FUSA AND ETHERNET HOW TO APPLY FUNCTIONAL SAFETY FEATURES TO SYSTEM USE CASES

Peng Liu
Senior Marketing Manager

AUG 2023

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

AGENDA

- Vehicle architecture transformation
- Functional Safety Introduction
- Functional Safety on Ethernet Products
- System Impact
- Summary and Conclusion

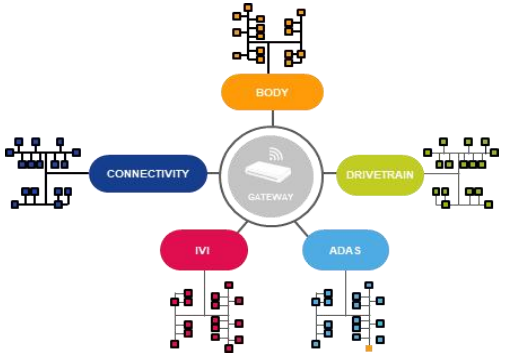
Vehicle architecture transformation

SECURE CONNECTIONS
FOR A SMARTER WORLD

EVOLUTION TOWARDS FULL ZONAL PLATFORMS → THE FOUNDATION FOR SDV

2022
Domain Platforms

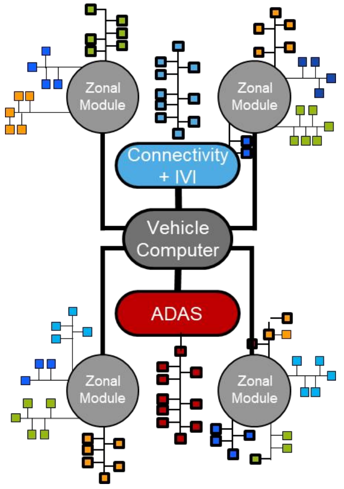
Logical Domains



Simplify HW
Create central
service area

2025+
Hybrid Zonal Platforms

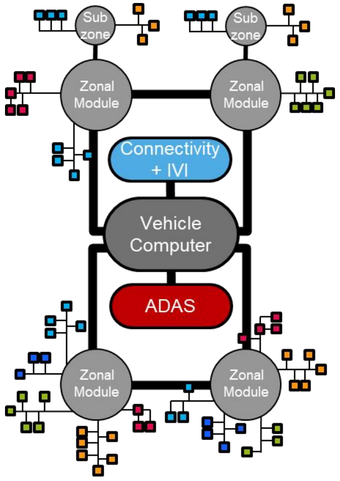
Body Domain Zone Clustering



High ECU aggregation
All functions
are services

2030+
Full Zonal Platforms

Multi-domain Zone Clustering



TWO PARALLEL ARCHITECTURAL CHANGES

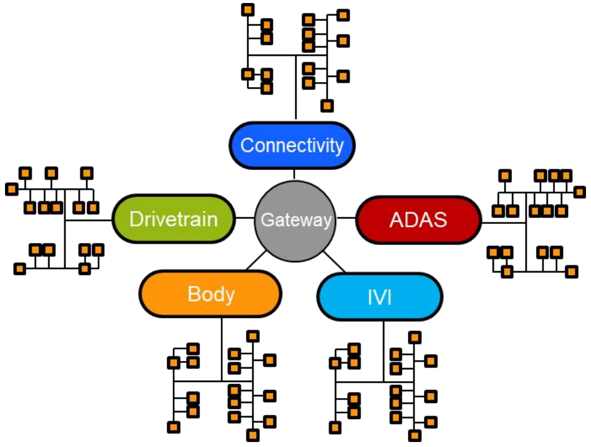
Logical transformation: 1
Scalable and centralized software development

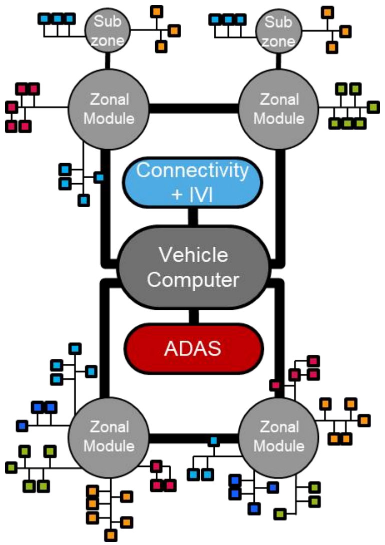
- First step toward software-defined vehicle
- More isolation for improved security
- Centralized over-the-air (OTA) update for software upgrades

Physical transformation: 2
Zonal aggregation and ECU clustering

- Dramatically reduced material and manufacturing cost
- Eases E/E upgrades and scalability
- Creates a central IP-based area for SOA

NEW VEHICLE ARCHITECTURES DEFINE NEW REQUIREMENTS FOR THE ETHERNET NETWORK





10B-T1S 100B-T1 1000B-T1 2.5GB-T1 10GB-T1 SerDes

Low

Mid
Switches

High

Several OEM challenges in the next decade

- Keep networks efficient and affordable
- Install scalable, robust Ethernet networks
  From 10 Mb to 10 Gb
- Engineer complex, mixed criticality traffic
- Transition video (sensor, display) to Ethernet network
- Enable 10 Mb bus, bring IP to the edge
  On-ramp CAN/LIN to Ethernet
- Guarantee safety & security at architecture level

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

Functional Safety Introduction

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

ISO 26262 – THE SCIENCE OF QUANTIFYING RISK

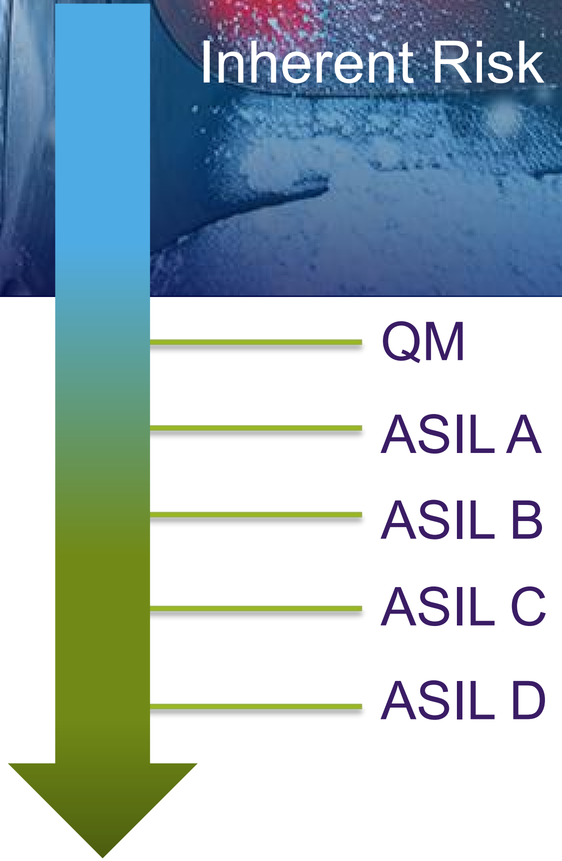
Severity Exposure Controllability → ASIL Automotive Safety Integrity Level

Severity: How much harm is done?

Exposure: How often is it likely to happen?

Controllability: Can the hazard be controlled?

ISO 26262, part 1:
“Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems”



Inherent Risk

QM

ASIL A

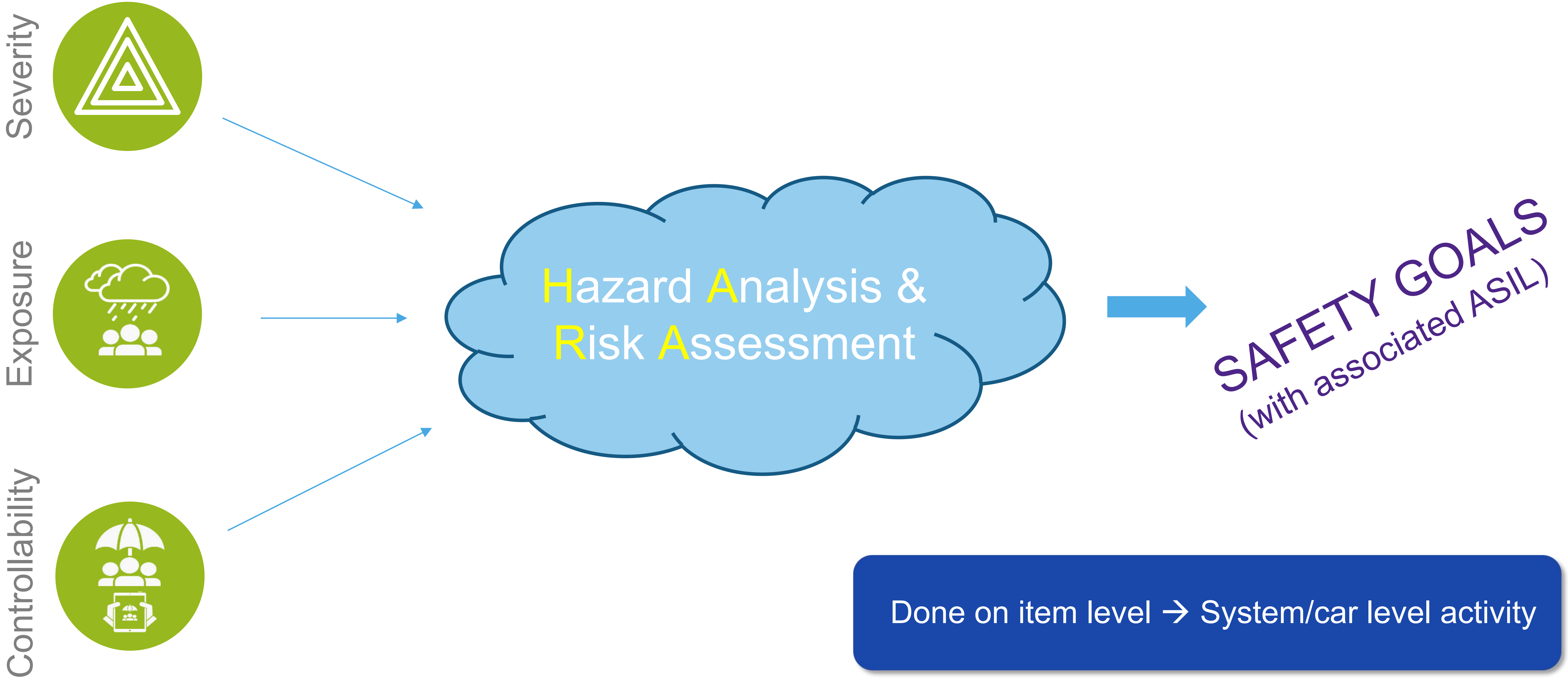
ASIL B

ASIL C

ASIL D

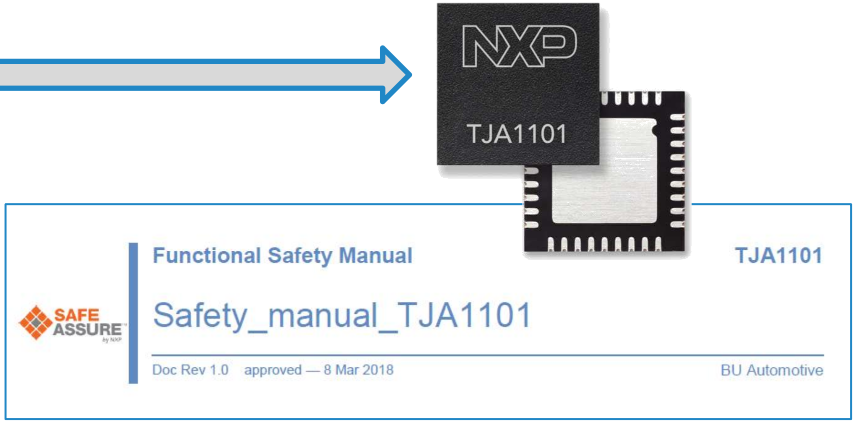
Reduce risk to an acceptable level

SAFETY - THE AUTOMOTIVE FRAMEWORK



Done on item level → System/car level activity

DEFINING SEMICONDUCTOR PRODUCTS AS “SAFETY ELEMENT OUT OF CONTEXT”

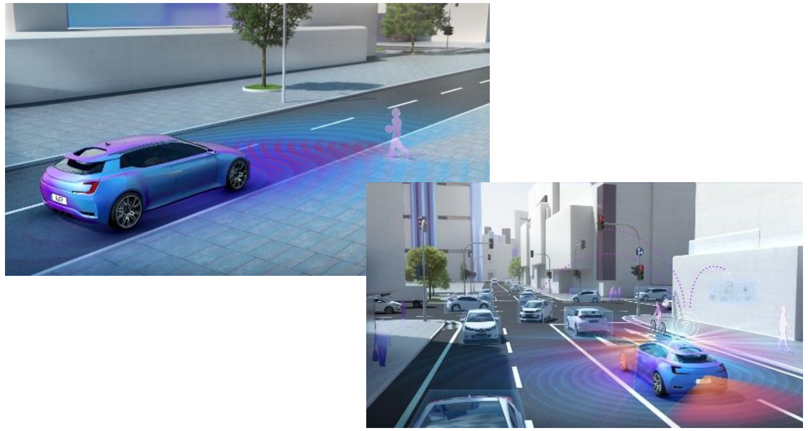

NXP
TJA1101
SAFE ASSURE

Functional Safety Manual TJA1101

Safety_manual_TJA1101

Doc Rev 1.0 approved — 8 Mar 2018 BU Automotive

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



Assume the acceptable risk level per function

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

→ 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.

→ Define goal: ASIL A/B/C/D

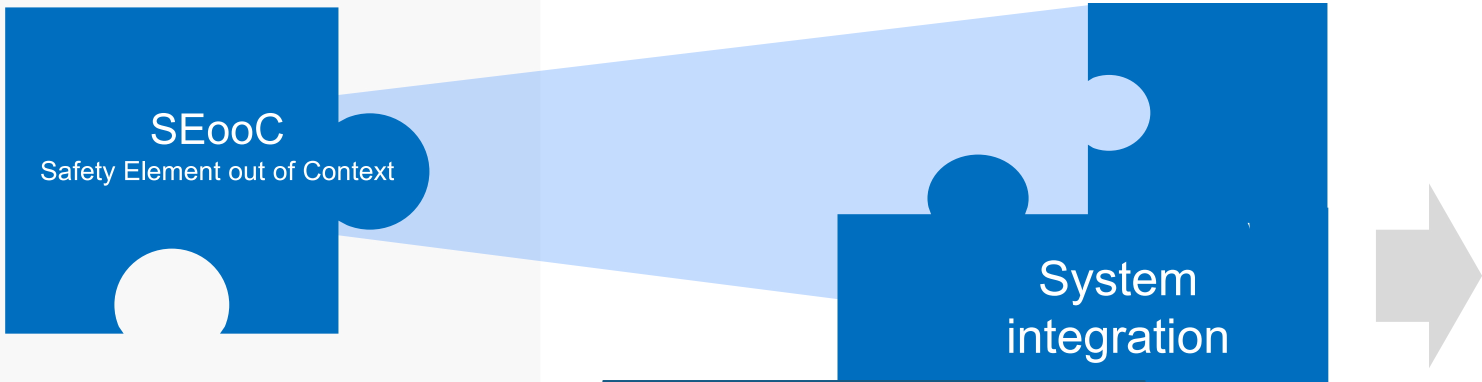
e.g. Which level of self diagnosis is required during operation and which part of the product is involved in diagnostics

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!

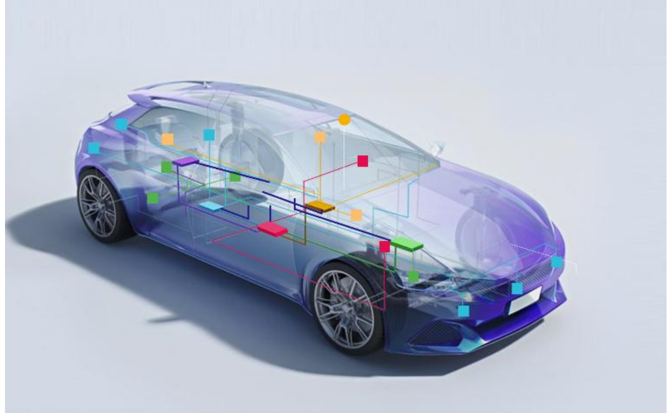


Chip development follows ISO 26262 recommendations

15.08 TJA1103 Safety Manual

TJA1103 Safety Manual

Rev. 0.5.1 — 7 Sept 2021 User manual



LATENT FAULTS

- If a safety mechanism is not working, the related fault gets uncovered
- It is a multiple-fault, but occurrence of two failures could be spread over long time
  - Probability of two independent faults happening at similar time is low
  - Much higher when no time constraint
- This creates a latent fault
- To prevent this, on regular base (e.g., startup) the safety mechanism is proven to work, e.g.
  - BIST
  - Functional check
- Contributes to the Latent fault metric

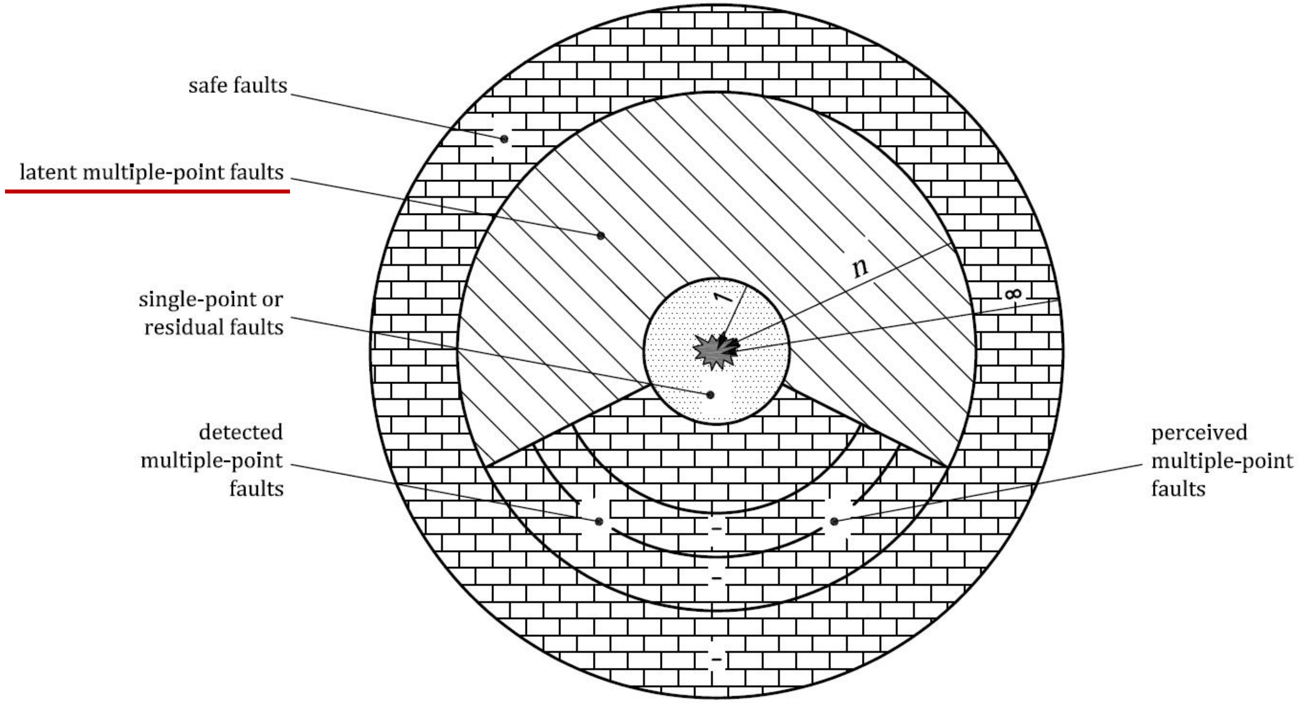
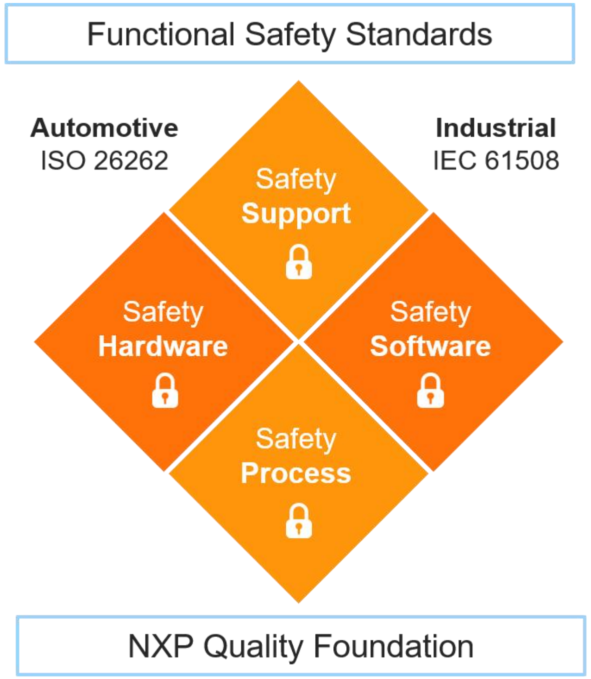

safe faults
latent multiple-point faults
single-point or residual faults
detected multiple-point faults
perceived multiple-point faults
n

Figure C.1 — Fault classification of safety-related hardware elements of an item

Source: ISO26262-5:2018

ETHERNET PRODUCTS BENEFIT FROM NXP'S SAFE ASSURE PROGRAM

- Launched in 2011, the NXP SafeAssure program aligns our development process to ISO 26262 across our businesses.
- The program is our corporate commitment to supporting functional safety through a safety-conscious culture, discipline and collaboration. It also:
  - Simplifies the process of system compliance, with solutions designed to address the requirements of automotive and industrial functional safety standards
  - Reduces the time and complexity required to develop safety systems that comply with ISO 26262 and IEC 61508 standards
  - Supports the most stringent safety integrity levels (SILs), helping designers to build with confidence
  - Adheres to a zero-defect methodology from design to manufacturing to help ensure our products meet the stringent demands of safety applications



Design for Functional Safety goes far beyond the single product.

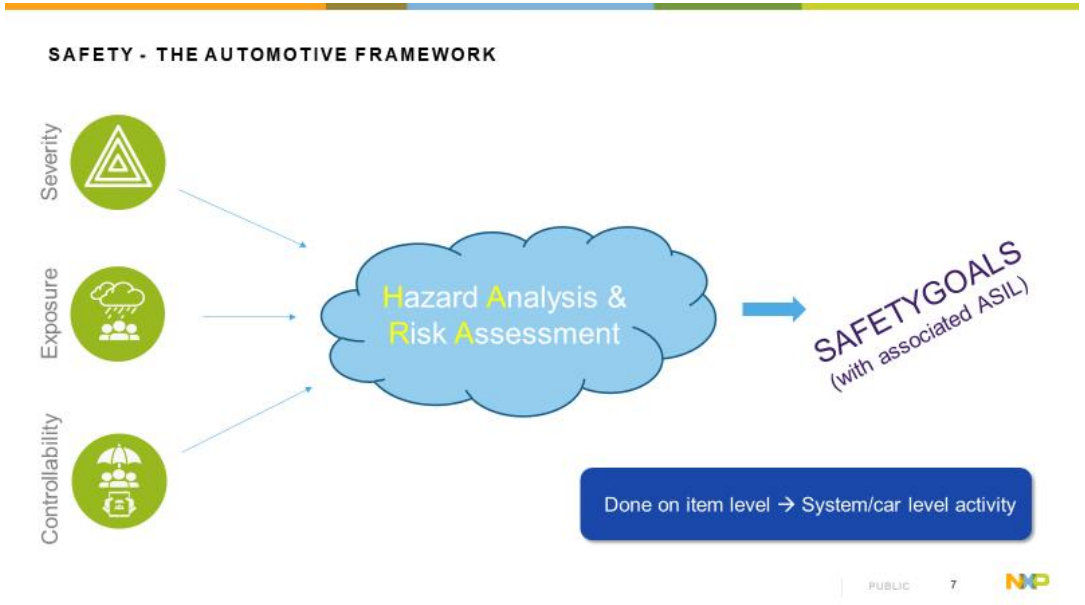
It requires a living culture and development process to enable the system advantage.

Functional Safety on Ethernet Products

SECURE CONNECTIONS
FOR A SMARTER WORLD

FUNCTIONAL SAFETY

- HARA done on item level
- Requirements assigned in safety concept to ensure safety goals
- Inherited to lower-level sub-system/components
- Typically relevant on Ethernet communication link
  - Unintended frame/data insertion
  - Unintended frame corruption
  - Undetected frame loss
  - Unintended frame delay, repetition or sequencing

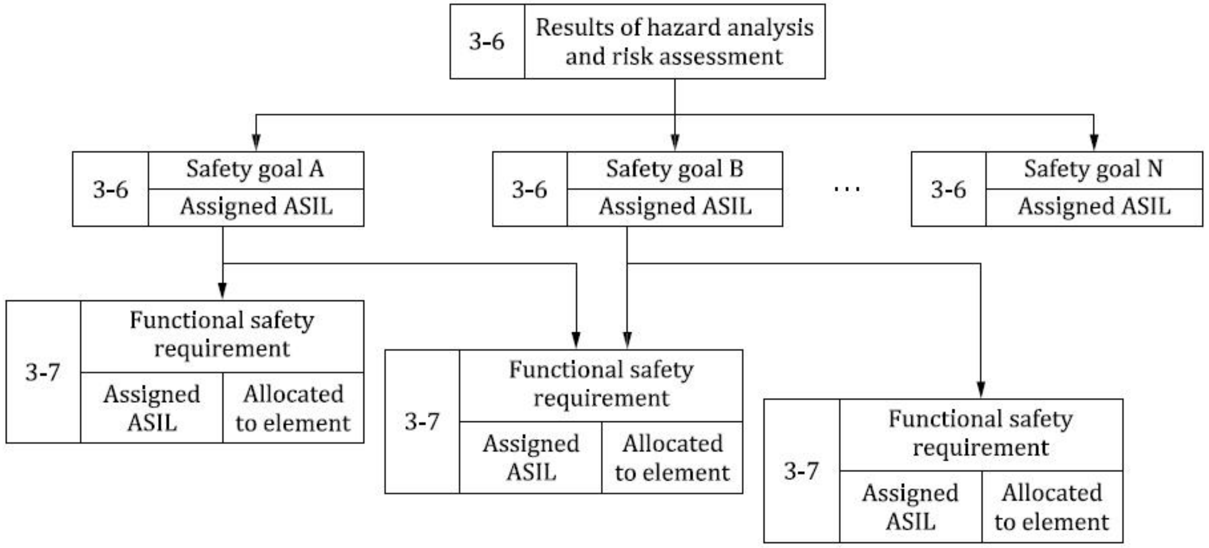


SAFETY - THE AUTOMOTIVE FRAMEWORK

Severity
Exposure
Controllability
Hazard Analysis & Risk Assessment
SAFETYGOALS (with associated ASIL)

Done on item level → System/car level activity

PUBLIC 7



Source: ISO26262-3:2018

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

- High reliability
- Freedom from interference

Predict Failure

- (Self-)Diagnostic features

React to Failure

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

HOW THE NETWORKING IC BRINGS SAFETY TO THE ZONE

Prevent Failure

- Manufacturing quality makes the difference
- Policing / access control
- Configuration monitoring
- Ensuring data integrity

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)
- Drop corrupted frames
- Entering safe state (for sub-system)

Example Reference FIT calculation

For Tjv / CL parameter details, please contact NXP

TJA1043U	Siemens Norm SN92500	HTOL Qual CAN Family	Production & Field Return Data CAN Family
Reference FIT calculation	42 FIT	3.0 FIT	0.04 FIT

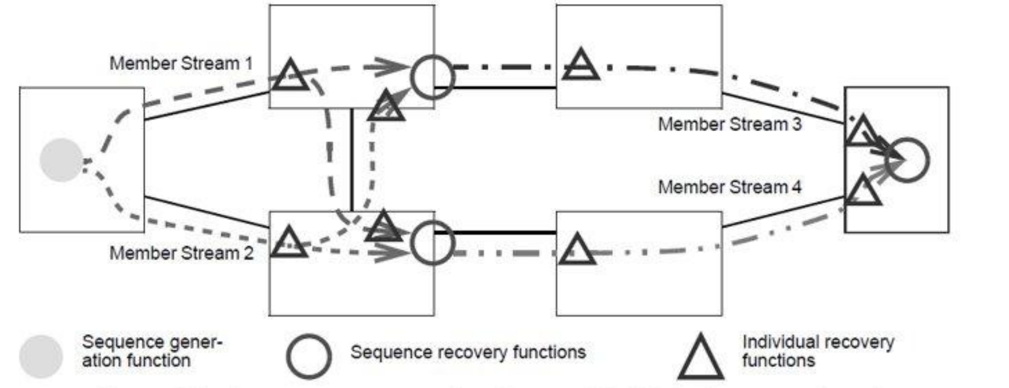
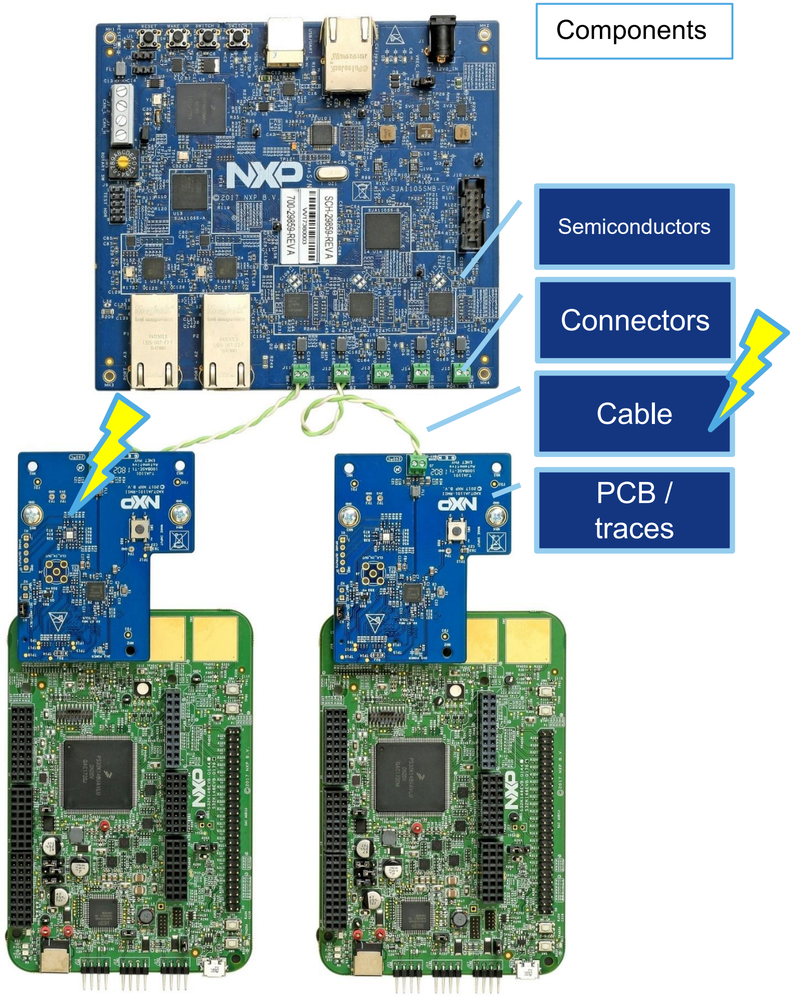

Member Stream 1
Member Stream 2
Member Stream 3
Member Stream 4
Sequence generation function
Sequence recovery functions
Individual recovery functions

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

RELATION BETWEEN AVAILABILITY, PREDICTION AND REACTION



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

- 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
    - Error counter
  - React:
    - Memory Failure Correction (ECC)
    - Faulty frame detection
    - 802.1CB (Replication & Elimination)

System Impact

Examples How It Helps

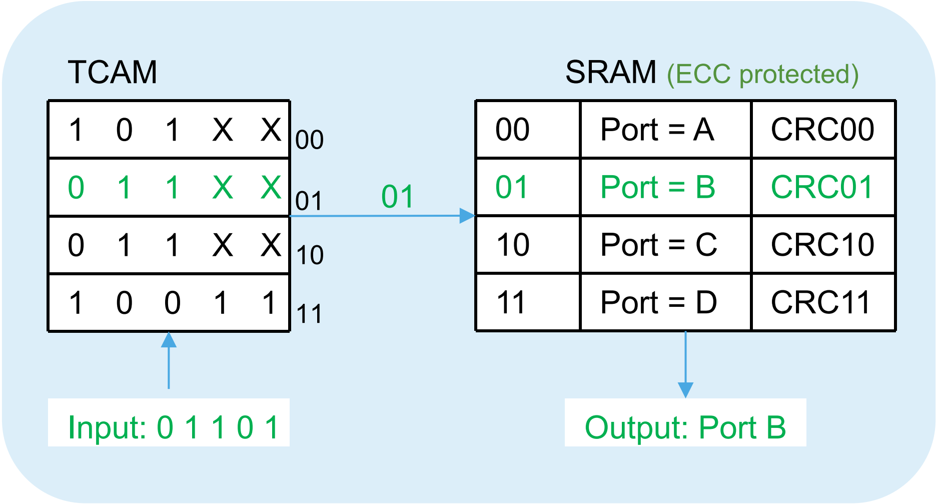
SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

SYSTEM ASPECTS – CONFIGURATION PROTECTION

- Protection of the switching table ensures proper forwarding
  - Including TCAM rules
- Modification in the switching information will be detected
  - Configuration can be corrected to ensure proper operation again
- Prevents ports from being over-loaded
  - No incorrect forwarding into other ports
- System misbehavior can be detected early (e.g., counter on dropped frames)
  - Allows for corrective actions, e.g., switch off certain port to protect ongoing communication for remaining network

Example indirect TCAM protection



TCAM

1	0	1	X	X	00
0	1	1	X	X	01
0	1	1	X	X	10
1	0	0	1	1	11

SRAM (ECC protected)

00	Port = A	CRC00
01	Port = B	CRC01
10	Port = C	CRC10
11	Port = D	CRC11

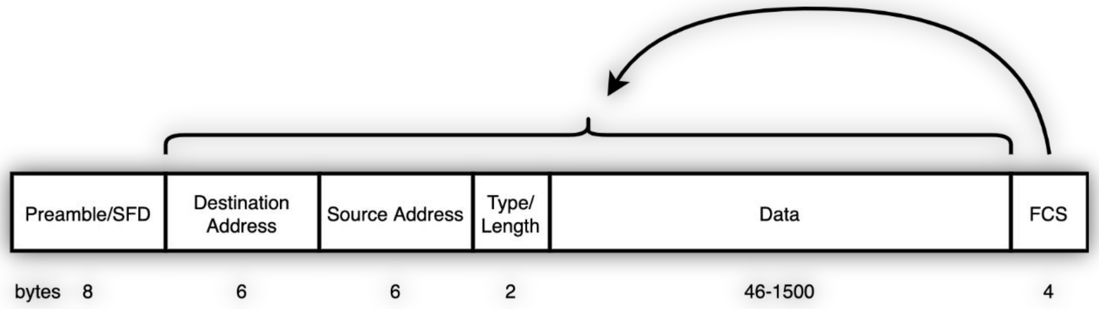
On E2E protection, only the consequence of the failure (missing frames) can only be detected.
No possibility to correct, as location of fault is unknown.

SYSTEM ASPECTS – DATA CORRECTNESS

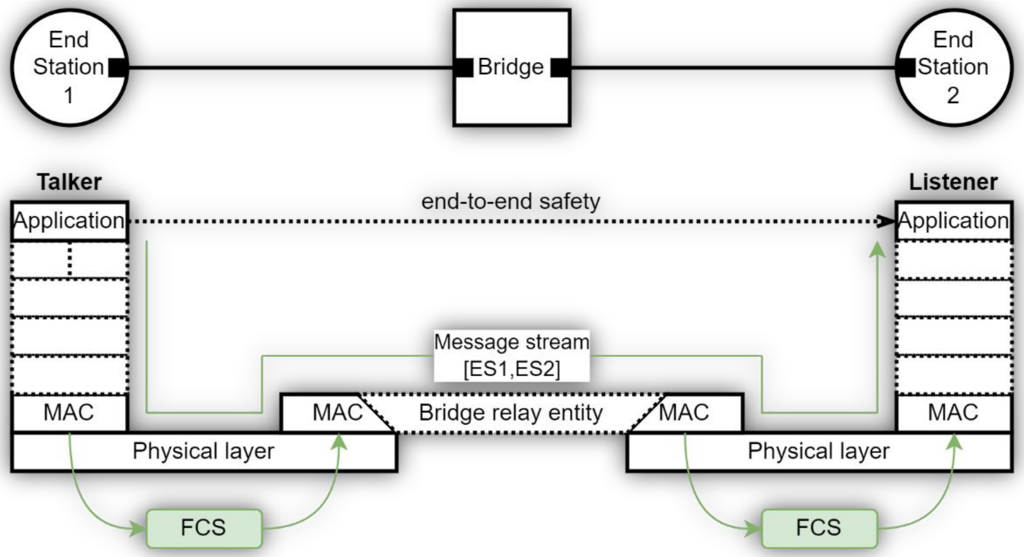
- All means of protecting data correctness (e.g., ECC for memory fault correction, low soft error probability, …) will help to ensure correct data at the receiver
  - System benefits from low data loss
- All means of detecting corrupted data and drop corrupted frames, make sure that
  - incorrect messages are not mistakenly used
  - incorrect frames do not interfere with ongoing traffic
  - the system is notified to take corrective action
- All means to detect a malfunction of the device or operation conditions (e.g., over temperature, under voltage), brings the device in a safe state to prevent messages getting corrupted

SYSTEM ASPECTS – FCS ESCAPE

- Ethernet Frame is FCS protected (CRC checksum)
  - Protection of Data as well as addresses
- Several entities in the chain may modify the FCS, e.g.
  - Re-tagging in the switch
  - MACsec
- Risk of FCS escape
  - Data or address may get corrupted between FCS removal/re-calculation
  - This would result in corrupted frame with valid FCS
  - Such frame will not be dropped by receiving MAC
- Our ASIL B Switch/PHY devices prevent FCS escapes

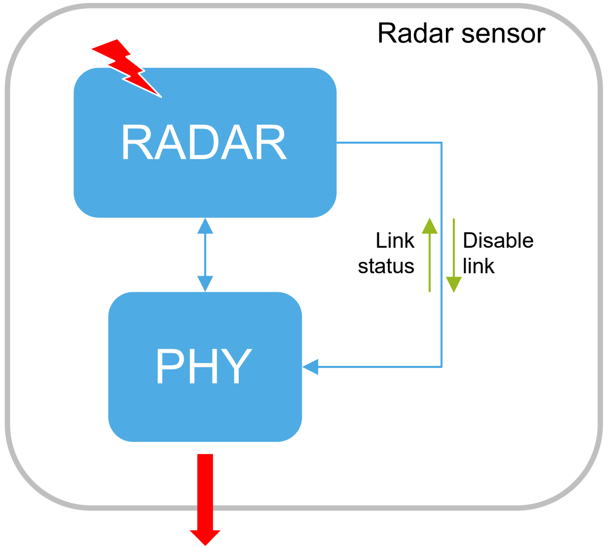


	Preamble/SFD	Destination Address	Source Address	Type/ Length	Data	FCS
bytes	8	6	6	2	46-1500	4



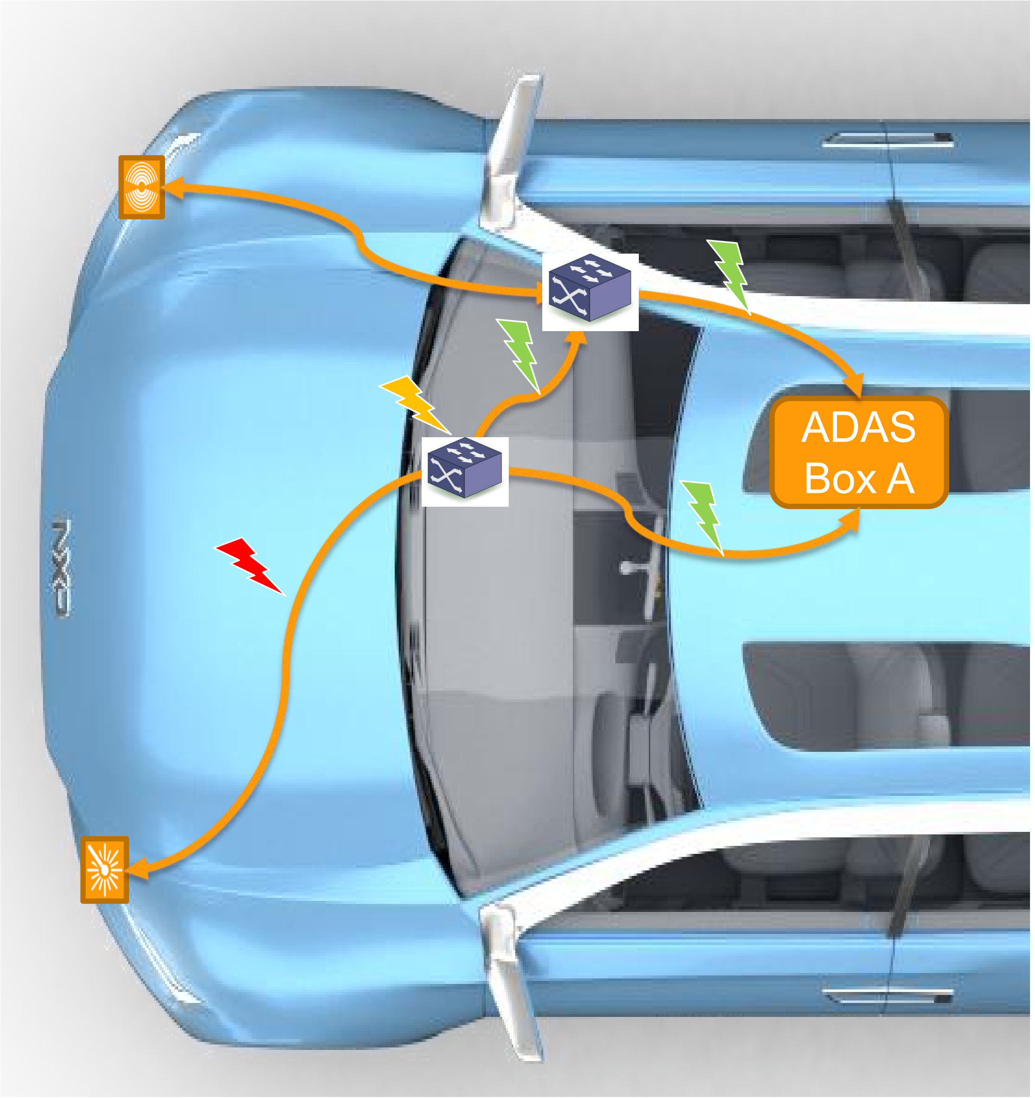
SYSTEM ASPECTS – LATENT FAULT TESTS

- Faults are detected during startup, reduces risk of service interruption while driving
  - Benefit for transportation service provider (autonomous driving cars)
- Latent fault tests ensure that safety functions can be trusted
  - Shut off functions will work, if needed as safe state
  - Prevents e.g., a malfunctioning sensor to flood the network
- Reliable information on communication status allows system to take right decision
  - E.g., reduce car functionality in case of missing redundancy



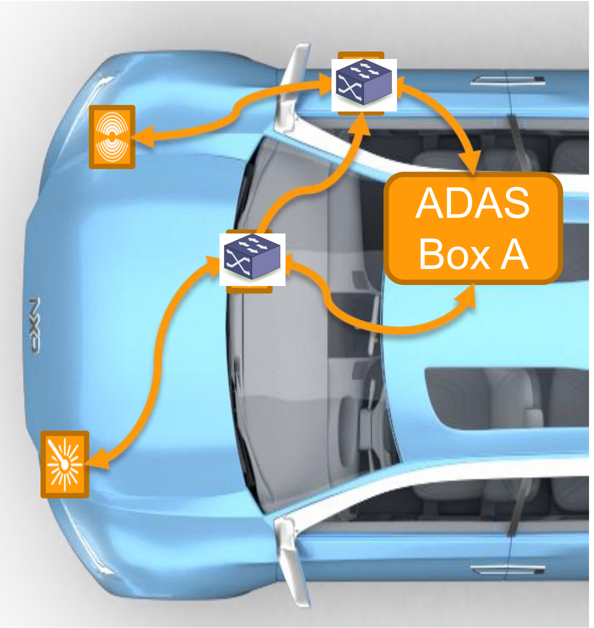
SYSTEM ASPECTS - REPLICATION AND ELIMINATION FEATURE (802.1CB)

- Whole system or part can be replicated
- Only safety critical portion of data relevant
- Level of redundancy depends on considered failures
  - Cable failures
  - Switch failures
  - Supply failures
- Integral part of network architecture
  - To be driven by OEMs
  - Tier-1s will inherit requirements
- Combination with full redundancy possible

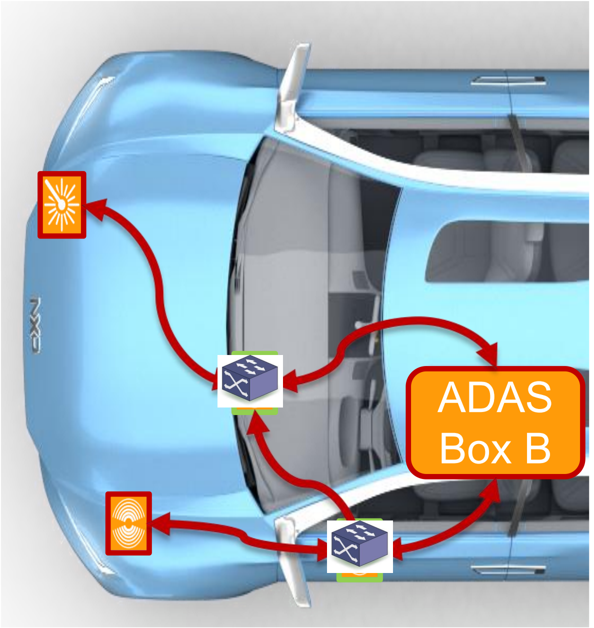


SYSTEM ASPECTS - REPLICATION AND ELIMINATION FEATURE (802.1CB)

Independent System A



Independent System B



Increased availability in each system by replication & elimination

Redundancy

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

SUMMARY AND CONCLUSION

- Zonal architectures bring new challenges – functions are spread over the network
- Functional safety becomes more relevant part of the network
- ASIL is not a checkmark item, but it is about the details
- Functional safety implemented in Switches and PHYs will not necessarily increase the safety level of the system
- But it helps to locate faults and increase system availability

TECHNOLOGY SHOWROOM

JOURNEYS BY DESIRED ENGAGEMENT

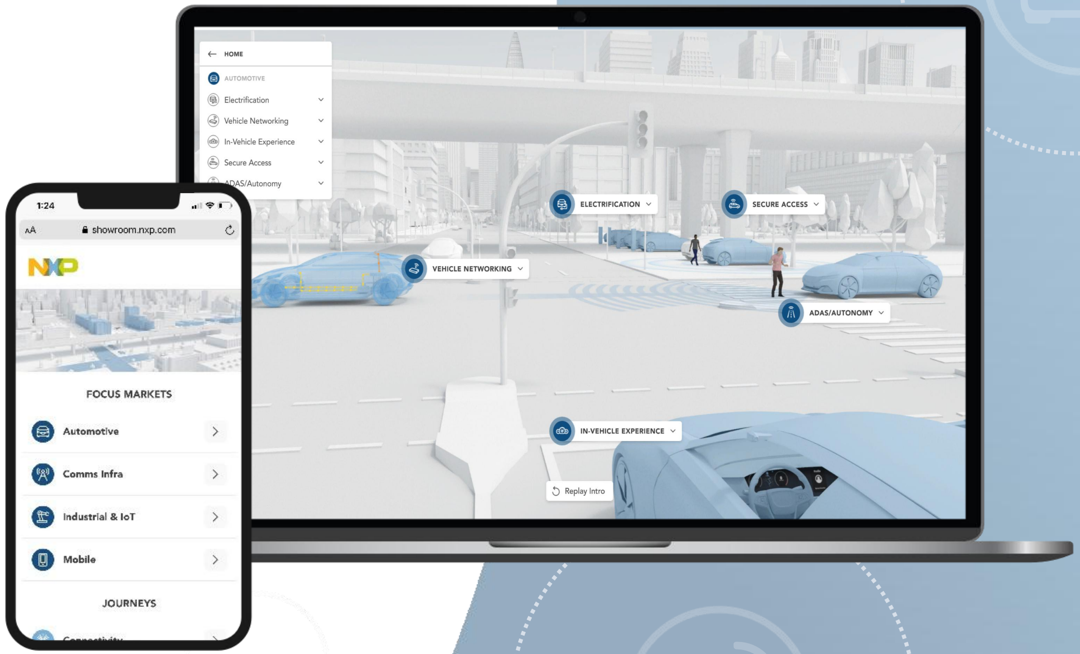
Self-guided tour
Live-streaming at set times
Guided tours

60+ VIRTUAL DEMOS

Focus on system solutions
Set up along NXP verticals

JOURNEYS BY DESIRED FOCUS

Low Power Innovations
Advanced Analog
Connectivity
Edge & AI/ML
Safety & Security

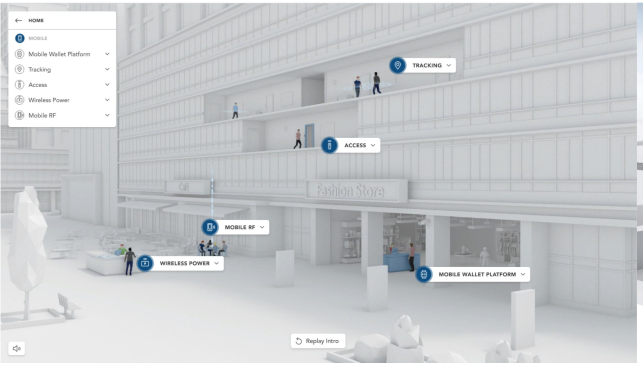


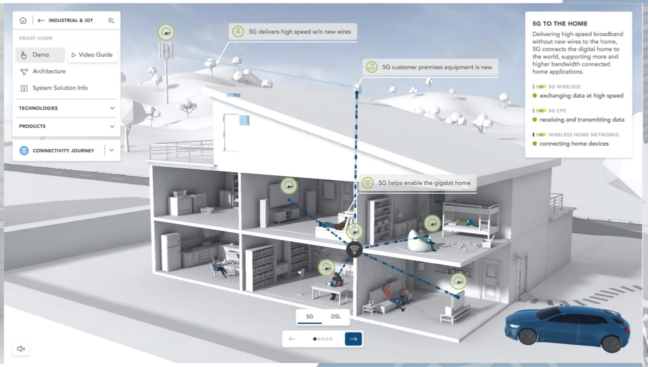
PROCESSING DATA AT THE EDGE

Enhanced calculations using a broader set of inputs.

GREENBOX II
- Processing local EV powertrain data only

CONNECTION MONITOR





5G TO THE HOME

Delivering high-speed broadband without new wires to the home, 5G connects the digital home to the world, supporting more and higher bandwidth connected home applications.

5G WIRELESS
- exchanging data at high speed

5G CPE
- receiving and transmitting data

WIRELESS HOME NETWORKS
- connecting home devices

CITY INFRASTRUCTURE SUB 6 GHZ

Integrated Small Cell for 5G infrastructure increased data speed for always on connected devices. Sub 6GHz 5G for increased range and ubiquitous access. Sub 6GHz 5G for Increased range and ubiquitous access.

Bandwidth 75%
Latency 25%
Range 75%

SUB 6GHZ 5G ANTENNA
- Increased range
- Ubiquitous access

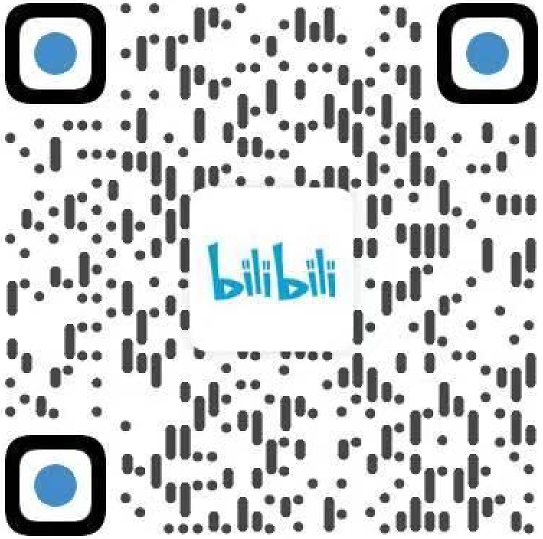
MULTIPLE DEVICES
- Dedicated Bandwidth
- Ubiquitous access
- Low latency

SHOWROOM.NXP.COM

WELCOME TO FOLLOW NXP AT SOCIAL PLATFORMS

欢迎您关注「恩智浦微招聘」公众号
及时获取恩智浦“芯”职位及员工
活动相关资讯

关注**NXP**客栈公众号，查看恩
智浦最新官方资讯及技术材料



关注恩智浦**B**站官方账号，观
看恩智浦最新技术视频

Q&A

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD