Functional Safety Architectural Challenges for Autonomous Drive

Ritesh Tyagi: August 2018

Copyright © Infineon Technologies AG 2018. All rights reserved.

Driving is still the same!

Copyright © Infineon Technologies AG 2018. All rights reserved.

Topics

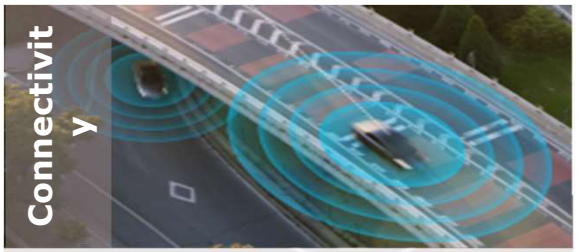
- Market Forces
- Functional Safety Overview
- Deeper Look
- Fail-Safe vs Fail-Operational
- Architectural Considerations
- Challenges

Copyright © Infineon Technologies AG 2018. All rights reserved.

Megatrends shaping the automotive market

Enabling safety towards Vision Zero

Enabling CO_2 reduction

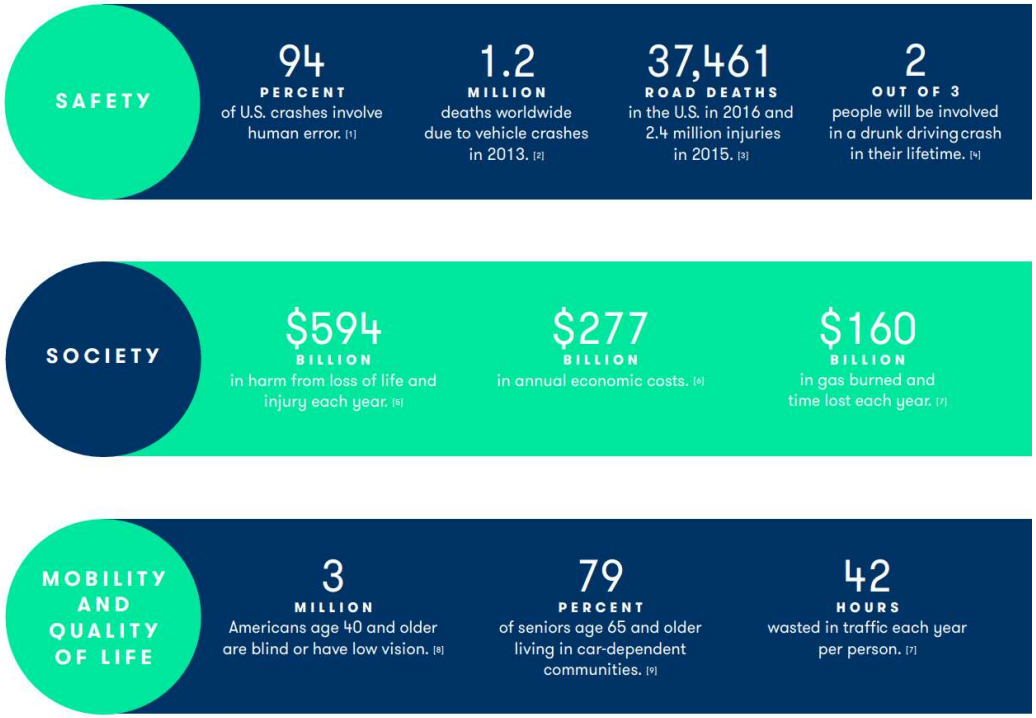


Enabling the communication of cars

Enabling security in connected cars

Copyright © Infineon Technologies AG 2018. All rights reserved.

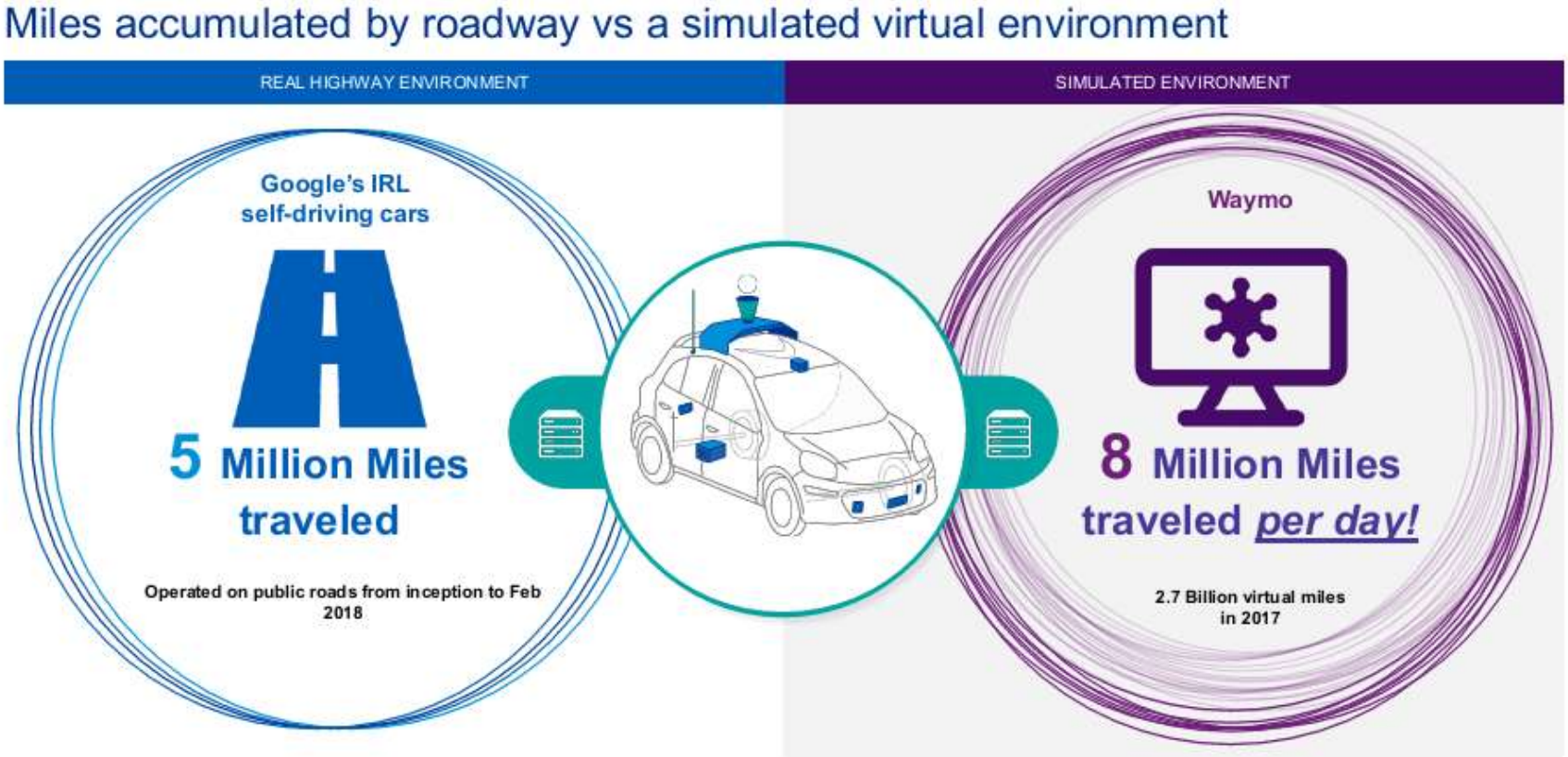
Socio-Economic Pressure



Source: Waymo Safety Report

Copyright © Infineon Technologies AG 2018. All rights reserved.

AD deployment can happen much earlier than we think



Source: https://www.theatlantic.com/technology/archive/2017/08/inside-waymos-secret-testing-and-simulation-facilities/537648/

Copyright © Infineon Technologies AG 2018. All rights reserved.

What is Functional Safety (FuSa)

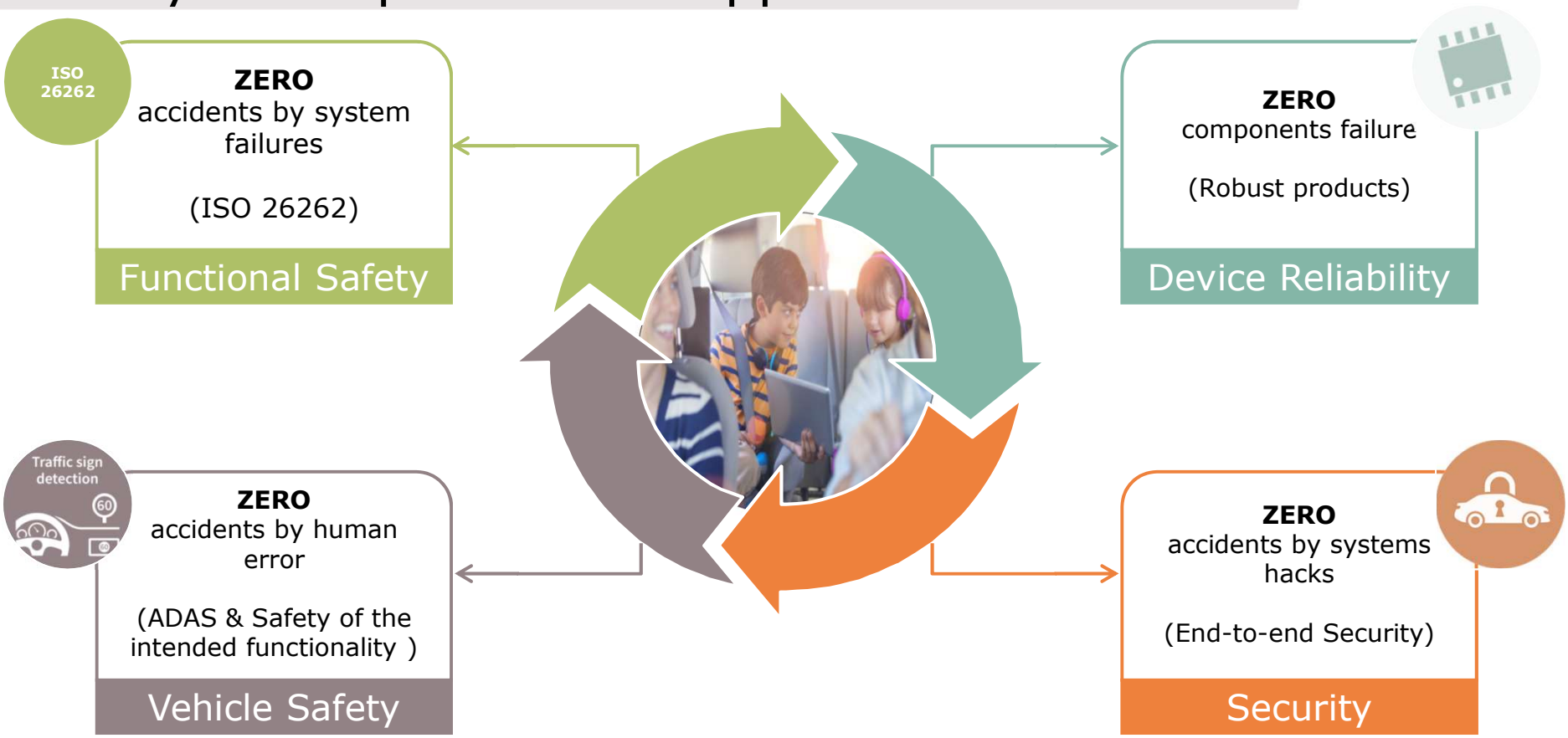
Does This Look Safe?

- Does redundancy help here?

- What could go wrong?

Copyright © Infineon Technologies AG 2018. All rights reserved.

Safety Concept: Holistic Approach



Copyright © Infineon Technologies AG 2018. All rights reserved.

What is Functional Safety?

Example of railroad crossing – How much is the probability of collision?

Root causes of danger are completely removed.

By adding functional measures, acceptable level of safety is ensured.

Assessment of the "functional measures" (safety functions) and its numerical evaluation is the basis of Functional Safety

Copyright © Infineon Technologies AG 2018. All rights reserved.

Functional Safety: Deeper Look

Vocabulary

Item

A system or array of systems which implements a safety related function e.g. steering, braking, transmission to which ISO26262 is applied

System

Consists of elements (sub-systems, components, HW, SW) and relates a sensor, controller and actuator with each other

Component

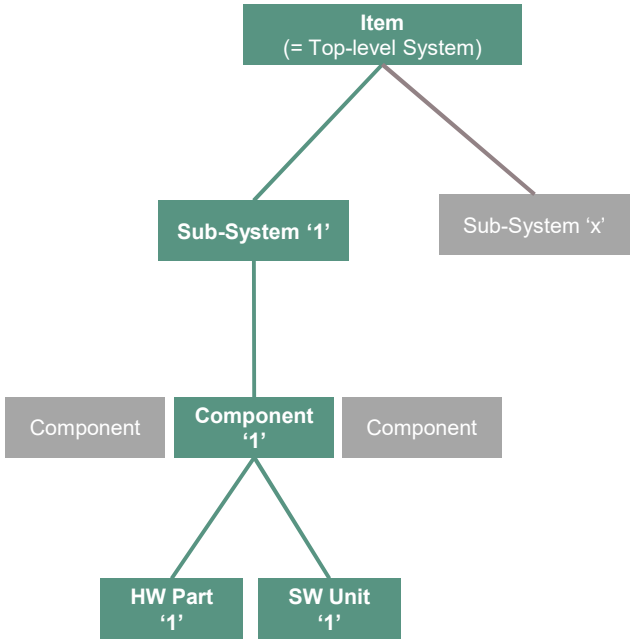
A none system level element which consists of more than one HW part or more than one SW unit

Hardware (HW) Part

Hardware which cannot be sub-divided

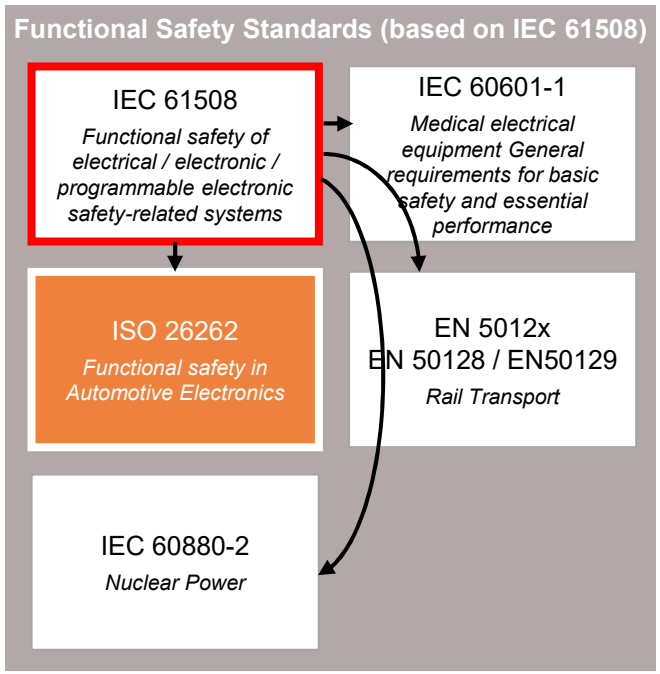
Software (SW) Unit

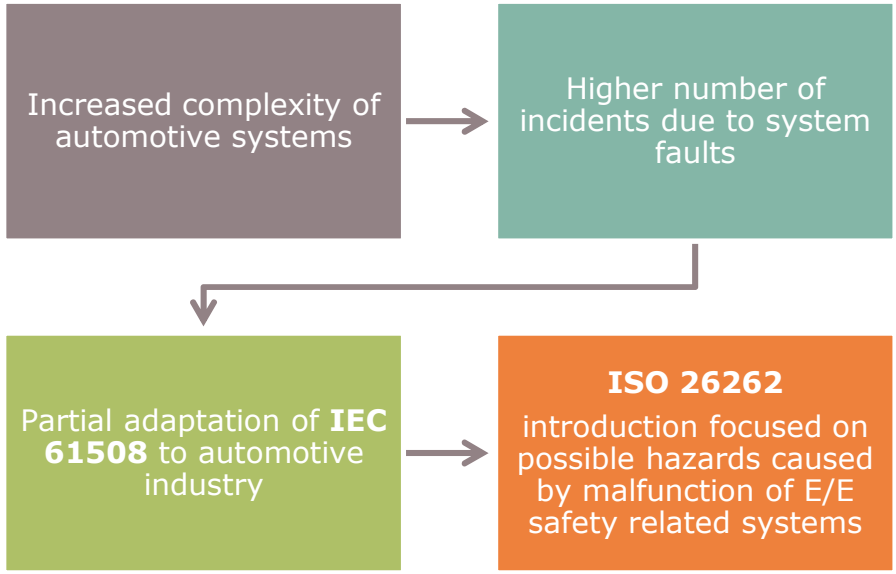
Atomic level of the SW architecture which can be tested as a standalone part of the SW



Copyright © Infineon Technologies AG 2018. All rights reserved.

Functional Safety Standard: ISO 26262 Origin





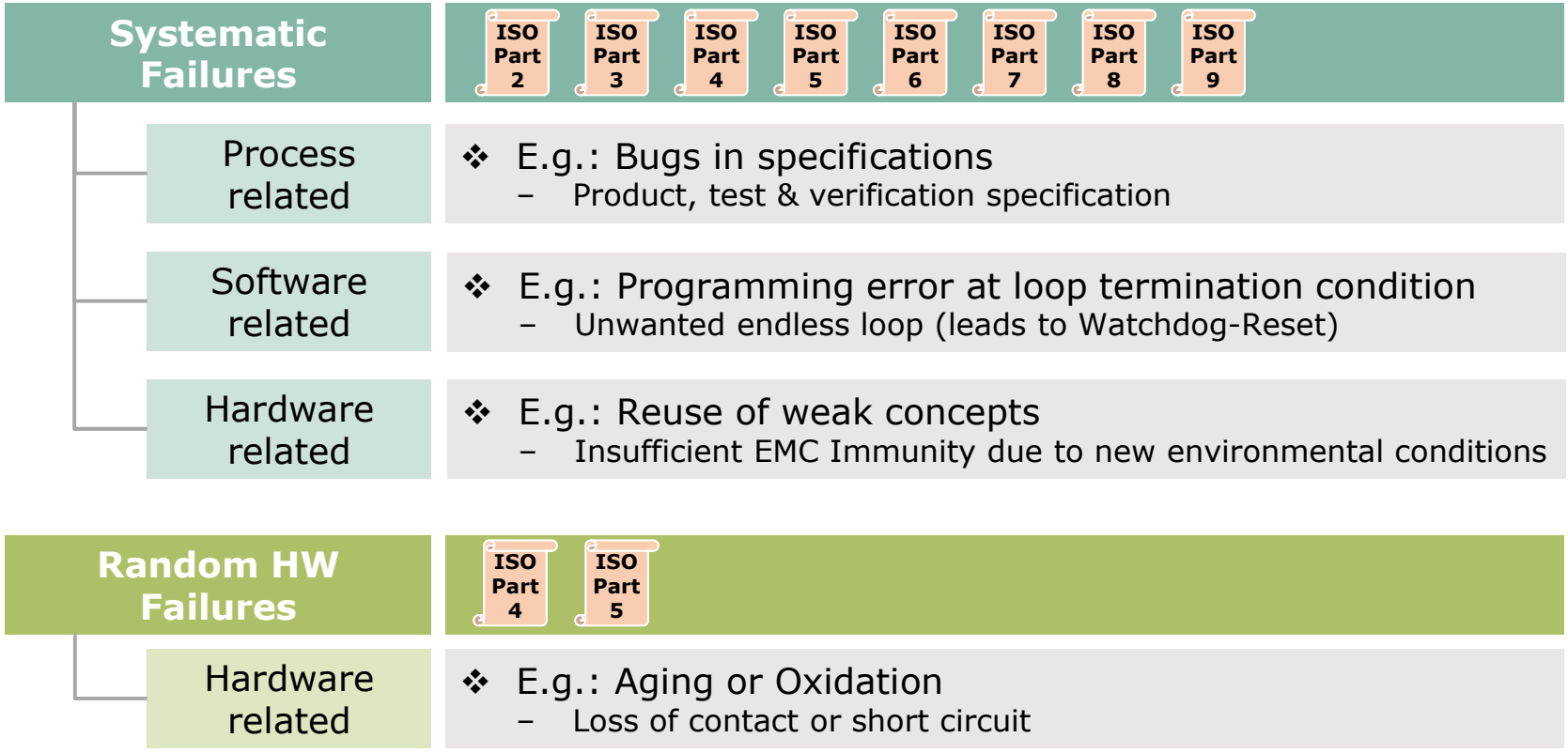
Copyright © Infineon Technologies AG 2018. All rights reserved.

ISO26262 Coverage

ISO 26262 **DOES** address	ISO 26262 **DOES NOT** address
• E/E systems in mass production vehicles • Possible hazards caused by malfunctioning E/E systems	• Hazards due to other factors (e.g.: smoke, fire), or technologies (unless directly caused by malfunctioning behavior of the E/E system) • Performance of the E/E Systems • Special purpose vehicles designed for drivers with disabilities

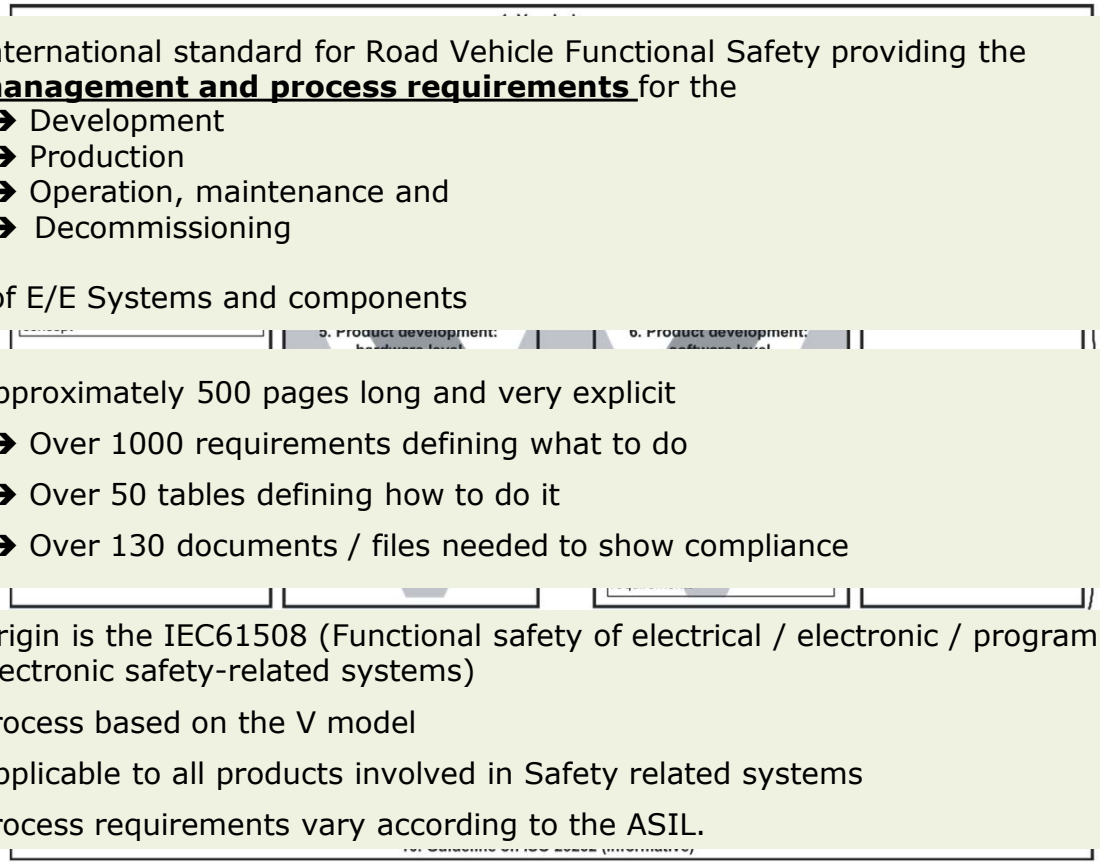
Copyright © Infineon Technologies AG 2018. All rights reserved.

Types of failures



Copyright © Infineon Technologies AG 2018. All rights reserved.

ISO26262 Process Overview



- International standard for Road Vehicle Functional Safety providing the **management and process requirements** for the
  - ➔ Development
  - ➔ Production
  - ➔ Operation, maintenance and
  - ➔ Decommissioning

  of E/E Systems and components

- Approximately 500 pages long and very explicit
  - ➔ Over 1000 requirements defining what to do
  - ➔ Over 50 tables defining how to do it
  - ➔ Over 130 documents / files needed to show compliance

- Origin is the IEC61508 (Functional safety of electrical / electronic / programmable electronic safety-related systems)
- Process based on the V model
- Applicable to all products involved in Safety related systems
- Process requirements vary according to the ASIL.

Copyright © Infineon Technologies AG 2018. All rights reserved.

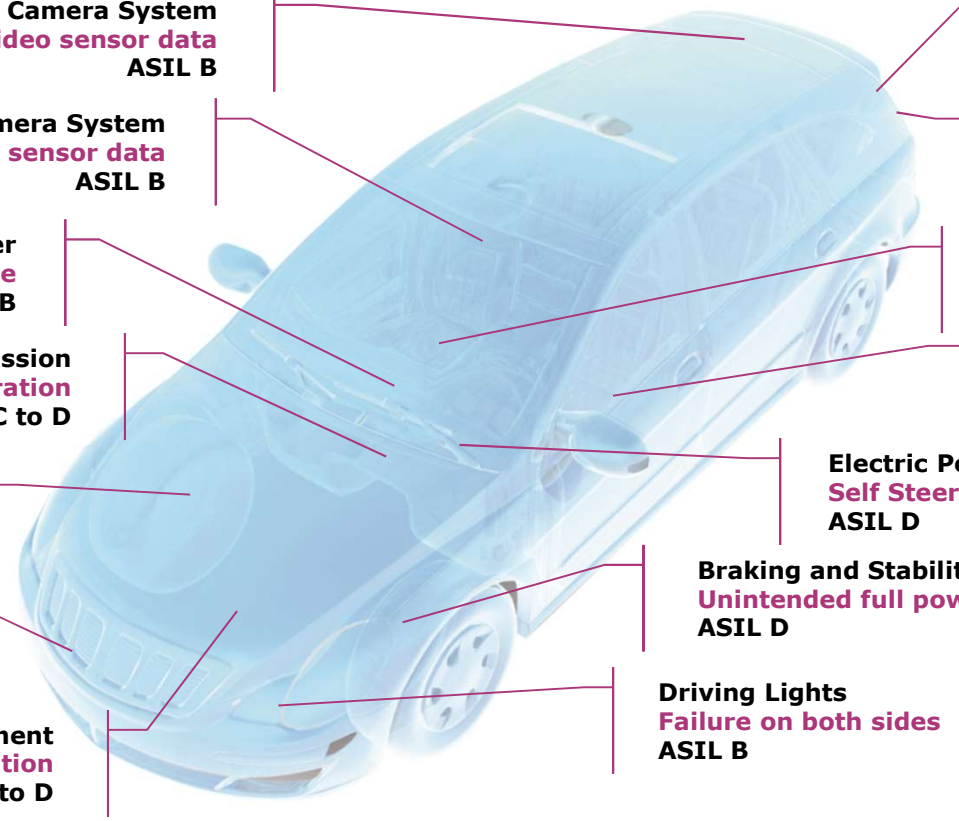
Automotive Safety Integrity Levels (ASILs) Concept

- At the top-level, Safety goals are defined through the process of hazard analysis and risk assessment(HARA)
- Safety goals are written in terms of avoiding harm during some vehicle operational condition, with a corresponding Automotive Safety Integrity Level (ASIL)
- ASIL applies to individual safety goal, not overall system!
- ASIL defines the required degree of rigor in technical, organizational, and process activities
- There are 5 ASIL levels QM, A, B, C & D

ASIL	Certainty that Safety Function is Correctly Performed
D	Very High
C	High
B	Medium
A	Low
QM	Quality Measures are Enough

Copyright © Infineon Technologies AG 2018. All rights reserved.

Functional Safety is relevant for the whole car



Smart Rear View Camera System
No valid video sensor data
ASIL B

Front View Camera System
No valid video sensor data
ASIL B

Instrument Cluster
Speedometer not available
ASIL B

Transmission
Unwanted vehicle deceleration
ASIL C to D

Active Suspension
Suspension oscillates
ASIL B to C

77GHz RADAR ACC
Inadvertent Braking
ASIL C

Engine Management
Unwanted vehicle acceleration
ASIL C to D

Break Lights
Loss of Brake Lights
ASIL B

Rear Lights
Failure on both sides
ASIL A

Airbag System
Inadvertent Deployment
ASIL D

Sensor Fusion ECU
Don't send incorrect commands
ASIL D

Electric Power Steering
Self Steering
ASIL D

Braking and Stability Systems
Unintended full power brake
ASIL D

Driving Lights
Failure on both sides
ASIL B

HMI

Body

Powertrain

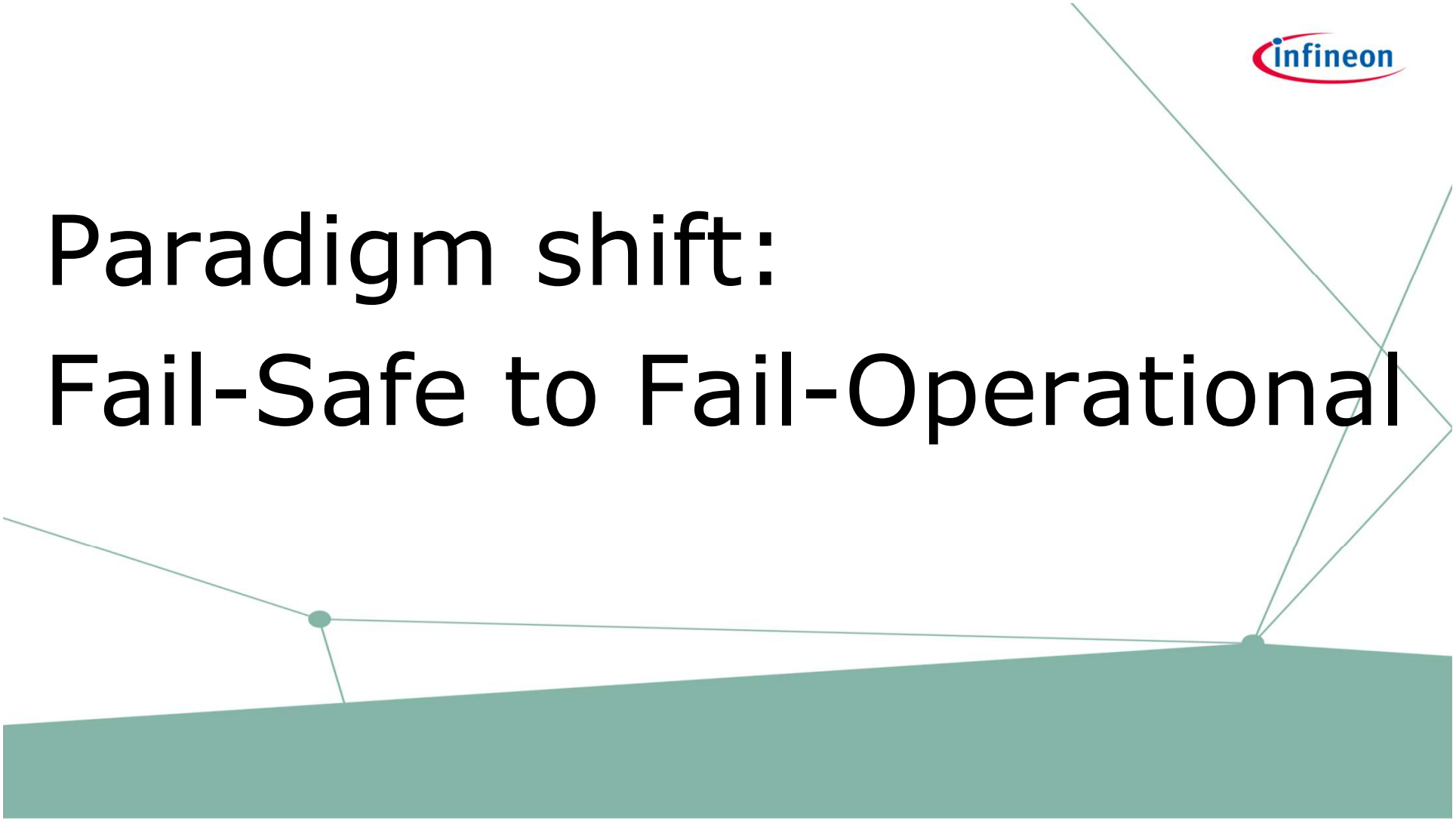
Safety & Chassis

The safety goals may differ, depending on the OEM, vehicle type and region.

HMI – Human Machine Interface

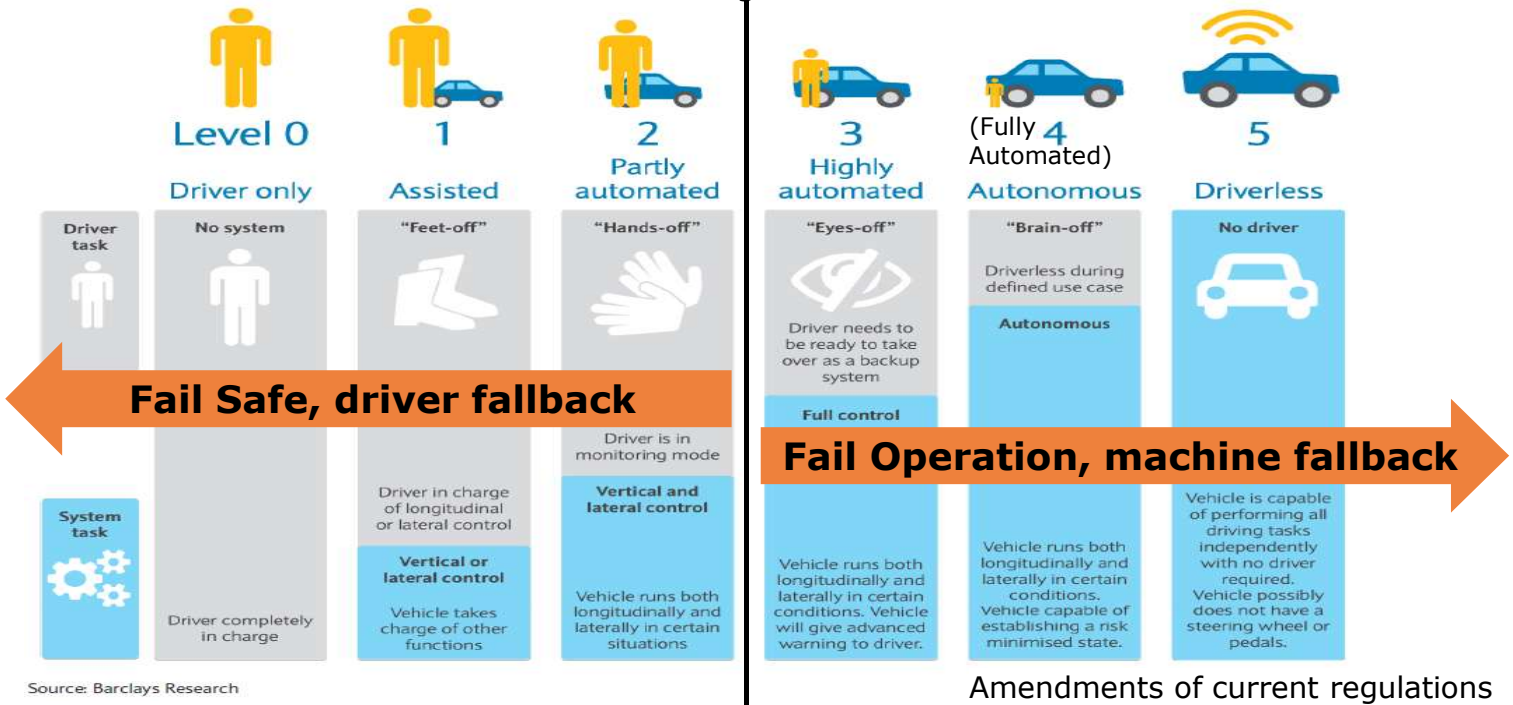
Copyright © Infineon Technologies AG 2018. All rights reserved.

Paradigm shift:
Fail-Safe to Fail-Operational



Fail-Operation : Foundation for AD

Level 0 – Level 5: SINGLE definition across the globe: NHTSA = VDA = SAE



Source: Barclays Research

Amendments of current regulations are necessary (e.g. Vienna StVO, ECE-R79)

ADAS Advanced driver assistance systems

AD Automated driving

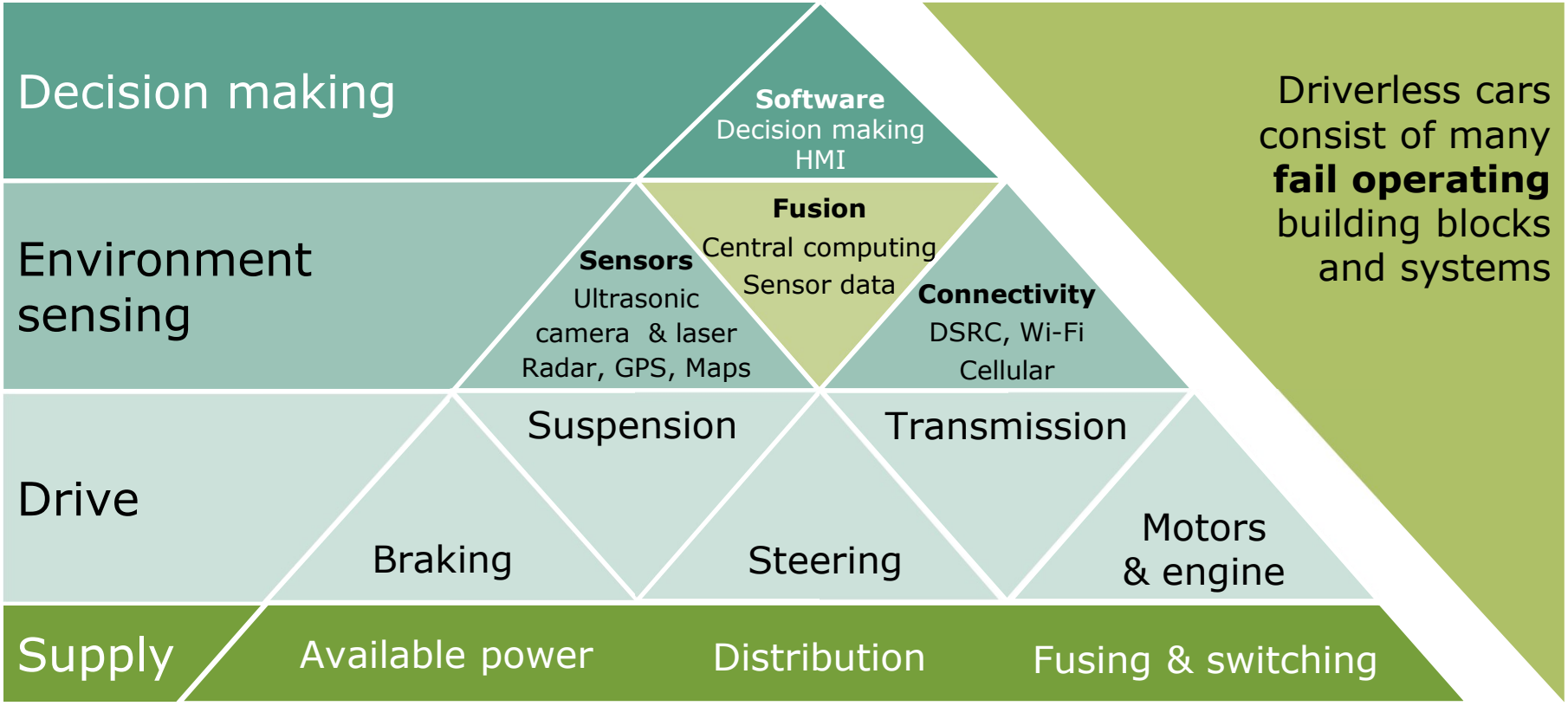
Copyright © Infineon Technologies AG 2018. All rights reserved.

Fail operational Response Time

Level 3: Eyes-off  e.g. driver sleeping	1 s – 10 s driver takes over after warning 10 s – 20s repeat warning if no driver response, prepare for stop 20 s – 30 s manage controlled and save stop
Level 4: Brain-off  e.g. driver on rear seat	1 min – 15 min car stops at next rest area >15 min prepare and manage controlled and save parking stop 10 s – 20s stop in a controlled way at very severe failures
Level 5: Driver-off  e.g. no driver in car	1 h – 10 h car is driving home >10 h car is driving to next partner service station 10 s – 20 s stop in a controlled way at very severe failures

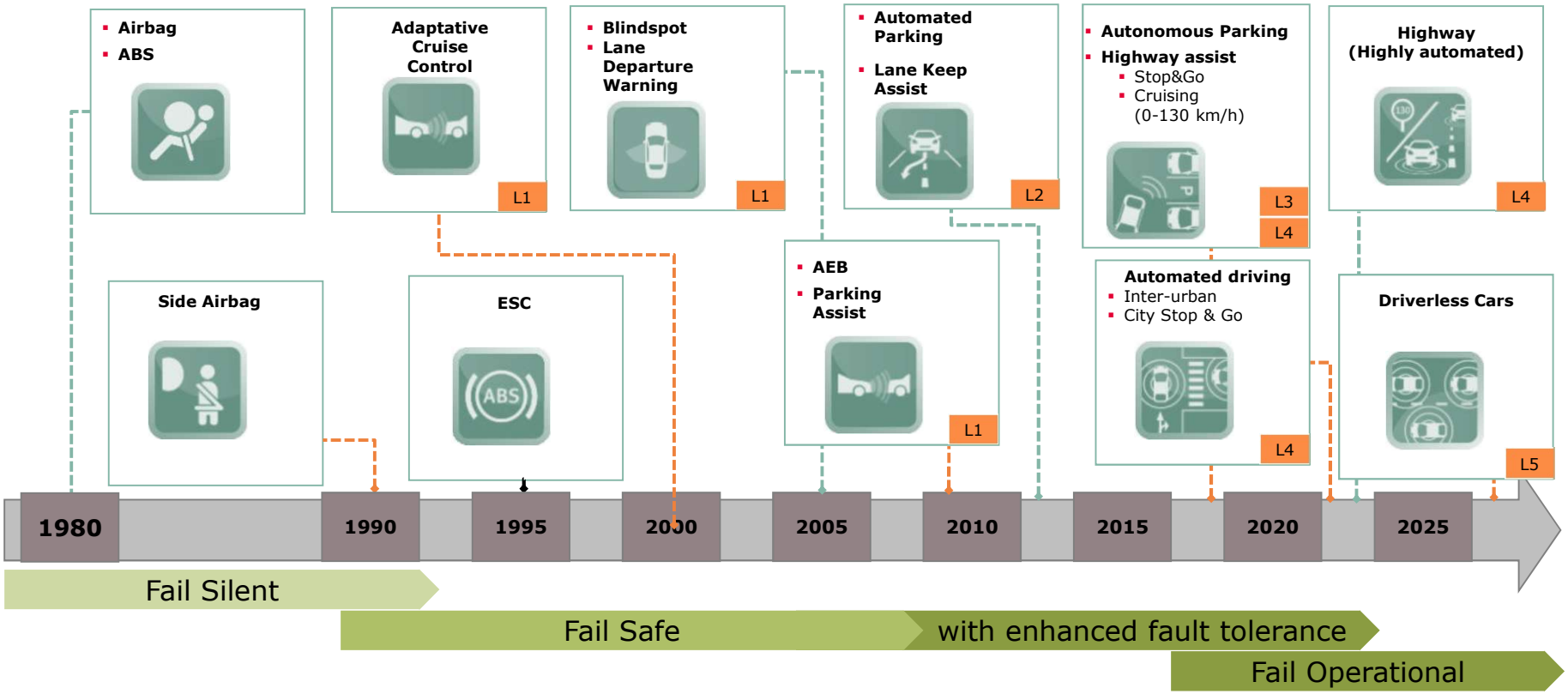
Copyright © Infineon Technologies AG 2018. All rights reserved.

System blocks of automated driving



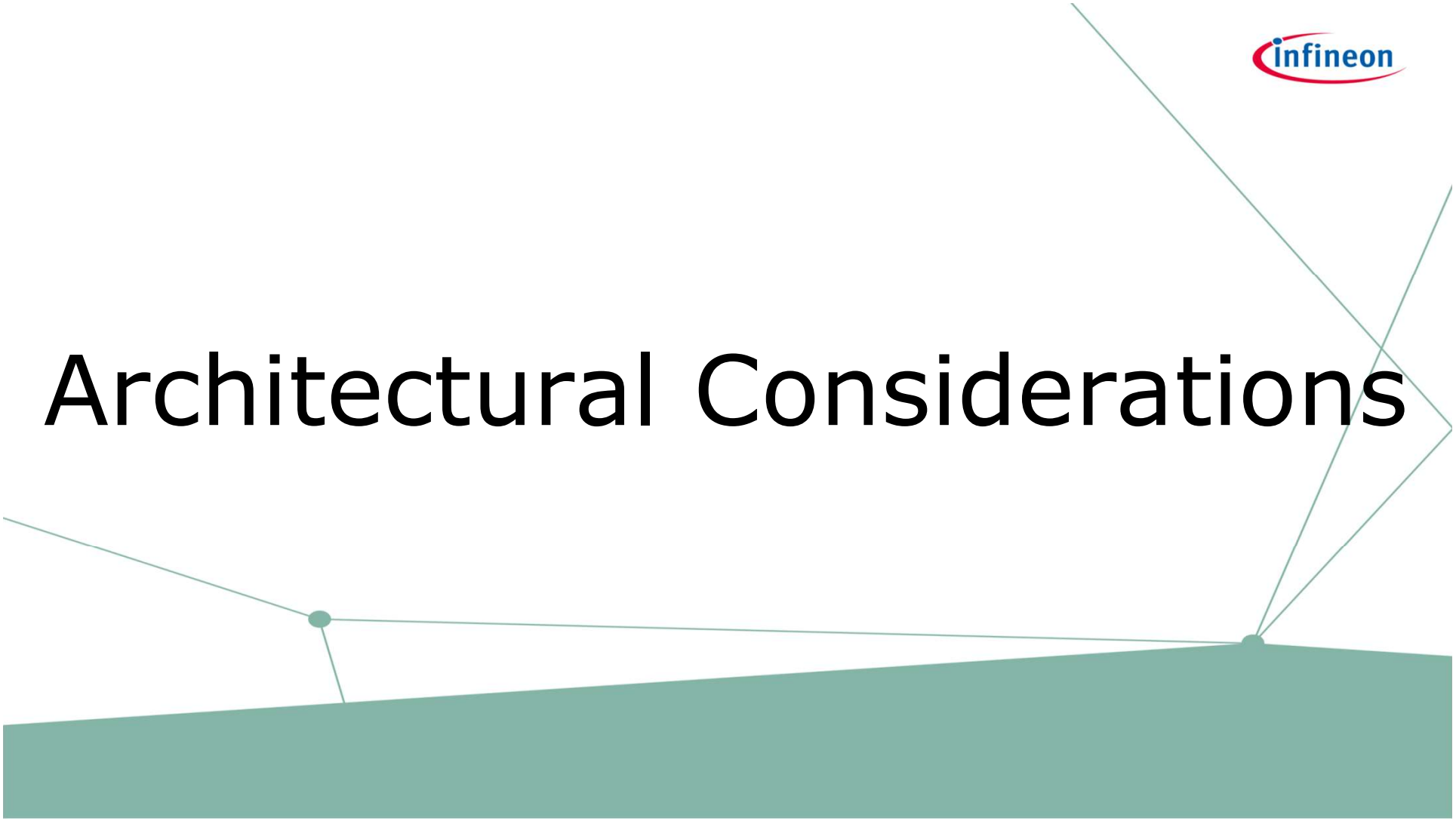
Copyright © Infineon Technologies AG 2018. All rights reserved.

AD demands high dependability across all systems



Copyright © Infineon Technologies AG 2018. All rights reserved.

Architectural Considerations



Fail-Operational Architecture

Diversity

Same task with different algorithms,
Architectural implementation

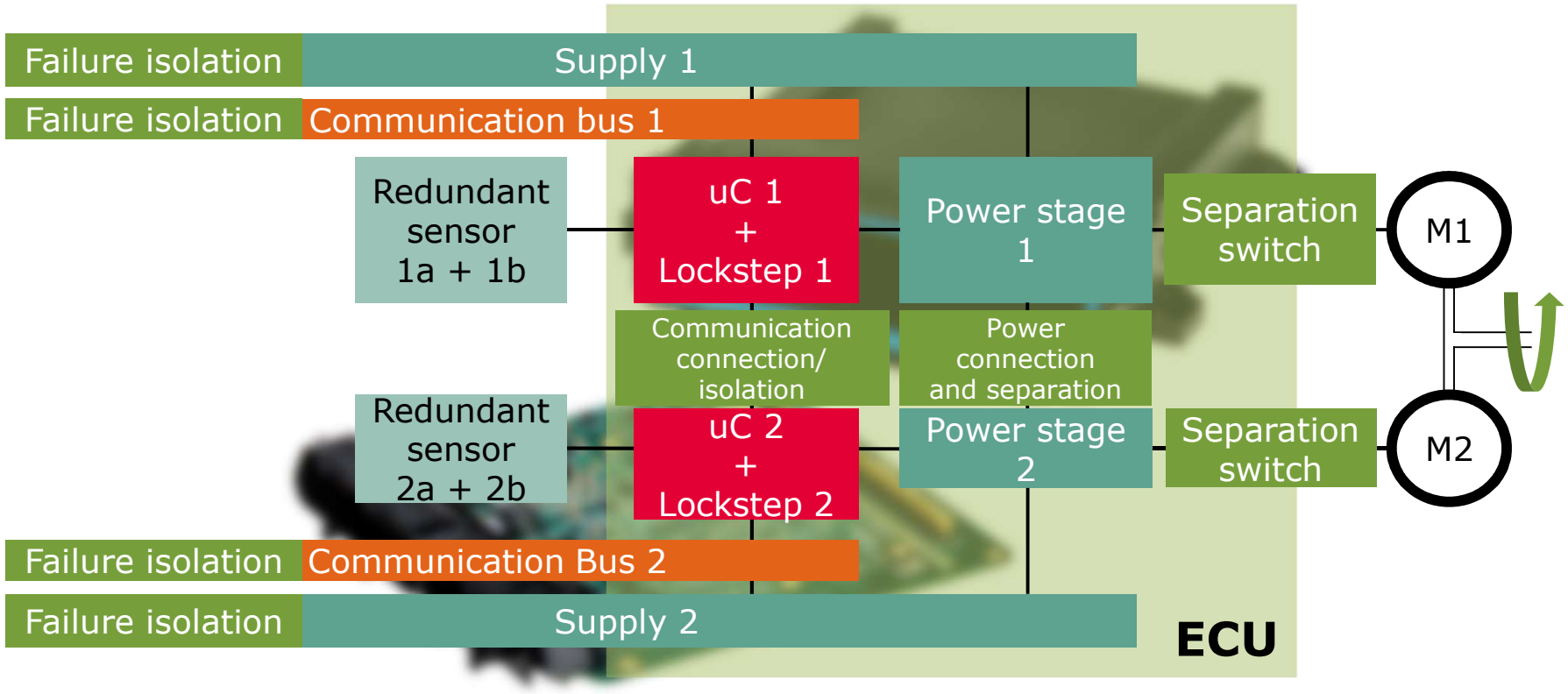
Redundancy

2oo2 DFS architecture,
2oo3 Triplex Modular Redundancy with voting

Copyright © Infineon Technologies AG 2018. All rights reserved.

Fail-operational system

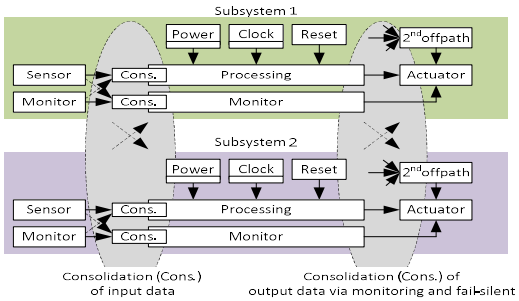
Electric Power Steering (EPS)



Copyright © Infineon Technologies AG 2018. All rights reserved.

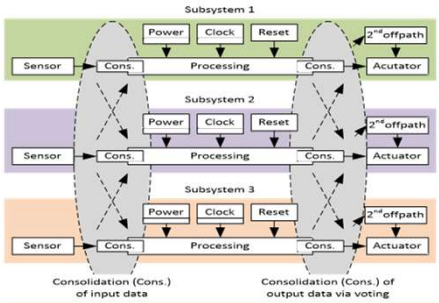
Redundant architecture considerations

2oo2 DFS (Dual Fail Safe)



- 2oo2 can be derived from todays Fail Safe systems
- Two redundant and robust channels with diagnostic monitor
- Implications of this architecture
  - Two systems with each being able to supply safe, secure, reliable and available Service
  - Two independent supply's for each channel
  - Optional isolated inter processor communication

2oo3 TMR (Triple Modular Redundancy)



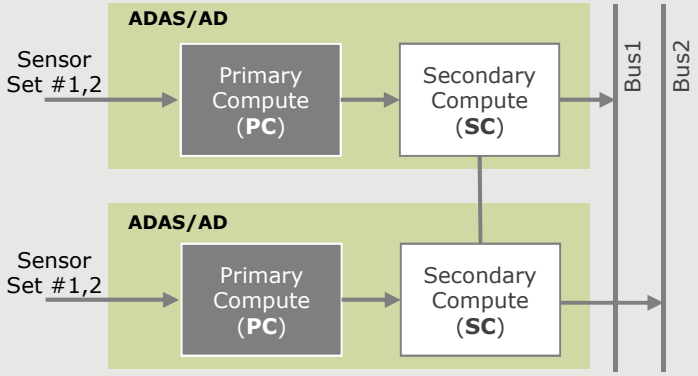
- 2oo3 is the reference architecture in aerospace and in several safety critical systems
- Concept = 3 different units whose results are compared using majority vote
- Implications of this architecture
  - Independent supply for each computing unit (3 supplies) and each voter
  - Need to compare results using a majority vote with voter
  - Voter Complexity might increase with data throughput

Copyright © Infineon Technologies AG 2018. All rights reserved.

2oo2DFS Architecture
(Symmetric vs. Asymmetric)

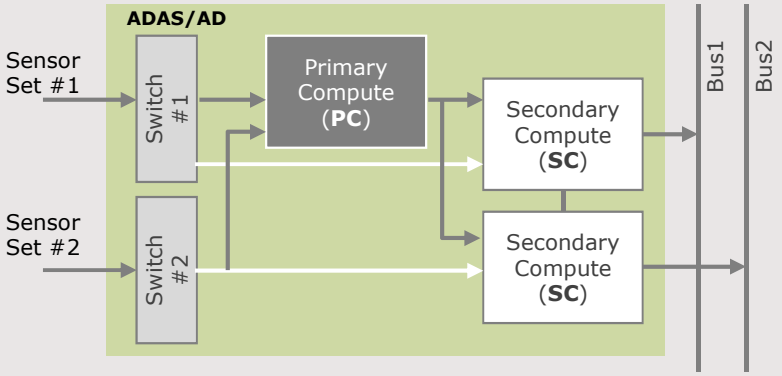
Performance, Power Budget, and Software Re-use Will Drive Architecture

Symmetric



Attributes:
- Higher cost
- Higher power consumption
- Full functionality in case of failure

Asymmetric

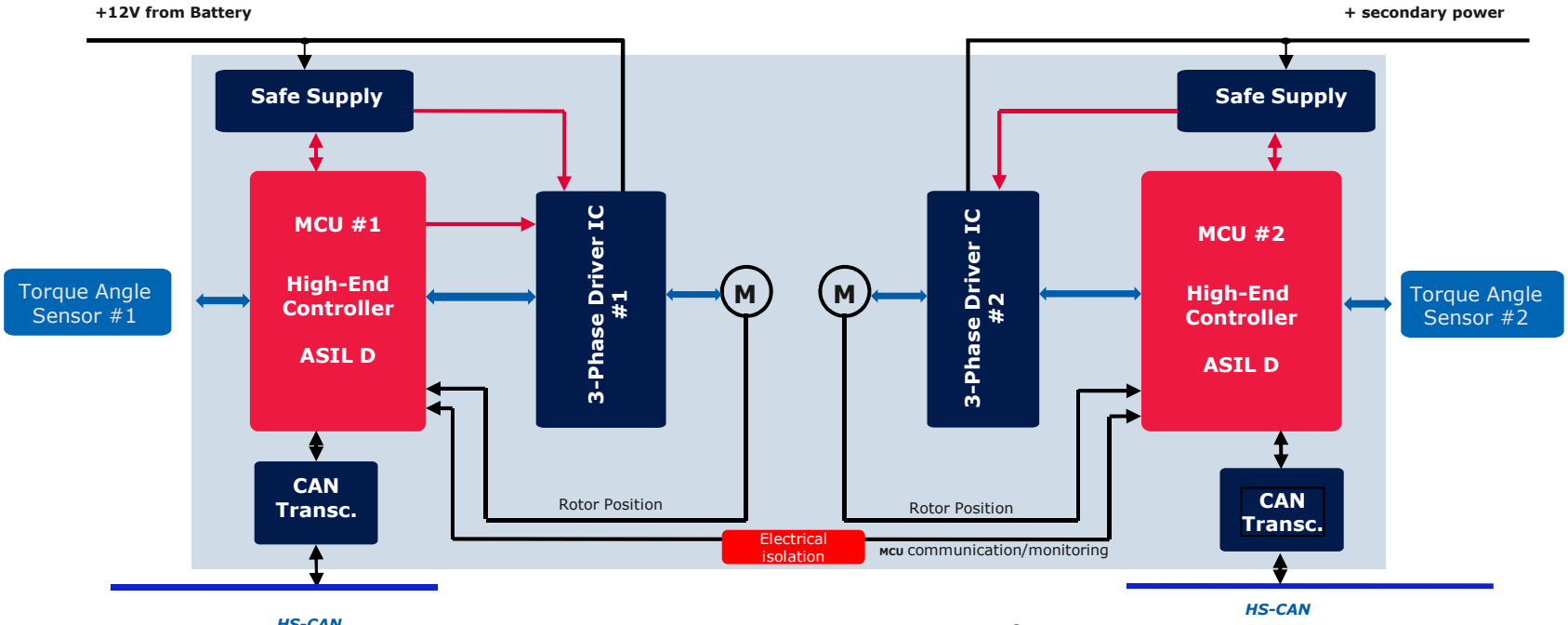


Attributes:
- Lower cost
- Lower power consumption
- Limited functionality in case of failure

PC: High Computation ("Number Cruncher")
SC: Object-level Fusion and ASIL-D Controller

Copyright © Infineon Technologies AG 2018. All rights reserved.

2oo2DFS Architecture
Symmetric Example: EPS



- 2oo2 DFS can be derived from todays Fail Safe systems
- Two redundant and robust channels with diagnostic monitor

Implications of this architecture

- Two systems with each being able to supply safe, secure, reliable and available Service
- Two independent supply's for each channel
- Optional isolated inter processor communication

Copyright © Infineon Technologies AG 2018. All rights reserved.

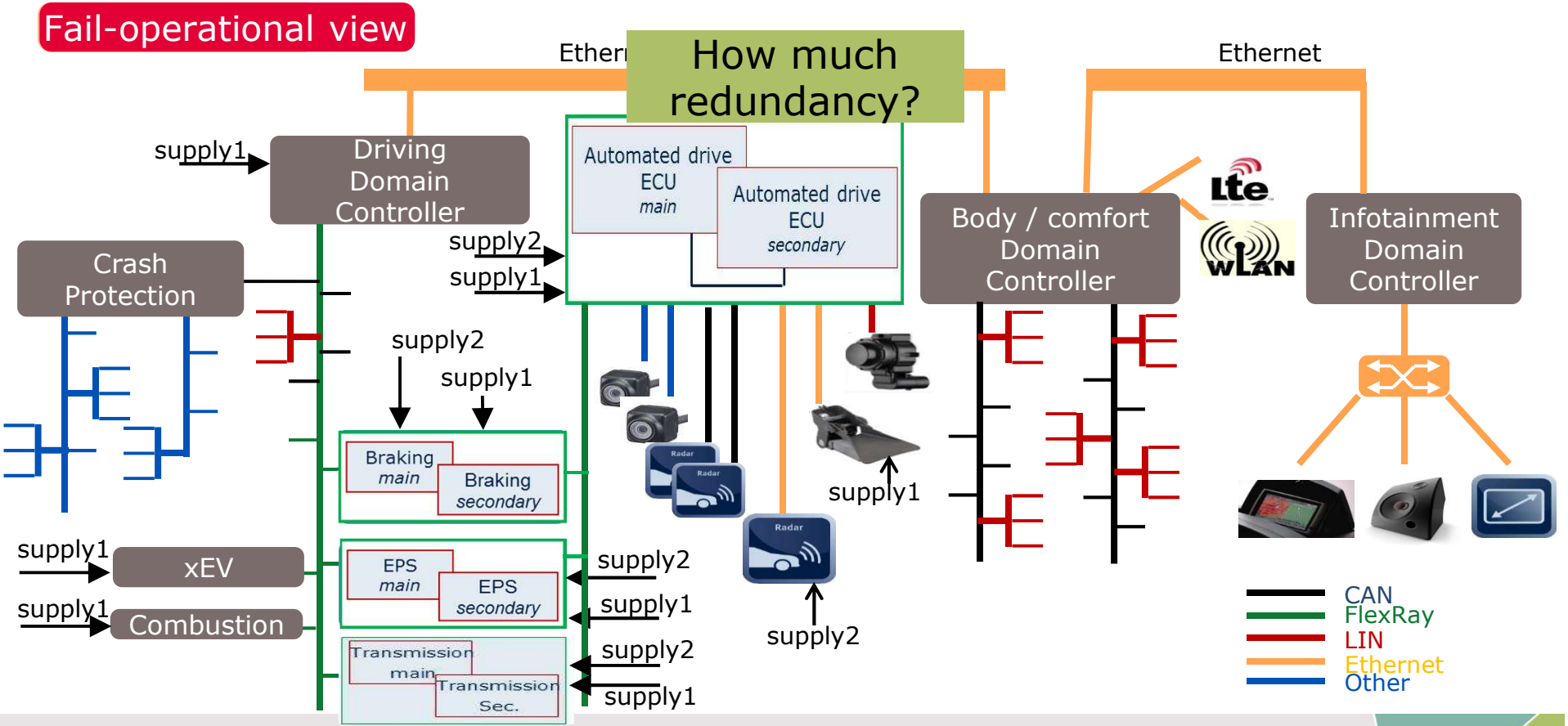
Challenges

Challenges in Fail Operation Systems

- Increase in hardware costs in cases of triple Redundancy systems
- Systems can’t be completely re-used because of diversity need
- Redundancy != Fail Operation
- Increase in ASIL levels for most of the systems for Highly Automated Driving
- Challenges in Testing and Validation of Fail Operational Systems
- Non-Deterministic Machine Algorithms used in Highly Automated Driving

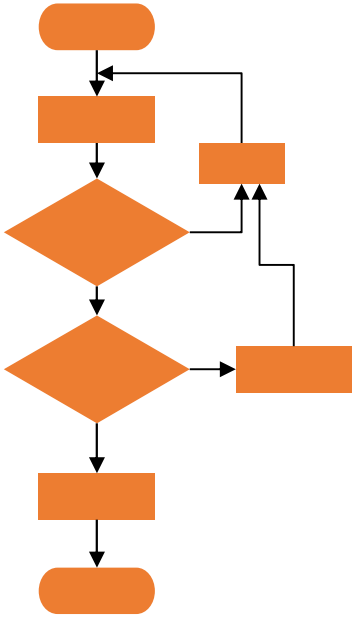
Copyright © Infineon Technologies AG 2018. All rights reserved.

Fail-Operational Architecture Complexity



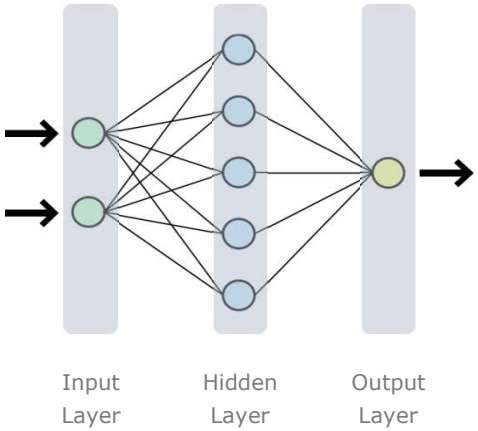
Copyright © Infineon Technologies AG 2018. All rights reserved.

Challenges in FuSa for Neural Networks



Traditional Systems

vs



Neural Networks

ISO 26262	Traditional Systems	Neural Networks
Included in 2nd Edition	✓	✗
Process Defined	✓	✗
Development Guidelines	✓	✗
Safety Concept	✓	✗
Software Tools	✓	✗

Uncertainties & Unknowns in Neural Networks	
1	Content and deterministic characteristic of software is uncertain as it learns over time
2	No existence of development standards or best practices
3	Unknown of what additional system measures are needed to argue/prove it's safe
4	Uncertainty in how much training sets are needed to claim a "Predictable and Trusted" behavior

Copyright © Infineon Technologies AG 2018. All rights reserved.

ISO26262 Limitations for ADAS/AD

- ISO26262 addresses the safety risk of a malfunctioning E/E in a vehicle.
- However:
  - In ADAS applications safety hazards (for driver, passengers, pedestrians, etc.) may come from a "fault-free" system:
    - Decision Algorithms (braking, steering).
    - Driving conditions (fog, snow, traffic, roadworks, etc.).
    - Environmental noise (EM, signal degradation, etc.).
- SOTIF: Safety of Intended Functionality (ISO/WD PAS 21448 – under development https://www.iso.org/standard/70939.html).

For SAE L3 or greater: ISO26262(2nd Edition) + SOTIF

Copyright © Infineon Technologies AG 2018. All rights reserved.

Part of your life. Part of tomorrow.

infineon