DESIGNING FOR ADVANCED FUNCTIONAL SAFETY REQUIREMENTS

MATHIEU BLAZY-WINNING
FUNCTIONAL SAFETY MANAGER

AMF-AUT-T2805 | AUGUST 2017

SECURE CONNECTIONS FOR A SMARTER WORLD

AGENDA

- Overview of ISO 26262 Standard
- NXP Approach to ISO 26262
- Conclusion

FROM AUTOMOTIVE … TO SAFE & SECURE MOBILITY

SEAMLESS CONNECTED MOBILITY EXPERIENCE	ADVANCED DRIVER ASSISTANCE ➔ SELF-DRIVING	ENERGY EFFICIENCY
		
Enjoying Life. *One hour per day* *in the car*	*Saving Lives.* *1.3M Road Fatalities* *Every Year*	*Reducing CO2.* *EU mandates 20%* *reduction by 2020*

ROAD TRAFFIC ACCIDENTS

THE CAUSES

Critical Reasons	Number	%
Driver	2,046,000	94%
Vehicles	44,000	2%
Environment	52,000	2%
Unknown	47,000	2%
Total	2,189,000	100%

Data source: NMVCCS

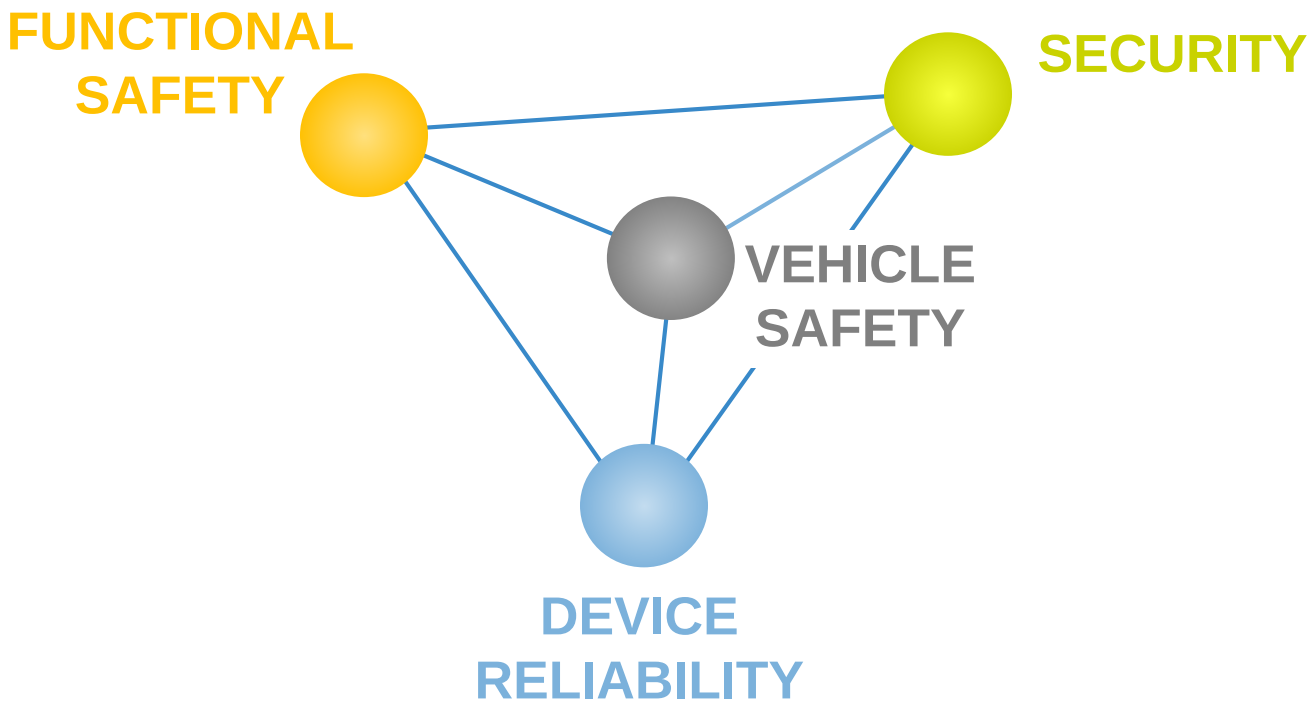
Driver-Related Critical Reasons	Number	%
Recognition Error	845,000	41%
Decision Error	684,000	33%
Performance Error	210,000	11%
Non-performance Error (e.g. Sleep)	145,000	7%
Other	162,000	8%
Total	2,046,000	100%

Every year!

- ~1.3 m fatalities
- >50 m people seriously injured
- >$3 trillion cost of road accidents
- >90% caused by human mistakes

We need to get the *Human Factor* out of the equation!

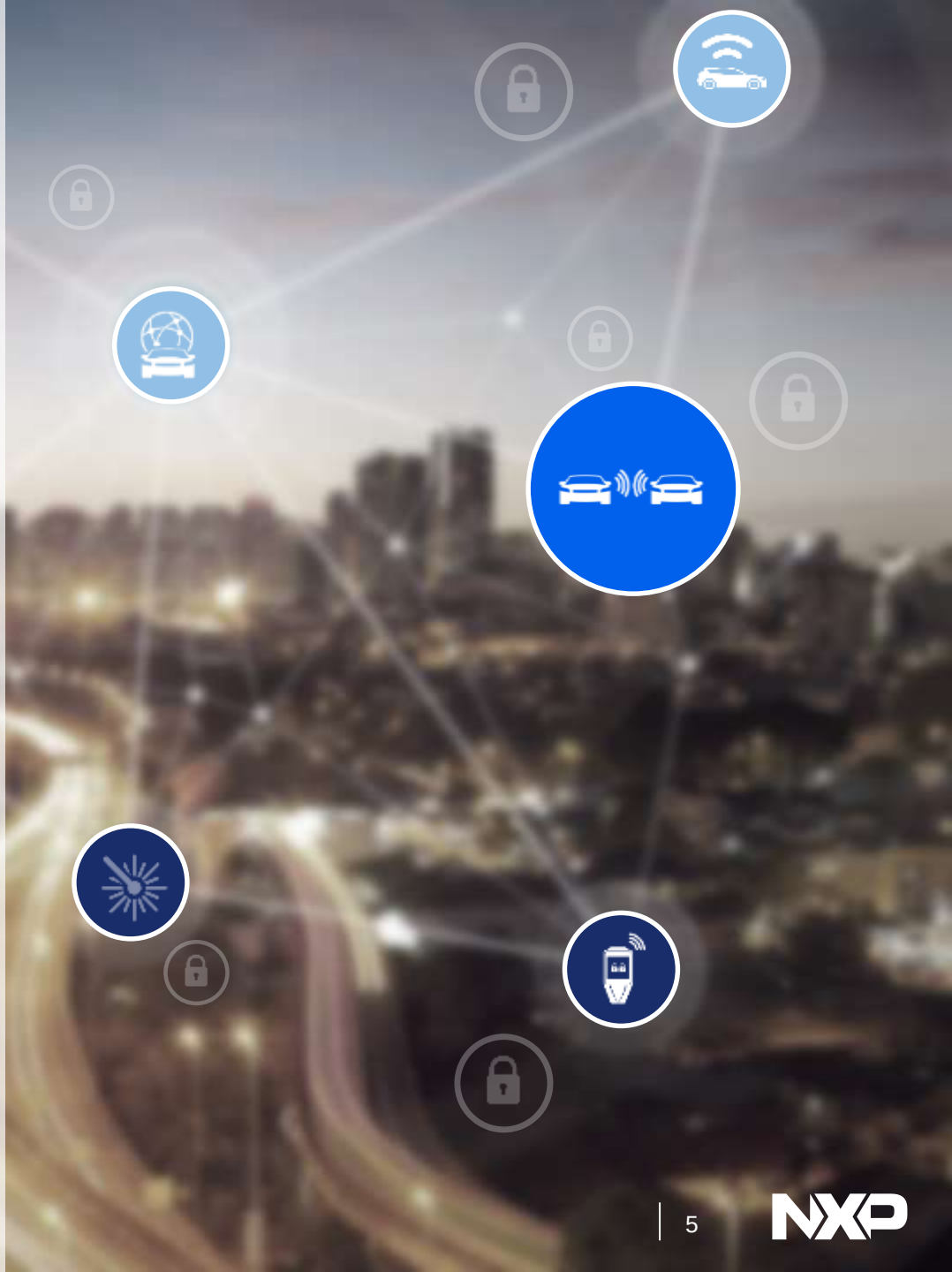
Elements of a Safe System



VEHICLE SAFETY:	Zero accidents by human error (ADAS & SOTIF)
SECURITY:	Zero accidents by system hacks
FUNCTIONAL SAFETY:	Zero accidents by system failures (ISO 26262)
DEVICE RELIABILITY:	Zero components failures (robust product)

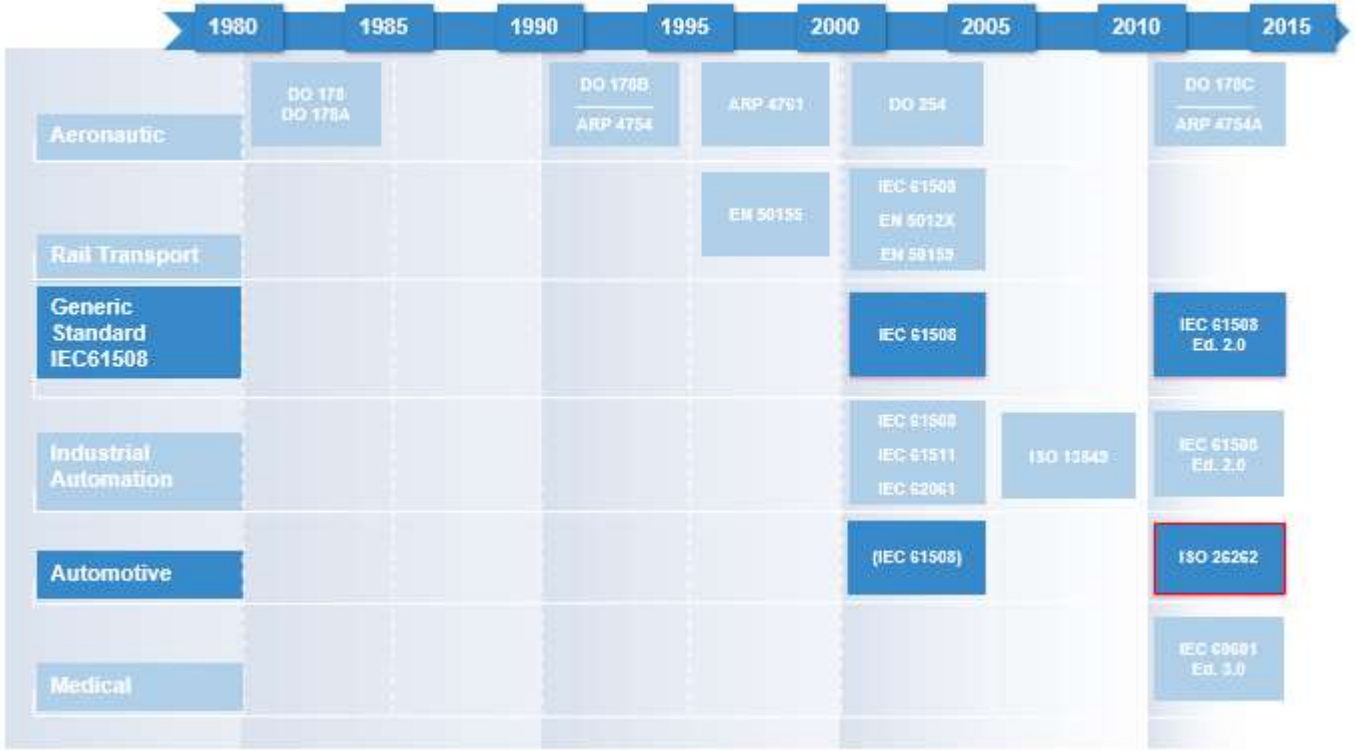
SOTIF: Safety of the intended functionality

Overview of ISO 26262 Standard



Functional Safety Standards

- **ISO 26262** is the **adaptation of IEC 61508** to comply with needs specific to electrical and/or electronic (E/E) systems within **road vehicles**.
- ISO 26262 addresses possible **hazards** caused by **malfunctioning** behavior of **E/E safety-related systems**.
- Addresses risks from **systematic failures** and **random hardware failures**.
- System safety is achieved through a number of **safety measures**.
- **ISO 26262** provides an **automotive-specific risk-based** approach to determine integrity levels [Automotive Safety Integrity Levels (**ASIL**)].
- **ISO 26262** uses **ASILs** to specify applicable requirements of ISO 26262 so as to **avoid unreasonable residual risk**.



Reference ISO 26262-1:2011

ISO 26262 Product Development

- ISO 26262 compliance is achieved between vehicle manufacturers, Automotive suppliers (Tier 1), semiconductor suppliers and IP providers

ANALYZE HAZARD & RISK (HARA)
DEFINE SAFETY GOALS (SG)
EVALUATE AUTOMOTIVE SAFETY INTEGRITY LEVEL (ASIL A, B, C or D)

INDENTIFY FAULTS
IMPLEMENT **SAFETY MEASURES** TO MITIGATE THE RISK

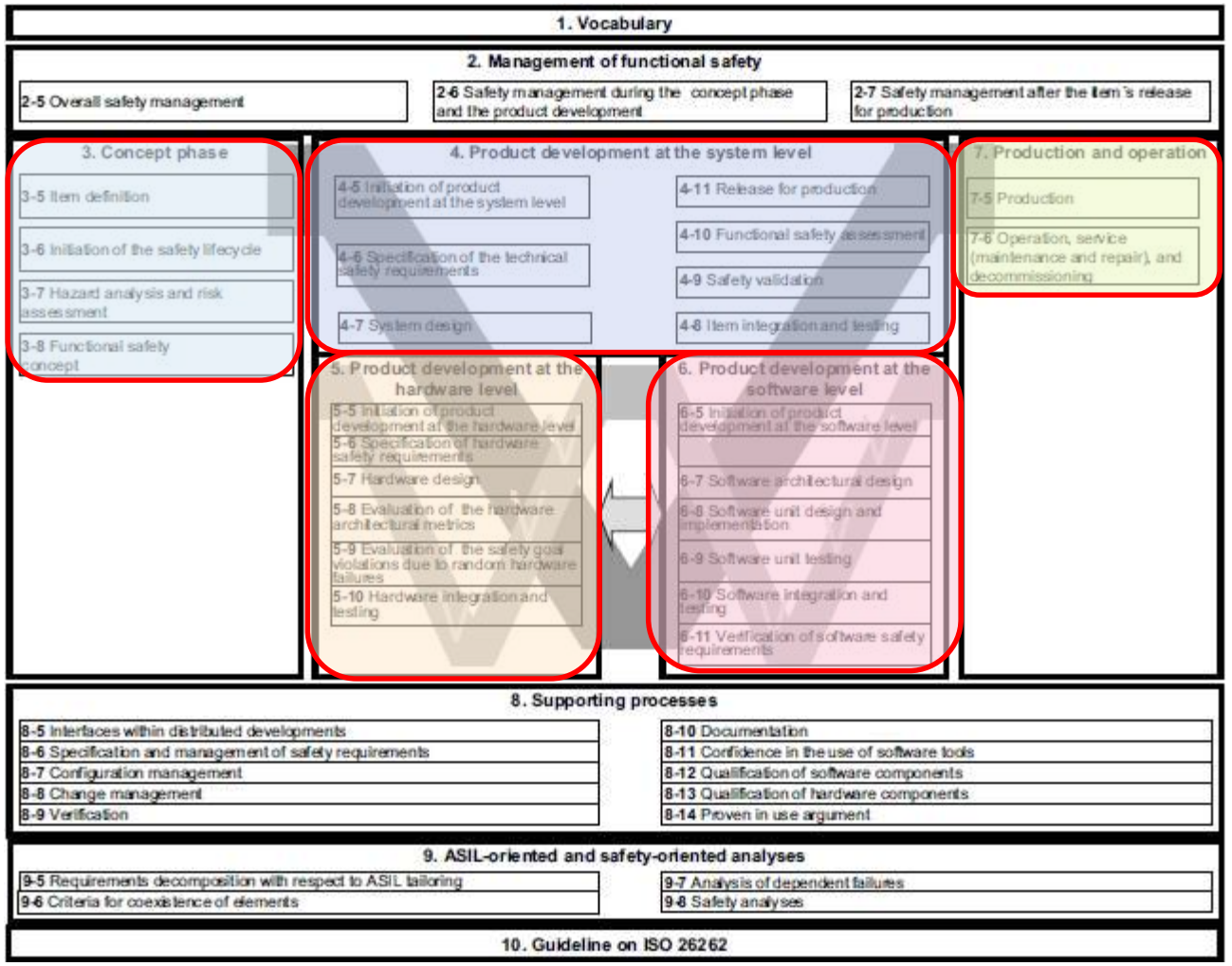
AVOID **SYSTEMATIC FAULTS**
(in development)

- Process
- Traceability
- Best practices
- Lessons learned
- Verification & validation

DETECT **RANDOM HW FAULTS**
(in operation)

- Safety concept / architecture
- Safety mechanisms
- Quantitative & qualitative analysis
- Documentation

Q: But who does what?



Focus of presentation

Reference ISO 26262-2:2011

Part 3 Concept

Determining ASIL

Severity

How much harm is done?

Exposure

How often is it likely to happen?

Controllability

Can the hazard be controlled?

ASIL

Concept

Hazard Analysis and Risk Assessment (HARA)

Concept

- Identify and categorize the hazards that can be triggered by malfunctions in the system
- The Risk Assessment is carried out using three criteria
  - **Severity** – how much harm is done?

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

  - **Exposure** – how often is it likely to happen?

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

  - **Controllability** – can the hazard be controlled?

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Reference ISO 26262-3:2011

Determination of ASIL and Safety Goals

Concept

- For each Hazardous event, determine the ASIL based on Severity, Exposure & Controllability
- Then formulate **safety goals** to prevent or mitigate each event, to avoid unreasonable risk

Q: So which ASIL should I target in my IC or IP?

Table 4 — ASIL determination

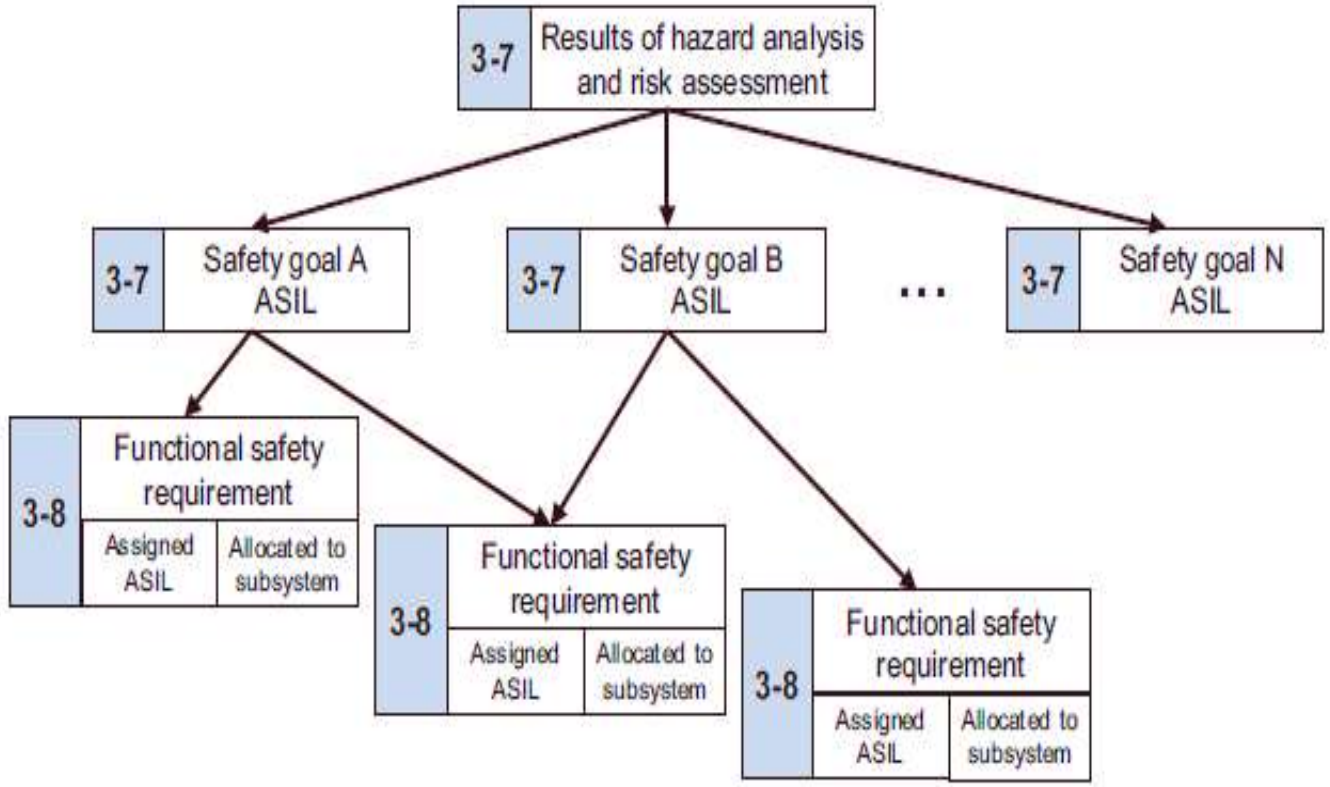
Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Reference ISO 26262-3:2011

Functional Safety Concept

Concept

- The functional safety concept addresses:
  - **Fault detection** and failure mitigation
  - **Safe State** transitioning
  - **Fault tolerance** mechanisms
  - **Driver warning**



Q: This is a top down approach, typically components & IP developed as Safety Element out of Context (SEooC), how to make assumptions?

*Note: An SEooC is a safety-related element which is **not developed for a specific item**. This means it is **not developed in the context of a particular vehicle**.*

Reference ISO 26262-3:2011

Part 4 System

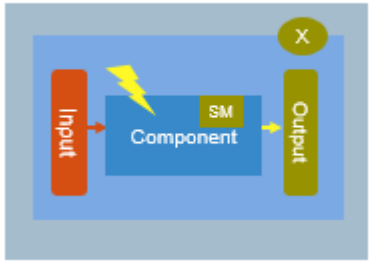
Safety Mechanisms & Faults

System

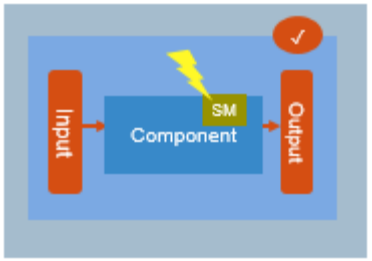
- A **safety mechanism** is a technical solution implemented by E/E functions or **elements**, or by **other technologies**, to detect **faults** or control **failures** in order to achieve or maintain a **safe state**

- **Safety mechanisms** are implemented to **prevent faults** from leading to **single-point failures** or to reduce **residual failures** and to prevent faults from being **latent**
  - **multiple-point fault** is a individual **fault** that, in combination with other independent faults, leads to a **multiple-point failure**.

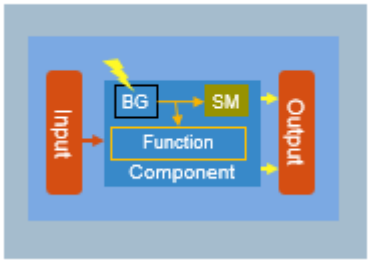
Single Point Fault



Latent Fault



Common Cause Fault



- Safety Mechanisms can take effect during
  - Power up (pre-drive checks)
  - During operation
  - During power-down (post-drive checks)
  - Part of maintenance.

Q: How to decide where to implement safety mechanisms? … in HW or SW, in system or component or IP…

Reference ISO 26262-1:2011

Fault Detection & Reaction Times

System

- **Diagnostic test interval**
  - amount of time between the executions of online diagnostic tests by a **safety mechanism**
- **Fault reaction time**
  - time-span from the detection of a **fault** to reaching the **safe state**
- **Fault tolerant time interval**
  - time-span in which a **fault** or faults can be present in a **system** before a **hazardous** event occurs
- **Multiple-point fault detection interval**
  - time span to **detect multiple-point fault** before it can contribute to a **multiple-point failure**

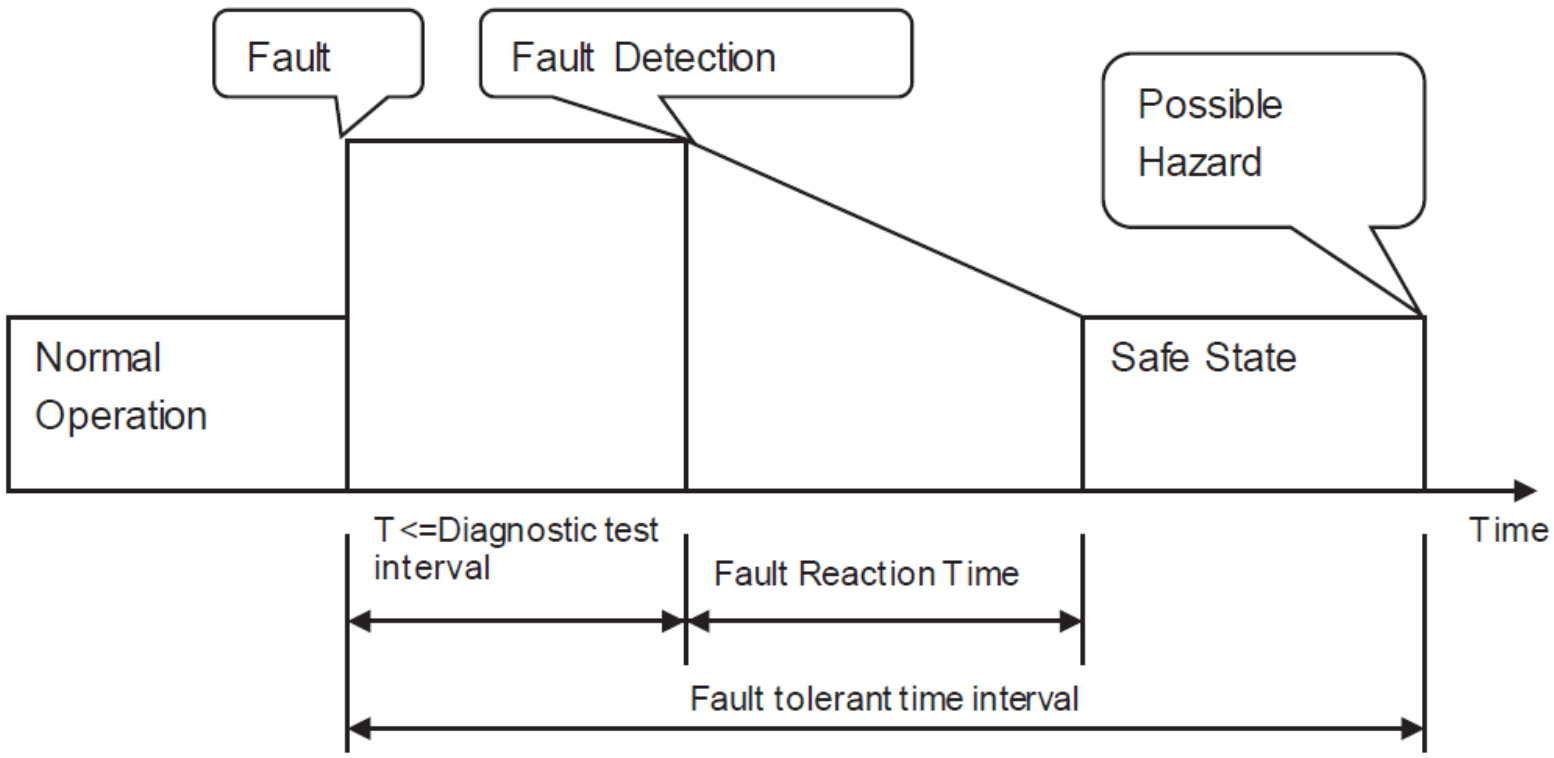
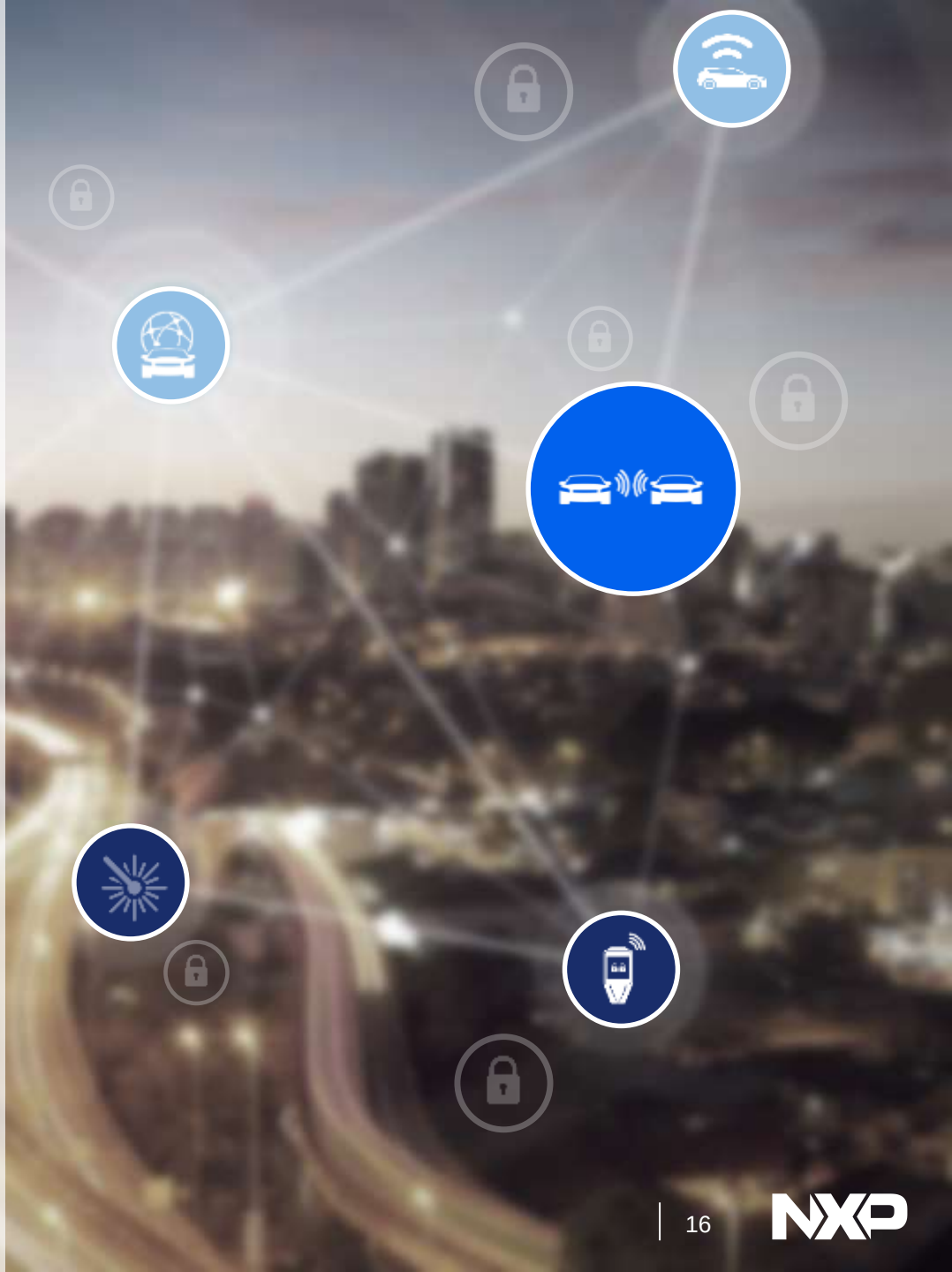


Figure 4 — Fault reaction time and fault tolerant time interval

Reference ISO 26262-1:2011

Q: How to know which times to use?
1ms, 10ms, 100ms, 1sec, 1hr, several hours etc

Part 5 Hardware



Target Metrics for ASIL

Hardware

- Associate the following target metrics to each **safety goal**
  - Single-point fault metric (SPFM)

Table 4 — Possible source for the derivation of the target "single-point fault metric" value

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

Q: Which faults to consider? How to justify diagnostic coverage? … Some guidance in Part 5 Annex D…

  - Latent-fault metric (LFM)

Table 5 — Possible source for the derivation of the target "latent-fault metric" value

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

  - Probabilistic Metric for random Hardware Failures (PMHF)

Table 6 — Possible source for the derivation of the random hardware failure target values

ASIL	Random hardware failure target values
D	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$

Q: Which portion of PMHF can an IC or IP use?

Reference ISO 26262-5:2011

Hardware Integration & Testing

Hardware

Table 11 — Hardware integration tests to verify the completeness and correctness of the safety mechanisms implementation with respect to the hardware safety requirements

Methods		ASIL			
		A	B	C	D
1	Functional testing[a]	++	++	++	++
2	Fault injection testing[b]	+	+	++	++
3	Electrical testing[c]	++	++	++	++

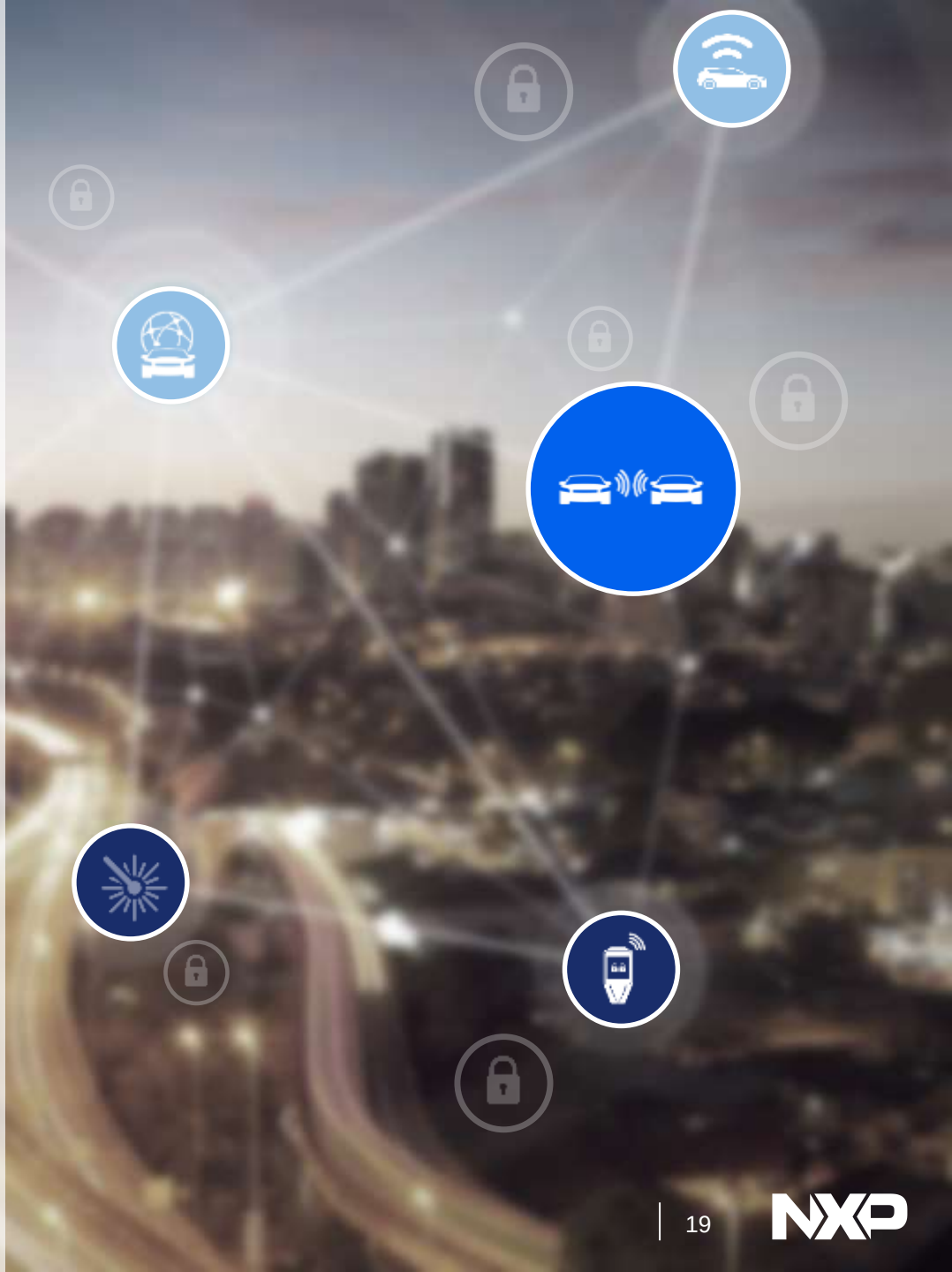
Table 12 — Hardware integration tests to verify robustness and operation under external stresses

Methods		ASIL			
		A	B	C	D
1a	Environmental testing with basic functional verification[a]	++	++	++	++
1b	Expanded functional test[b]	o	+	+	++
1c	Statistical test[c]	o	o	+	++
1d	Worst case test[d]	o	o	o	+
1e	Over limit test[e]	+	+	+	+
1f	Mechanical test[f]	++	++	++	++
1g	Accelerated life test[g]	+	+	++	++
1h	Mechanical Endurance test[h]	++	++	++	++
1i	EMC and ESD test[i]	++	++	++	++
1j	Chemical test [j]	++	++	++	++

Reference ISO 26262-5:2011

Q: Fairly standards tests, except for fault injection?

Part 6 Software



SW Safety Mechanisms

Software

Table 4 — Mechanisms for error detection at the software architectural level

Methods		ASIL			
		A	B	C	D
1a	Range checks of input and output data	++	++	++	++
1b	Plausibility check[a]	+	+	+	++
1c	Detection of data errors[b]	+	+	+	+
1d	External monitoring facility[c]	o	+	+	++
1e	Control flow monitoring	o	+	++	++
1f	Diverse software design	o	o	+	++

[a] Plausibility checks can include using a reference model of the desired behaviour, assertion checks, or comparing signals from different sources.

[b] Types of methods that may be used to detect data errors include error detecting codes and multiple data storage.

[c] An external monitoring facility can be, for example, an ASIC or another software element performing a watchdog function.

Table 5 — Mechanisms for error handling at the software architectural level

Methods		ASIL			
		A	B	C	D
1a	Static recovery mechanism[a]	+	+	+	+
1b	Graceful degradation[b]	+	+	++	++
1c	Independent parallel redundancy[c]	o	o	+	++
1d	Correcting codes for data	+	+	+	+

[a] Static recovery mechanisms can include the use of recovery blocks, backward recovery, forward recovery and recovery through repetition.

[b] Graceful degradation at the software level refers to prioritizing functions to minimize the adverse effects of potential failures on functional safety.

[c] Independent parallel redundancy can be realized as dissimilar software in each parallel path.

Reference ISO 26262-6:2011

Part 7 Production

Part 7 Production

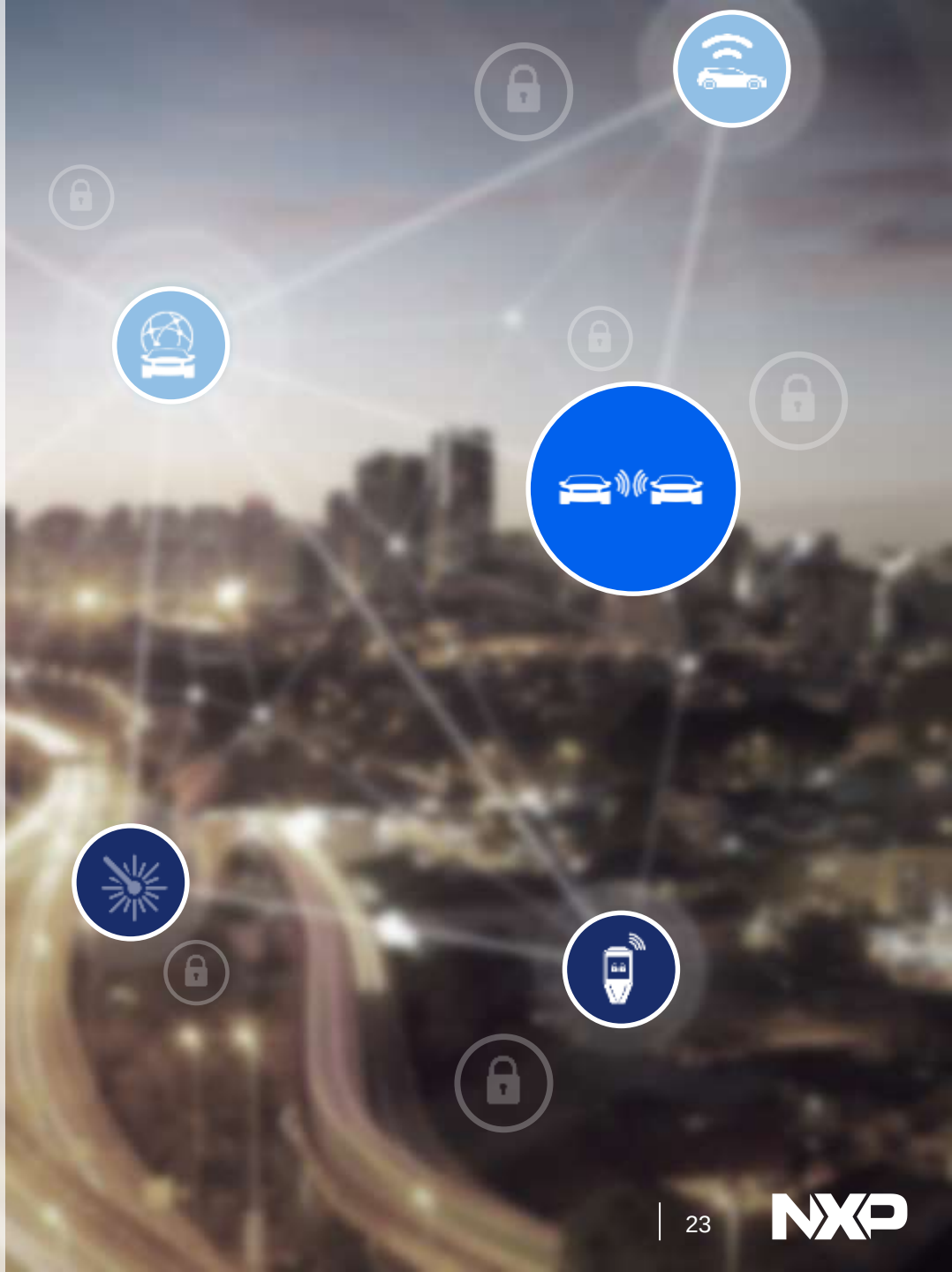
Production

- Develop and maintain a production process for safety-related elements or items that are intended to be installed in road vehicles.
  - **Typically existing production processes aligned with ISO TS 16949 are also well aligned with ISO 26262 requirements**

- In addition, the compliance with **safety-related special characteristics** may be required
  - Examples of such safety-related special characteristics are
    - specific process parameters (e.g. temperature range or fastening torque)
    - material characteristics
    - production tolerance
    - Configuration

- Also, safety impact analysis of changes or field returns is required during production -> augmenting standard processes to comply.

ISO 26262 2nd Edition



ISO 26262 2nd Edition

- The **2nd edition of ISO 26262** is planned for release in **2018**.

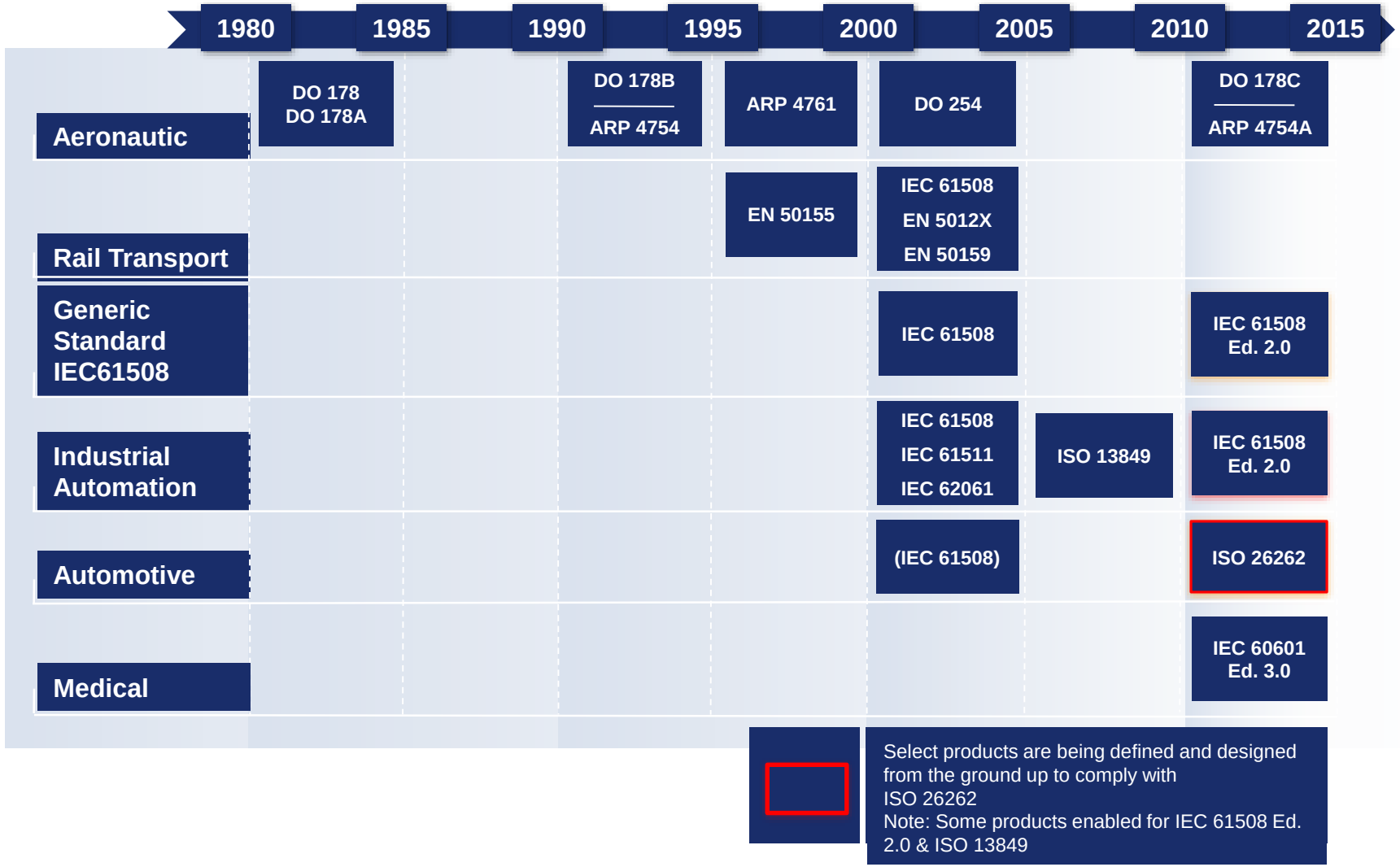
- **Most notable changes**
  - Scope now for series production road vehicles, except mopeds.
  - Specific content added for **Trucks, Buses, Trailers, Semitrailers** and **motorcycles** (although very minimal)
  - **Part 11** guideline added for **Semiconductors**
  - **Part 12** added for **motorcycles** (mapping of **MSIL** to ASIL)
  - Interaction between safety and **security** organizations mentioned (no specifics)
  - Method for **dependent failure analysis** provided in multiple examples
  - Guidance for **fault tolerance**
  - **Part 8.13** Hardware Qualification reworked to focus on non ISO 26262 developed hardware
  - Overall improvements to clarify understanding

- **Limited** new content towards **fail operational** / **autonomous vehicles** indicating not yet mature enough in industry to standardize

Disclaimer: Above notes from DIS version, may change in final release

NXP Approach to ISO 26262

Functional Safety Standards

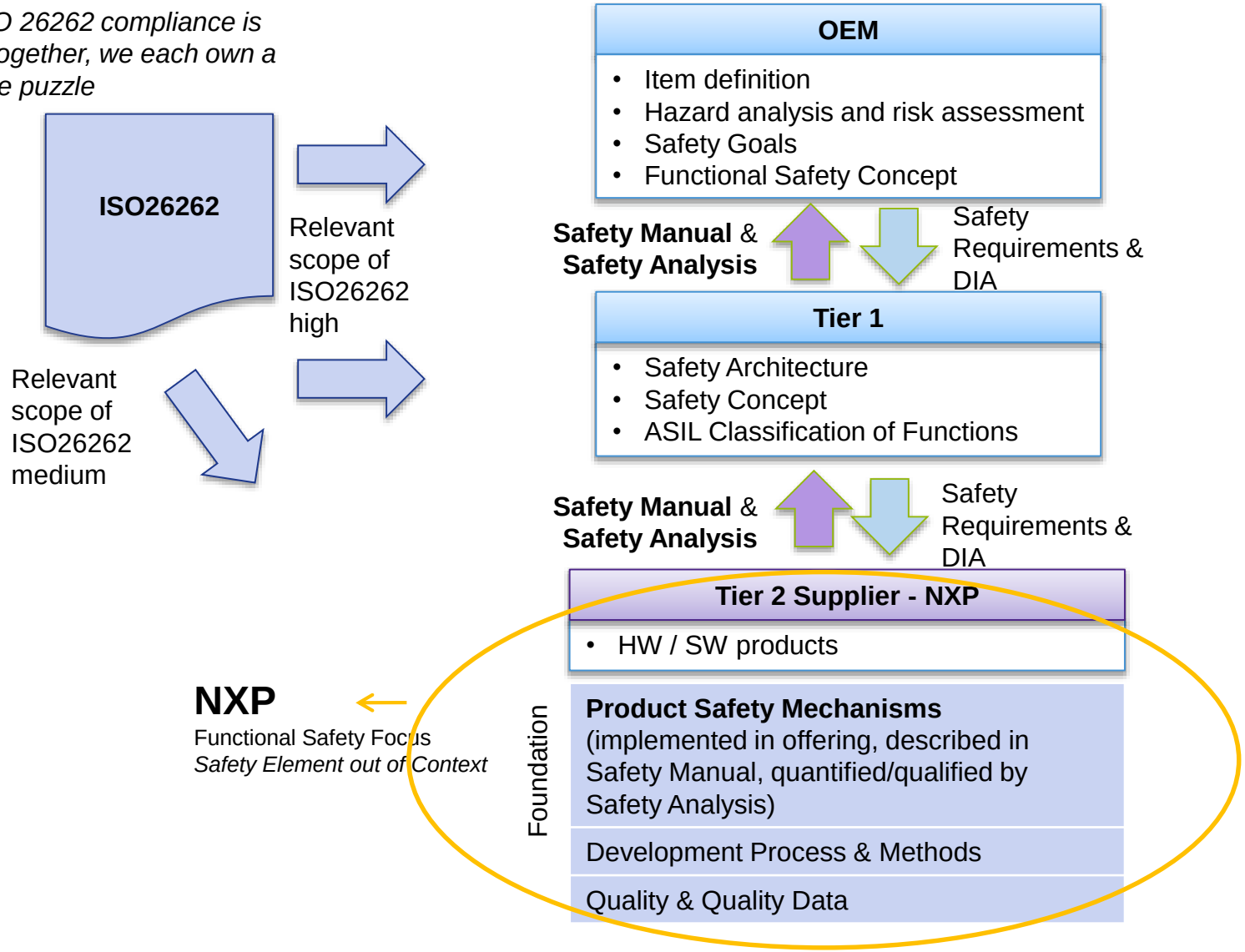


NXP's Safe Assure Program

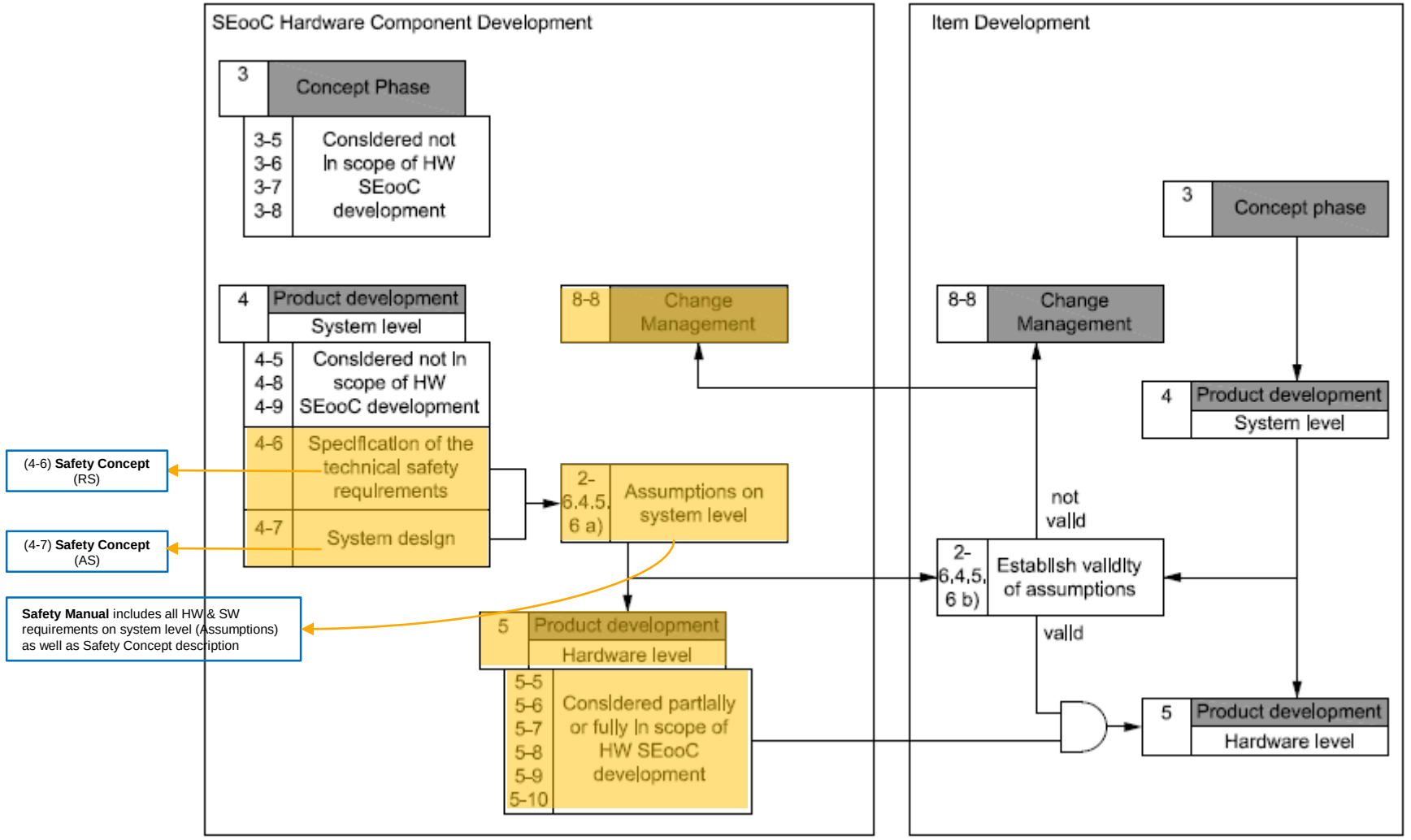
- Launched SafeAssure initiative in September 2011 focusing on NXP's functional safety solutions
- **NXP Development Processes** are aligned with ISO 26262 since 2013 across product lines
  - **BCaM7** deployment will align at BU Auto level
- **100+ Products** being developed to target ISO 26262:
  - Aug 2012 AMP HW – Leopard (MPC564xL) 32-bit MCU – Certified by Exida
  - 2013 AMP SW – First release of Safety MCAL (sMCAL)
  - 2014 AAA HW – Analog – PowerSBC
  - Many more products are in the development pipeline and will come to completion in the years to come

Example Interaction Between Car OEM, Tier 1 & Tier 2 (NXP)

Overall ISO 26262 compliance is achieved together, we each own a piece of the puzzle



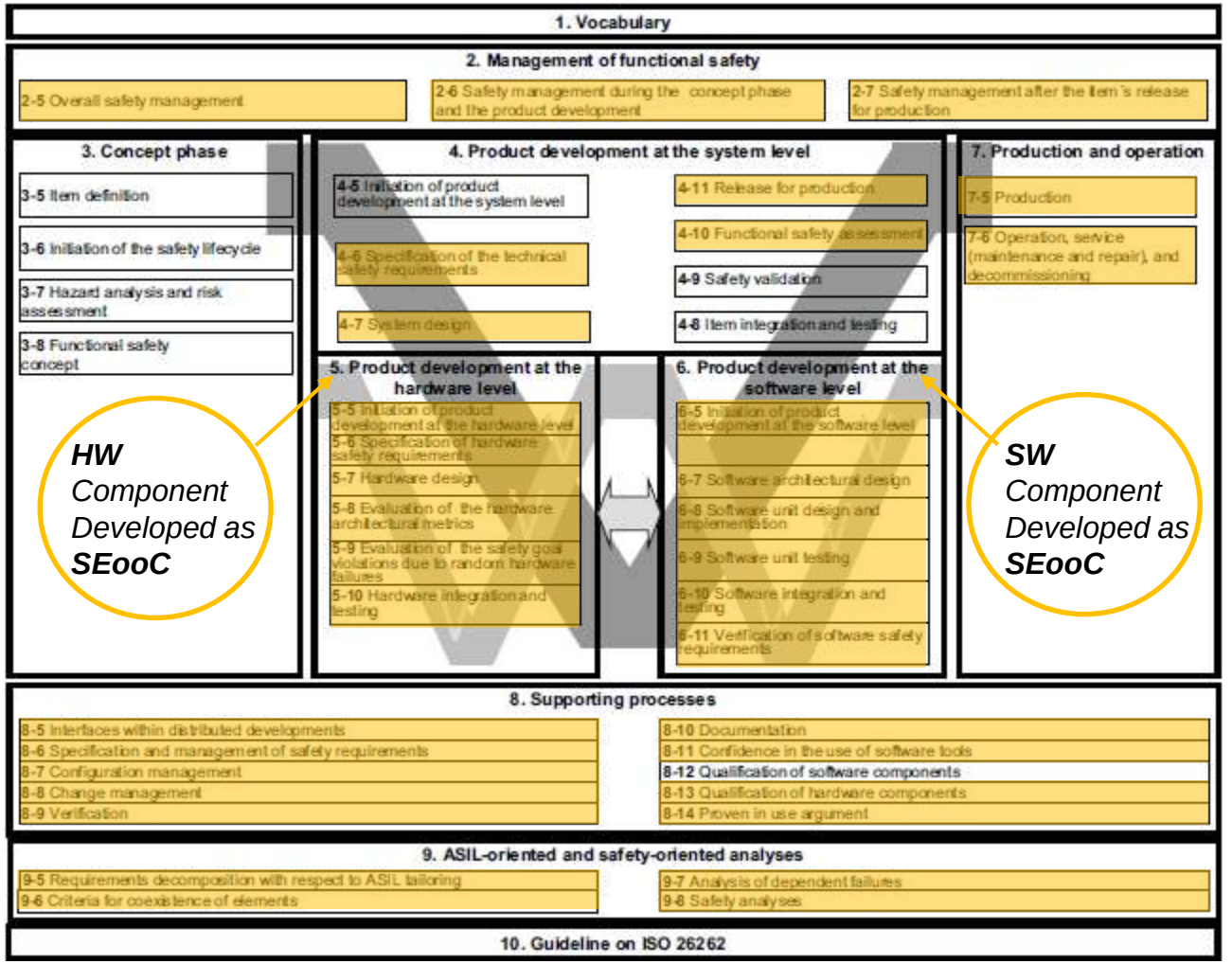
HW & SW Components developed as SEooC



Applicable to HW Component developed as SEooC

Reference ISO 26262-10:2012

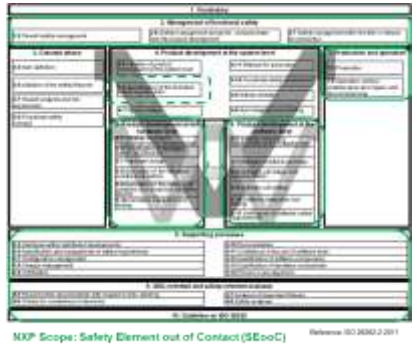
Tailoring of ISO26262 to Component developed as Safety Element out of Context (SEooC)



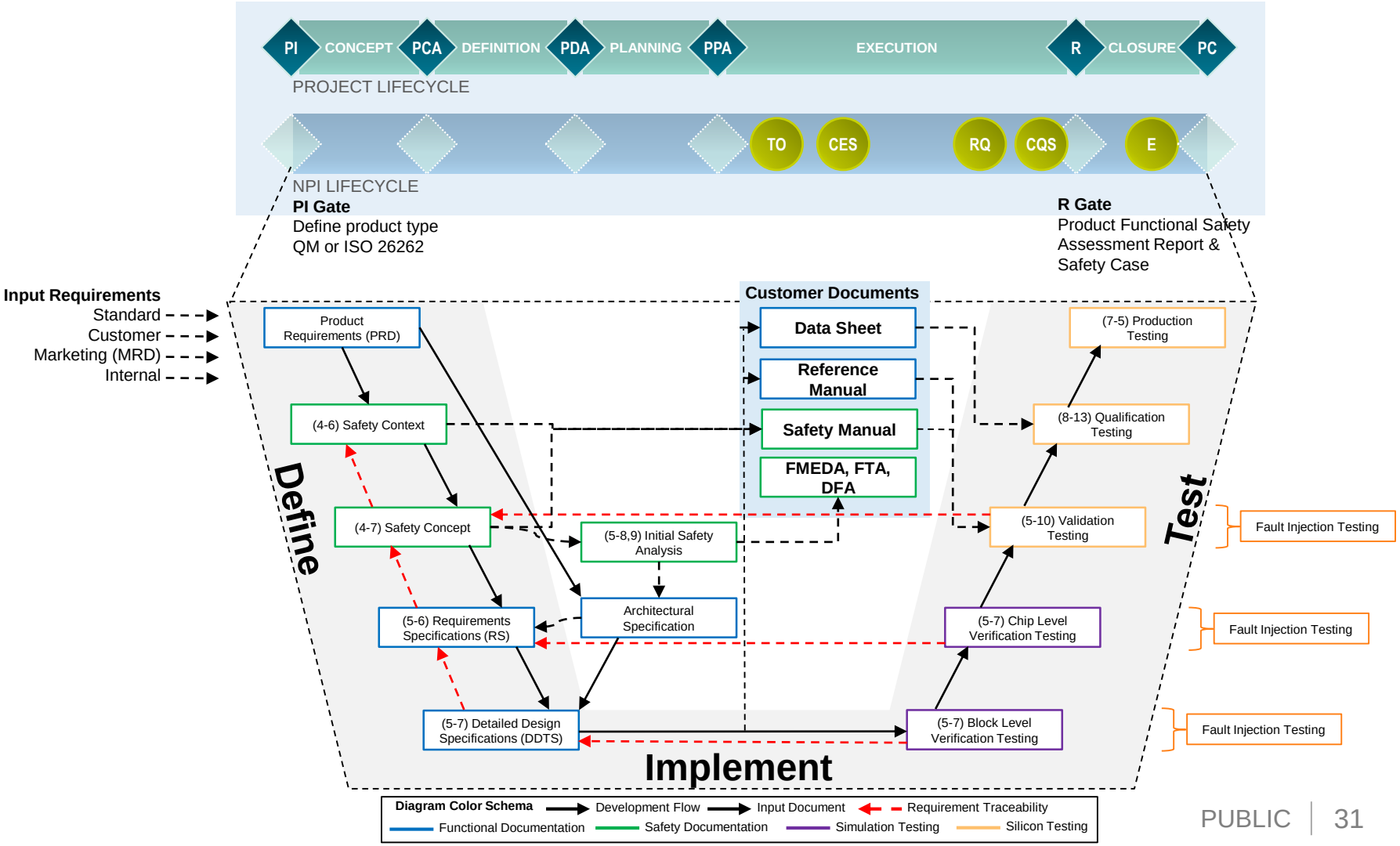
Applicable to Component developed as SEooC

Reference ISO 26262-10:2012

ISO 26262 Product Development - BCaM7



- ISO 26262 compliance is achieved between vehicle manufacturers, Automotive suppliers (Tier 1), semiconductor suppliers and IP providers



NXP Processes aligned with ISO 26262

- NXP ISO 26262 process complies with **all** applicable ISO 26262 **ASIL D** requirements for HW or SW SEooC development

ISO 26262	NXP Process	ASIL A	ASIL B	ASIL C	ASIL D
Part 2 Management	Safety Plan, Safety Case, Confirmation Measures	Yes			
***Part 3** Concept*	*OEM / Tier 1 responsibility*	*NA*			
Part 4 System	System assumptions & Safety Requirements – HW/SW	**Yes**, only partially applicable			
Part 5 Hardware	HW – Safety requirements traced to implementation and testing	Yes			
Part 6 Software	SW – Safety requirements traced to implementation and testing	Yes			
Part 7 Production	Standard processes, aligned with ISO 26262	Yes			
Part 8 Processes	Standard processes, aligned with ISO 26262	Yes			
Part 9 Analysis	FMEDA, FTA & DFA	Yes			
Part 10 Guideline	SEooC Development & application of ISO 26262 to components	**Yes**, SEooC development			

- **One process for all products**, regardless of safety architecture ASIL target
- Only **difference** is for Confirmation Measures which are tailored to ASIL target

NXP ISO 26262 Confirmation Measures

- NXP performs ISO 26262 Confirmation Reviews (CR), Audit and Assessment as required by ISO 26262 for SEooC development

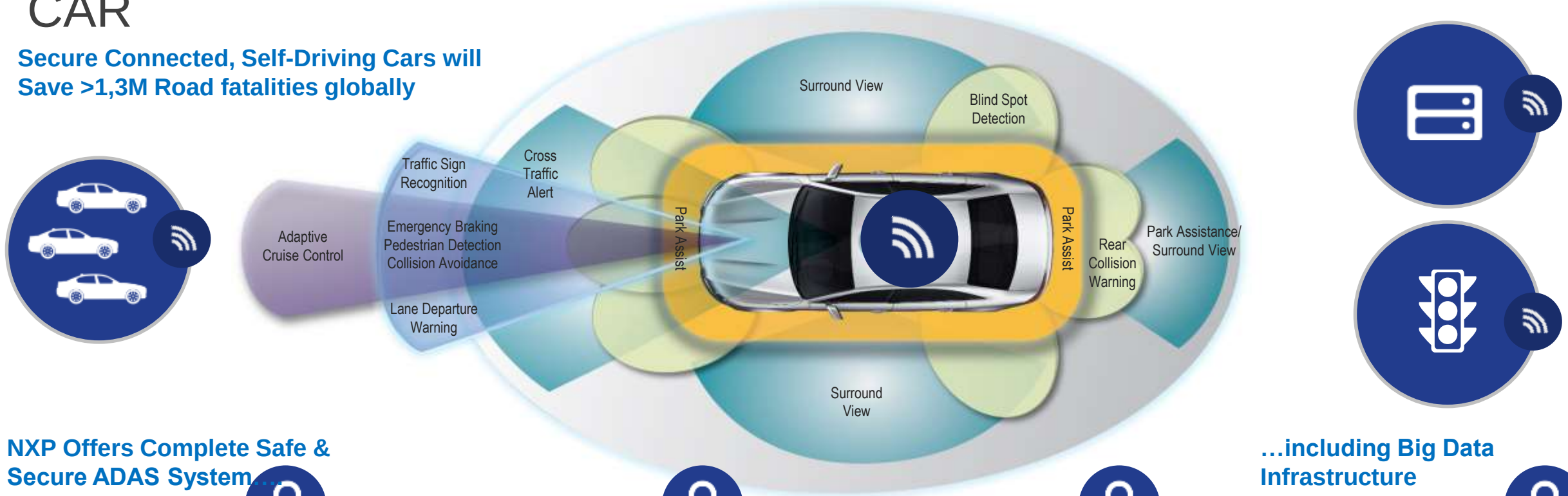
Confirmation Measures	ASIL A	ASIL B	ASIL C	ASIL D
CR Safety Analysis	Yes	Yes	Yes	Yes
CR Safety Plan		Yes	Yes	Yes
CR Safety Case		Yes	Yes	Yes
CR Software Tools			Yes	Yes
Audit			Yes	Yes
Assessment			Yes	Yes

Note: The following confirmation reviews are not applicable: hazard analysis and risk assessment, item integration and testing, validation plan & proven in use argument

- Confirmation Measures (CM) performed depending on ASIL
  - All checks executed with **independence level I3** by NXP Quality organization
  - NXP Assessors **certified** by SGS-TÜV Saar as *Automotive Functional Safety Professional (AFSP)*
  - NXP CM process **certified** by SGS-TÜV Saar as ISO 26262 ASIL D

TOMORROW: ENABLING THE SAFE & SECURE CONNECTED CAR

Secure Connected, Self-Driving Cars will Save >1,3M Road fatalities globally



NXP Offers Complete Safe & Secure ADAS System…

SENSE	Secure Network	THINK	Secure Network	ACT
Radar Vision Secure V2X		Processing Sensor Fusion Security		Powertrain Chassis Braking

…including Big Data Infrastructure

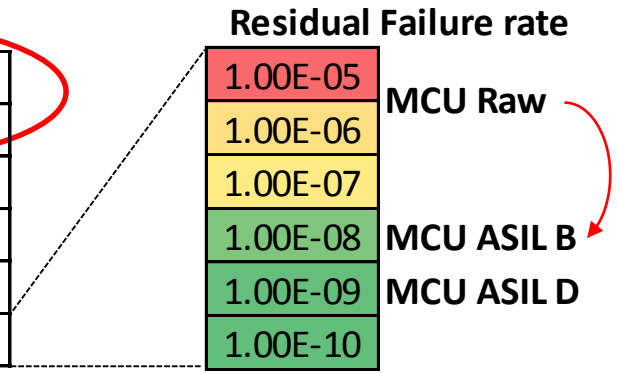
BIG DATA
Digital Networking Infrastructure Security

Where the Failures Come From

- Typically, dangerous failures in a safety system come from a combination of the following
  - **Development bugs** – **Software** or **hardware**
  - **Insufficient system safety architecture**
  - **Transient failures** in semiconductors, primarily **SRAM** – very high rate of occurrence
  - **Permanent failures** in **hardware**

- For a MCU the break down of Failures is typically:

Failure Type	per hour	FIT	%
MCU SRAM Transient Failure rate	7.00E-07	700	70.00%
MCU FF Transient Failure rate	2.00E-07	200	20.00%
MCU Package Permanent Failure rate	8.00E-08	80	8.00%
MCU Die Permanent Failure rate	2.00E-08	20	2.00%
MCU Total Failure rate	1.00E-06	1000	100%



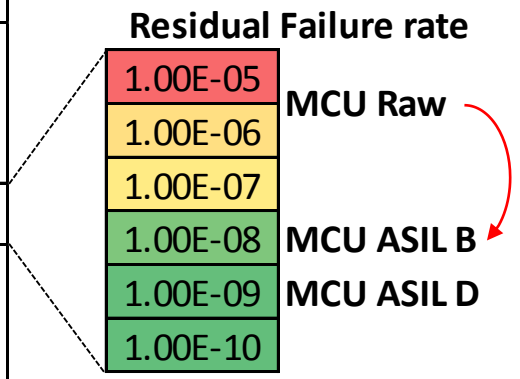
Note: Assumption - MCU is allocated only 10% of System ASIL target

MCU Safety Context

- Applications have different safety requirements driven by different safety contexts, but the need for safe SW execution is common across all

- The objective is to make SW execution safe to achieve **ASIL B or ASIL D** depending on target market

		ASIL B	ASIL D
Detect incorrect operation during runtime	Fault Detection Time Interval	**10 ms**	
	Diagnostic Coverage (transient & permanent faults)	**90%**	**99%**
	Residual Failure rate	**1 x 10^{-8} / h**	**1 x 10^{-9} / h**
Start-up / Shut-down periodic test	Diagnostic Coverage (permanent faults)	**60%**	**90%**
MCU HW to support SW Independence		**MPU**	



Note: Assumption - MCU is allocated only 10% of System ASIL target

Defining the Safety Concept

- Objective
  - Define how ASIL targets will be achieved between a mix of on-chip HW safety measures and system level safety measures (HW/SW)

- ISO 26262-5 Annex D – Elements related to HW Components
  - Low application dependency: Power, Clock, Flash, SRAM & Processing Unit
  - High application dependency: Digital IO & Analog IO

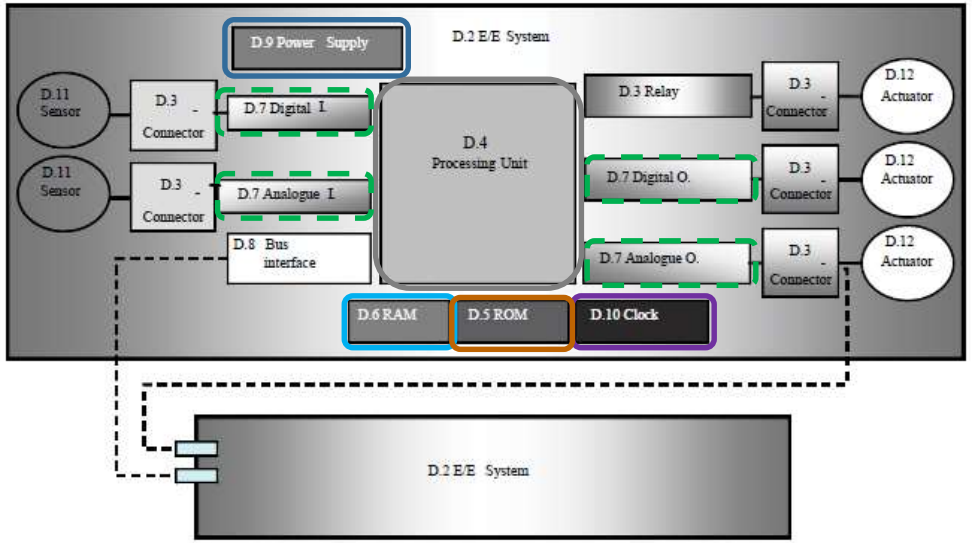


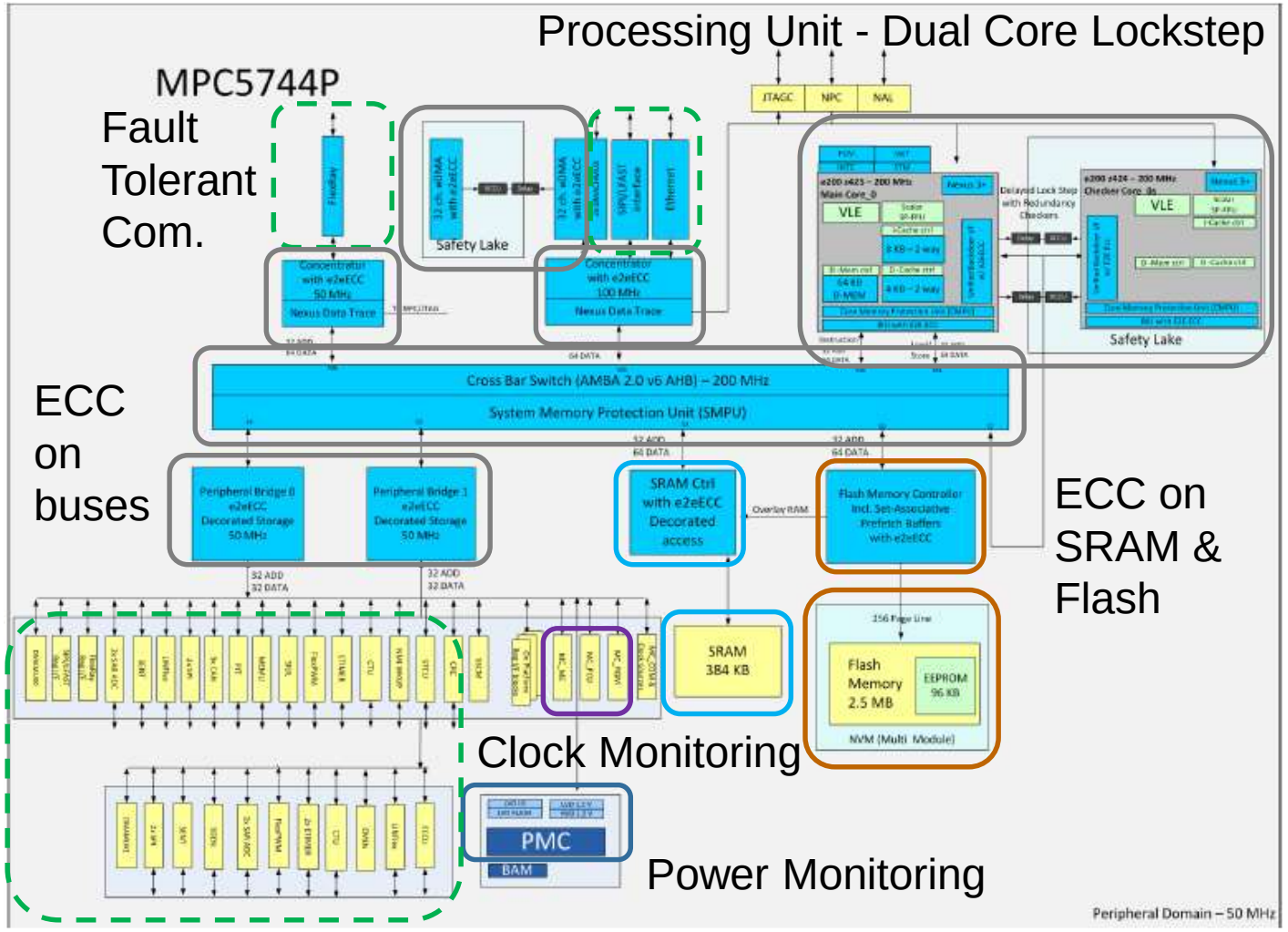
Figure D.1 — Generic hardware of a system *Reference ISO 26262-5:2011*

Module Classification - Safety

- Each module on the MCU is classified as Safety Related or Not Safety Related

Elements in ISO 26262-5, Table D.1	MPC5744P FMEDA	MPC5744P Module	Part of Software Execution Function	Safety Mechanism	Comments
Power Supply	**Power**	Power Management Controller (PMC)	YES		
		Power Control Unit (MC_PCU)	YES		
Clock	**Clock**	Phase Lock Loop (2 x PLL)	YES		
		Clock Monitor Unit (5 x CMU)		YES	
		Clock Generation Module (MC_CGM)	YES		
		External Oscillator (XOSC)	YES		
		Internal RC Oscillator (IRCOSC)	YES		
Non-Volatile Memory	**Flash**	Embedded Flash Memory (c55fmc)	YES		
		Flash Memory Controller (PFLASH)	YES		
		End-to-end Error Correction Code (e2eECC)		YES	
Volatile Memory	**SRAM**	System SRAM	YES		
		RAM Controller (PRAMC)	YES		
		End-to-end Error Correction Code (e2eECC)		YES	
Processing Unit	**Core**	Main Core_0 (e200z4251n3)	YES		
		Checker Core_0s (e200z424) *(Delayed Lockstep)*		YES	
		Crossbar Switch (XBAR)	YES		
		JTAG Controller (JTAGC)			Not Safety Related module - Debug logic
		Nexus debug modules (NXMC, NPC, NAL & NAP)			Not Safety Related module - Debug logic
		Cyclic Redundancy Check (CRC)		YES	
		Fault Collection and Control Unit (FCCU)		YES	
		Memory Error Management Unit (MEMU)		YES	
		Self-Test Control Unit (STCU2) *(includes MBIST & LBIST)*		YES	
		Register Protection (REG_PROT)		YES	
Communication (External)	**Peripheral**	CAN (3 x FlexCAN)			Peripheral module - High application dependency (failure rates only)
		Serial Interprocessor Interface (SIPI)			Peripheral module - High application dependency (failure rates only)
		10/100-Mbps Ethernet MAC (ENET)			Peripheral module - High application dependency (failure rates only)
Analogue I/O and Digital I/O		Peripheral Bridge (2 x PBRIDGE)			Peripheral module - High application dependency (failure rates only)
		System Integration Unit Lite2 (SIUL2)			Peripheral module - High application dependency (failure rates only)
		Analog to Digital Converter (4 x ADC)			Peripheral module - High application dependency (failure rates only)
		Wakeup Unit (WKPU)			Peripheral module - High application dependency (failure rates only)

Realizing the MCU Safety Concept - MPC5744P

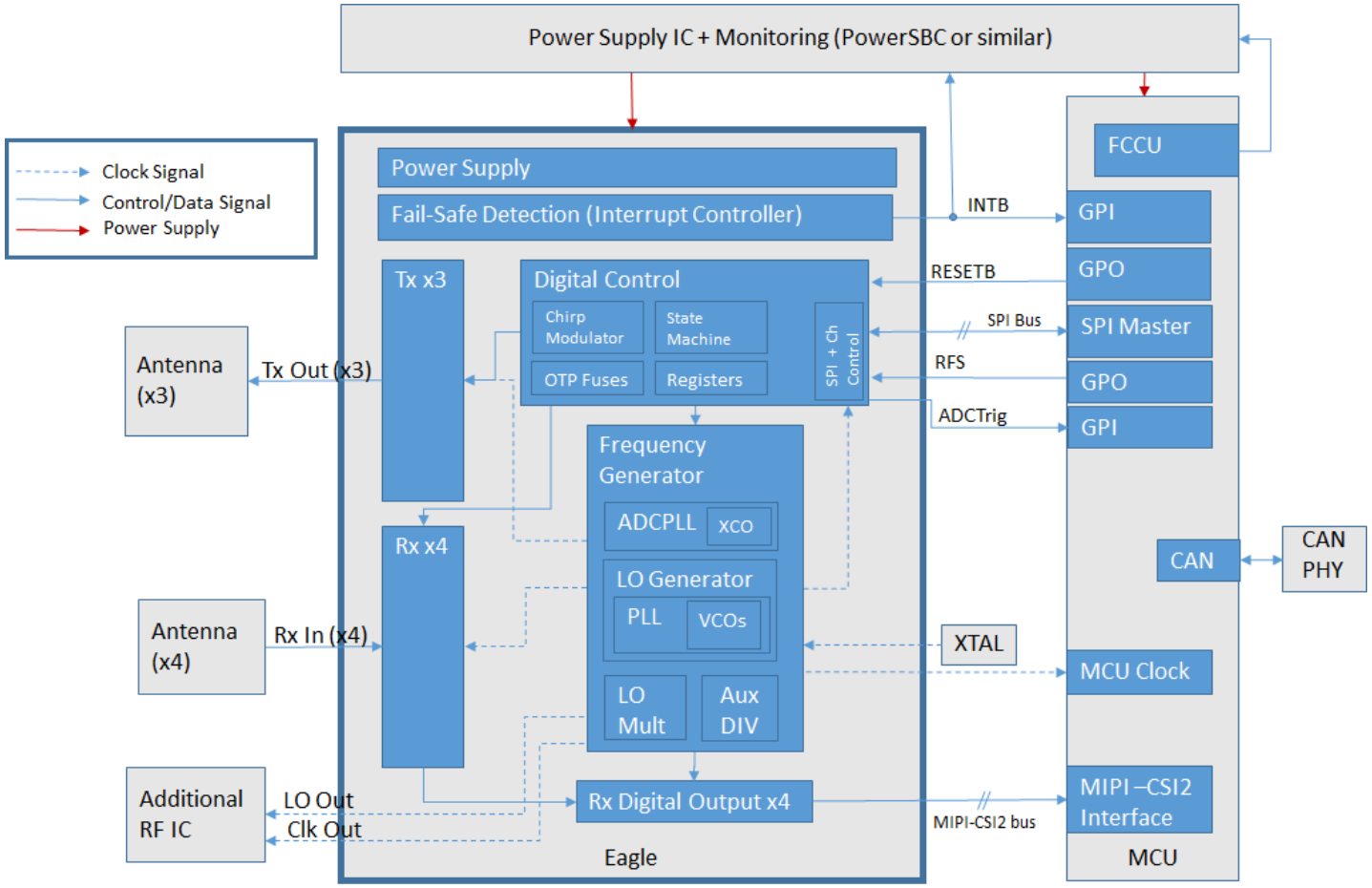


Redundant use of IO & Application checks

Defining the Safety Concept – RADAR Example

- Objective
  - Define how ASIL targets will be achieved between a mix of on-chip HW safety measures and system level safety measures (HW/SW)

- ISO 26262-5 Annex D – Elements related to HW Components
  - Low application dependency: Power, Clock, Flash, SRAM & Processing Unit
  - High application dependency: RF, Digital & Analog IO



Customer Deliverables

NXP SafeAssure Products

To support the customer to build his safety system, the following deliverables are provided **as standard** for **all** ISO 26262 developed products.

- **Public Information available via NXP Website**
  - Quality Certificates
  - Safety Manual
  - Reference Manual
  - Data Sheet

- **Confidential Information available under NDA**
  - Safety Plan
  - ISO 26262 Safety Case
  - Permanent Failure Rate data (Die & Package) - IEC/TR 62380 or SN29500
  - Transient Failure Rate data (Die) - JEDEC Standard JESD89
  - Safety Analysis (FMEDA, FTA, DFA) & Report
  - PPAP
  - Confirmation Measures Report (summary of all applicable confirmation measures)

Safety Manual

Safety Manual

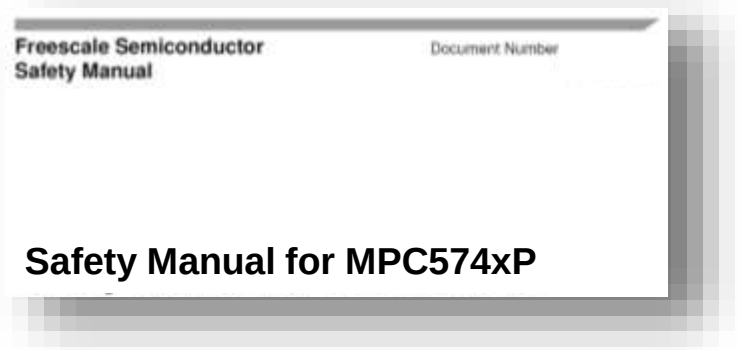
Objective

- Enables customers to build their safety system using the MCU safety mechanisms and defines system level HW & SW assumptions
- Simplify integration of NXP's safety products into applications
- A comprehensible description of all information relating to FS in a single entity to ensure integrity of information

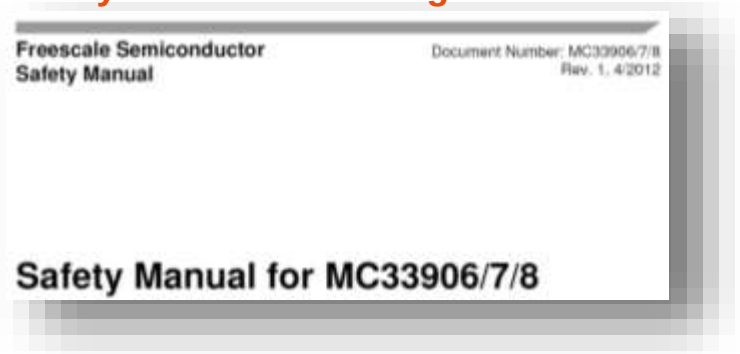
Content

- MCU Safety Context
- MCU Safety Concept
- System level hardware assumptions
- System level software assumptions
- FMEDA summary
- Dependent Failures Analysis summary

Safety Manual for MCU Solution



Safety Manual for Analog Solution



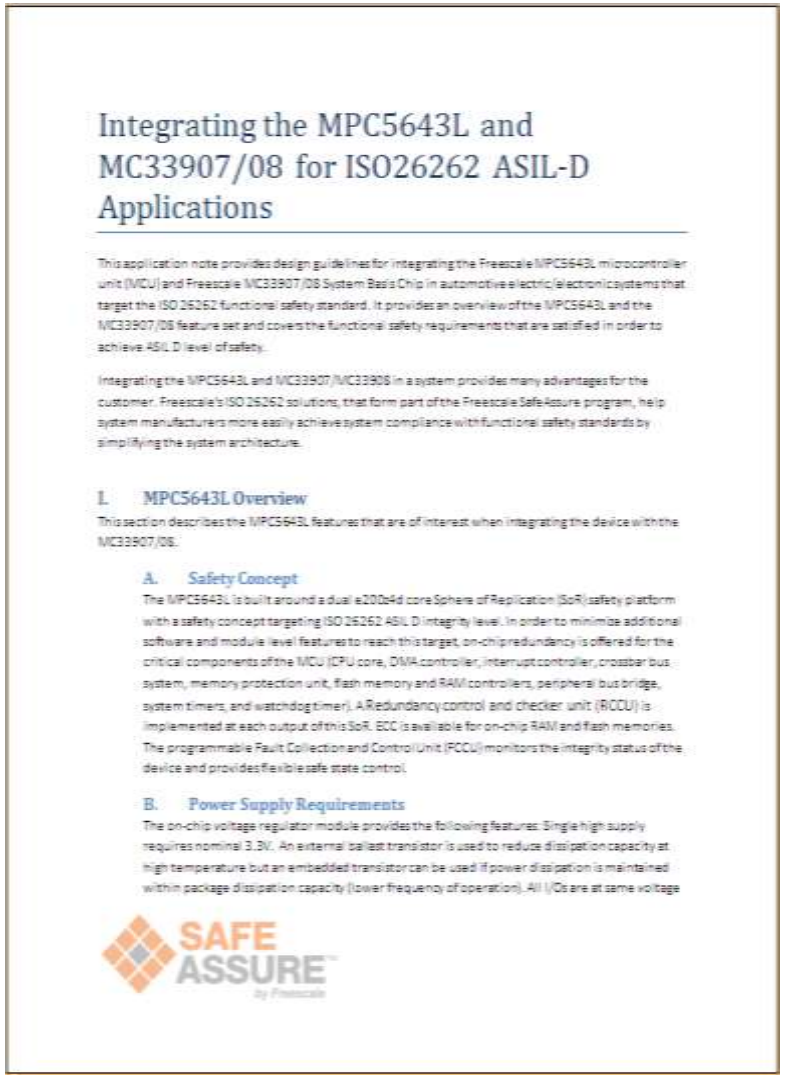
Safety Manual: Structure

- **MCU Safety Context**
  - Safe states, Fault tolerant time interval
- **MCU Safety Concept**
  - Describes the safety concept of the device (what is implemented and how does it work)
- **System level hardware assumptions**
  - Describes the functions required by external hardware to complement the MCU safety concept (Error out monitor)
- **System level software assumptions**
  - Description of necessary or recommended sw mechanisms for each module (Initial checks, configuration & runtime checks)
- **Failure Rates and FMEDA**
  - Short introduction to FMEDA
- **Dependent Failure Analysis**
  - βic – IEC 61508 Ed. 2.0 part 2, Annex E: Analysis of dependent failures
  - Countermeasures against common cause failures on chip level

Safety Support – System Level Application Notes

Design Guidelines for

- Integration of Microcontroller and Analog & Power Management device
- Explains main individual product Safety features
- Uses a typical Electrical Power steering application to explain product alignment
- Covers the ASIL D safety requirements that are satisfied by using both products:
  - MPC5643L requires external measures to support a system level ASIL D safety level
  - MC33907/08 provides those external measures:
    - External power supply and monitor
    - External watchdog timer
    - Error output monitor



Integrating the MPC5643L and MC33907/08 for ISO26262 ASIL-D Applications

This application note provides design guidelines for integrating the Freescale MPC5643L microcontroller unit (MCU) and Freescale MC33907/08 System Basis Chip in automotive electric/electronic systems that target the ISO 26262 functional safety standard. It provides an overview of the MPC5643L and the MC33907/08 feature set and covers the functional safety requirements that are satisfied in order to achieve ASIL D level of safety.

Integrating the MPC5643L and MC33907/MC33908 in a system provides many advantages for the customer. Freescale's ISO 26262 solutions, that form part of the Freescale SafeAssure program, help system manufacturers more easily achieve system compliance with functional safety standards by simplifying the system architecture.

I. MPC5643L Overview

This section describes the MPC5643L features that are of interest when integrating the device with the MC33907/08.

A. Safety Concept

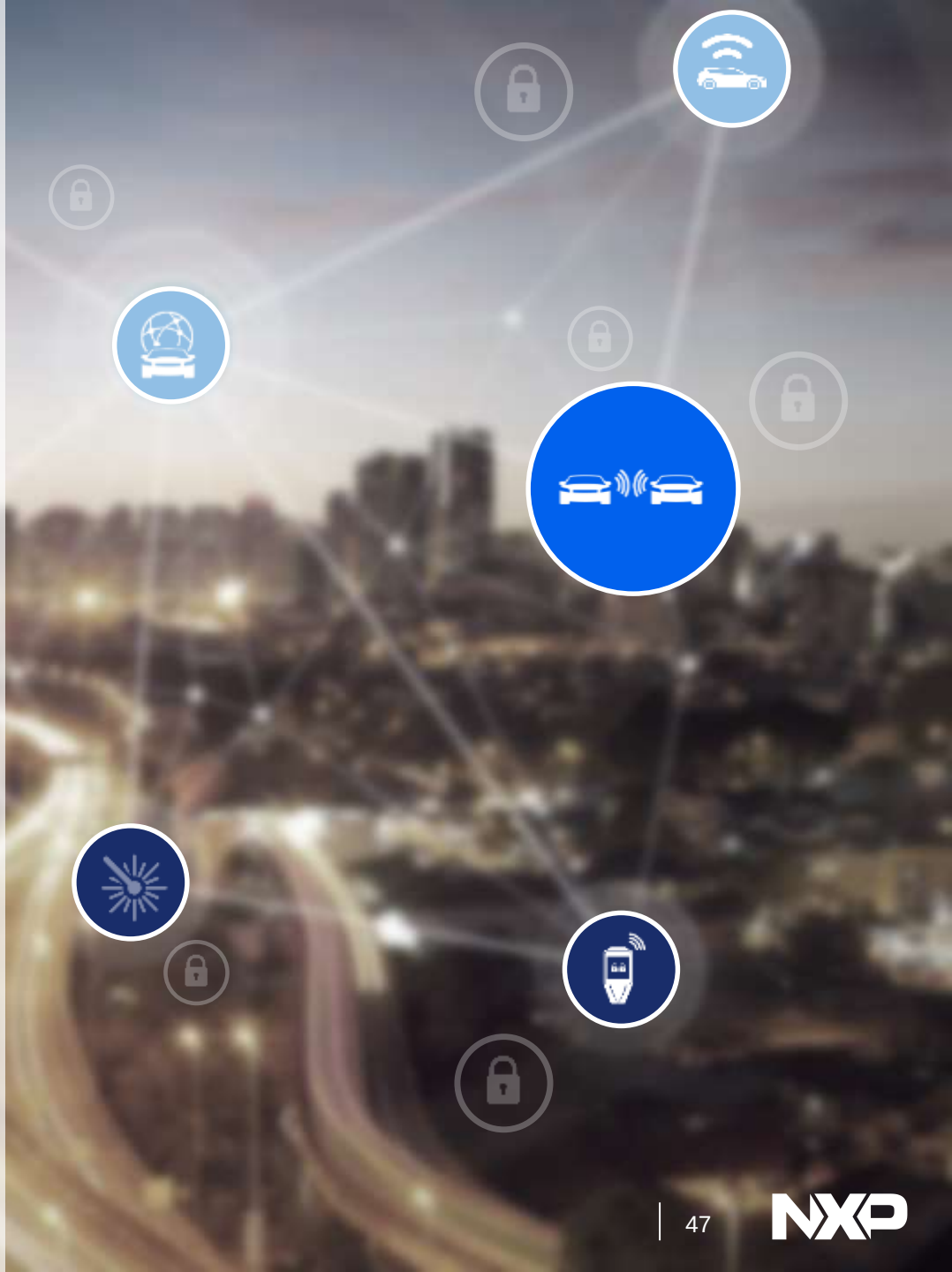
The MPC5643L is built around a dual e200z4d core Sphere of Replication (SoR) safety platform with a safety concept targeting ISO 26262 ASIL D integrity level. In order to minimize additional software and module level features to reach this target, on-chip redundancy is offered for the critical components of the MCU (CPU core, DMA controller, interrupt controller, crossbar bus system, memory protection unit, flash memory and RAM controllers, peripheral bus bridge, system timers, and watchdog timer). A Redundancy control and checker unit (RCCU) is implemented at each output of this SoR. ECC is available for on-chip RAM and flash memories. The programmable Fault Collection and Control Unit (FCCU) monitors the integrity status of the device and provides flexible safe state control.

B. Power Supply Requirements

The on-chip voltage regulator module provides the following features: Single high supply requires nominal 3.3V. An external ballast transistor is used to reduce dissipation capacity at high temperature but an embedded transistor can be used if power dissipation is maintained within package dissipation capacity (lower frequency of operation). All I/Os are at same voltage

SAFE ASSURE

Dynamic FMEDA



Safety Support – Dynamic FMEDA

Objective

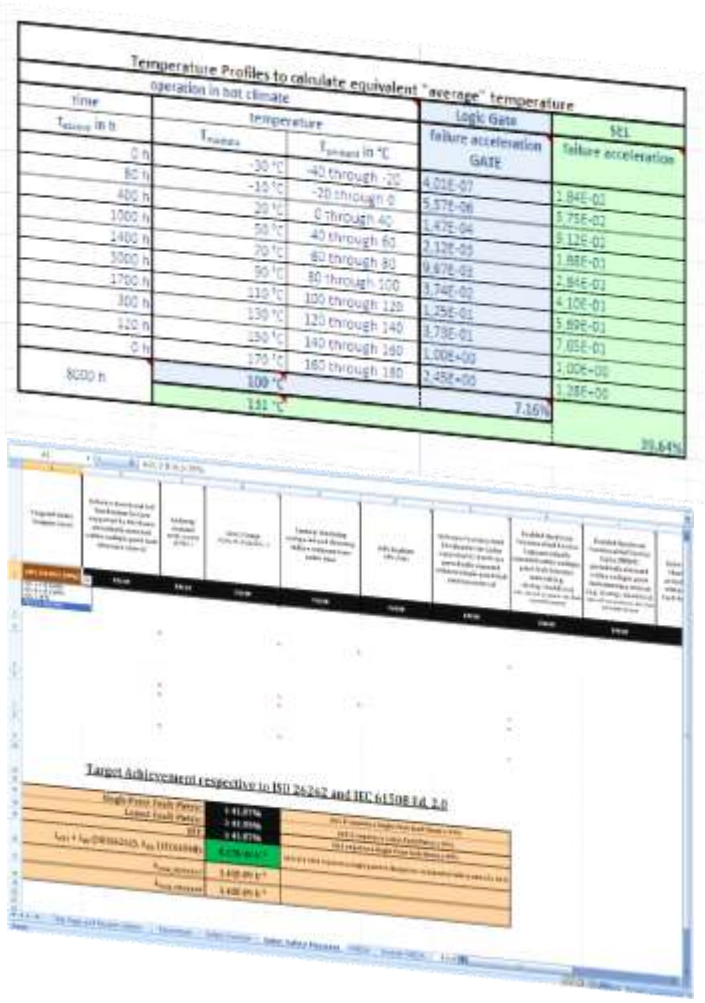
- Tailor FMEDA to match application configuration
- Enables customers, by supporting their system level architectural choices

Content

- FMEDA methods aligned with functional safety standards
  - SPFM & LFM, PMFH – ISO 26262
  - SFF & PFH- IEC 61508 Ed. 2.0
  - βic – IEC 61508 Ed. 2.0 part 2, Annex E
- Dynamic FMEDA covers elements with low application dependency: Clock, Power Supply, Flash, SRAM, Processing Unit…

Work flow and result

- Customer specifies the failure model (dependent on Safety Integrity Level) required by their application, and then confirms the Safety Measures that will be used or not be used
- A tailored FMEDA is then supplied to customer's for their specific application



ISO 26262-5 (Elements and Failure Models)

FMEDA Supply

FMEDA Clock

FMEDA Flash

FMEDA SRAM

Failure Rate Table

Table D.1 — Analyzed faults or failures modes in the derivation of diagnostic coverage

Element	See Tables	Analyzed failure modes for 60 %/90 %/99 % DC		
		Low (60 %)	Medium (90 %)	High (99 %)
General semiconductor elements				
Power supply	D.9	Under and over Voltage	Drift Under and over Voltage	Drift and oscillation Under and over Voltage Power spikes
Clock	D.10	Stuck-at[a]	d.c. fault model[b]	d.c. fault model[b] Incorrect frequency Period jitter
Non-volatile memory	D.5	Stuck-at[a] for data and addresses and control interface, lines and logic	d.c. fault model[b] for data and addresses (includes address lines within same block) and control interface, lines and logic	d.c. fault model[b] for data, addresses (includes address lines within same block) and control interface, lines and logic
Volatile memory	D.6	Stuck-at[a] for data, addresses and control interface, lines and logic	d.c. fault model[b] for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model[c] for bit cells	d.c. fault model[b] for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model[c] for bit cells
Digital I/O	D.7	Stuck-at[a] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation
Analogue I/O		Stuck-at[a] (including signal lines outside of the microcontroller)	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation	d.c. fault model[b] (including signal lines outside of the microcontroller) Drift and oscillation

Reference ISO 26262-5:2011

ISO 26262-5 (Elements and Failure Models)

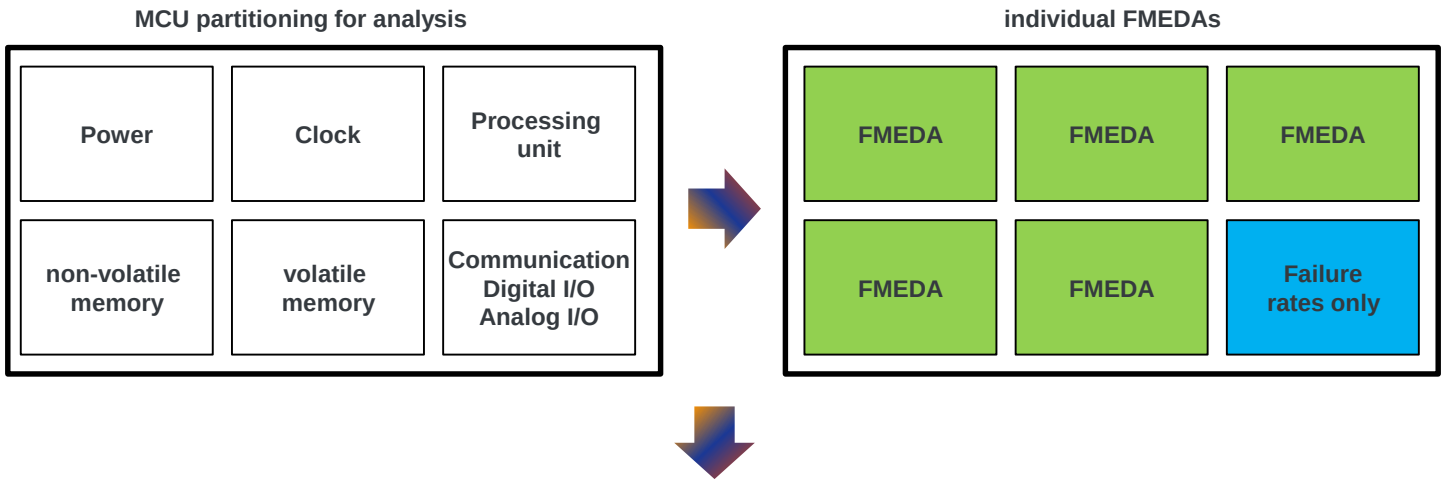
FMEDA
Processing
Unit

Table D.1 — Analyzed faults or failures modes in the derivation of diagnostic coverage

	Element	See Tables	Analyzed failure modes for 60 %/90 %/99 % DC		
			Low (60 %)	Medium (90 %)	High (99 %)
	Specific semiconductor elements				
Processing units	ALU - Data Path	D.4/D.13	Stuck-at[a]	Stuck-at[a] at gate level	d.c. fault model[b] Soft error model[c] (for sequential parts)
	Registers (general purpose registers bank, DMA transfer registers…), internal RAM	D.4	Stuck-at[a]	Stuck-at[a] at gate level Soft error model[c]	d.c. fault model[b] including no, wrong or multiple addressing of registers Soft error model[c]
	Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	D.4/D.5/D.6	Stuck-at[a]	Stuck-at[a] at gate level Soft error model[c] (for sequential parts)	d.c. fault model[b] including no, wrong or multiple addressing Soft error model[c] (for sequential parts)
	Interrupt handling	D.4/D.10	Omission of or continuous interrupts	Omission of or continuous interrupts Incorrect interrupt executed	Omission of or continuous interrupts Incorrect interrupt executed Wrong priority Slow or interfered interrupt handling causing missed or delayed interrupts service
	Control logic (Sequencer, coding and execution logic including flag registers and stack control)	D.4/D.10	No code execution Execution too slow Stack overflow/underflow	Wrong coding or no execution Execution too slow Stack overflow/underflow	Wrong coding, wrong or no execution Execution out of order Execution too fast or too slow Stack overflow/underflow
	Configuration Registers	D.4	—	Stuck-at[a] wrong value	Corruption of registers (soft errors) Stuck-at[a] fault model
	Other sub-elements not belonging to previous classes	D.4/D.13	Stuck-at[a]	Stuck-at[a] at gate level	d.c. fault model[b] Soft error model[c] (for sequential part)

Reference ISO 26262-5:2011

Dynamic FMEDA Metrics



- FMEDAs must **individually** fulfill the target relative metrics (SPFM, LFM)
- **Sum** of individual PMHF must fulfill the absolute target

Dynamic FMEDA

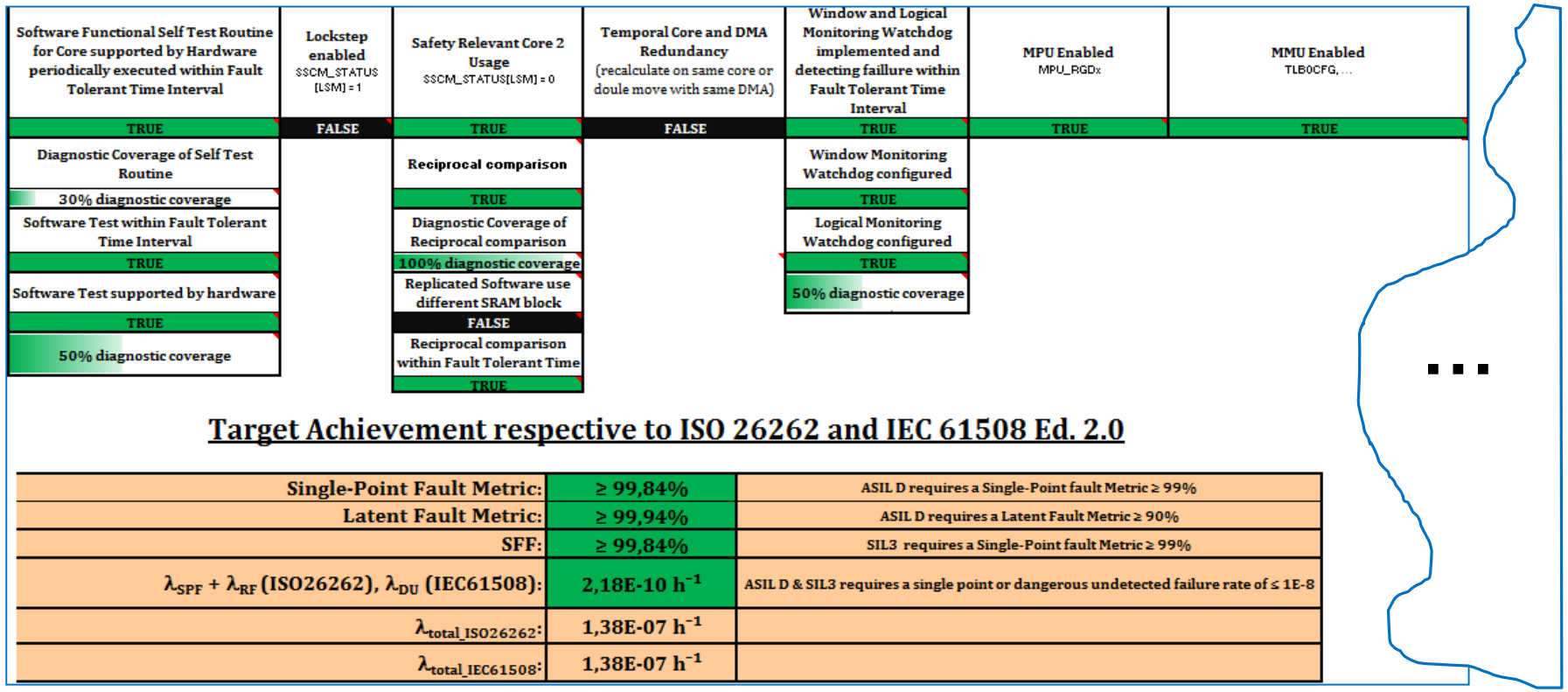
- Failure Mode, Effect and Diagnostic Analysis
- A systematic way to **identify** and **evaluate failure modes**, **effects** and **diagnostic techniques**, and to **document** the system.

- FMEDA can be **tailored** to **application** use-case:
  - FMEDA allows adaptation of temperature profile and ASIL level
  - FMEDA allows selection of package used
  - FMEDA allows selection / de-selection of modules
  - FMEDA allows selection / de-selection of diagnostic measures
  - FMEDA allows to change particular DCs

Called “Dynamic FMEDA”

  - FMEDA can generate a specific (static) “**customer FMEDA**”

Dynamic FMEDA



Software Functional Self Test Routine for Core supported by Hardware periodically executed within Fault Tolerant Time Interval	Lockstep enabled SSCM_STATUS [LSM] = 1	Safety Relevant Core 2 Usage SSCM_STATUS[LSM] = 0	Temporal Core and DMA Redundancy (recalculate on same core or doule move with same DMA)	Window and Logical Monitoring Watchdog implemented and detecting faillure within Fault Tolerant Time Interval	MPU Enabled MPU_RGDx	MMU Enabled TLB0CFG, ...
TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
Diagnostic Coverage of Self Test Routine		Reciprocal comparison		Window Monitoring Watchdog configured		
30% diagnostic coverage		TRUE		TRUE		
Software Test within Fault Tolerant Time Interval		Diagnostic Coverage of Reciprocal comparison		Logical Monitoring Watchdog configured		
TRUE		100% diagnostic coverage		TRUE		
Software Test supported by hardware		Replicated Software use different SRAM block		50% diagnostic coverage		
TRUE		FALSE				
50% diagnostic coverage		Reciprocal comparison within Fault Tolerant Time				
		TRUE				

Target Achievement respective to ISO 26262 and IEC 61508 Ed. 2.0

Single-Point Fault Metric:	≥ 99,84%	ASIL D requires a Single-Point fault Metric ≥ 99%
Latent Fault Metric:	≥ 99,94%	ASIL D requires a Latent Fault Metric ≥ 90%
SFF:	≥ 99,84%	SIL3 requires a Single-Point fault Metric ≥ 99%
$\lambda_{SPF} + \lambda_{RF}$ (ISO26262), λ_{DU} (IEC61508):	2,18E-10 h^{-1}	ASIL D & SIL3 requires a single point or dangerous undetected failure rate of ≤ 1E-8
$\lambda_{total\_ISO26262}$:	1,38E-07 h^{-1}	
$\lambda_{total\_IEC61508}$:	1,38E-07 h^{-1}	

Additionally - FMEDA Report

• Summarizing the assumptions and the method of the inductive functional safety analysis activities based on the FMEDA carried out for the MCU

Safety Plan, Safety Case & Confirmation Measures

Safety Plan

- Describes the overall approach to functional safety management during the development of the hardware or software components in accordance with ISO 26262 requirements.
- The Safety Plan is based on ISO 26262:2011
- The Safety Plan follows the standard NXP BCaM7 Process, which defines the overall product lifecycle.
- The MCU safety activities are planned and tracked in the as part of standard project plans:
  - The safety deliverables are identified by “fs:”
  - Key safety activities addressed, including
    - safety requirements definition and review
    - safety analysis and review
    - design implementation and associated testing in verification simulation, silicon validation and qualification
    - key safety management activities of confirmation reviews, audit activities and assessment.

Key Roles and Responsibilities for ISO 26262

- **Functional Safety Architect**
  - Specification of Functional Safety requirements and performing Functional Safety analysis
- **Project Functional Safety Manager**
  - Project specific set up and maintenance of Functional Safety activities according to organizational Functional Safety standards and product requirements
- **Functional Safety Assessor**
  - Planning and execution of functional safety assessments according to ISO26262 standard and the NXP Functional Safety process
- **Organisation Functional Safety Manager**
  - Implementation of ISO 26262 standard including training into the organization

ISO 26262 Safety Case

- Lists the ISO 26262 Work Products applicable to the development, as well as progressively compiles the deliverables generated during the safety lifecycle which form the safety case along with the safety argument.

- The complete list of information exchanged between NXP (MCU Supplier) and the customer (System developer) is detailed in the ISO 26262 Safety Case, including how the information is exchanged:

  - **Public** Information available via the NXP Website
  - **Confidential** Information available under NDA
  - **Internal** Information available during onsite Audit

- In case NXP enters into a Customer Development Interface Agreement (Customer DIA) for a system, then the Customer DIA takes precedence over the ISO 26262 Safety Case.

ISO26262-10 Table A.8 Checklist

- ISO 26262-10 Annex A.3.7 deals with techniques or measures to detect or avoid systematic failures during MCU design
- It proposes a checklist according to table A.8 to provide evidence that sufficient measures for avoidance of systematic failures are taken during MCU design

Design phase	Design owner for:		ISO 26262-5 requirement	ISO 26262-10 Table A.8 Checklist Conform	
	ARM IP	FSL IP		ARM IP	FSL IP
Design entry	ARM (IP-level)	FSL	7.4.1.6 Modular design properties	ARM: YES	FSL: YES
			7.4.2.4 Robust design principles		
			7.4.4 Verification of HW design (IP-level)		
	FSL (SoC-level)		7.4.4 Verification of HW design (SoC-level)	FSL: YES	
Synthesis	FSL	FSL	7.4.4 Verification of HW design	FSL: YES	FSL: YES
			7.4.1.6 Modular design properties		
			7.4.2.4 Robust design principles		
Test insertion and test pattern generation	FSL	FSL	7.4.1.6 Modular design properties (testability)	FSL: YES	FSL: YES
			7.4.4 Verification of HW design		
Placement, routing, layout generation	FSL	FSL	7.4.4 Verification of HW design	FSL: YES	FSL: YES
Chip production	FSL	FSL	7.4.4 Verification of HW design	FSL: YES	FSL: YES
Qualification of HW component	FSL	FSL	7.4.4 Verification of HW design	FSL: YES	FSL: YES

Checklist summary

- Checklist complied with for each NXP design.

- When integrating 3rd party IP, for example from ARM, then major design steps to integrate the 3rd party IP like synthesis, test insertion, backend etc. is in NXP's responsibility and NXP provides the data for the checklist.
- 3rd party IP providers give the data for the IP-design part to enable NXP to fill in the checklist

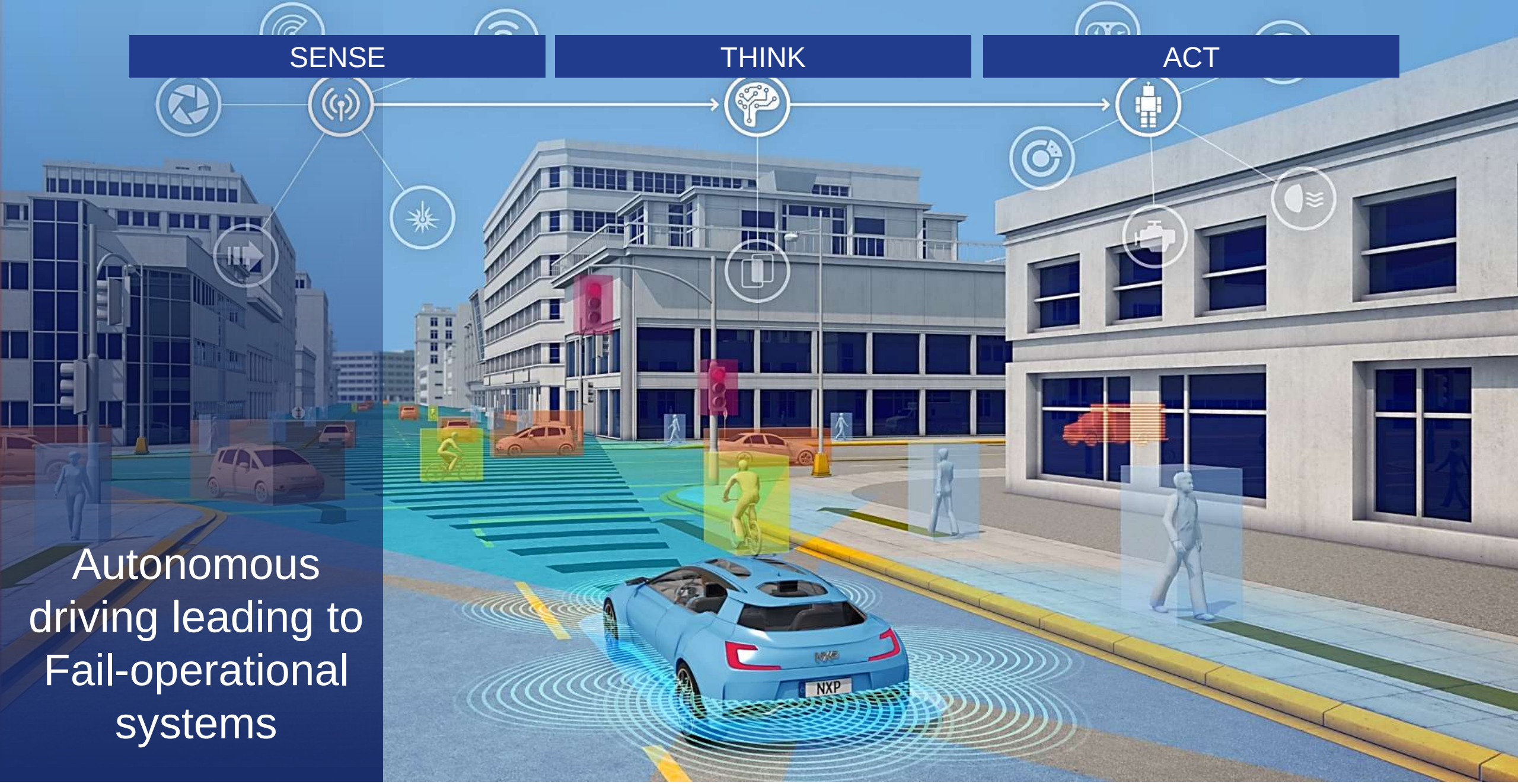
NXP ISO 26262 Confirmation Measures

- NXP performs ISO 26262 Confirmation Reviews (CR), Audit and Assessment as required by ISO 26262 for SEooC development

Confirmation Measures	ASIL A	ASIL B	ASIL C	ASIL D
CR Safety Analysis	Yes	Yes	Yes	Yes
CR Safety Plan		Yes	Yes	Yes
CR Safety Case		Yes	Yes	Yes
CR Software Tools			Yes	Yes
Audit			Yes	Yes
Assessment			Yes	Yes

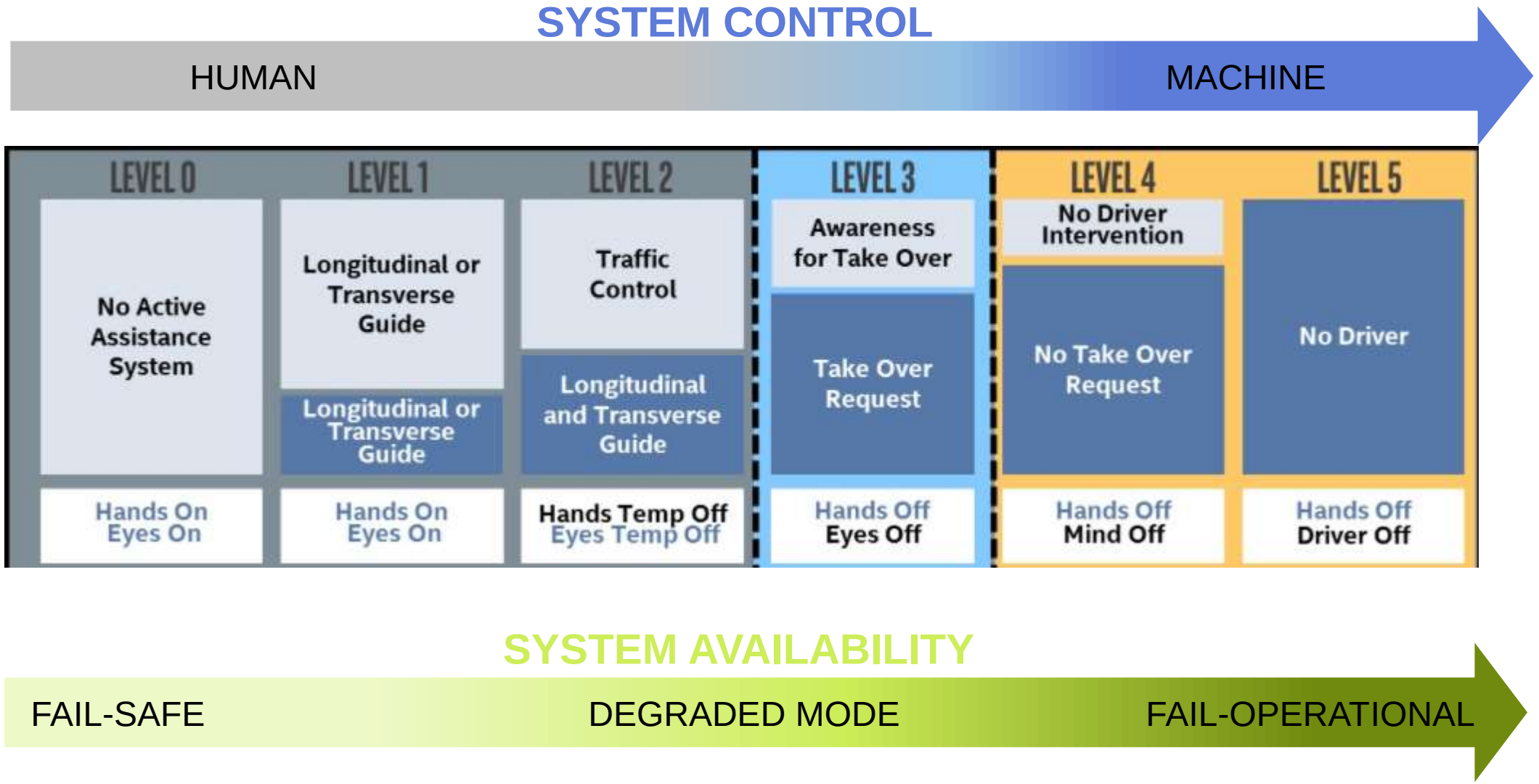
Note: The following confirmation reviews are not applicable: hazard analysis and risk assessment, item integration and testing, validation plan & proven in use argument

- Confirmation Measures (CM) performed depending on ASIL
  - All checks executed with **independence level I3** by NXP Quality organization
  - NXP Assessors **certified** by SGS-TÜV Saar as *Automotive Functional Safety Professional (AFSP)*
  - NXP CM process **certified** by SGS-TÜV Saar as ISO 26262 ASIL D



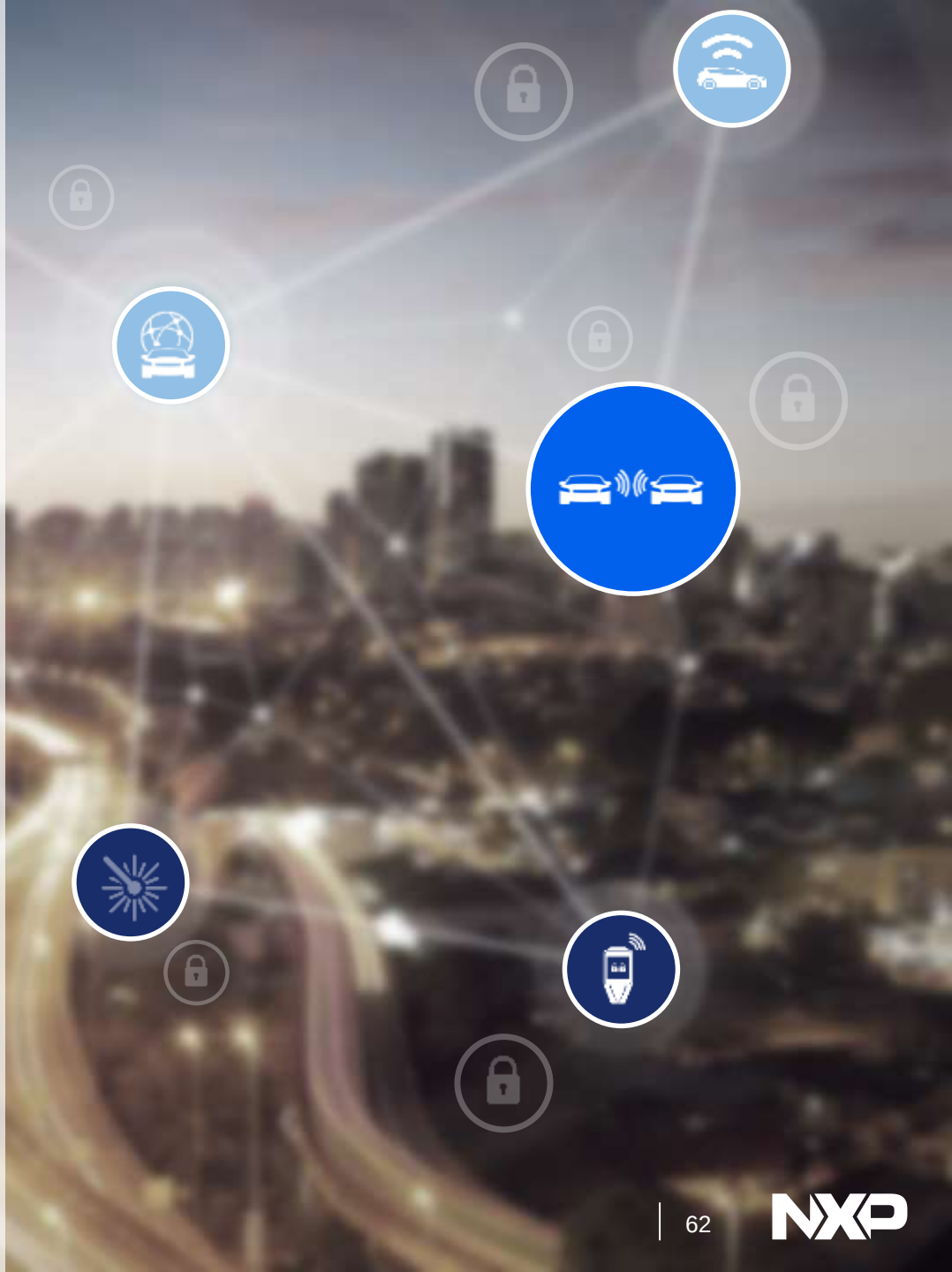
Autonomous driving leading to Fail-operational systems

Functional Safety
Autonomous Driving – SAE Levels



Conclusion

- ISO 26262 addresses functional safety in automotive
- NXP applies ISO 26262 across Automotive developments
- Faults & Safety Mechanisms are determined for HW & SW components, NXP safety concepts enable customers to design their safety systems
- ISO 26262 evolving to address the requirements for safe autonomous vehicle



SECURE CONNECTIONS
FOR A SMARTER WORLD