Next Generation Safety Architecture

Dev Pradhan

Sr. Director, Central Systems Solutions

Automotive Microcontrollers & Processors

October 2019 | Session #AMF-AUT-T3624

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

Agenda

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

Recap on Functional Safety

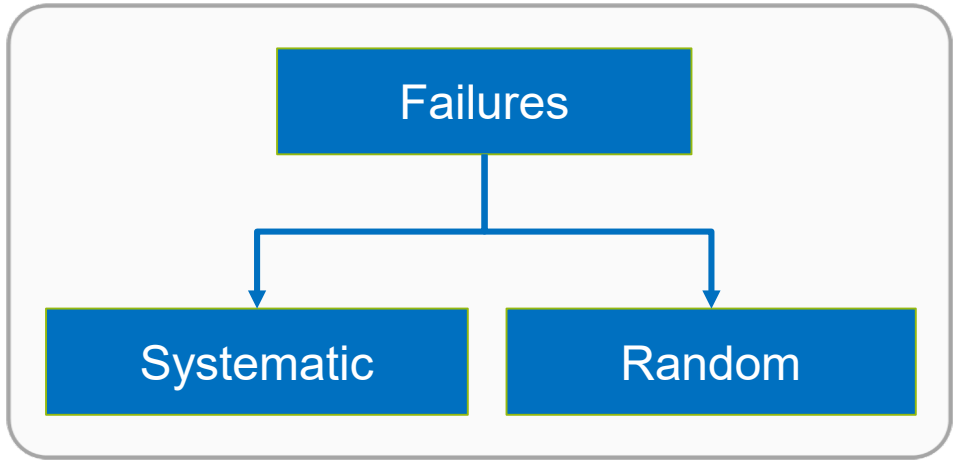
Implementing Functional Safety is About Managing Risk

The Risk of Failure

How products are developed:

Leads to Systematic Failures

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



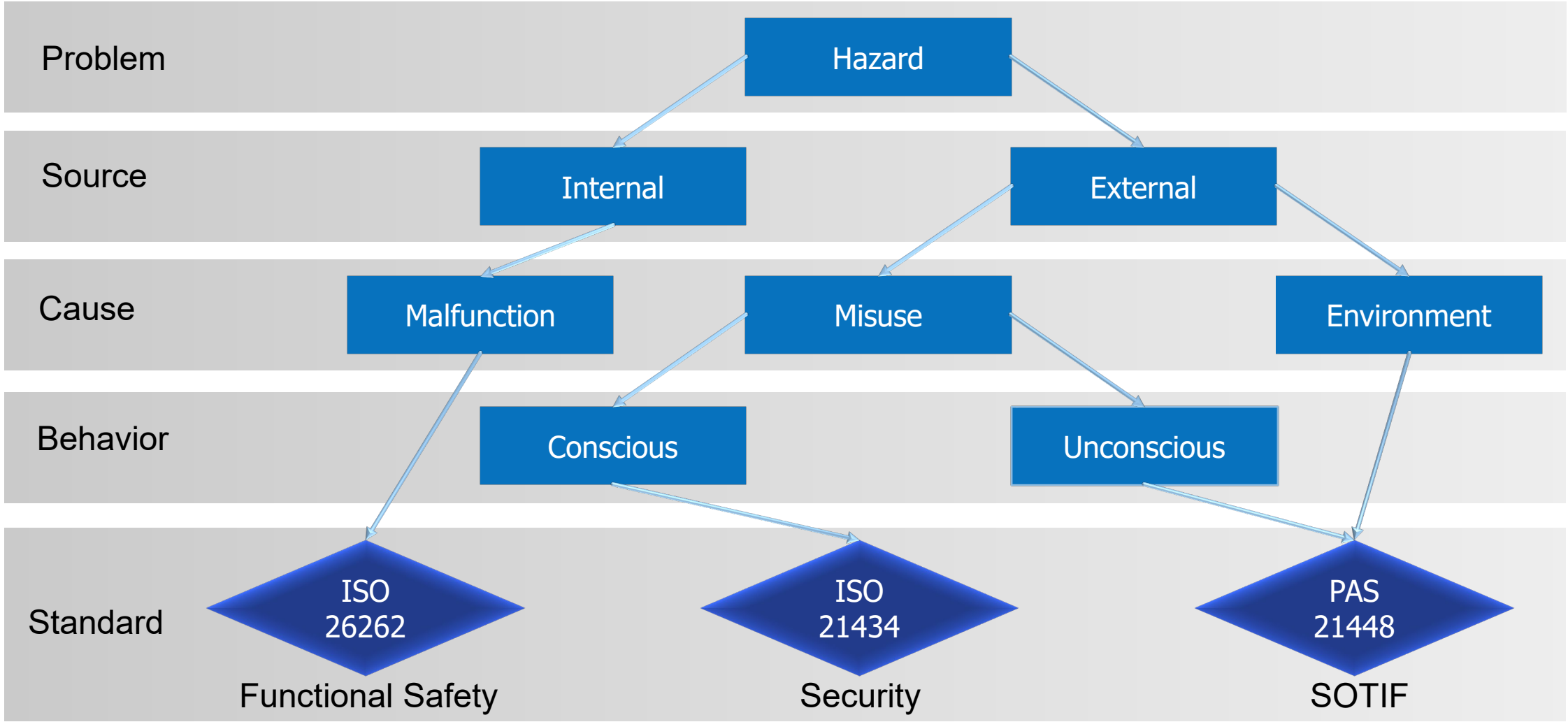
Unpredictable Events:

Leads to Random Failures

- Addressed by including mechanisms to detect and report faults
- Inherent to Process or usage condition
- Relevant to Hardware only
- FMEDA*, Dependency and Fault Tree Analysis help determine sufficiency of detection mechanisms

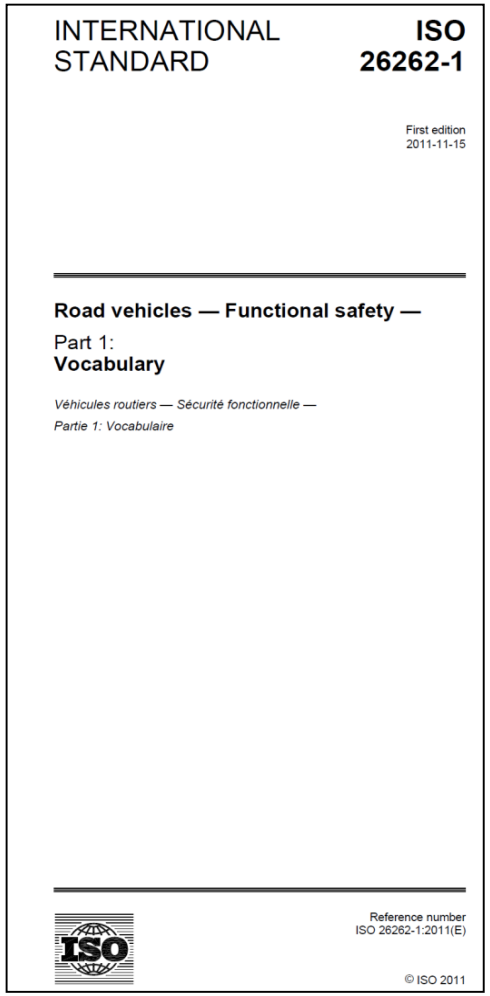
FMEDA – Failure Mode Effects and Diagnostic Analysis

Risk Assessment Correlated to Standards



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, second edition released in 2018 adding guidelines for motorcycles and semiconductor
  - Generic guidelines (partitioning IC, IP, DFA, fault injection, etc..)
  - Technology specific guidelines (digital, analog, PLD, MCU, sensors)
- Follows similar structure to IEC 61508, but totally replaces instead of augmenting.
- Separates system design from hardware component design. As a result, most components used require compliance.

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 

E = Exposure 

C = Controllability 

		C1 – Simple	C2 – Normal	C3 – Difficult
S1 Light	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 Severe	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 Fatal	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

(QM: "quality managed" → no requirements from standard applied explicitly)

Automotive Applications and ASIL Level (e.g.)

Note: that in the context of Autonomous there is the concept of SOTIF (ISO PAS 21448) that is not covered by ISO 26262 and any ASIL

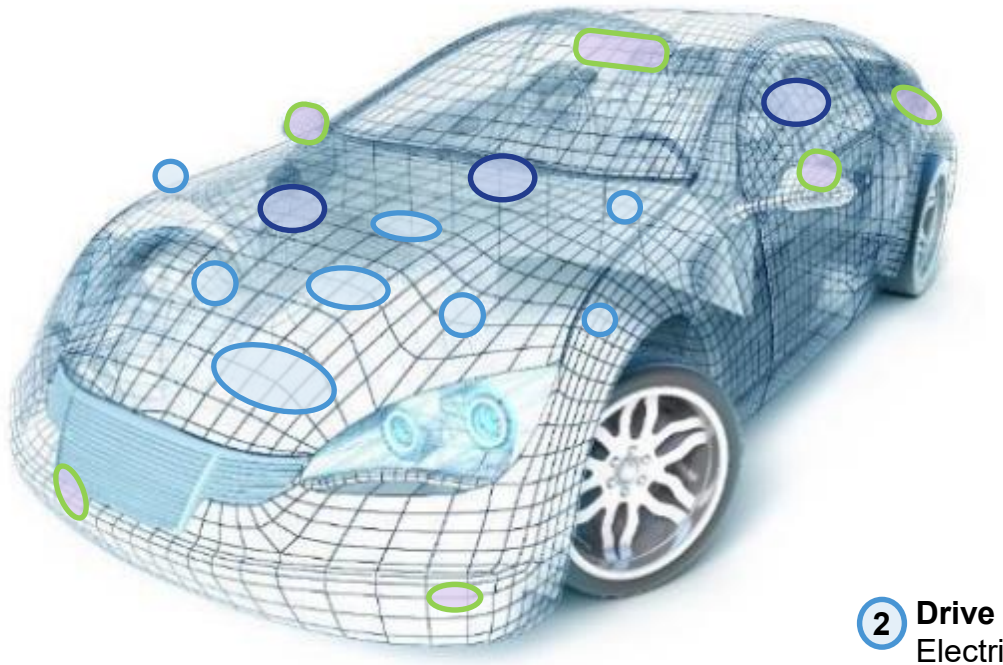
ADAS – Vision
1 Data Fusion – **ASIL B, up to ASIL D** (Autonomous Drive)

1 **Domain Gateway**
Body, Safety, Chassis – up to **ASIL D**

8 **Drive Train – S&C**
Suspension / Dumping – **ASIL C**

ADAS – RADAR
2 SRR, MRR, LRR – **ASIL B**

7 **Drive Train – S&C**
Electric Power Steering – **ASIL D**



ADAS – ACC
3 Adaptive Cruise Control – **ASIL C**

6 **Drive Train – S&C**
ABS, ESP – **ASIL D**

1 **Drive Train – Electrification**
Battery Management (12V, 48V, HV) – **ASIL C**

5 **Drive Train – PowerTrain**
Engine Management Unit – **ASIL B**

2 **Drive Train – Electrification**
Electric Motor (Alterno Starter, eAxel drive…) – **ASIL C**

4 **Drive Train – PowerTrain**
Transmission, Transfer Case – **ASIL D**

3 **Drive Train – Electrification**
Inverter, DCDC Converter - **ASIL C**

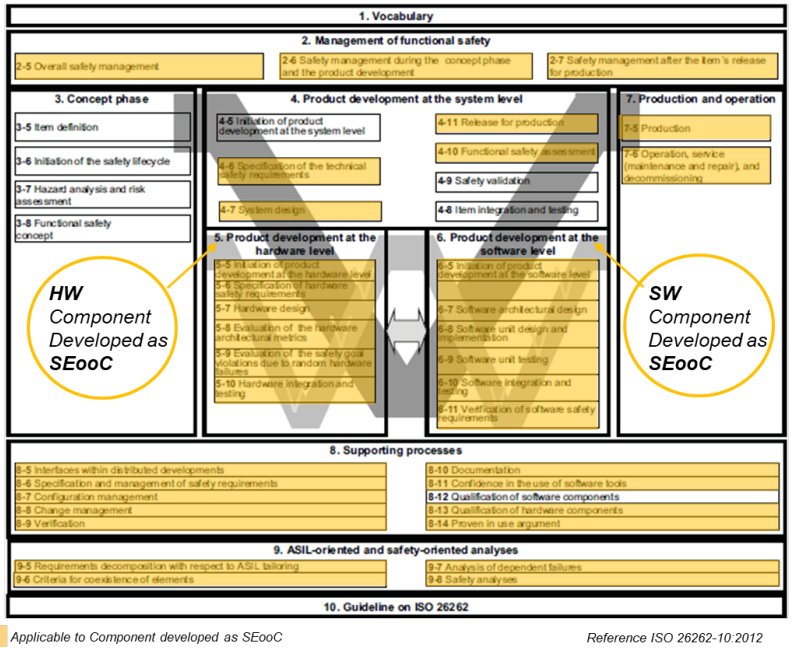
ASIL
D
C
B
A
QM
LEGEND

Functional Safety Process

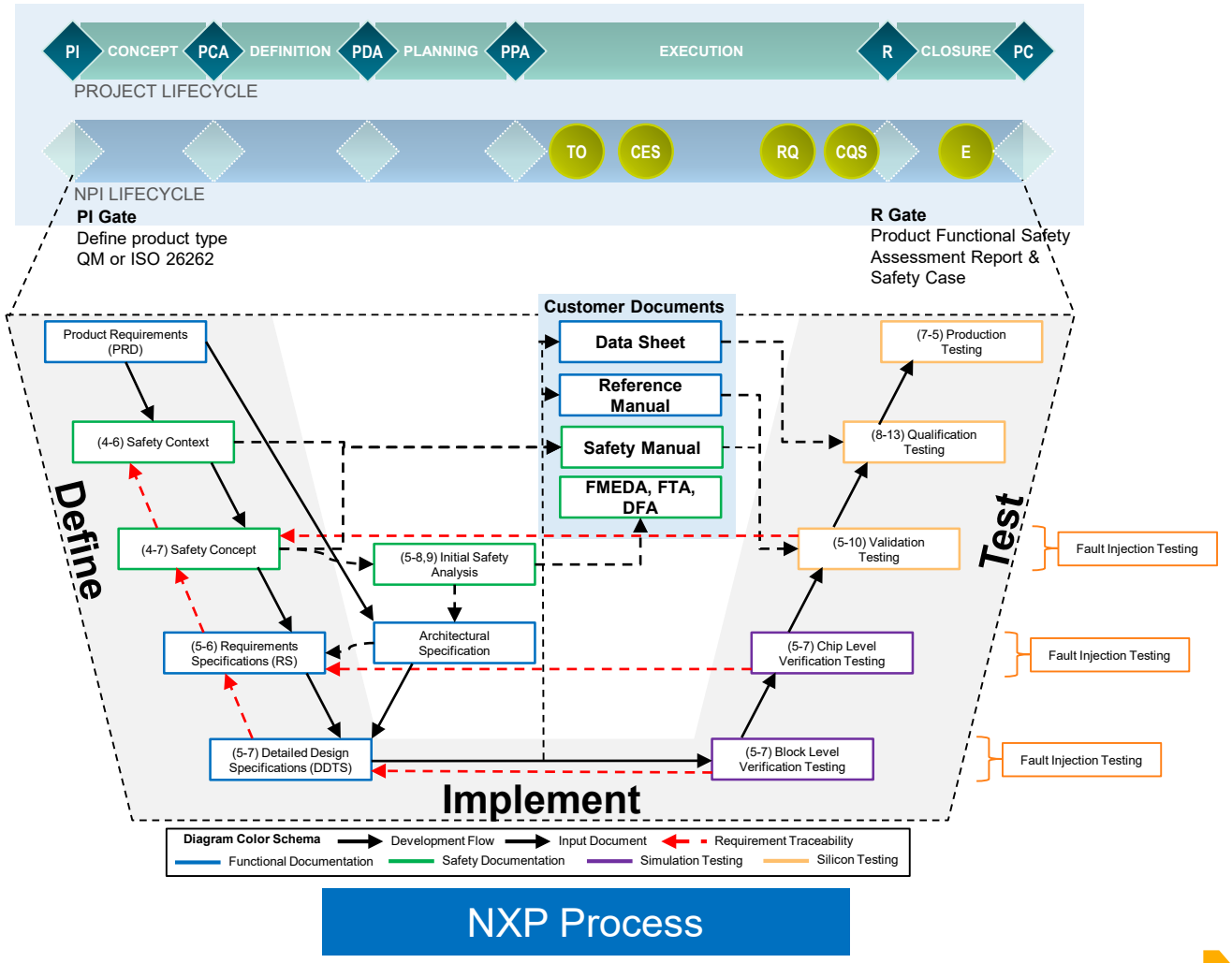
Assessed to Meet ISO 26262 ASIL-D

Product Service

ISO 26262 Process



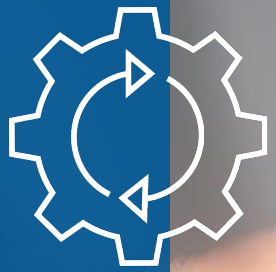
Input Requirements
Standard
Customer
Marketing (MRD)
Internal



NXP Process

S32 Automotive Platform Safety Concept Architecture

S32 Automotive Processing Platform



Highest performing ASIL-D processors

of today's best performing safe automotive platforms[1]

Maximizes software

Re-use within and across application domains

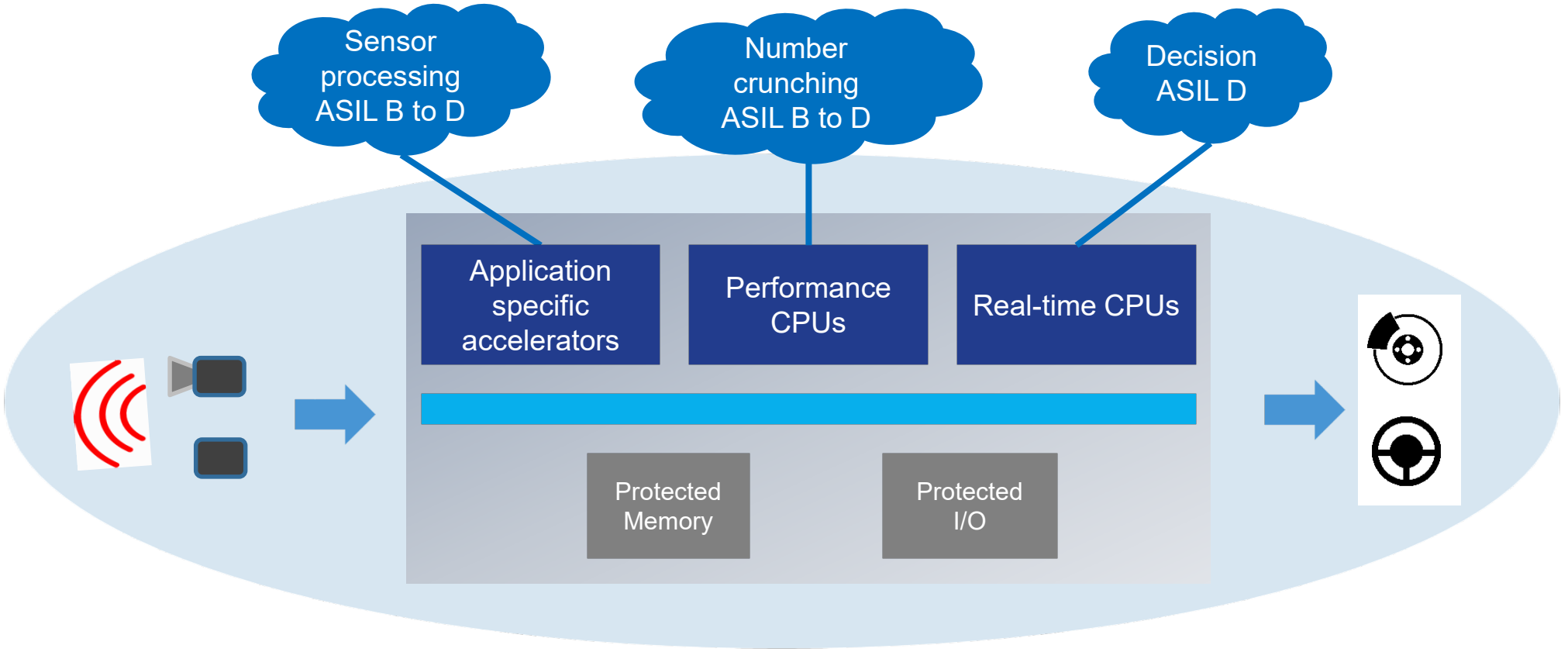
Delivers new levels of automotive safety, security and over-the-air (OTA) capabilities

1 Based on publicly available competitor roadmap performance statements.

S32 Automotive Computing Portfolio

Powertrain & Vehicle Dynamics	Body & Comfort	Driver Replacement	Gateway
Vehicle Dynamics & Safety	General Purpose & Integrated Solutions	Advanced Driver Assistance Systems	Connectivity & Security
			
Chassis, Safety, Torque and Energy Management	Body Electronics Edge Nodes	Radar, LIDAR, Vision Sensor Fusion	Vehicle Network Processing
MPC577 S32S	S32K S12Z	S32R S32V	MPC574 S32

Safety Targets for Next-Generation Platform

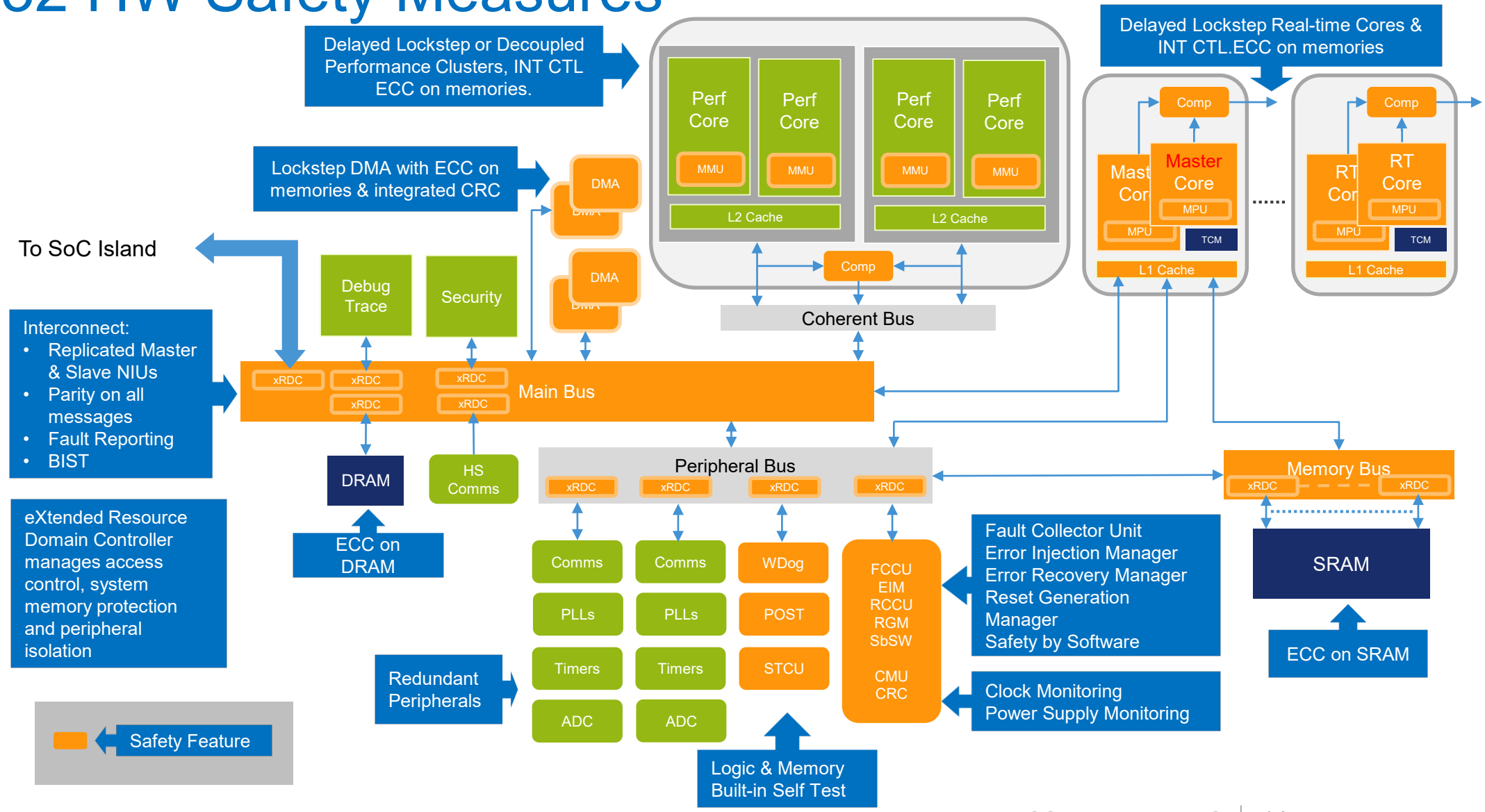


Developed as a Safety Element Out of Context (SEooC)

Following an ISO 26262 ASIL-D Safety Development Process

Supported with Complementary Safety Collateral

S32 HW Safety Measures

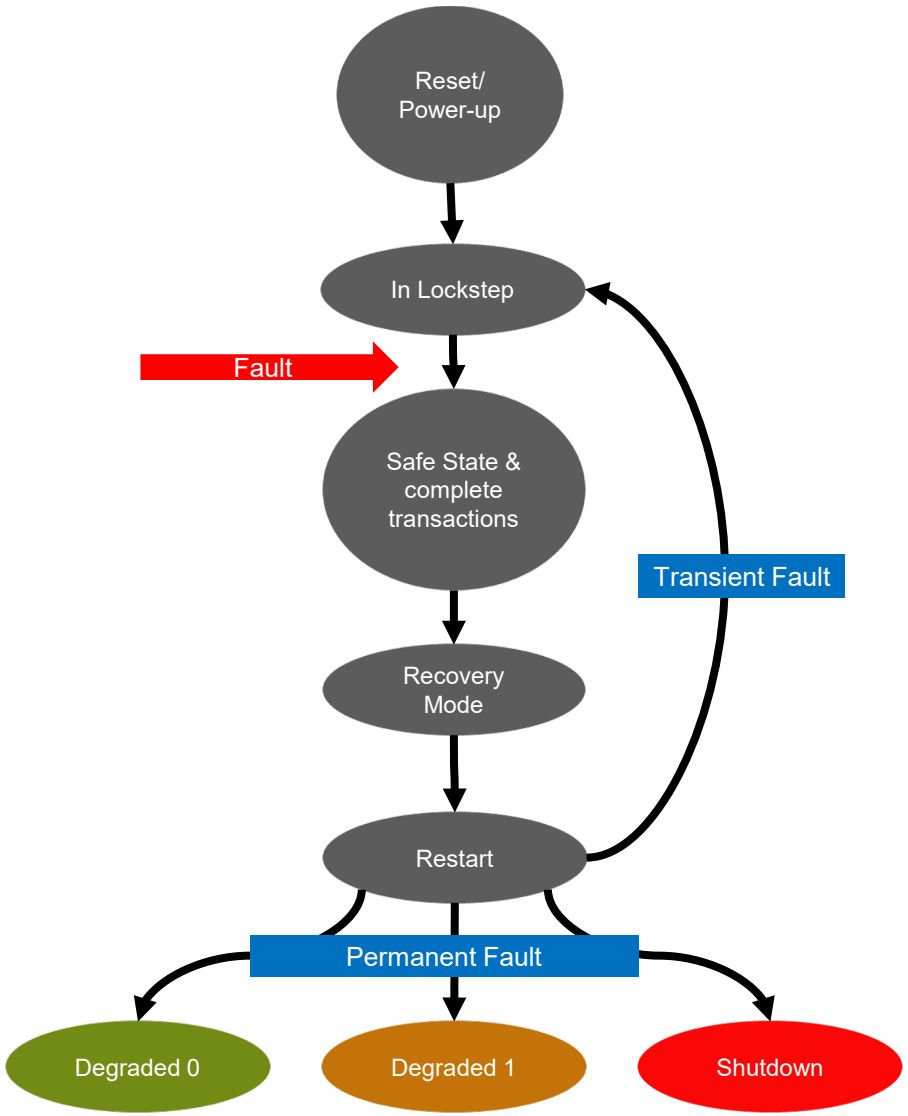


Fault Management and Availability

Previous Generation – State of the Art Functional Safety	S32x – Introducing availability 2019+
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 SoC itself is developed as a **SEooC** to provide functionaly 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 to 100ms**

- Multiple Point Fault Detection Interval (multi-point faults are latent faults)
  - **$MPFDI_{MCU}$= defined by application (e.g. 12hrs typical auto)**

- To detect multiple-point faults in the **most critical 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

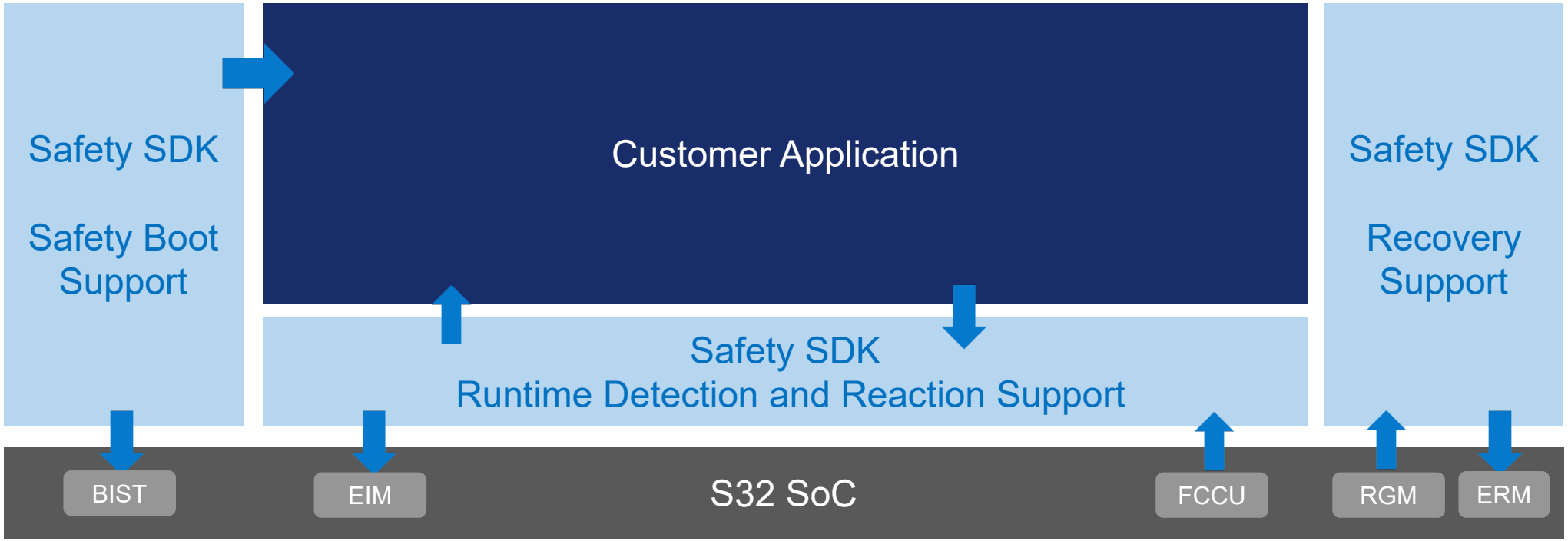
Fault Reactions – FCCU

- When a fault is routed to the **FCCU** there are 3 reactions possible to bring the SoC to a **safe state**:
  - **R1**: Alarm interrupt with FCCU timer, if timer expires interrupt and error out asserted (local recovery)
  - **R2**: Interrupt and error out asserted (global recovery)
  - **R3**: No interrupt, error out asserted and reset (no recovery configured)

- If a fault is Not Safety Related, the FCCU could be configured to the following reactions:
  - Fault is disabled, no FCCU reaction
  - Interrupt

S32 Automotive Platform Safety SW and Tools

Safety Software Support (Safety SDK)



- Successful boot of safety-related components is required to start a safety application.
- Runtime fault detection is mediated by Safety SDK – faults are detected by both HW and SW mechanisms
- Runtime error recovery is managed via Safety SDK
- Safety SDK manages a global, destructive SoC recovery.

Safety SDK Components

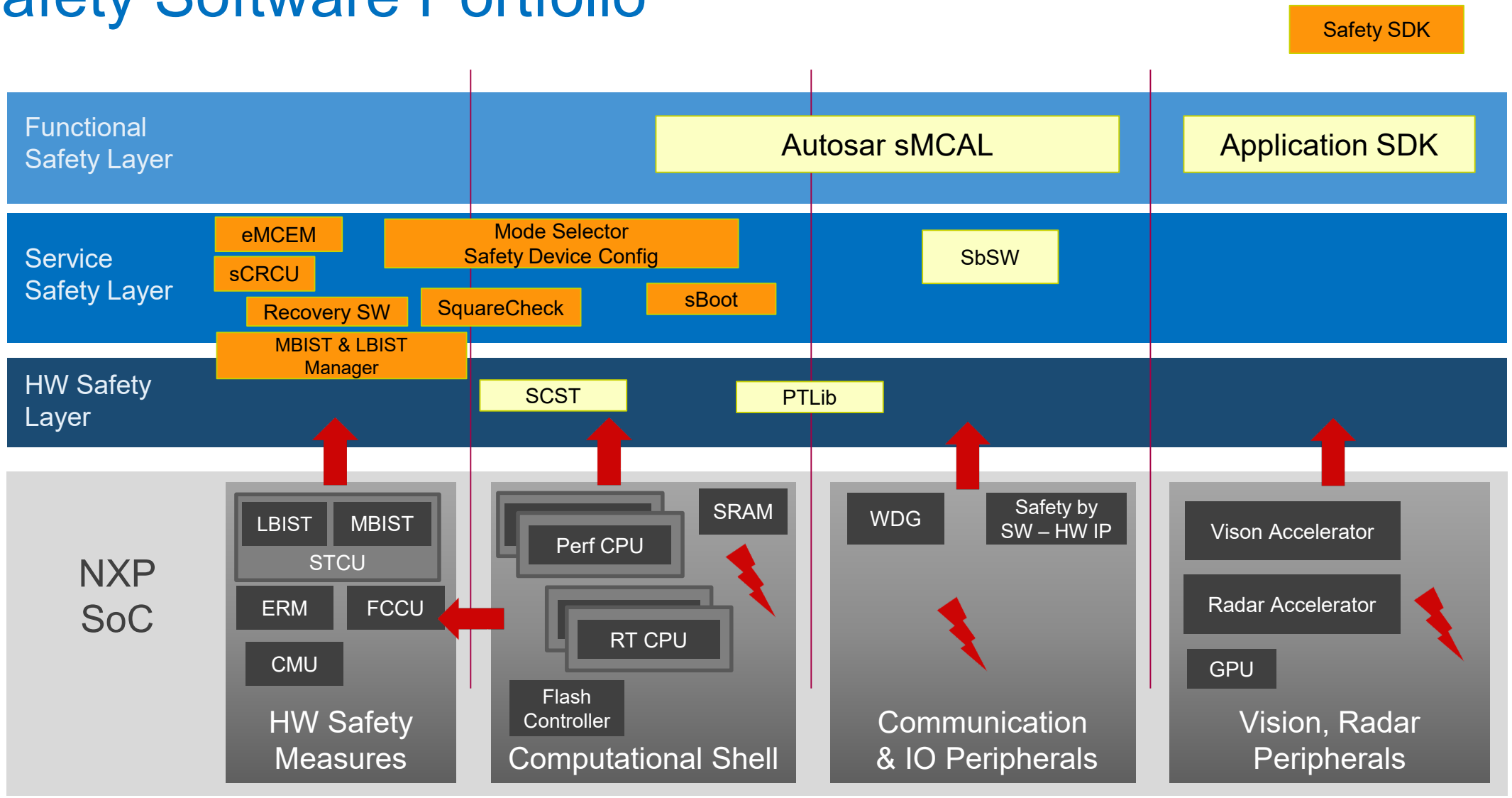
Detection Components

- 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

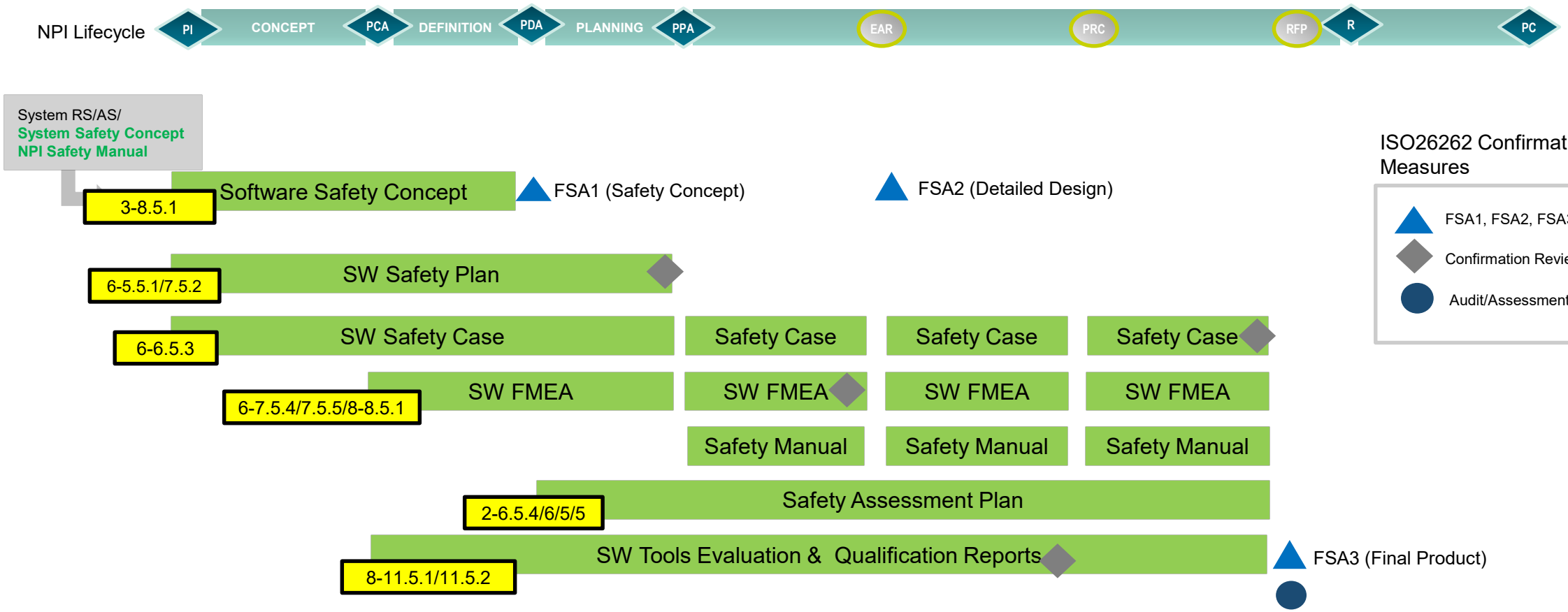
Reaction Components

- eMCEM – Error Manager configures FCCU and provides handlers to faults signaled to FCCU
- SW Recovery – initiates the global recovery process
- Mode Selector – depending on the SoC fault status selects the appropriate operating mode

Safety Software Portfolio

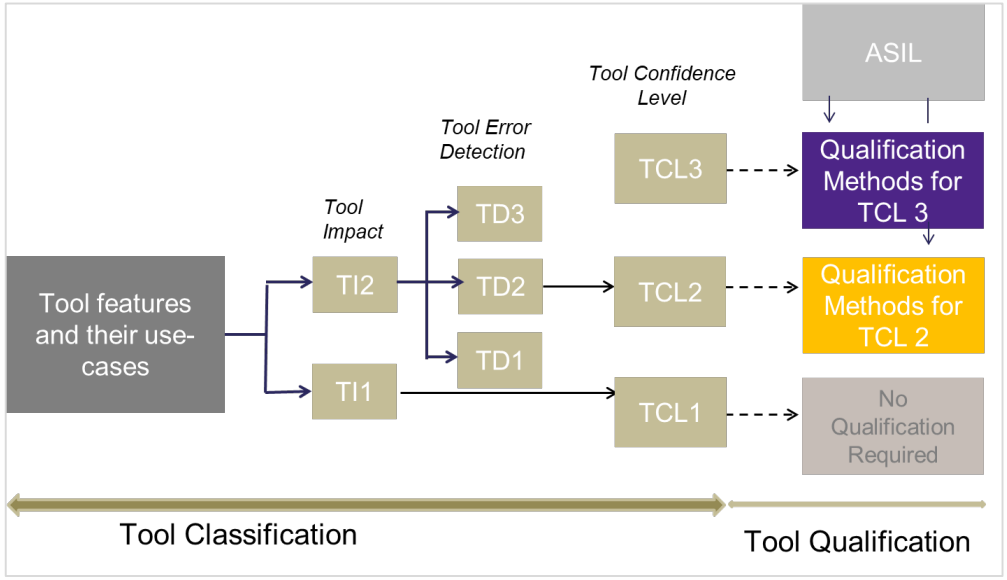


SW Safety Deliverables

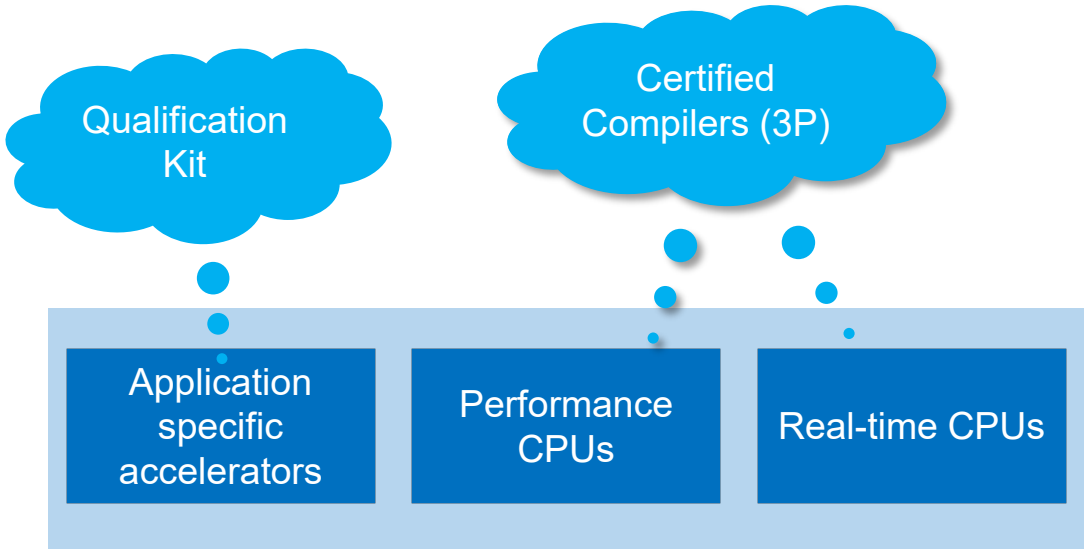


Automotive SPICE + Safety Extensions = ISO 26262

Tool Compliance



- Classification Report
- Qualification Plan
- Qualification Report
- Safety Manual
- ISO26262 compliance report



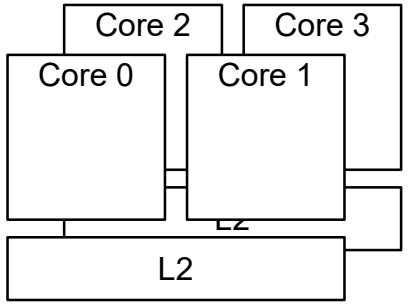
	Methods required for TCL2	ASIL A	ASIL B	ASIL C	ASIL D
1a	Increased confidence from use	++	++	++	+
1b	Evaluation of the tool development process	++	++	++	+
1c	Validation of the software tool	+	+	+	++
1d	Development in accordance with a safety standard *	+	+	+	++

	Methods required for TCL3	ASIL A	ASIL B	ASIL C	ASIL D
1a	Increased confidence from use	++	++	+	+
1b	Evaluation of the tool development process	++	++	+	+
1c	Validation of the software tool	+	+	++	++
1d	Development in accordance with a safety standard *	+	+	++	++

Validas AG

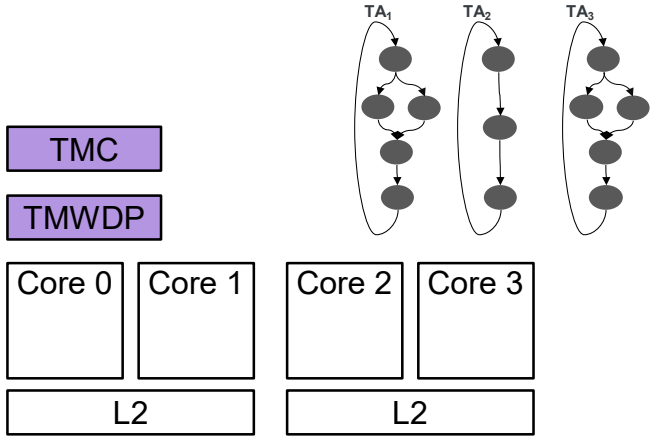
S32 Safety Alternatives for Performance Cores

HW Lockstep



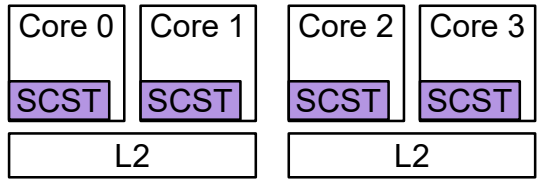
- Targets **ASIL D**
- Delayed Lock-step Clusters
- Configured at Boot
- Fully transparent to SW
- Fallback to degraded mode in case of a permanent fault

Safety by SW



- Enable **ASIL B/D** by application monitoring
- Detects loss of integrity and data error caused by SW & HW faults
- Time Monitored Comparator (TMC)
  - Detects data and timing errors
- Timed Multi-Watchdog Processor (TMWDP)
  - Operational logical flow errors

Core Self Test



- Targets **ASIL B** (with minimal SW overhead)
- Core self-test (SCST)
- Executed @ runtime on each CPU
- High diagnostic coverage with low performance impact

Getting Safety Support

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

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

NXP SafeAssure™ Products

To support the customer to build their 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)

SECURE CONNECTIONS
FOR A SMARTER WORLD