FROM TC10 TO SYSTEM WAKE-UP

SAFETY SYSTEM SOLUTIONS

ETHERNET & IP @ AUTOMOTIVE TECHNOLOGY DAY

Steffen Lorenz

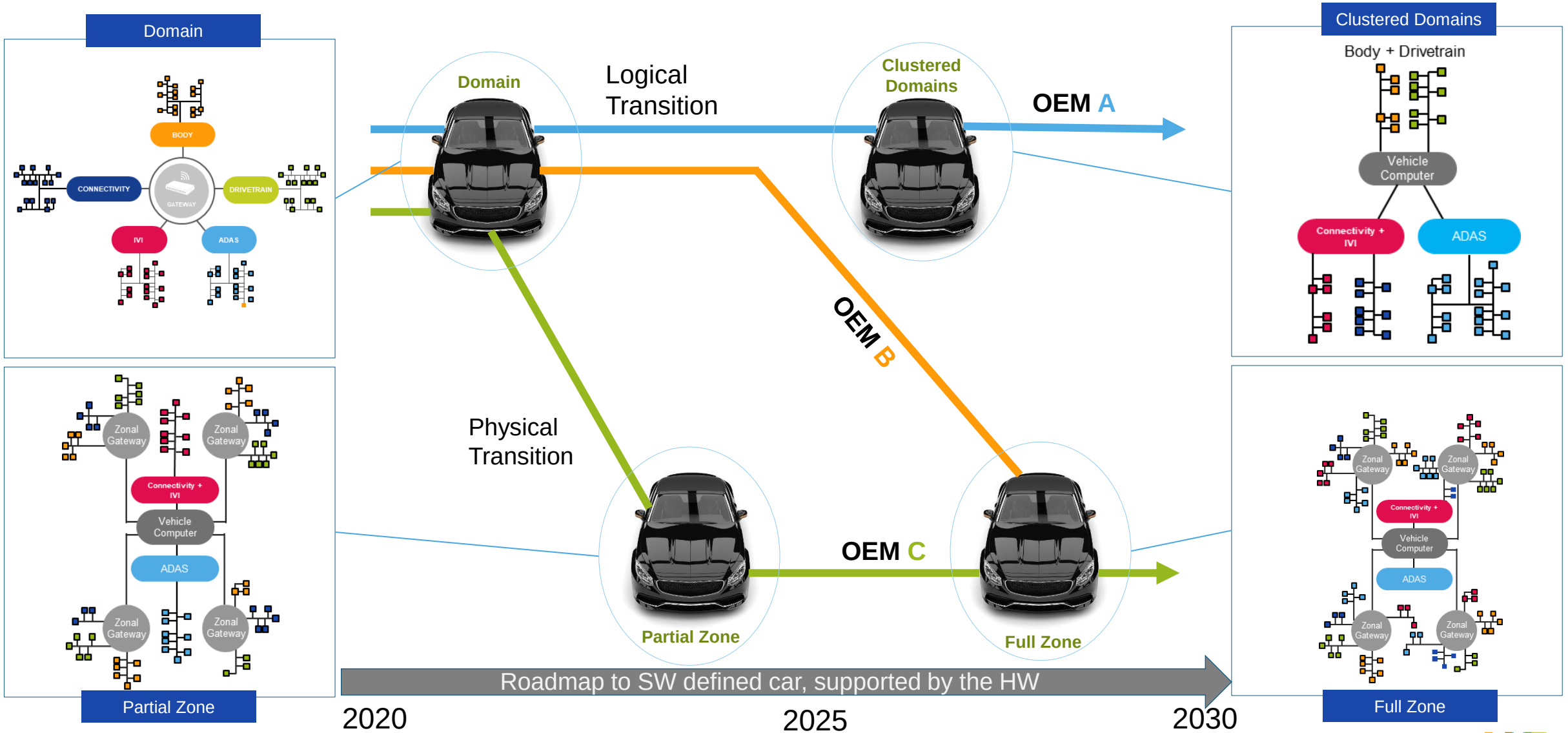
NOVEMBER 2022

SECURE CONNECTIONS
FOR A SMARTER WORLD

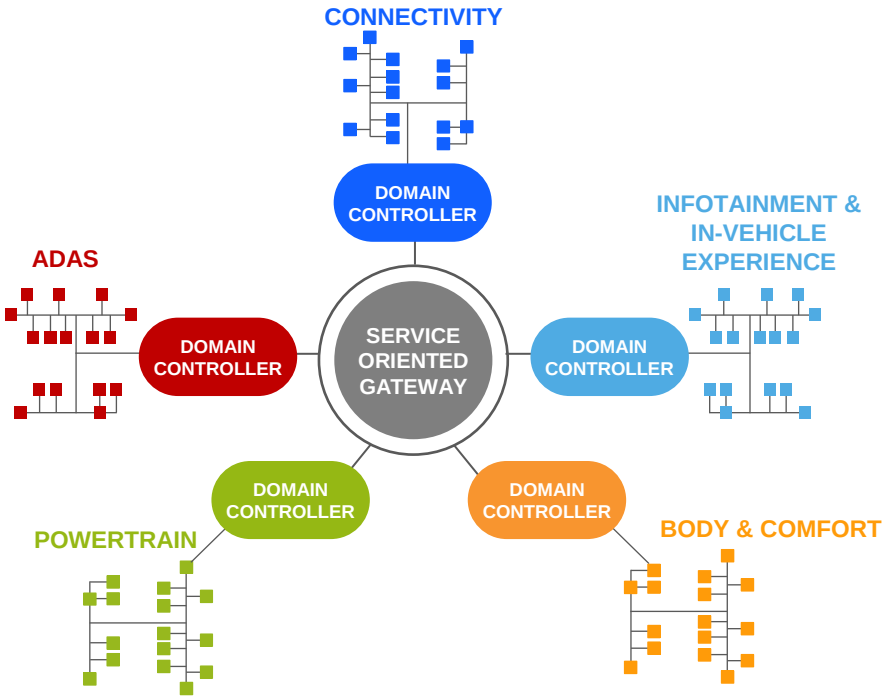
AGENDA

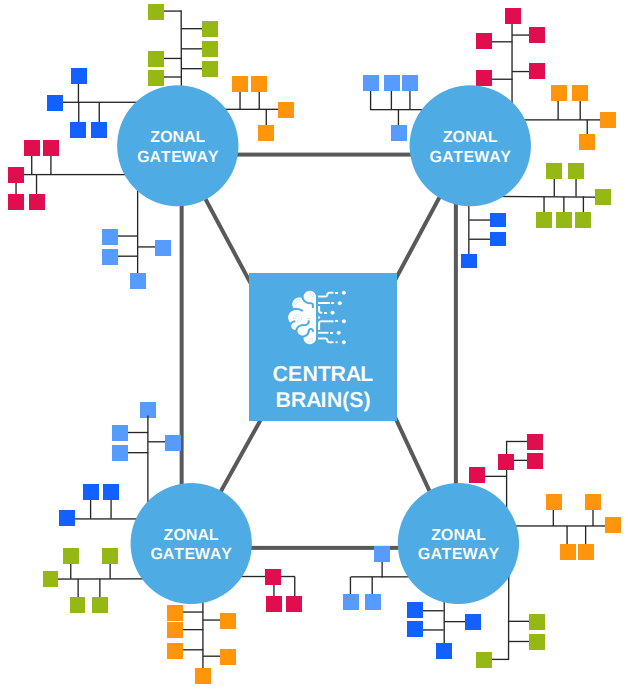
- *Motivation/Introduction*
- *Sleep & Wakeup concepts*
- *Functional Safety*
- *Zonal system aspects*
- *Summary and conclusion*

ARCHITECTURE IS SHIFTING TOWARDS ETHERNET-BASED ZONAL MODEL



ARCHITECTURE IS SHIFTING TOWARDS ETHERNET-BASED ZONAL MODEL

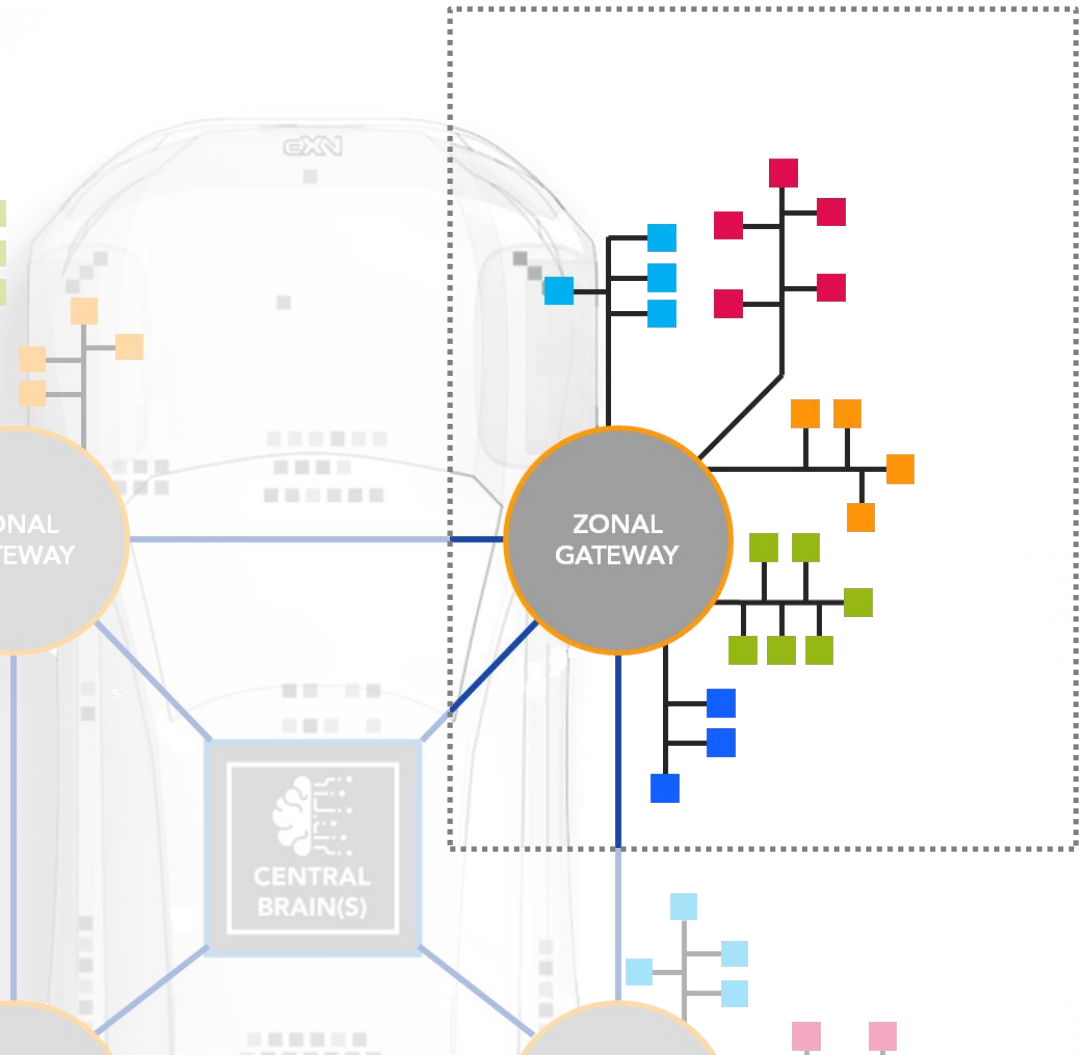




- Availability of nodes handled by domain controller
- Nodes of a function mostly in same network
- X-domain wakeup handled by central gateway

- Service oriented availability requests
- Nodes are spread over whole network
- wakeup to be handled by zonal gateways

ZONAL GATEWAY / ZONAL AGGREGATOR



- Aggregation of data & gateway function
- Connects diverse technologies
  - (Switched) Point-to-Point Ethernet
  - 10BASE-T1S
  - CAN
  - …
- Connects to high-speed backbone
- Connections belong to several functional domains

- And it consumes power!

→ Switch off parts, which are not needed

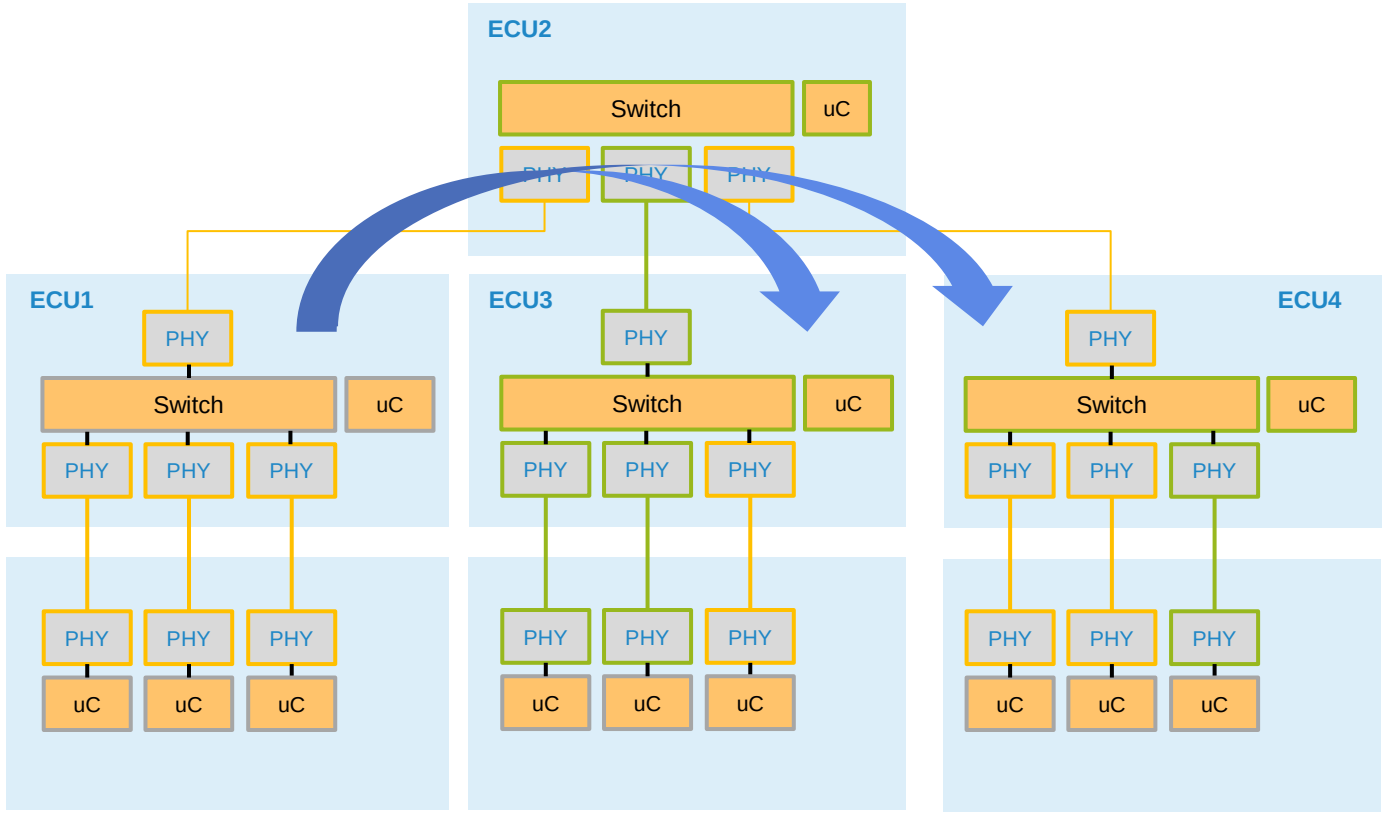
Sleep and Wakeup

Concepts

SECURE CONNECTIONS
FOR A SMARTER WORLD

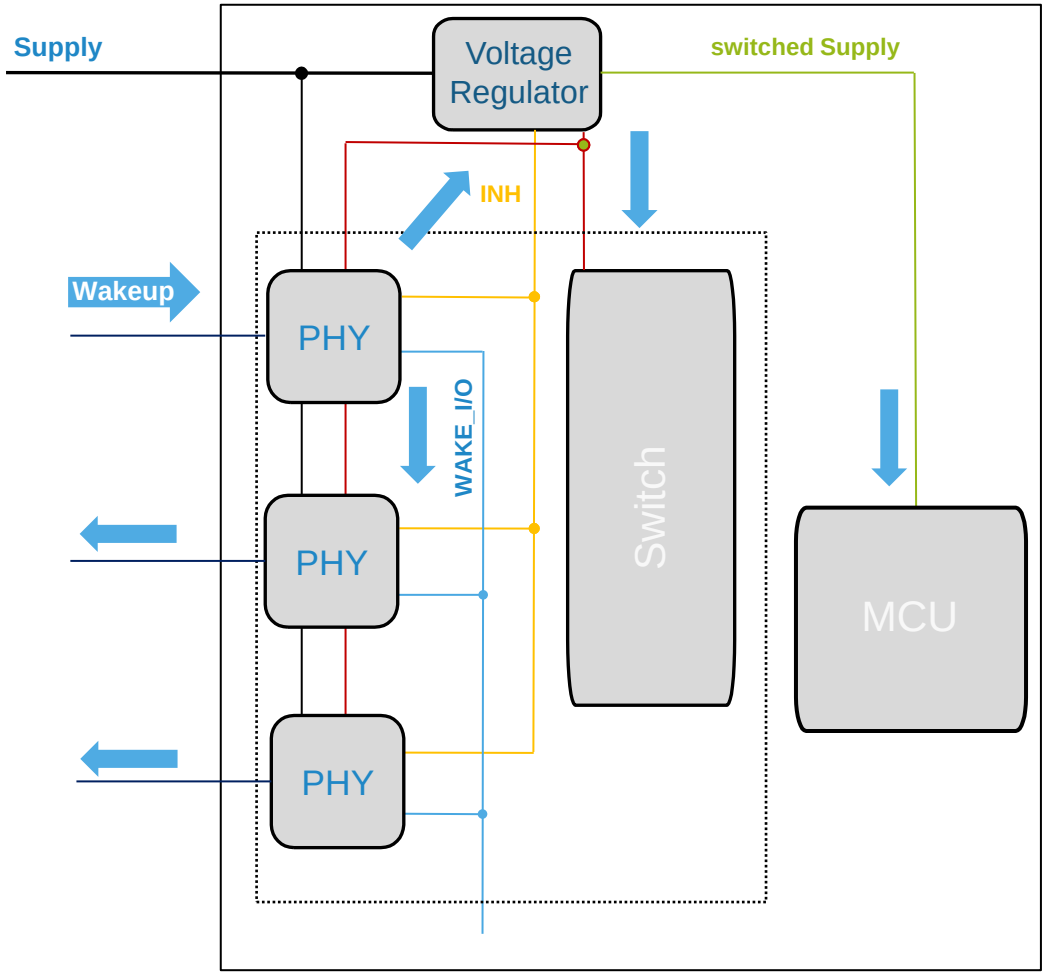
TC10 WAKEUP 100/1000BASE-T1

- Sleep/Wake on PHY level
  - defined by TC10 of OPEN Alliance
  - 100BASE-T1 & 1000BASE-T1
- Partial sleep
  - Negotiation on NM level
  - sleep handshake on PHY level
- Fast forwarding on PHY level
  - Linkup parallel to ECU startup
  - Wakeup over an active link (WUR)



TC10 WAKEUP 100/1000BASE-T1

- PHY centric concept, but can control whole ECU
- Unused ports can be switched off to safe power
- Ports can be woken up remotely
- Wakeup forwarding to wake remote PHYs
- If all ports are off, switch can be switched off
- The MCU may be off as well,
  - with or without communication running
  - with local or remote wakeup (via TC10)
- Whole ECU may be in Sleep, wakeable via remote wakeup



Functional Safety

SECURE CONNECTIONS
FOR A SMARTER WORLD

ISO 26262 – The Science of Quantifying Risk

Severity Exposure Controllability →

ASIL
Automotive Safety Integrity level

How much harm is done?

How often is it likely to happen?

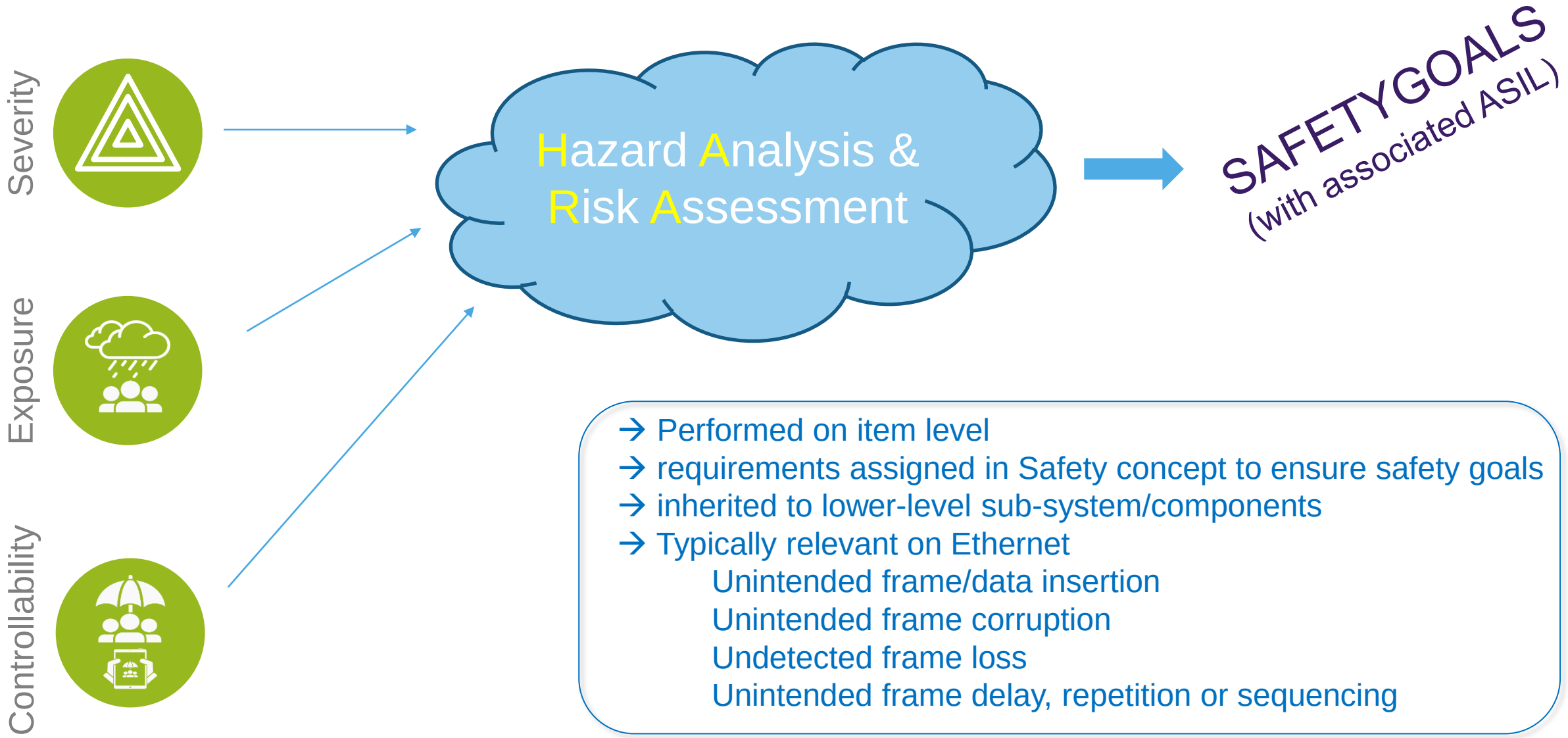
Can the hazard be controlled?

Inherent Risk

ISO 26262, part 1:
"absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems"

Reduce risk to an acceptable level

- QM
- ASIL A
- ASIL B
- ASIL C
- ASIL D



- → Performed on item level
- → requirements assigned in Safety concept to ensure safety goals
- → inherited to lower-level sub-system/components
- → Typically relevant on Ethernet
  - Unintended frame/data insertion
  - Unintended frame corruption
  - Undetected frame loss
  - Unintended frame delay, repetition or sequencing

HOW THE NETWORKING IC BRINGS SAFETY TO THE ZONE

Vehicle service availability can be improved by ensuring the availability of communication services in the vehicle. Networking chips can:

- Prevent Failure
  - Very high reliability
  - Freedom from interference

- Predict Failure
  - (Self-)Diagnostic features

- React to Failure
  - Quickest response time to increase FTTI margin
  - Even correct some failures

Design for Functional Safety goes far beyond the single product…
It requires a living safety culture and development process.

HOW THE NETWORKING IC BRINGS SAFETY TO THE ZONE

- Prevent Failure
  - Manufacturing quality makes the difference
  - Policing / access control
  - Configuration monitoring
- Predict Failure
  - Build-in self-test
  - Temperature/Voltage monitoring
  - Counter/diagnosis monitoring
  - Latent fault tests
- React to Failure
  - Memory failure correction (ECC)
  - IEEE 802.1CB (stream replication/elimination)
  - Even correct some failures
  - Entering safe state (for sub-system)

Example Reference FIT calculation

For Tjv / CL parameter details, please contact NXP

TJA1043U	Siemens Norm SN29500	HTOL Qual CAN Family	Production & Field Return Data CAN Family
Reference FIT calculation	42 FIT	3.0 FIT	0.04 FIT

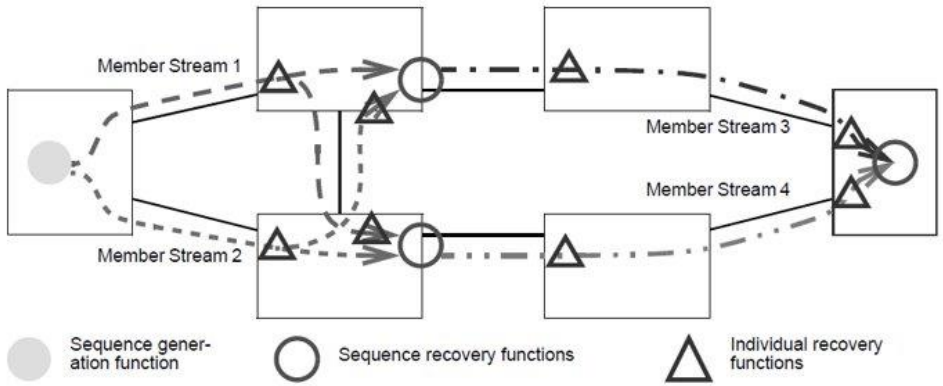


Figure 7-3—Sequence recovery functions and Individual recovery functions

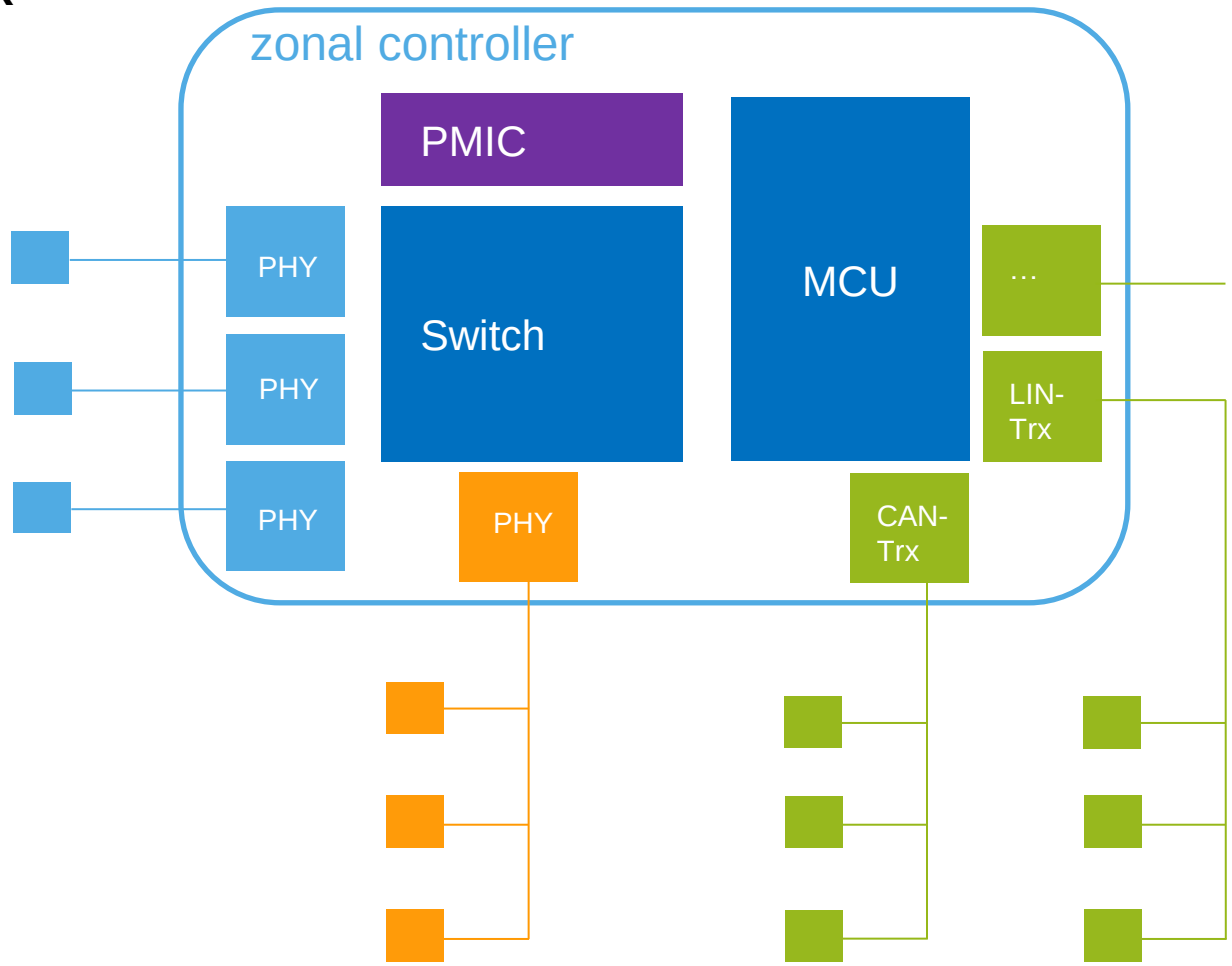
System view

Functional Safety & Sleep

SECURE CONNECTIONS
FOR A SMARTER WORLD

SYSTEM ASPECTS IN ZONAL CONTROLLER

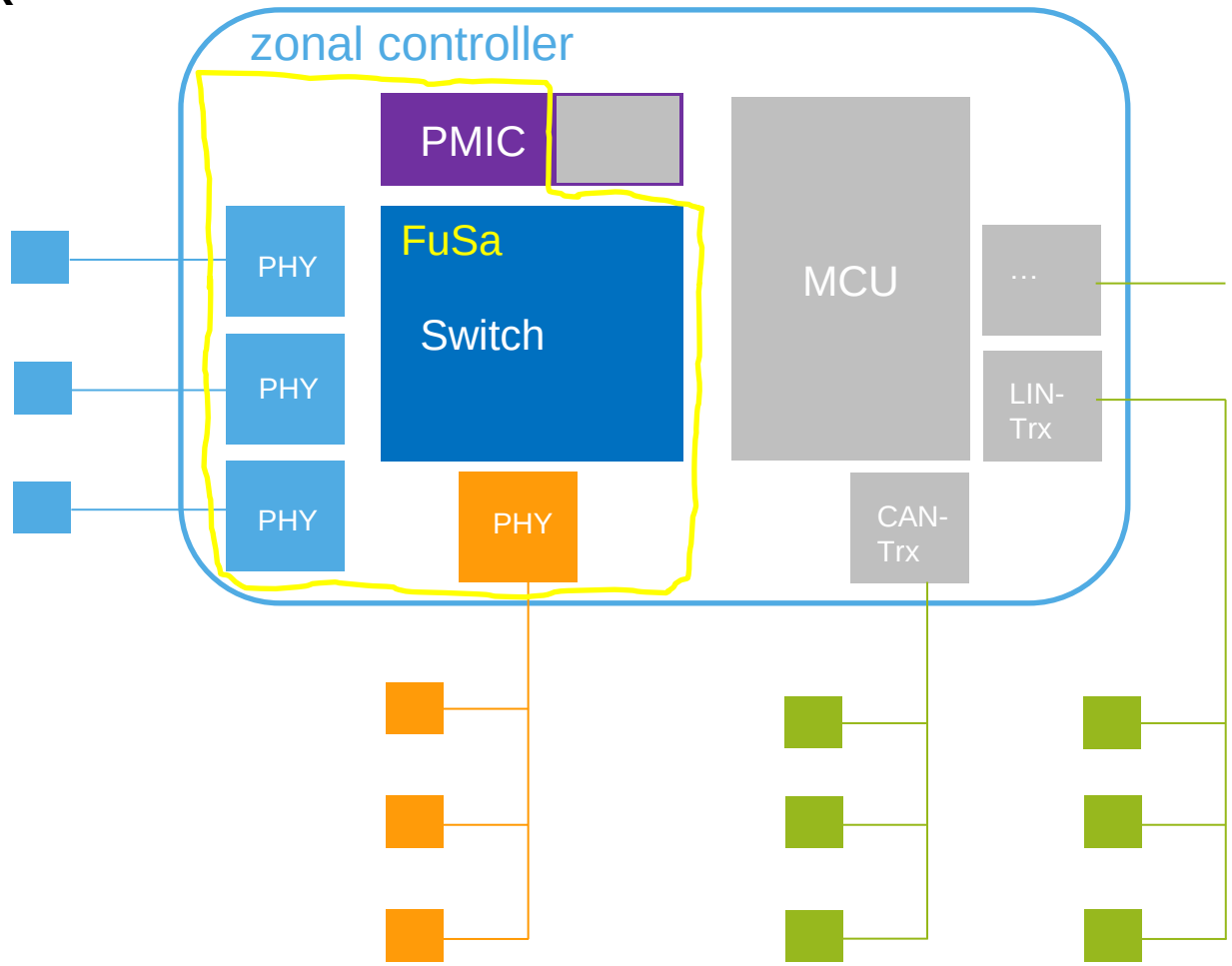
- Example for a zonal controller
  - Several communication interfaces
  - Switch for high-speed data links
  - MCU for local pre-processing and data aggregation of local networks
  - Power controller (PMIC) for supply
- Safety requirements on the communication and processing



SYSTEM ASPECTS IN ZONAL CONTROLLER

- Standalone communication
  - In case no local processing needed, e.g. charging, ADAS functions off,…
  - MCU and related peripheral is off
  - Communication is active

- Functional Safety of communication subsystem must be independent from MCU
- Requires safety compute in the switch
- PMIC is supervising the switch

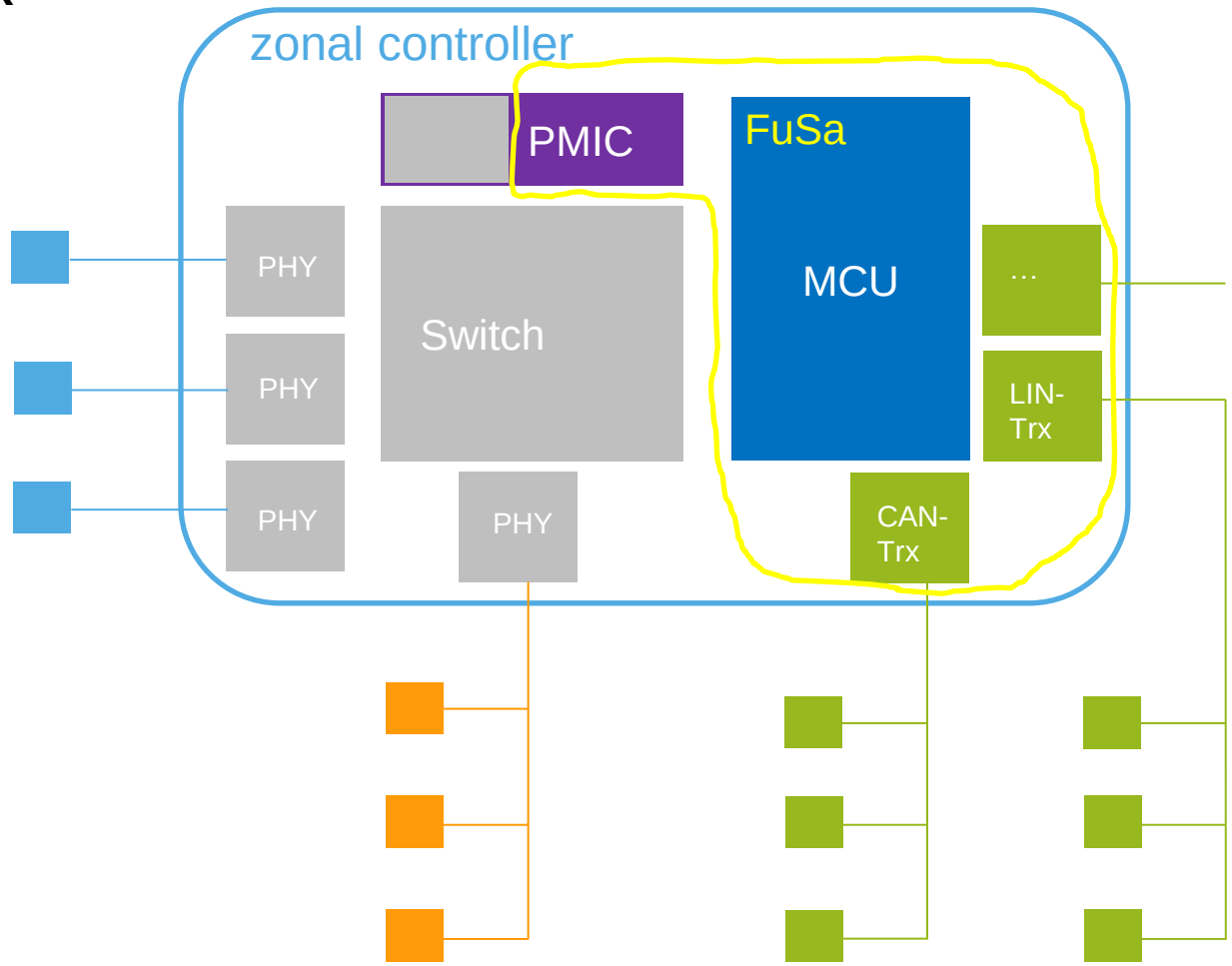


xBASE-T1
10BASE-T1S
CAN/LIN/other

SYSTEM ASPECTS IN ZONAL CONTROLLER

- Standalone processing / data aggregation
  - In case no high-speed communication needed, e.g. local …
  - MCU and related peripheral is active
  - Communication is off

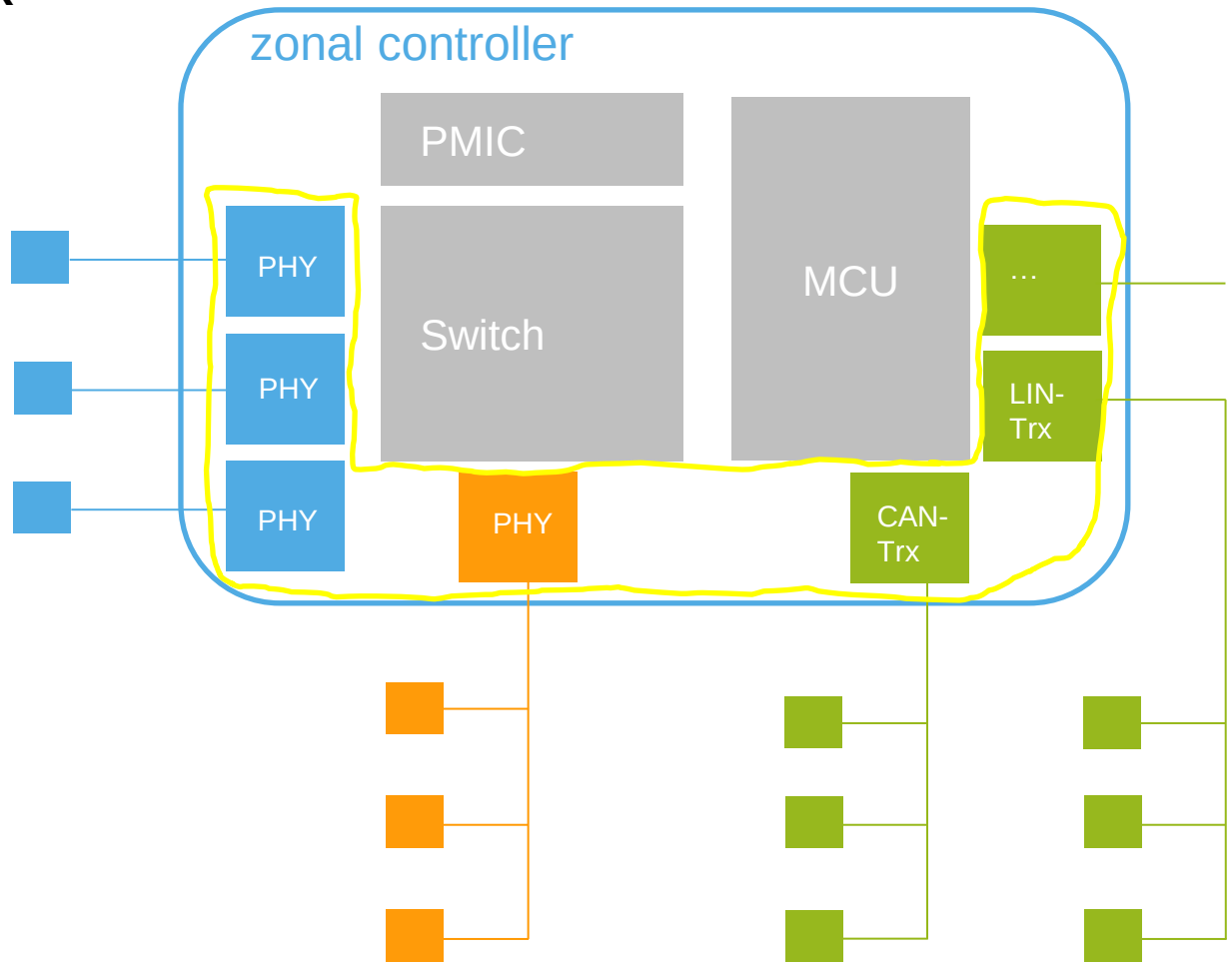
- Functional Safety runs in the active sub-system
- Independent from back-bone communication
- PMIC is supervising the MCU



SYSTEM ASPECTS IN ZONAL CONTROLLER

- Wakeup from diverse sources
  - System wakeup may be requested from local network, central brain or another zonal controller.
  - Required action differs between wakeup sources

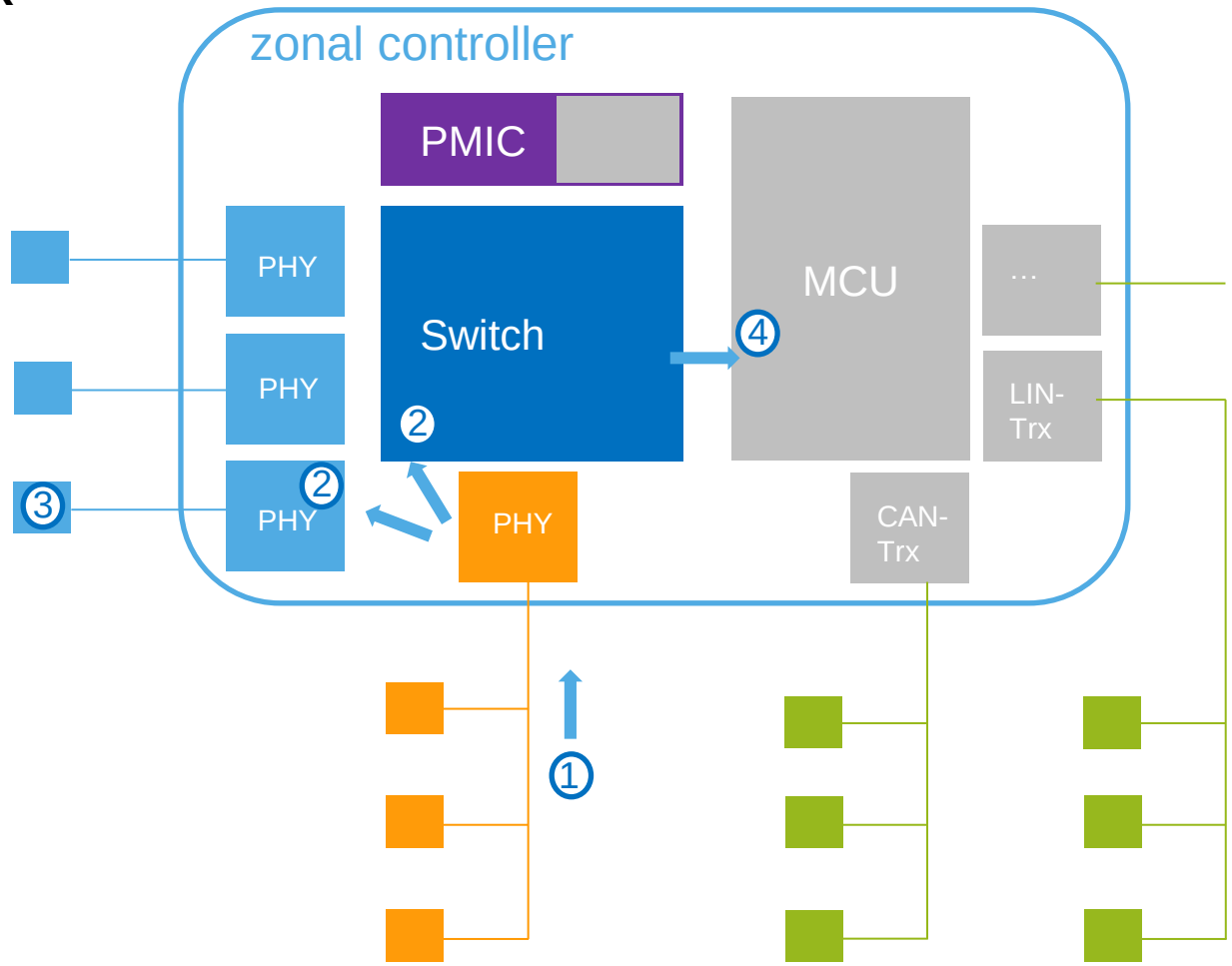
- Wakeup reaction must allow for flexible wakeup reaction
- Allow for independent operation
- Further wakeup may be situation dependent



SYSTEM ASPECTS IN ZONAL CONTROLLER

- Example
  - Wakeup from 10BASE-T1S
  - Communication with “central brain” is required
  - Later the “brain” requests full operation

1. Wakeup from 10BASE-T1S
2. Forward to related PHY port and wakeup switch
3. Build up link and start communication
4. Wakeup MCU by switch on request



xBASE-T1
10BASE-T1S
CAN/LIN/other

SUMMARY AND CONCLUSIONS

- Zonal architectures bring new challenges – functions are spread over the network
- Partial sleep/standby scenarios are required for power savings
- Functional safety concepts must address mixed safety level of communication
- Functional safety concepts must consider part of the network not always being available
- System solutions will help addressing this challenge

SECURE CONNECTIONS
FOR A SMARTER WORLD