potential solution
- This reduces the complexity of network migration to only the Gateway
  - Legacy nodes talk e.g. CAN, FlexRay
  - New nodes talk IP, Service based communication
- An additional benefit of this approach is, that for specific needs ultra low latency routing of legacy messages could be achieved
- This also provides a redundant communication path to avoid single point of failures



3+1 Compute elements of E/E architectures



Cloud Services

Seamless Integration of Cloud Services into vehicle architecture

3 Centralized Computing (e.g. blade server)

Could be centralized box or Compute Blade Server, IT Industry like. This will mainly run new, not traditional Automotive ECU functions

2 Domain (Integration ECUs)

Includes Gateway between Service Based “IP World” and legacy, static “Signal based world”. Examples are BCM, Powertrain Domain Controller, …

1 Sensor and Actuator

Majority of nodes. Include legacy automotive ECUs and in some cases could be commodity across many OEMs

1. Smart Sensors / Actuators

- **Large majority of nodes in the car**
- Potential commoditization
- Sensors related to self driving (radar, camera, positioning, lidar, V2X) currently on a performance/cost/power/form factor race.
- Function→ HW mapping still evolving towards maturity.
- Still significant potential to differentiate by performance, power dissipation, form factor, ...
- Reuse of existing Automotive ECUs or new developments with similar development flow and architecture concepts
  - e.g. Autosar Classic SW, ISO-26262 Functional Safety, …
  - Majority of nodes with static configuration and signal based communication (classic CAN, LIN, FlexRay), transition to Ethernet where required by application.
- Potential to be reused across many or all OEMs

2. Domain (Controller)

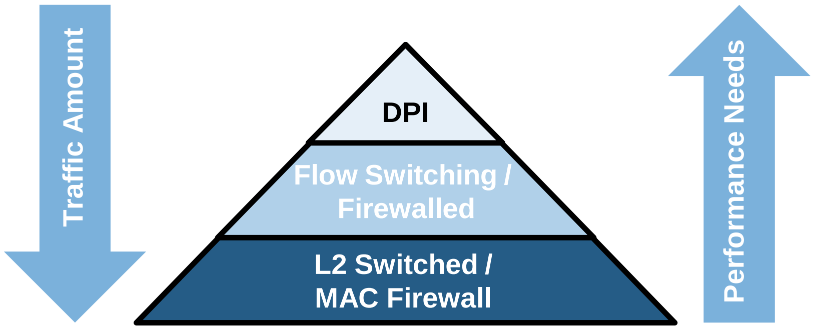
- Bridge between Automotive legacy world (CAN, FlexRay, LIN, static configuration, signal based communication) and “new” IP based “service oriented communication world”
- Backbone connection through Ethernet (100 or 1000 Mbps, depending on node)
- Integration of multiple traditional functions into one ECU
- Dynamic Software environment, e.g. Autosar Adaptive or Linux
- “Sandbox environment” / Hypervisor / Partioning for Software functions coming from different sources (3d parties, tier ones, OEM)
- Example: Vehicle Dynamics Domain Controller, Powertrain Domain Controller or Main Body Domain Controller

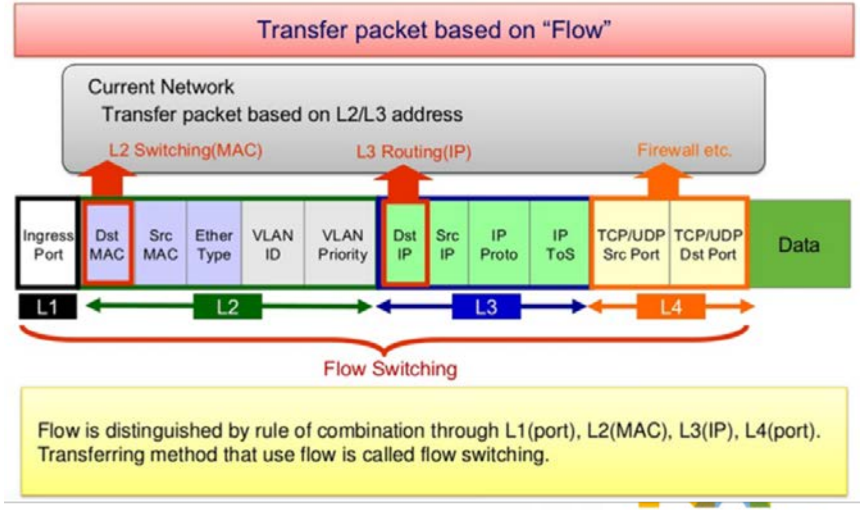
3. Centralized Computing

- Enters Automotive from IT / Networking Server Farms. Different system thinking.
- Host functions, that only require communication and compute, but no dedicated I/O and deploy them in a scalable fashion.
  - Software isolation: Hypervisor / Virtual Machines / Linux Containers
  - Most important requirement is, that functions can be deployed without compromising already existing functions
- Ethernet (1, 2.5, 5 or 10 Gbit) as Packet Interconnect
- PCIe as bulk data communications mechanism within boards / chassis
- Could be centralized box or Compute Blade Server concept from IT Industry
- Availability and Fail Operational by having multiple redundant compute resources (e.g. blades) and redundant communication links.
- Examples: Sensor Fusion, HMI, Function Integration Server, Gaming/Apps

Ethernet Network Security

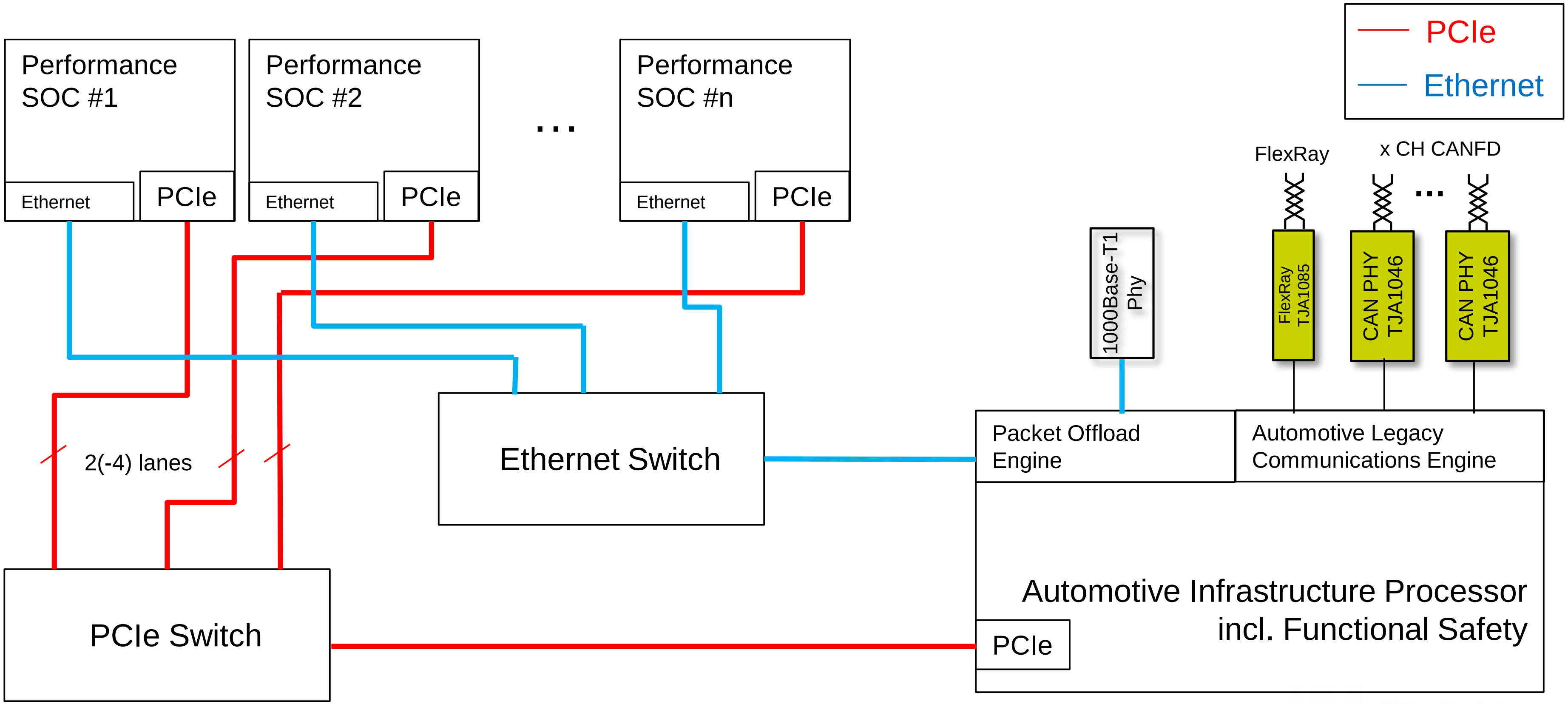
- **Ethernet Traffic should be sorted in different hierarchies**
  - Within same VLAN traffic can be switched through classical L2 Ethernet switching
  - Traffic crossing VLANs should be inspected using “Flow Switching”. This allows also some quite sophisticated analysis including stateful inspection. Depending on amount of traffic, this can be implemented through optimized “Fast Path” Software or a dedicated offload engine
  - Finally some traffic might require detailed “deep packet inspection”
- **Layered Network Security**
  - As it is common in the IT industry, network security can only be achieved with a layered approach to implement multiple layers of defense
  - Networks MUST be designed to protect vital vehicle functions even if individual nodes have been hacked!





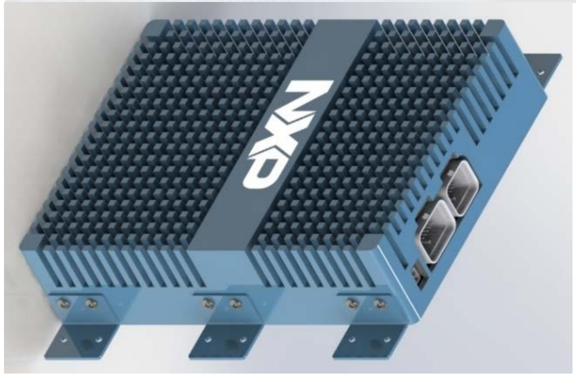
Courtesy of AdTran

High Performance Automotive Compute Architecture

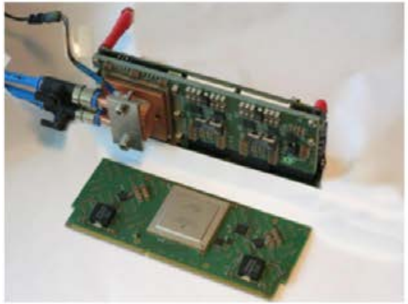


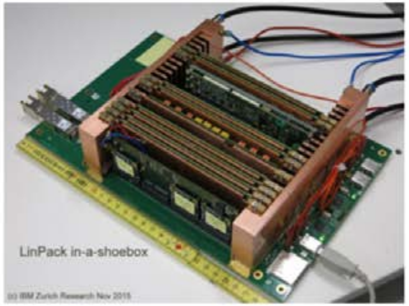
BlueBox 2.0

- A prototyping platform for Automated Drive and Sensor Fusion applications
- Different enclosure styles possible for lab use and in-vehicle use
- 12V/24V vehicle compatible power input
- High performance compute with 16GB DDR4 and 250GB SSD
  - ASIL-B compute, automotive interfaces, with vision acceleration
  - ASIL-D subsystem, with dedicated interfaces
- Automotive I/O, numerous interfaces
  - Ethernet 100M/1G/10G, SFP+, 8*100BASE-T1, CAN[-FD], FlexRay, 8*Camera Coax, others
- Ships with near-desktop style embedded Yocto Linux for ease of use



Datacenter in a vehicle – not your server room's 19 inch





Ronald Luijten, Data motion architect,
IBM Research

Node	ISA	DRAM	I/O
T4240ZMS	ppc64	24 GB	4x 10GbE
28nm Bulk	24 core	3 channel	PCI x8
43W TDP	1.8GHz	DDR3	2 SATA
	e6500	72bit ECC	USB, µSD
LS2088ZMS	ARMv8	32 GB	6x10GbE
28nm Bulk	8 core	2 channel	PCI x4,x2,x1,x1
35W TDP	2+GHz	DDR4	2 SATA
	A72	72bit ECC	USB, µSD

https://www.zurich.ibm.com/microserver/

Conclusion

- New trends in Automotive require a fundamental redesign of EE architectures
- Investment in Legacy functionality can be protected through proper network architecture
- Complete Immunity of individual nodes against hacks cannot be guaranteed and therefore the vehicle network must mitigate the impact of those
- Layered Security Architecture from the IT industry needs to be applied for that reason
- High Performance Compute Concepts from other industries can be applied, but automotive specific requirements need to be taken serious

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD