Vehicle Safety, beyond ISO and ASIL: How Ethernet networking components will enhance the safety of self-driving cars

- **Steffen Lorenz**, Principal Application Architect - NXP Automotive Ethernet Solutions
- **Claude R. Gauthier**, Director of Strategic Innovation - NXP Automotive Ethernet Solutions
- **Jochen Schyma**, Product Manager - NXP Automotive Ethernet Solutions

AGENDA

- Trends in EE architectures
- Functional safety today
- Functional safety in the robot-car era

Trends in EE Architectures

SECURE CONNECTIONS
FOR A SMARTER WORLD

Automotive Mega-Trends

Autonomous
Accident Free

Safe Transport

Optimized Routing

Driving Comfort

Electrification
Oil-Independent

Zero Emission

Service Oriented
User Defined

Entertainment

Security

Customization

MEGA TRENDS FORCE VEHICLE ARCHITECTURE TRANSFORMATION

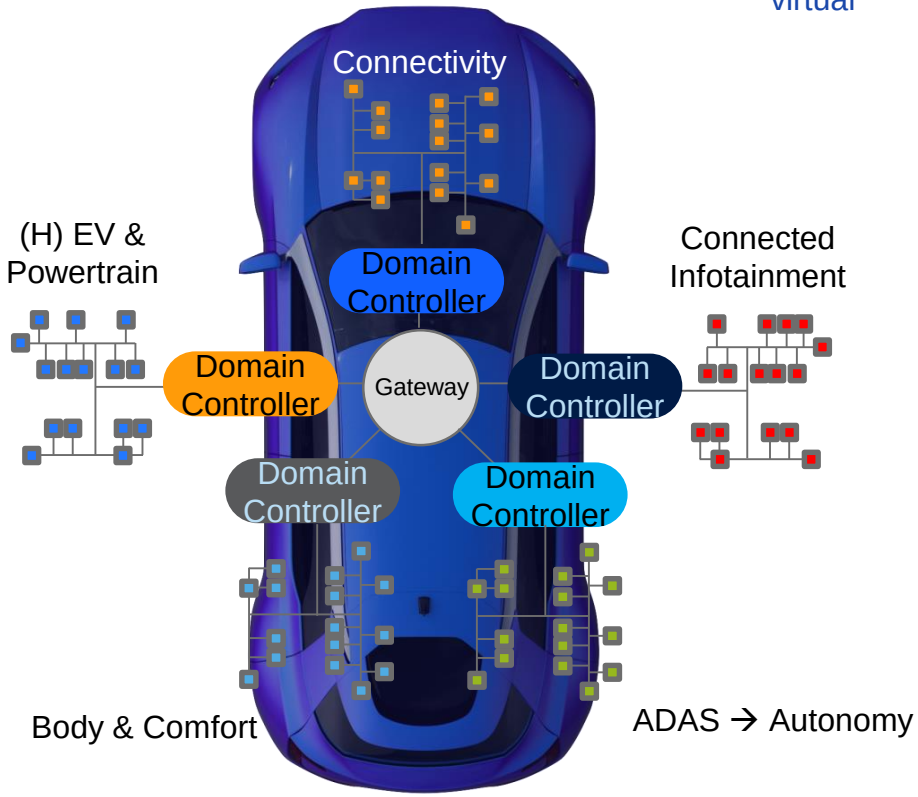
TODAY: FLAT

Low bandwidth, flat network
One MCU per application

UNFIT FOR FUTURE MOBILITY

Flat to hierarchical

TOMORROW: DOMAINS

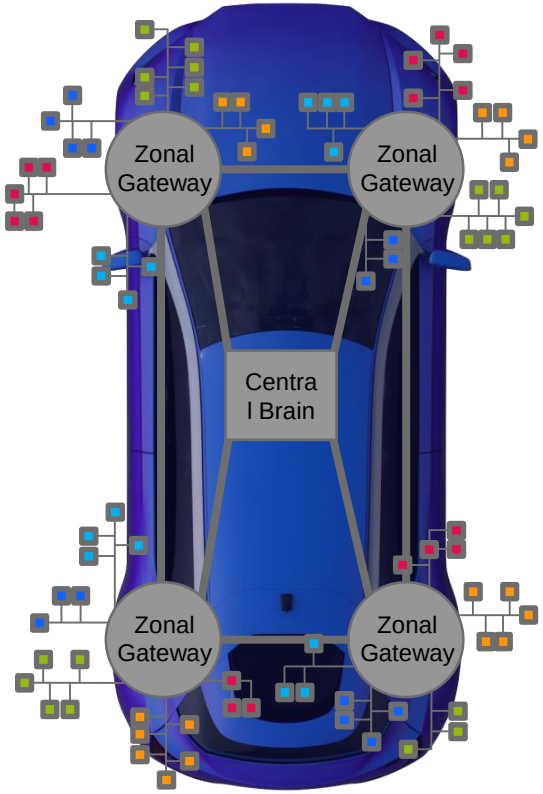


High bandwidth network
Gateway key to communication between domains

STEP TO AUTONOMOUS CAR

Wires go virtual

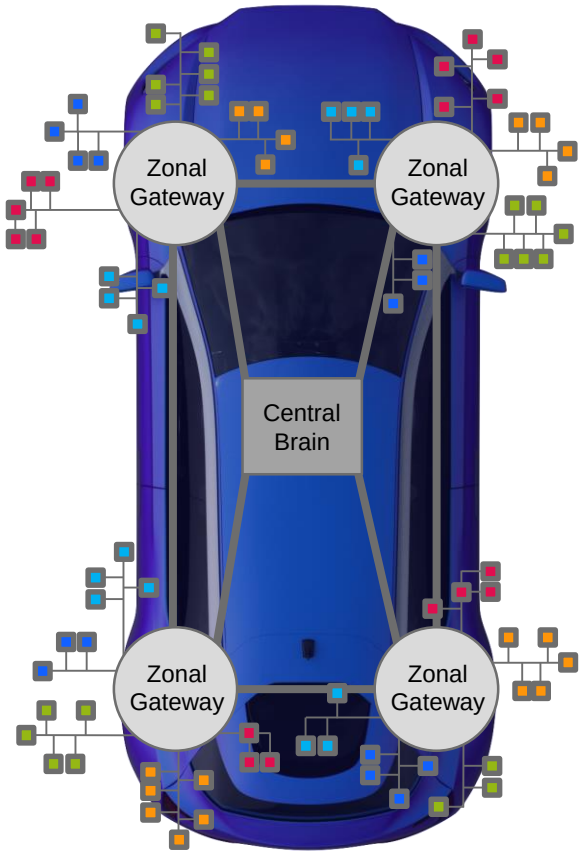
AFTER TOMORROW: ZONES

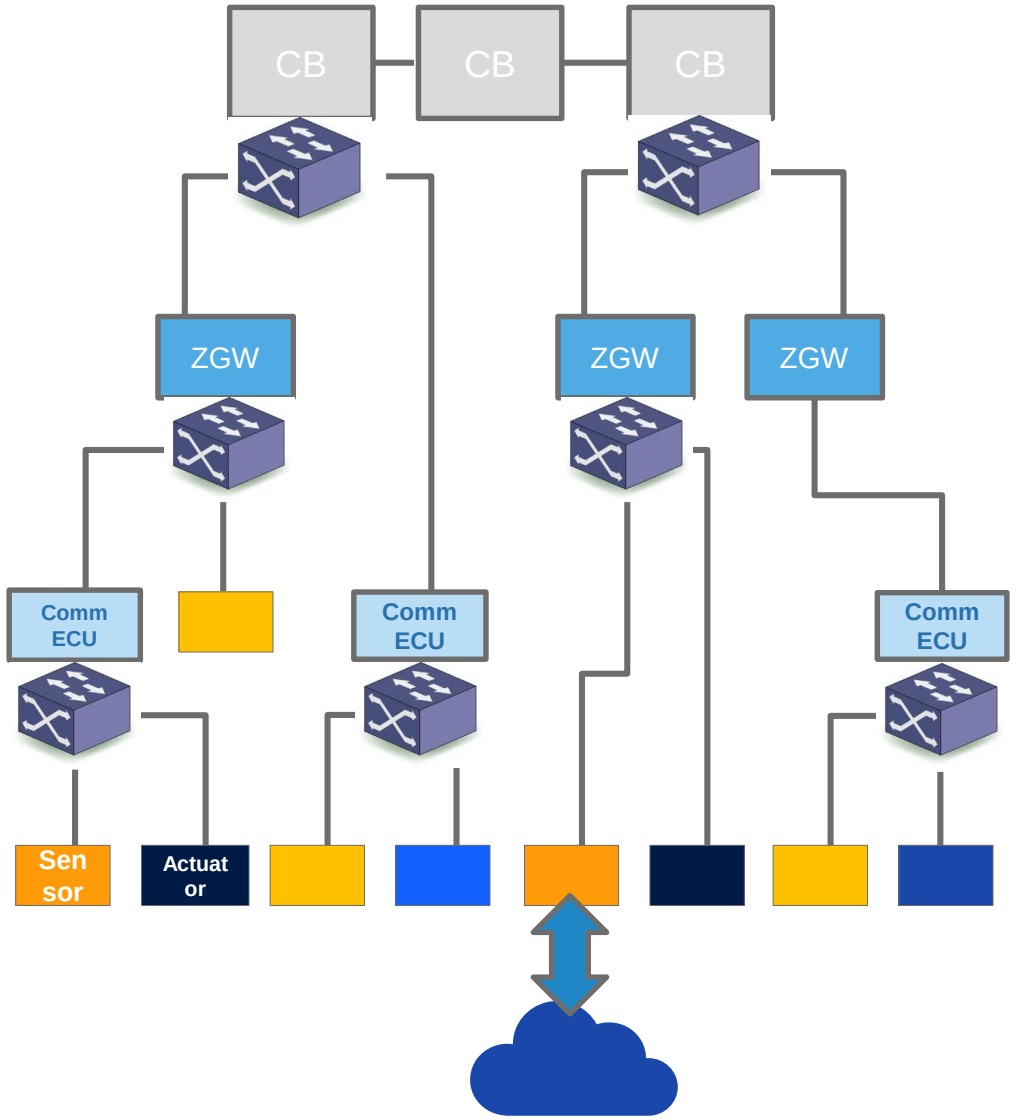


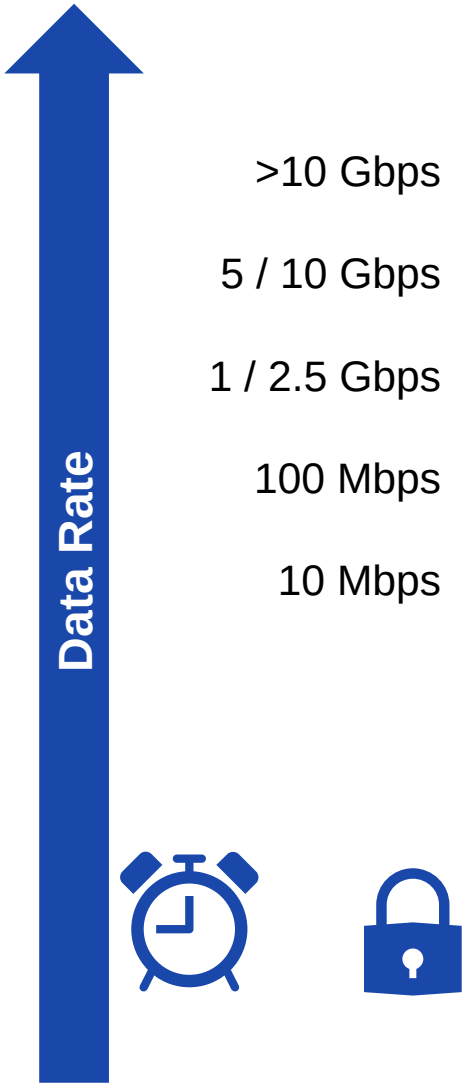
Domains virtualized by SW – enabling high flexibility
Easy enable/disable or update functions

STEP TO USER-DEFINED CAR

…TREND TO FULLY HIERARCHICAL ETHERNET NETWORK







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?

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

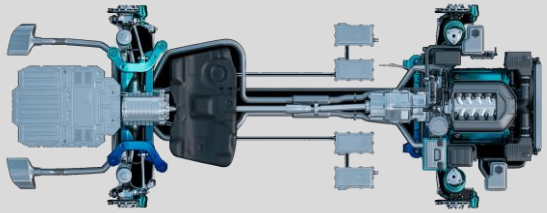
6

Functional Safety Today

SECURE CONNECTIONS
FOR A SMARTER WORLD

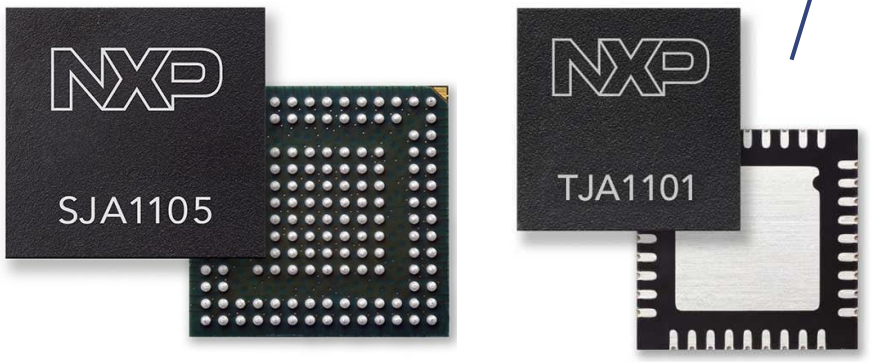
MAPPING OF FUNCTIONAL SAFETY REQUIREMENTS TO SEMICONDUCTORS

Contains functions with certain safety requirements (specific “context”):



Derived Functional Safety requirement: ???

In-Vehicle Networking products enable many different functions. Detailed information of the system requirements of the actual use cases are usually not available



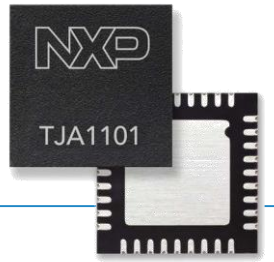
System definition → System safety concept → System safety analysis

OEM A, B, C…

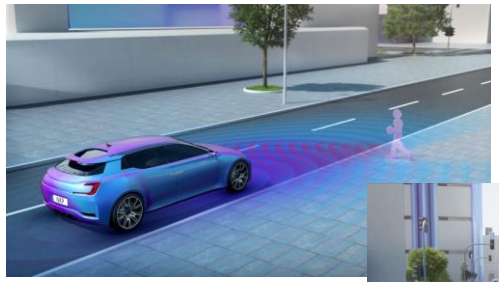
Map to semiconductor product safety concept (hardware, software)

Semiconductor Manufacturer A, B, C…

DEFINING SEMICONDUCTOR PRODUCTS AS “SAFETY ELEMENT OUT OF CONTEXT”



- **Assume** the use cases in the car (context)
- **Assume** safety goals

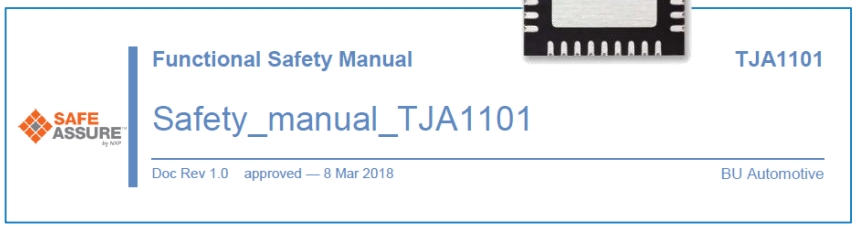


→ Assume the context, derive commonalities with relevance for In-Vehicle Networking

→ E.g. ADAS, like adaptive cruise control or parking assistant with multiple sensors, like radar and camera.

Assume the acceptable risk level per function

→ Define goal: ASIL A/B/C/D



Transfer the assumed system requirement into product requirements and identify the related functional blocks.

e.g. Which level of self diagnosis is required during operation and which part of the product is involved in diagnostics

INTEGRATION FLOW – FROM CHIP TO SYSTEM

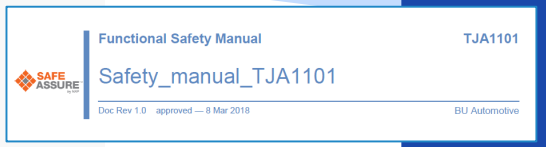
NXP adds safety features based on assumptions

Customer to match assumptions to real use case

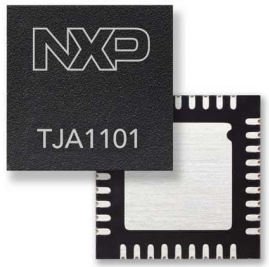
Matched! chip ASIL rating is valid when the assumptions are valid

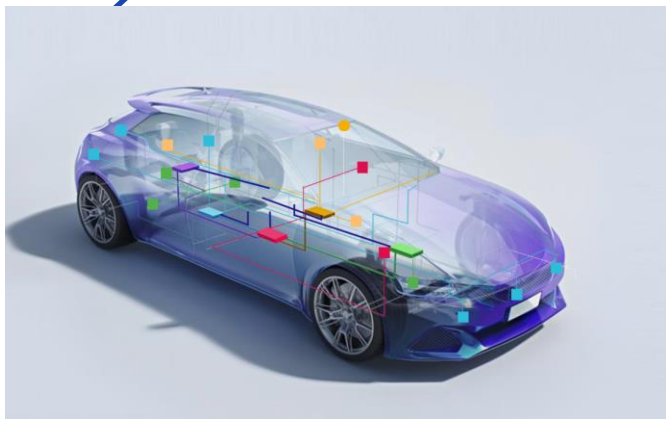
SEooC
Safety Element out of Context

Chip development follows ISO 26262 recommendations



System integration



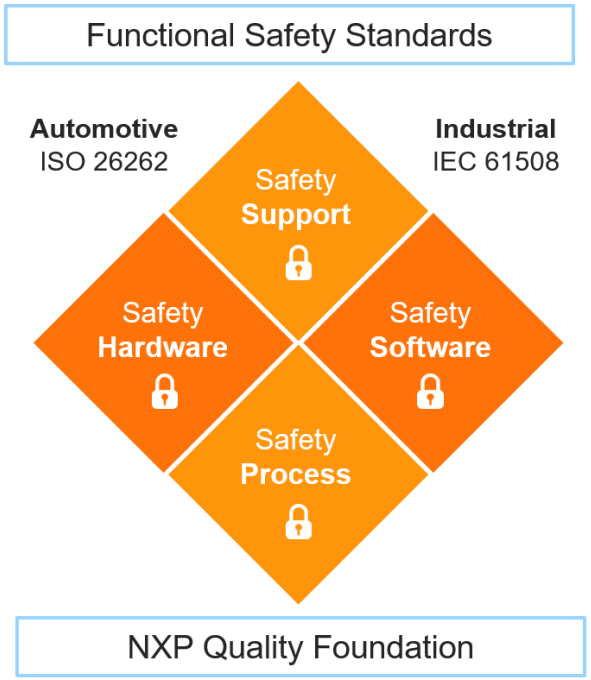


FUNCTIONAL SAFETY COMMITMENT
SAFEASSURE

The **SafeAssure** program →NXP's commitment to supporting functional safety through a safety-conscious culture, discipline and collaboration

- **Hardware**
  - Detect and mitigate random hardware failures using built-in safety features
  - Automotive Ethernet, MCUs, analog and power management ICs and sensors
- **Software**
  - Works seamlessly with hardware for system-level functional safety goals
- **Support**
  - Safety documents, Technical support
  - SafeAssure product-specific safety documents, upon request
- **Process**
  - ISO 26262 certified hardware development process

  → Preventing systematic failures



Design for Functional Safety goes far beyond the single product…

It requires a living culture and development process to enable the system advantage.

Functional Safety in The Robot-Car Era

SECURE CONNECTIONS FOR A SMARTER WORLD

END-TO-END FUSA IMPLEMENTATION EXAMPLE UP TO AD LEVEL 2

Data tagged at origin;
e.g. CRC, counter, time stamp, water mark, “watch dog” / sign of life signal

Data complete, correct / as expected, current, on time?
Take appropriate action!

Inform or warn the driver

Sensor ECU

Fusion ECU

Instrument Cluster ECU

Failure! Sensor defect, image frozen!
→ Data transferred correctly
→ Content not changing over time

→ Continue normal operation

→ Assess criticality, take action → Initiate fail safe or fail operational process, inform driver

HOW IS AUTONOMOUS DRIVING CHANGING THE GAME?

	FAILURE IDENTIFIED	REACTION TO FAILURE	SAFE STATE
Level 1/2	Machine informs driver	Driver takes control	Manual drive of the car
Level 3+	Machine evaluates actions	Machine executes transition into safe state	Car stops

Functional Safety has now direct impact on **availability** of the vehicle services

HOW THE NETWORKING IC KEEPS YOUR ROBO-CAR DRIVING?

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

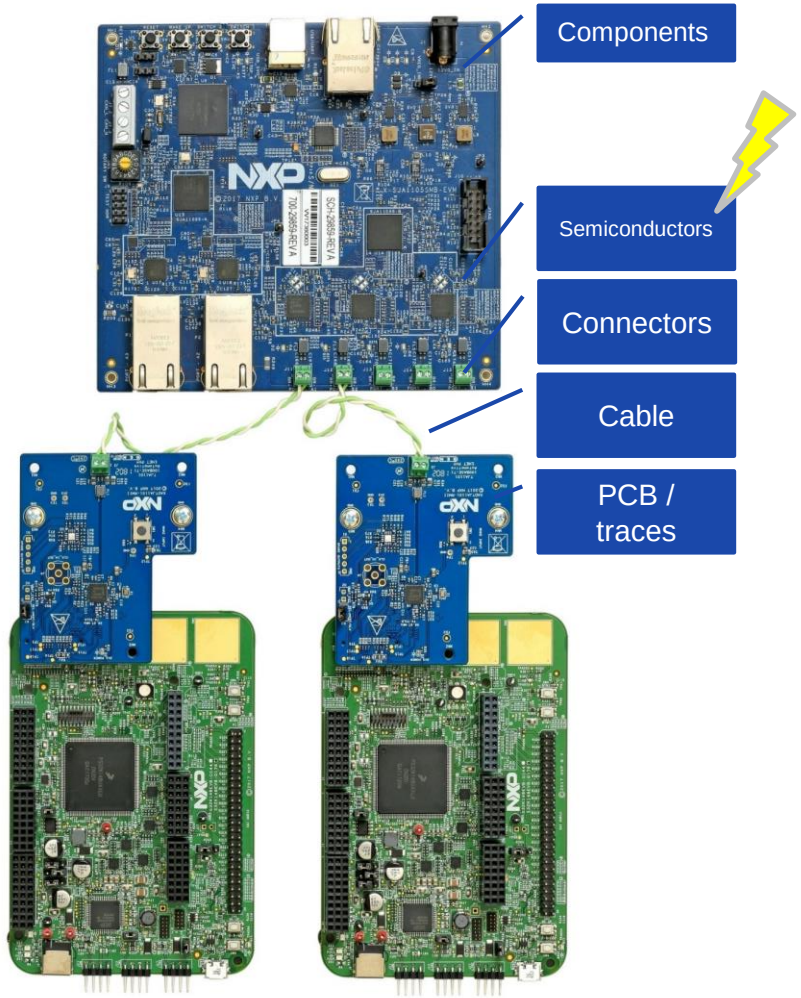
- Prevent Failure
  - Highest reliability

- Predict Failure
  - (Self-)Diagnostic features

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

FTTI: Fault tolerant time interval

FAILURE PREVENTION - RELATION BETWEEN AVAILABILITY AND RELIABILITY



- Availability of communication is determined by the reliability of components in the signal path
- Total FIT = SUM (Component FIT)
- FIT (Failure In Time)
  - describes the probability that a component fails, i.e. random HW failure
  - Initially estimated based on technology parameters for future products (e.g. SN29500)
- Manufacturing quality directly impacts the FIT rate and probability of failure

MEASURE OF FAILURE PREVENTION
FROM FAILURE RATE TO SAFETY METRICS

Calculate
HW failure rate (FIT)

SafeAssure — FMEDA

FMEDA calculates the **Safety Metrics** required by ISO26262

SPFM
LFM
PMHF

Compare
with standard [ISO-26262, part 5]

ASIL	SPFM	LFM	PMHF
B	≥ 90 %	≥ 60 %	< 10^{-7} h^{-1}
C	≥ 97 %	≥ 80 %	< 10^{-7} h^{-1}
D	≥ 99 %	≥ 90 %	< 10^{-8} h^{-1}

FMEDA: Failure Mode Effects and Diagnostic Analysis

LFM: Latent Fault Metric

PMHF: Probabilistic Metric for (Random) Hardware Failures

SPFM: Single Point Fault Metric

Example Reference FIT calculation

For Tjv / CL parameter details, please contact NXP

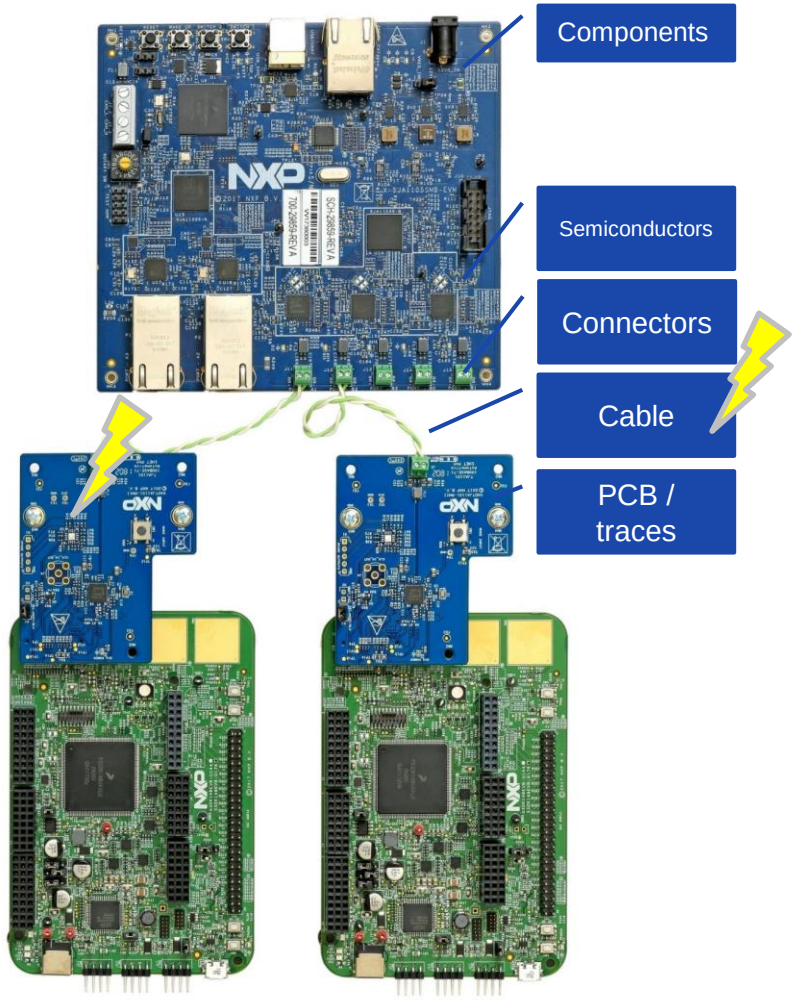
TJA1043U	Siemens Norm SN29500	HTOL Qual CAN Family	Production & Field Return Data CAN Family
Reference FIT calculation	42 FIT	3.0 FIT	0.04 FIT

Manufacturing quality makes the difference

- NXP applies screening & continuous improvement of screening methodology based on production and field return data
- The methodology is independent of process technology

HTOL: High-Temperature Over Life

RELATION BETWEEN AVAILABILITY, PREDICTION AND REACTION

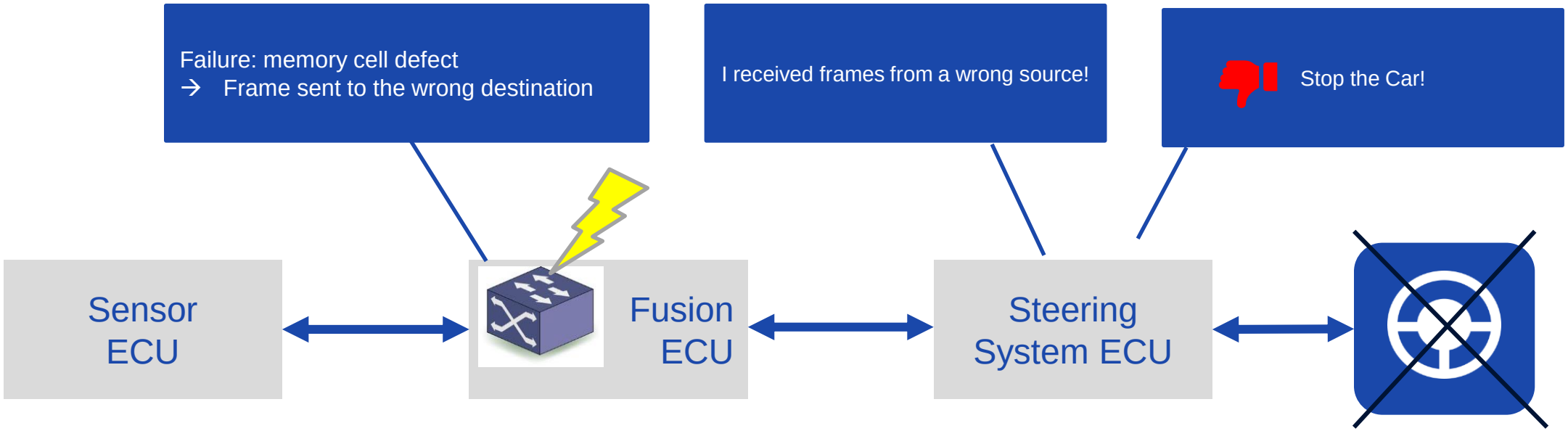


- Failure may occur anywhere in the communication chain, e.g. cable degradation or weak PCB solder connections

- Availability of communication is further determined by
  - The time it takes to detect (localize / categorize) issues
  - The ability to respond depending on the criticality of issues

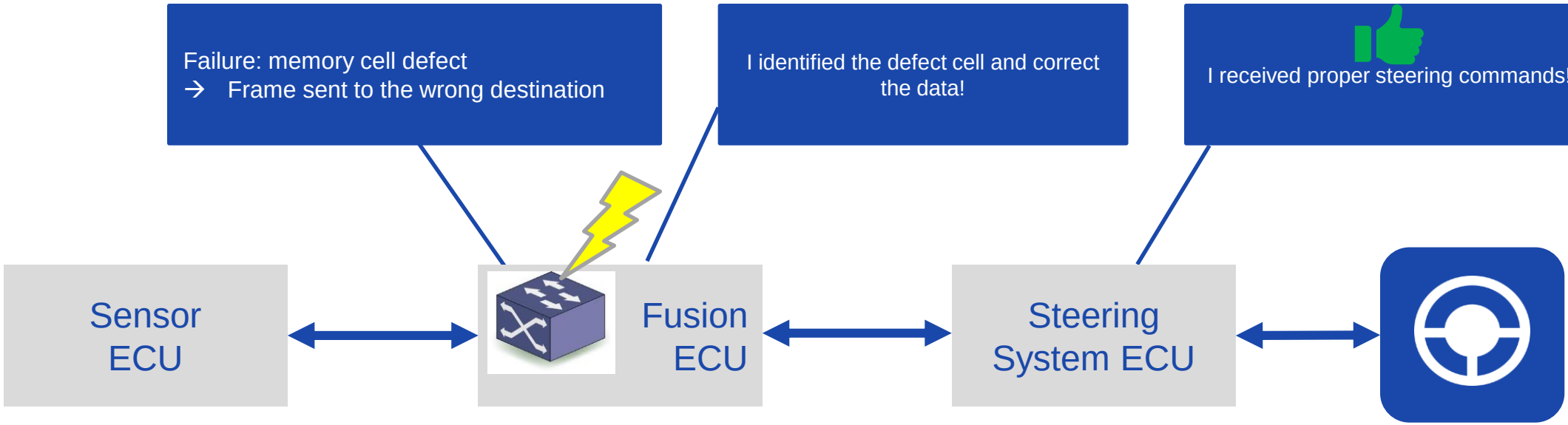
- Examples of FuSa features on IC level
  - Predict:
    - Temperature / Voltage Monitoring
    - Signal Quality Indicator
  - React:
    - Memory Failure Correction (ECC)
    - IEEE 802.1CB (Stream replication / elimination)

FROM E2E PROTECTION TO HIGHLY AVAILABLE COMMUNICATION PATH EXAMPLE: ECC



- Solution 1) Detected by end2end FuSa implementation!
  → system decision: trigger safe state → stop the car!

FROM E2E PROTECTION TO HIGHLY AVAILABLE COMMUNICATION PATH EXAMPLE: ECC



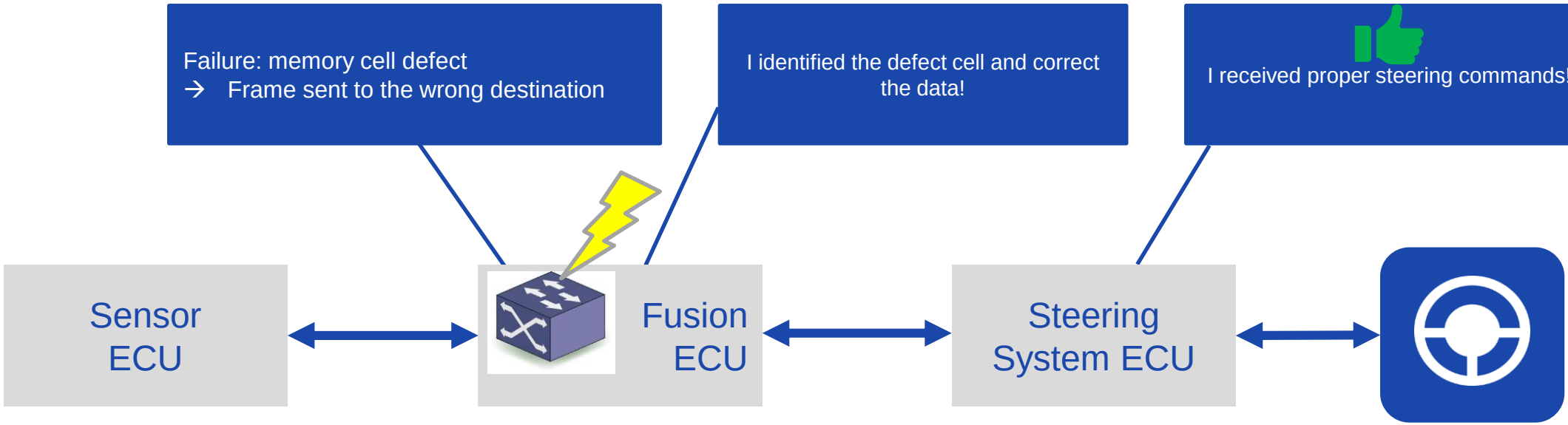
- Solutions 2) Handled by highly available system:
  - Local detection and correction
  - ECC: defective memory cell detected by the switch itself
  - Action triggered by the switch: report and / or repair!

  → System decision: → continue normal operation!

    → Request further data for evaluation

    → Trigger service stop & ECU exchange

FROM E2E PROTECTION TO HIGHLY AVAILABLE COMMUNICATION PATH EXAMPLE: ECC

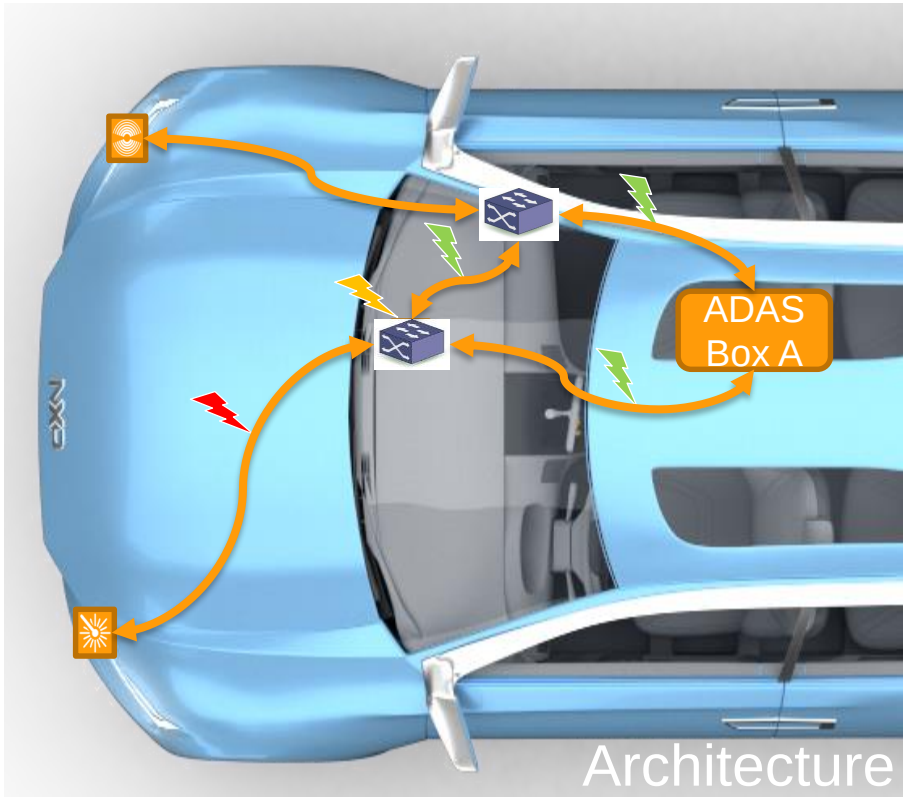


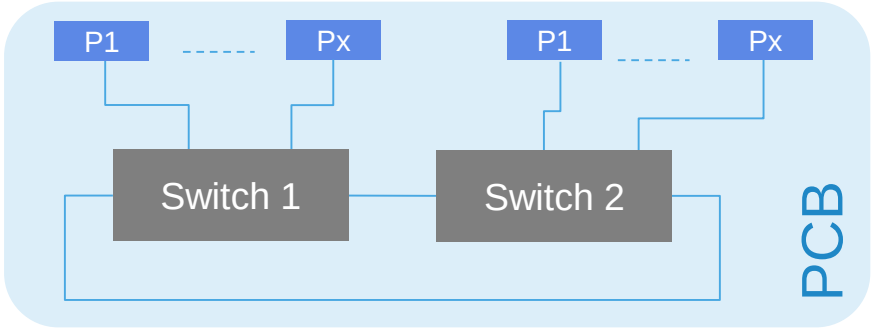
- Solutions 2) Handled by highly available system:
  - Local detection and correction
  - ECC: defective memory cell detected by the switch itself
  - Action triggered by the switch: report and / or repair!
  - → System decision: → continue normal operation!
    - → Request further data for evaluation
    - → Trigger service stop & ECU exchange

- Both system solutions achieve the same ASIL!
- Only the highly available system is enhanced by local detection / correction, plus the availability of information to the system level for more fine grain resolution of action
- In a redundant system, a part of the system may even be restarted during operation

ENABLE TO REACT: REPLICATION & ELIMINATION FEATURE (802.1CB)

- Create redundant data paths within the network
- Typically a part of network and data flow will be replicated
- Increases the availability of safety critical communication
  - Redundancy coverage determined by considered failures
    - e.g. cable failures, link interruption, switch failures, …
    - Does not cover all failures, e.g. power supply loss.
- Prevents entering a safe state on transient faults (e.g. link down)
- Can be combined with full redundant system
- Integral part of network architecture
- Same concept on PCB level possible

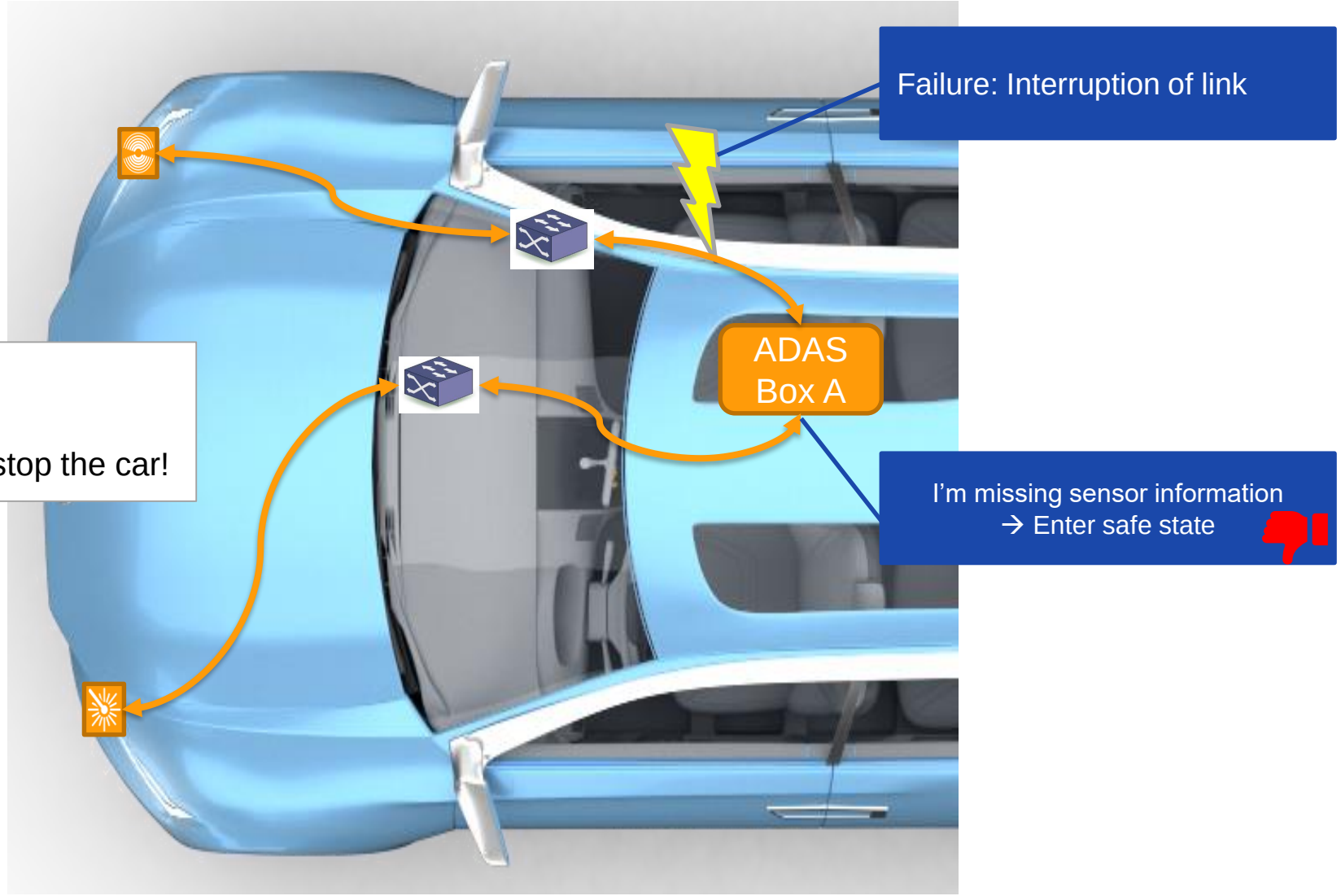




EXAMPLE: W/O REPLICATION & ELIMINATION FEATURE (802.1CB)

Solution 1) Detected by end2end FuSa implementation!

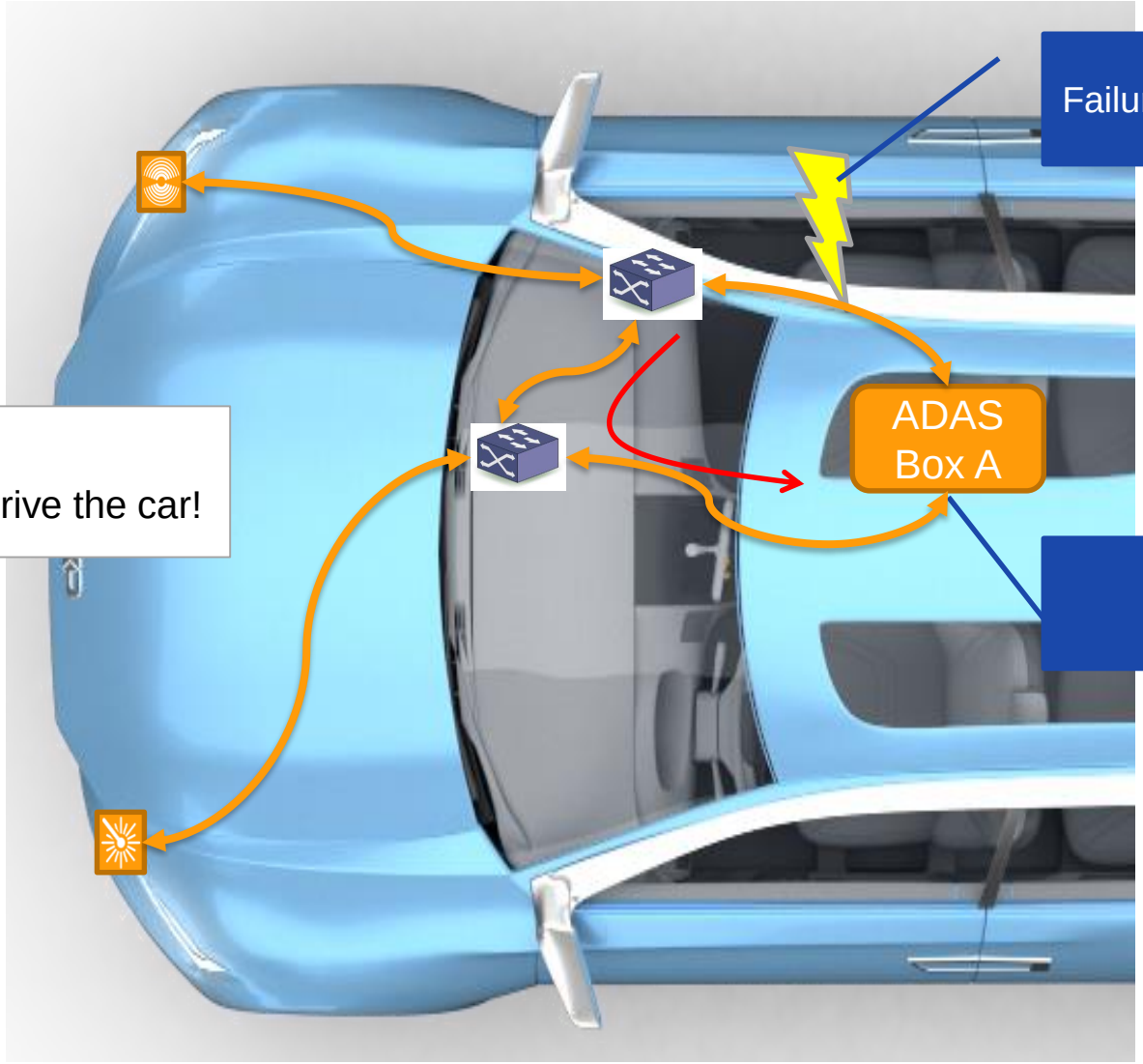
→ system decision: trigger safe state → stop the car!



EXAMPLE: WITH REPLICATION & ELIMINATION FEATURE (802.1CB)

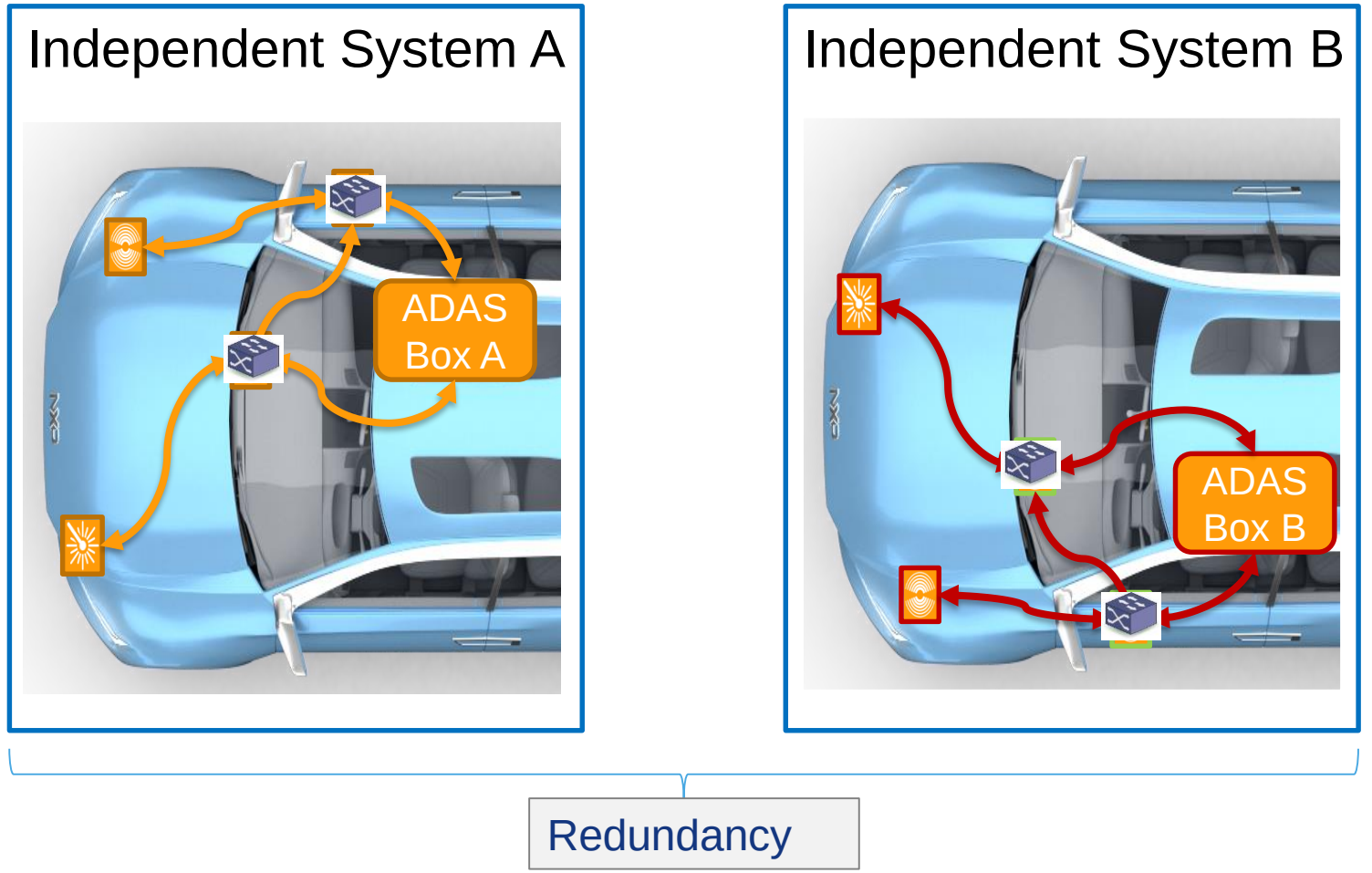
Solution 2) Using 802.1CB

→ system decision: continue operation → drive the car!



EXAMPLE: REPLICATION & ELIMINATION FEATURE (802.1CB)

Increased availability in each system by 802.1CB



CB for enhanced system availability, not for full system redundancy.

CONCLUSION

- Chip ASIL ratings are valid when the assumptions match the use case!
- Cars are safe today, future cars remain safe
- Vehicle availability (customer experience) can be enhanced
- Networking IC features can increase the vehicle availability by preventing, predicting and reacting to failure scenarios
- Manufacturing quality and development process are the basis for highly available systems
- NXP is a unique partner to co-define and realize safety & availability concepts for
  - Predictive Maintenance
  - Fail operational networks

SECURE CONNECTIONS
FOR A SMARTER WORLD