Functional Safety & Security: Next-Generation Functional Safety Architecture

Dev Pradhan

AMP Engineering Director

June 2018 | AMF-AUT-T3182

SECURE CONNECTIONS FOR A SMARTER WORLD

Company Public – NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.

AGENDA

- Recap on Functional Safety
- Recap on ISO 26262
- Next Generation Safety Concept
  - Process
  - Hardware
  - Software
- Getting Safety Support

Recap on Functional Safety

What is Functional Safety?

ISO 26262 Definition:

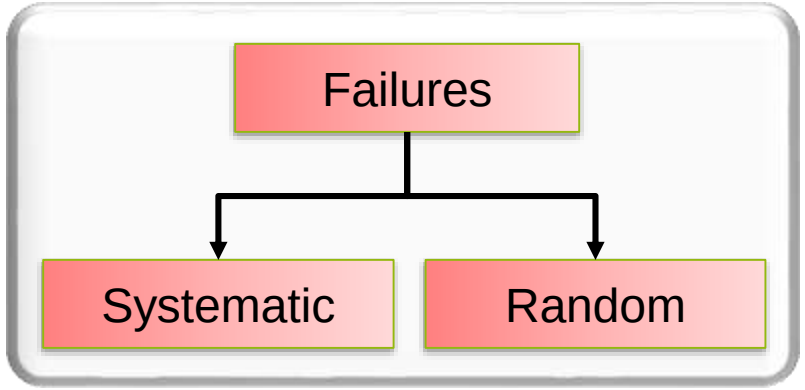
Absence of unacceptable risk due to hazards caused by mal-functional behavior of electrical and/or electronic systems

IEC 61508 Definition:

- Safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
- Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

What is relevant to NXP is that for the first time these standards call out requirements for electronic components

Implementing Functional Safety is about detecting and managing failures



How products are developed:

Addresses the aspect of Systematic Failures

- Result from a failure in design or manufacturing
- Relevant to Hardware and Software
- Occurrence of failures can be reduced through continual and rigorous process improvement

Products that detect and handle faults:

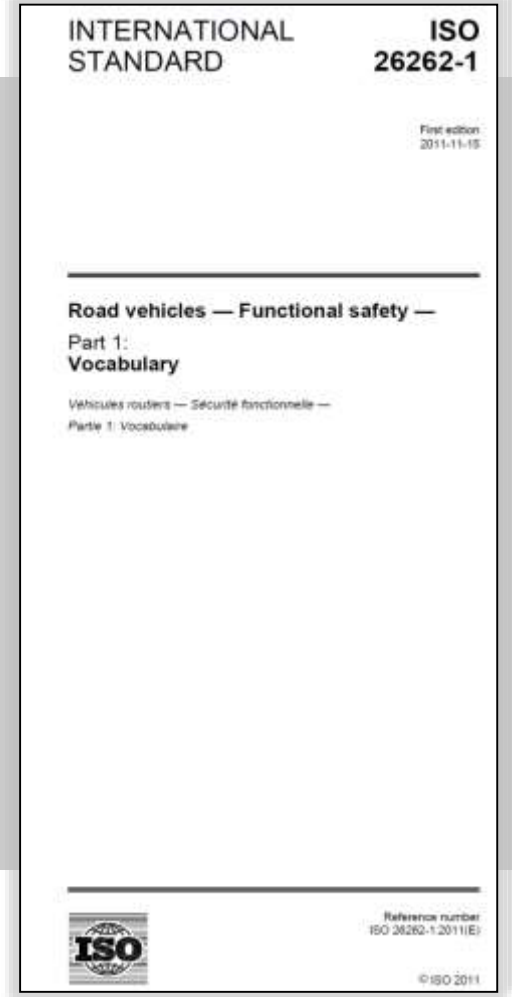
Addresses the aspect of Random Failures

- Inclusion of mechanisms to detect and handle random defects inherent to process or usage condition
- Relevant to Hardware only
- Supported by FMEDA*, Dependency and Fault Tree Analysis and communicated as FIT*

- FMEDA – Failure Mode Effects and Diagnostic Analysis
- FIT – Failure in Time

Recap on ISO 26262

ISO 26262 – Functional Safety of Road Vehicles


INTERNATIONAL STANDARD

ISO 26262-1

First edition
2011-11-15

Road vehicles — Functional safety —

Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2011(E)

© ISO 2011

- Vertical standard, performance based.
- First edition published in 2011.
- Follows similar structure to IEC 61508, but totally replaces instead of augmenting.
- Separates system design from hardware component design. As a result, most <u>components</u> used require compliance.
- 2nd edition to be released this year: ISO 26262:2018

Determining ISO 26262 ASIL Level

- To determine the ASIL level of a system a Risk Assessment must be performed for all Hazards identified.
- Risk is comprised of three components: **Severity, Exposure & Controllability**

S = Severity

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

C = Controllability

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

E = Exposure

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

Automotive Application Safety levels (e.g.)

Subsystem	ASIL Safety Level
ADAS – Vision/Radar	B-D
Airbags	D
Alternator	C-D
Body Control Module	A-B
Brake System (ABS, ESC, Boost)	A-D
Collision Warning -	A-B
Cruise Control	A-D
Drowsiness Monitor	A-B
E-Call / Telematics	A-B
Fuel Pump	B
Engine Oil Pump	B
Electric Mirrors	A-B
Electrochromatic Mirrors	A-B
Engine Control	B-D
Lighting	A-B
Night Vision	A-B
Power Door, Liftgate, Roof, Trunk	A-B
Rain Sense Wipers	A-B
Steering (EPS)	D
Throttle Control	A-D
Tire Pressure Warning	A-B
Transmission	B-D
Transmission Oil Pump	B-C
Window Lift	A-B

- Many applications that don't have strict safety requirements today may have them in the future.
- For example, **SAE** is providing guidelines for determining ASILs. Applying these guidelines will mean that auto apps that haven't been "safety" to-date could be held subject to ISO26262.
- Over time the expectations on sub-systems will change depending on how much the safety of the vehicle depends on them.

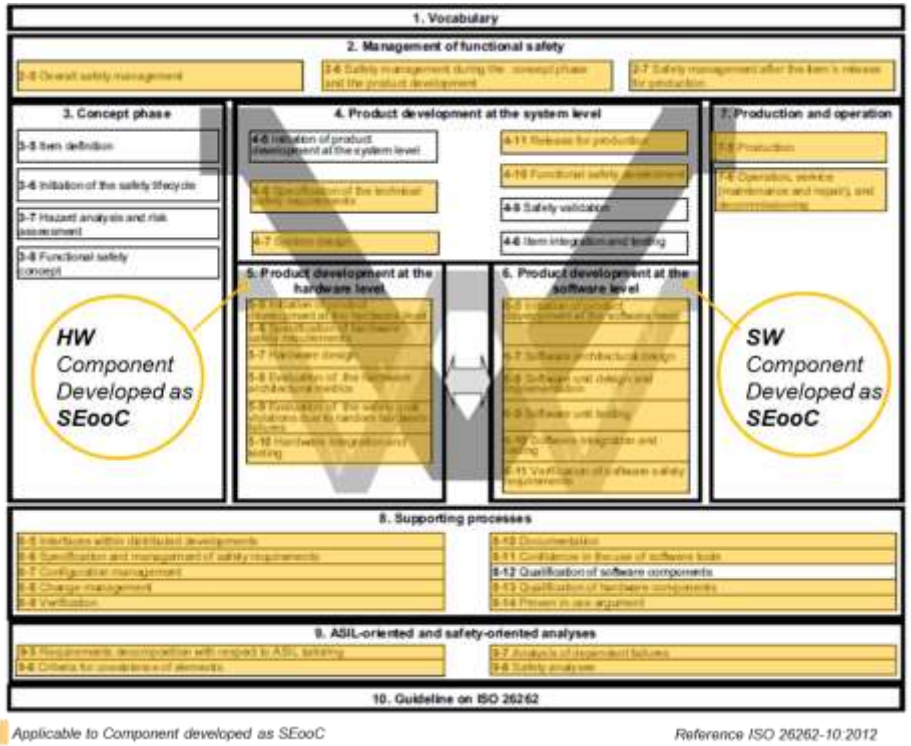
Next Generation Safety Concept

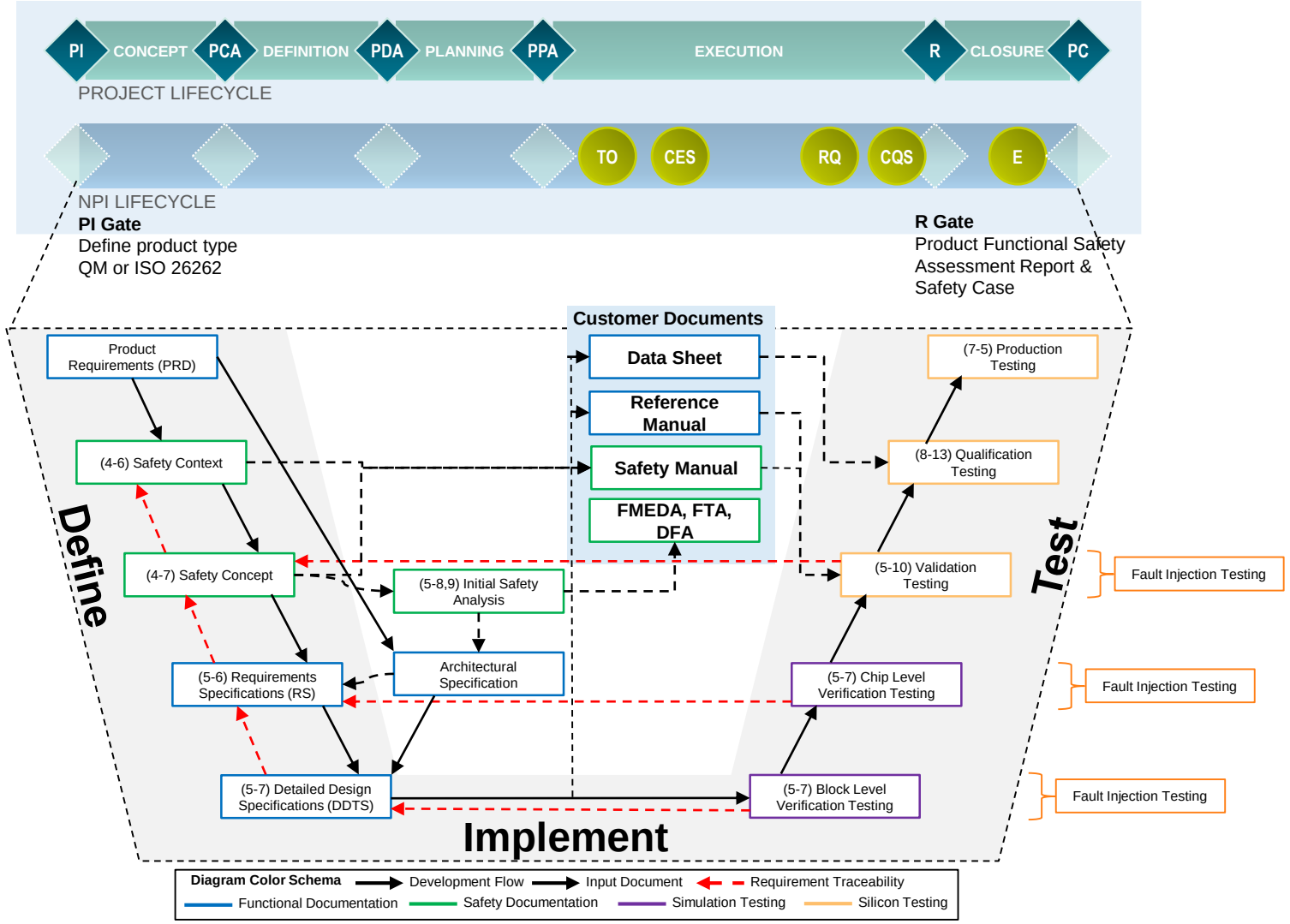
Process, Hardware, Software

Functional Safety Process – assessed to meet ISO 26262 ASIL-D

Product Service

ISO 26262 PROCESS





NXP BCAM7 PROCESS

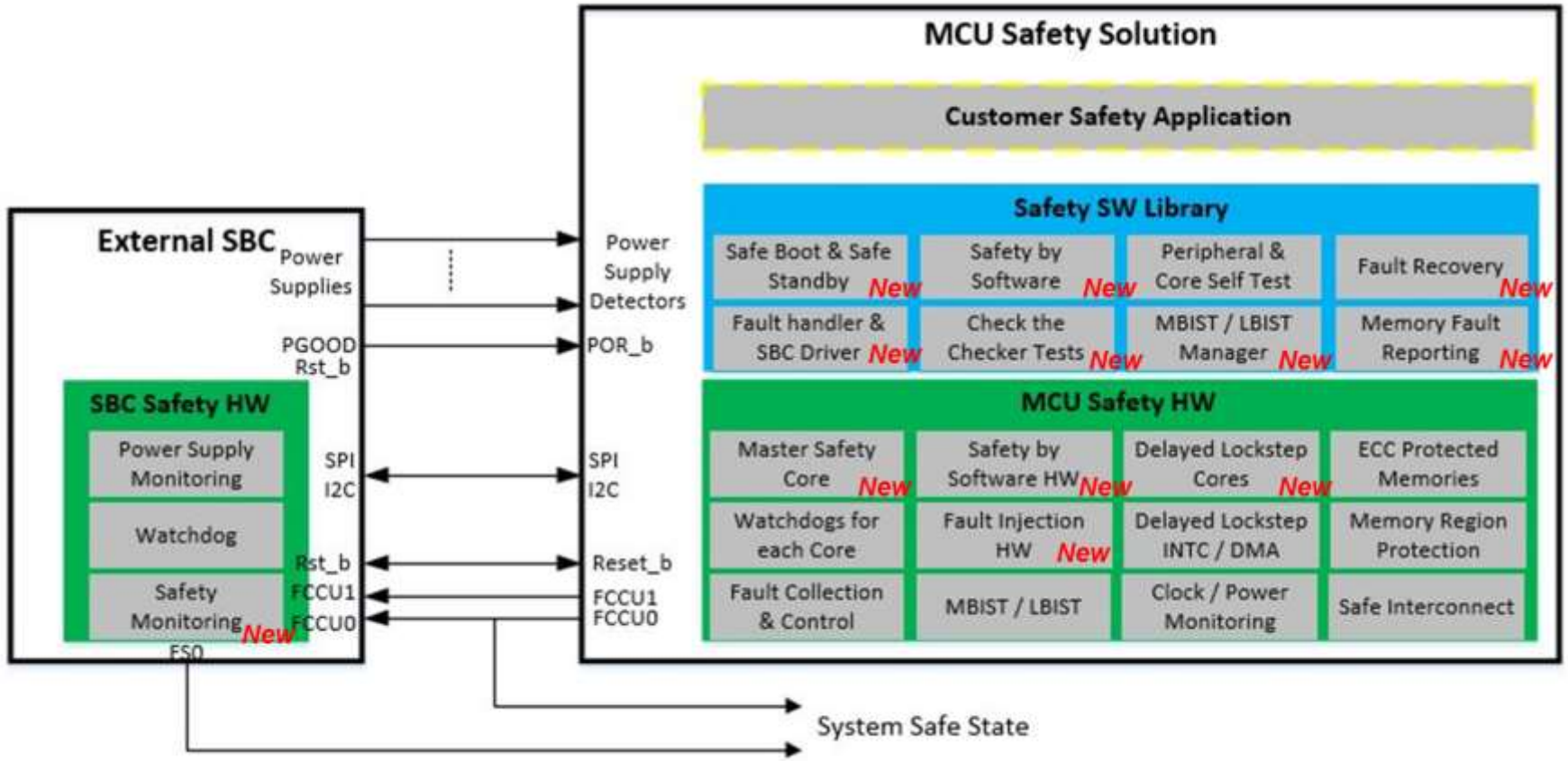
NXP Development Processes aligned with ISO 26262

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			

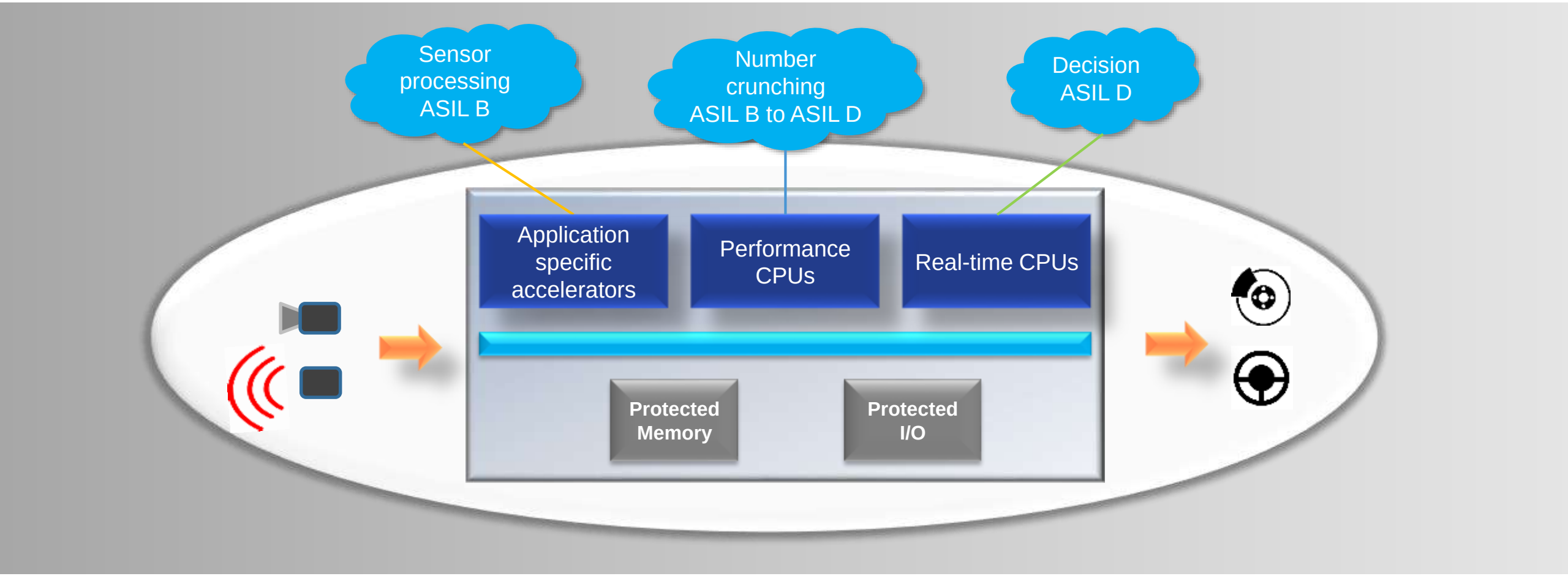
NXP BCAM7 automotive process complies with all applicable ISO 26262 ASIL-D requirements for HW and SW SEooC (safety element out of context) development and is **TUV SUD certified**.

Safety Chipset = SoC (Hardware/Software) + Power Supply

- **ASIL-D ready Safety**
  - Certified Process
  - Random Failure Detection
  - Collateral
- **System Solution**
  - SW Safety Library
  - MCU
  - SBC
- **Differentiation**
  - Highest ASIL-D DMIPs
  - Failure Recovery
  - ASIL-B Acceleration

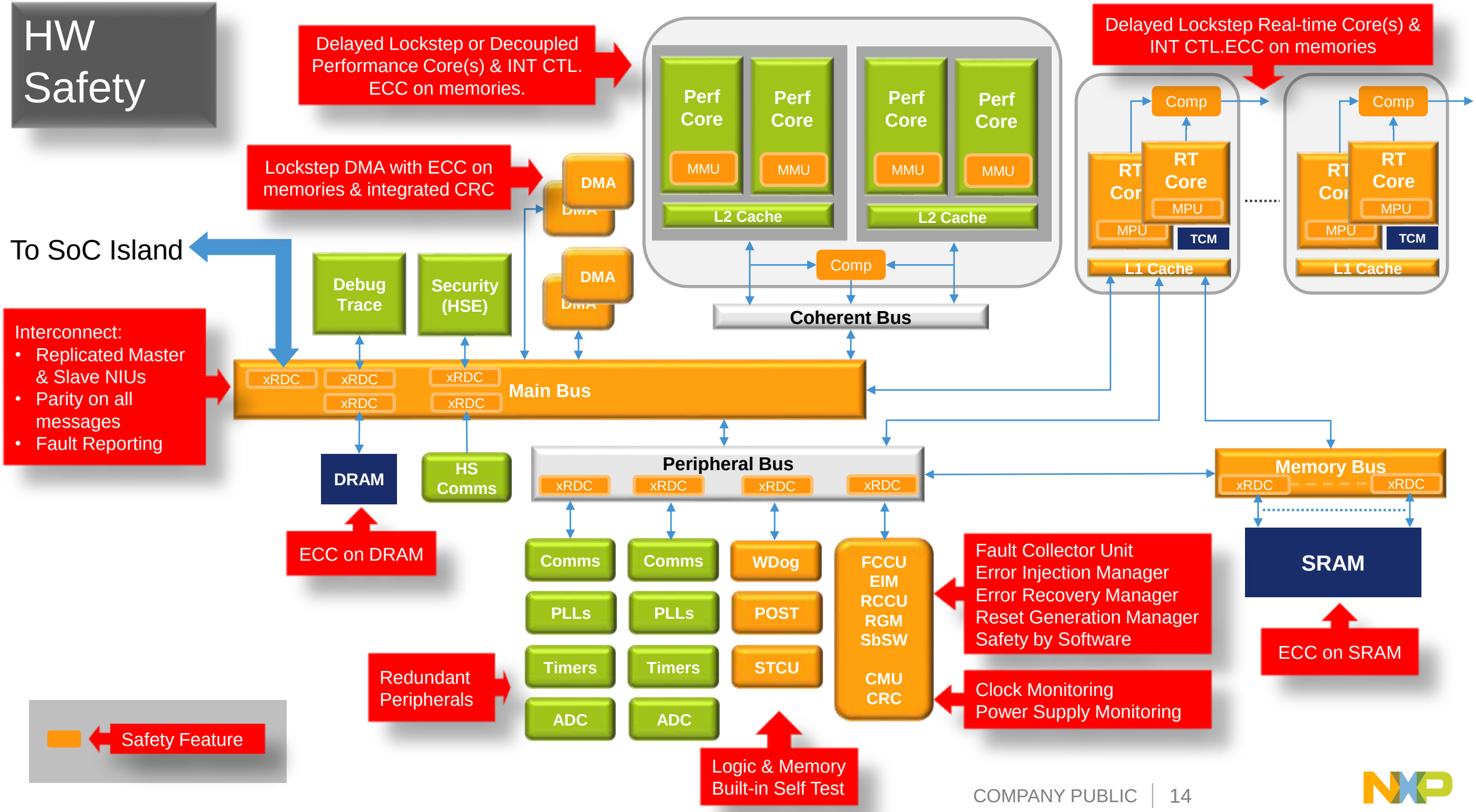


Safety targets for Next-Generation Platform



- **Developed as a Safety Element out of Context (SEooC)**
- **Following an ISO 26262 ASIL-D Safety Development Process**
- **Supported with complementary safety collateral**

HW Safety

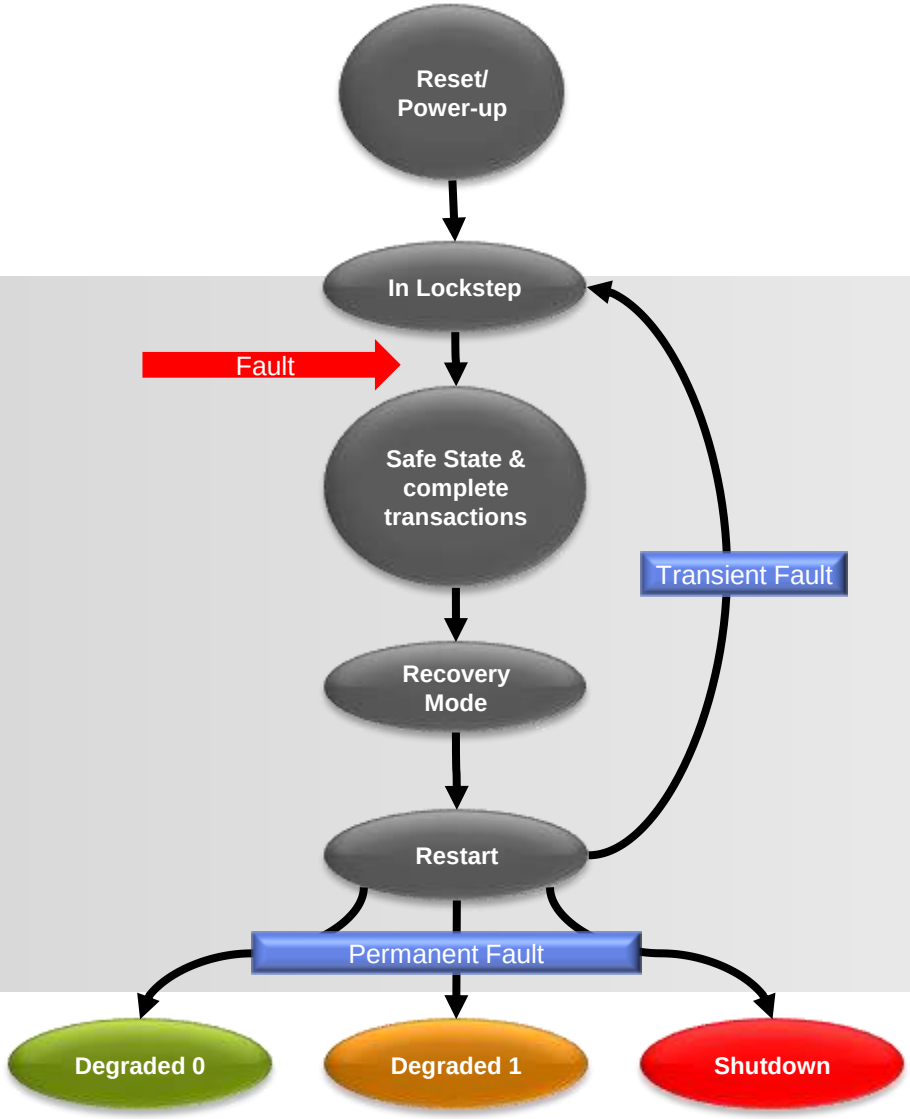

Delayed Lockstep or Decoupled Performance Core(s) & INT CTL. ECC on memories.
Perf Core
MMU
L2 Cache
Comp
Coherent Bus
Delayed Lockstep Real-time Core(s) & INT CTL.ECC on memories
RT Core
MPU
TCM
L1 Cache
Lockstep DMA with ECC on memories & integrated CRC
DMA
To SoC Island
Debug Trace
Security (HSE)
Interconnect:
• Replicated Master & Slave NIUs
• Parity on all messages
• Fault Reporting
xRDC
Main Bus
DRAM
HS Comms
ECC on DRAM
Peripheral Bus
Memory Bus
SRAM
ECC on SRAM
Comms
PLLs
Timers
ADC
WDog
POST
STCU
FCCU
EIM
RCCU
RGM
SbSW
CMU
CRC
Fault Collector Unit
Error Injection Manager
Error Recovery Manager
Reset Generation Manager
Safety by Software
Clock Monitoring
Power Supply Monitoring
Redundant Peripherals
Logic & Memory Built-in Self Test
Safety Feature

Fault Management and availability

Previous Generation - State of the art functional safety 2012	S32x - Introducing availability 2018+
Lockstep mismatch → MCU reset	Lockstep mismatch → begin availability flow
No localization of fault beyond lockstep core pair	**Localization of fault** possible to individual core
No continued operation possible with safety coverage	Continued operation possible with loss of core, or loss of cluster **Remaining core/cluster functional**
Not possible to distinguish between permanent and transient faults in core complex	All transient faults recoverable Cache faults recoverable without BIST – reset only

Fail Safe Strategy

Fault Tolerant Strategy



Top level safety requirements

- The MCU itself is developed as a **SEooC** to provide the MCU functionalities with appropriate assumed safety integrity – **ASIL D**
  - **SPFM (Single Point Failure Metric): 99%** for transient & permanent faults
  - **LFM (Latent Failure Metric): 90%** for permanent faults
  - **PMHF (Probabilistic Metric Hardware Failure): 10^{-9} h^{-1}** (10% of system target for ASIL-D (<10^{-8} h^{-1}))

- Fault Tolerant Time Interval (time a Fault occurrence and the system transitions to a Safe state)
  - **$FTTI_{MCU}$= 10ms**

- Multiple Point Fault Detection Interval (multi-point faults are latent faults)
  - **$MPFDI_{MCU}$= 12hrs**

- To detect multiple-point faults in the **most critical MCU safety mechanisms**, **software initiated fault injection tests** can be periodically triggered within the FTTI.

Top level availability requirements

- The contribution of the SoC to the **Fault Recovery Time** of the application is targeted to be

  FRT <= 50 ms.
- This time is split between fault recovery (**FRT_{MCU}**) and reset/boot (**$BootTime_{MCU}$**)
  - Note: This includes the time to perform SoC fault diagnostics, reset and boot the SoC to the point to handover to load full application code. It does not include the application re-initialization time.

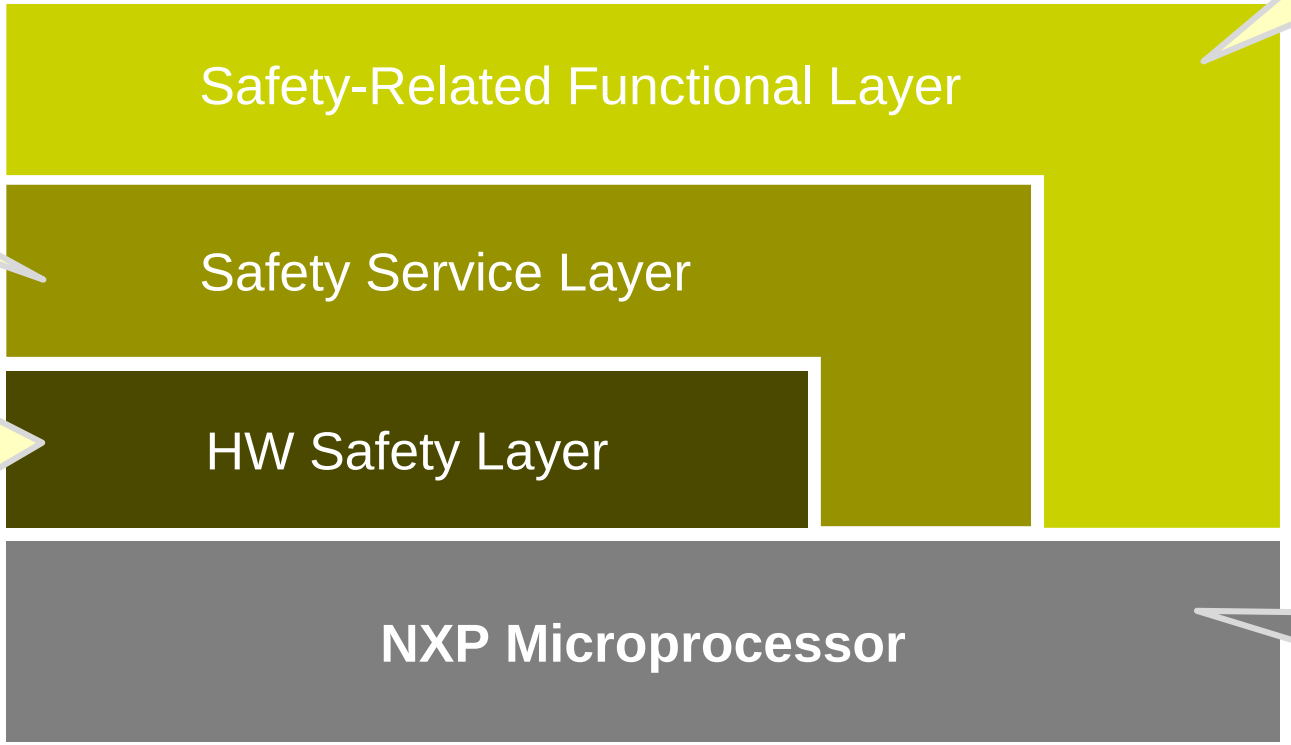
- Fault Tolerance (Availability) of the SoC is targeted to be:

  < 100 FIT (10^{-7} h^{-1}) of failures should lead to application Shutdown

Safety Software Architecture

Software functional components that may carry out safety-related functions

Software components that facilitate and support safety- related applications.

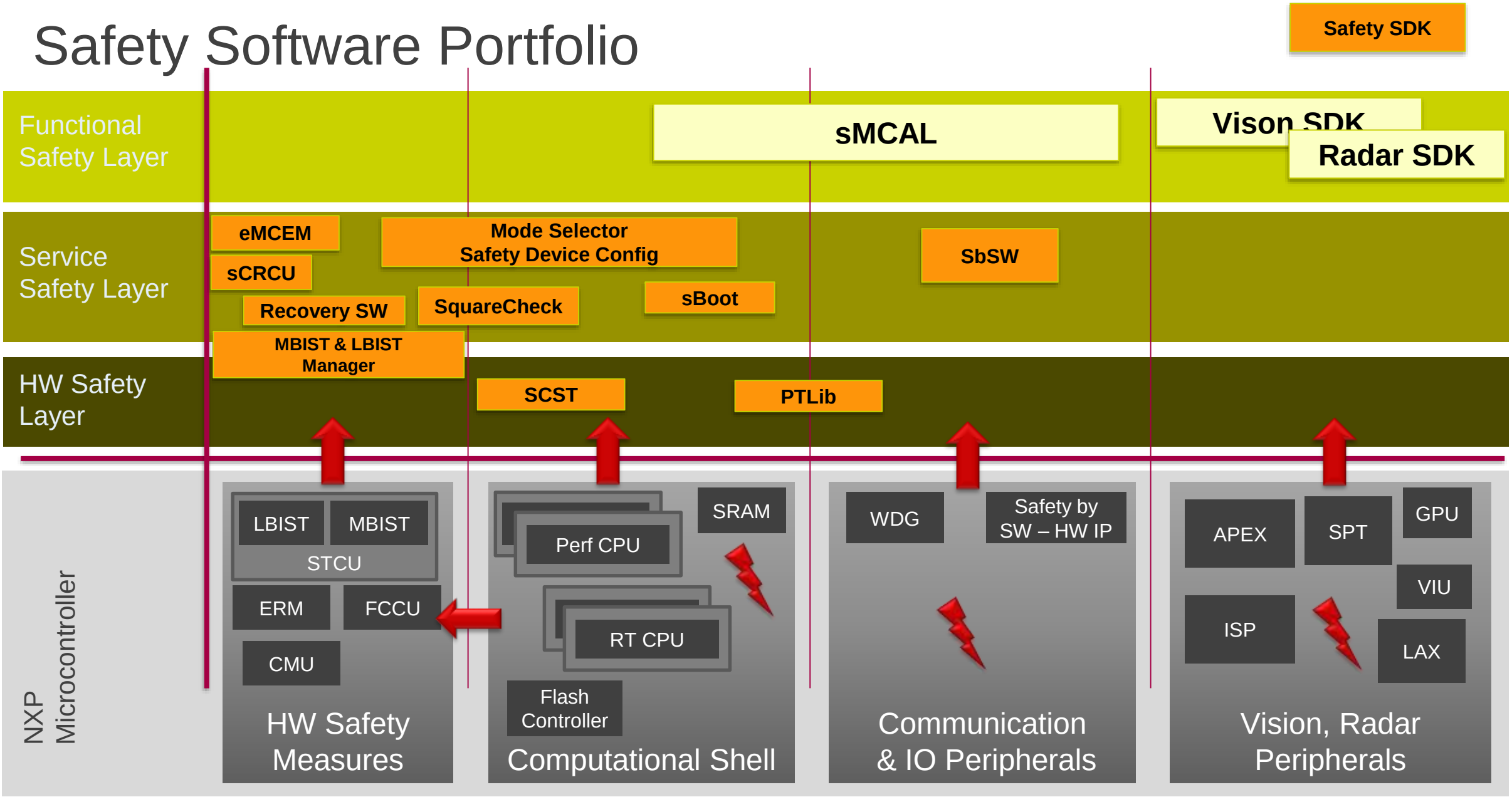


Software components for detecting hardware faults to support compliance with ISO26262 hardware architectural metrics:

- SPFM
- LFM

µPs with different set of safety measures and safety support functions

Safety Software Portfolio



Safety SDK components

Detection components

- SquareCheck – detects latent faults in HW safety mechanism
- BIST Manager – configures, initiates, and provides access to MBIST and LBIST
- sBoot – detects violations of HW safety configuration
- sCRCU – detects faults in CRC; also, it computes CRC

Reaction Components

- eMCEM – configures FCCU and provides handlers to faults signaled to FCCU.
- SW Recovery – initiates the global recovery process
- Mode Selector – depending on the MCU fault status selects the appropriate operating mode. Device configuration is part of the selection and invocation of the respective mode.

Getting Safety Support

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
  - Reference Manual
  - Data Sheet

- **Confidential Information available under NDA**
  - Safety Plan
  - Safety Manual
  - 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)

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

SafeAssure Community
Customer support for Functional Safety

SafeAssure Community

Public Space for knowledge distribution and industry-wide news
here

SafeAssure NDA

Private NDA space for customer to access safety documentation
here

Support

Safety Expert Group composed of Safety Managers and Architects, Field and Application Engineers

Self Sufficient

Community users find answers to their questions an safety documentation requests

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com

NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.