满足ISO 26262 ASIL B&D RISC-V CPU内核开发

芯来科技 范添彬

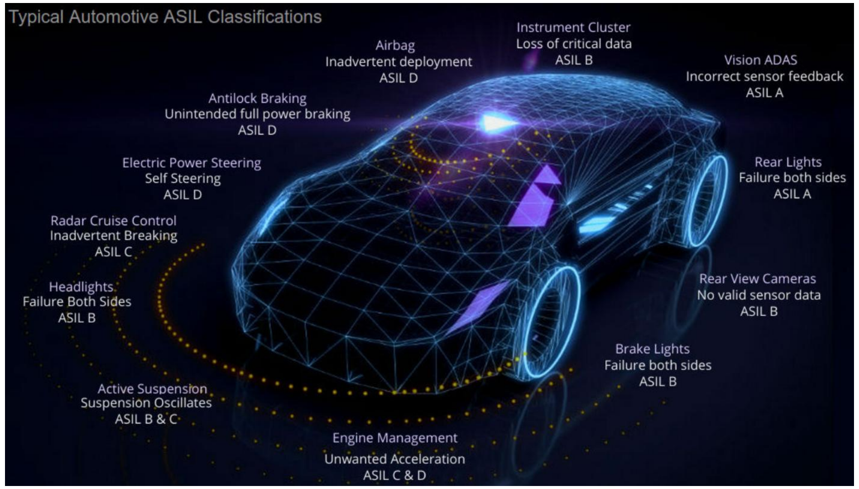
Functional Safety- ISO 26262

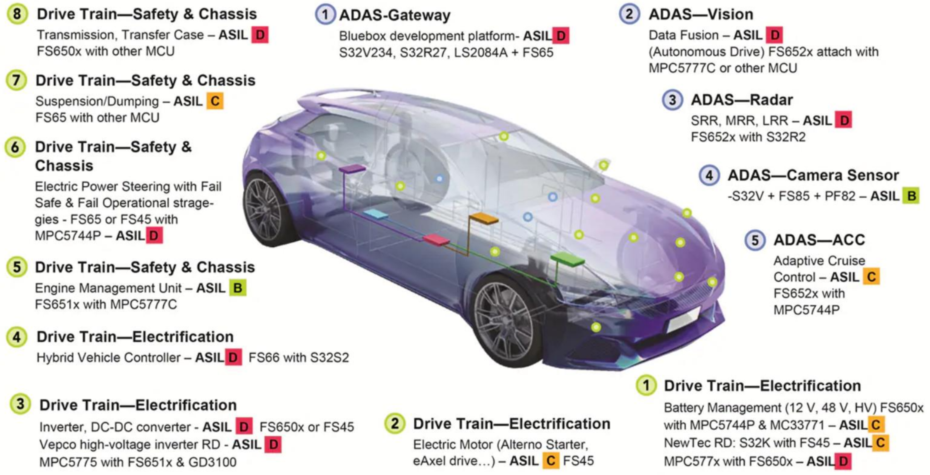
ASIL comes from Functional Safety, ISO 26262

Absence of unacceptable risk due to hazards casue by malfunctioning behaviour of E/E (electrical / electronic) systems.

Root causes for malfunctioning behaviour :

- Systematic errors (during specification, development, manufacturing, …)
- Random hardware faults (during operation in the field)
- Foreseeable operational errors and misuse (during operation)




8 Drive Train—Safety & Chassis
Transmission, Transfer Case – ASIL D
FS650x with other MCU
7 Drive Train—Safety & Chassis
Suspension/Dumping – ASIL C
FS65 with other MCU
6 Drive Train—Safety & Chassis
Electric Power Steering with Fail Safe & Fail Operational strage-gies - FS65 or FS45 with MPC5744P – ASIL D
5 Drive Train—Safety & Chassis
Engine Management Unit – ASIL B
FS651x with MPC5777C
4 Drive Train—Electrification
Hybrid Vehicle Controller – ASIL D FS66 with S32S2
3 Drive Train—Electrification
Inverter, DC-DC converter - ASIL D FS650x or FS45
Vepco high-voltage inverter RD - ASIL D
MPC5775 with FS651x & GD3100
1 ADAS-Gateway
Bluebox development platform- ASIL D
S32V234, S32R27, LS2084A + FS65
2 ADAS—Vision
Data Fusion – ASIL D
(Autonomous Drive) FS652x attach with MPC5777C or other MCU
3 ADAS—Radar
SRR, MRR, LRR – ASIL D
FS652x with S32R2
4 ADAS—Camera Sensor
-S32V + FS85 + PF82 – ASIL B
5 ADAS—ACC
Adaptive Cruise Control – ASIL C
FS652x with MPC5744P
2 Drive Train—Electrification
Electric Motor (Alterno Starter, eAxel drive…) – ASIL C FS45
1 Drive Train—Electrification
Battery Management (12 V, 48 V, HV) FS650x with MPC5744P & MC33771 – ASIL C
NewTec RD: S32K with FS45 – ASIL C
MPC577x with FS650x – ASIL D

Original from Mentor&NXP

Quantitative ASIL effect on IP design

	ASIL D	ASIL C	ASIL B	(ASIL A)
SPFM	> 99 %	> 97 %	> 90 %	> 60 % *not normative*
LFM	> 90 %	> 80 %	> 60 %	n/a

ASIL Level	Random hardware failure target values *)
D	$< 10^{-8}\ h^{-1}$ (10 FIT)
C	$< 10^{-7}\ h^{-1}$ (100 FIT)
(B)	$< 10^{-7}\ h^{-1}$ (100 FIT)
(A)	$< 10^{-6}\ h^{-1}$ (1000 FIT) *not normative*

*Target values from ISO 26262-5

Detect/Control failure

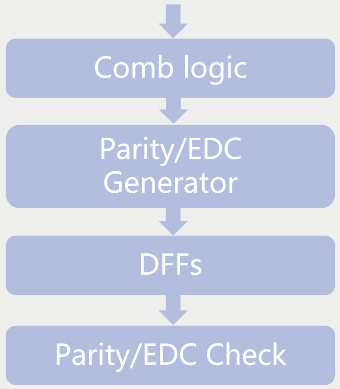
- Effective safety mechanism to handle transient&permanent faults
- Verification of safety mechansim to achieve target values from ISO 26262-5

Safety Mechanisms on CPU IP design

STL

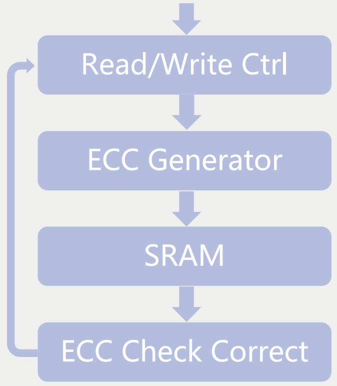
Providing STL(software test library)

DFF Parity/EDC



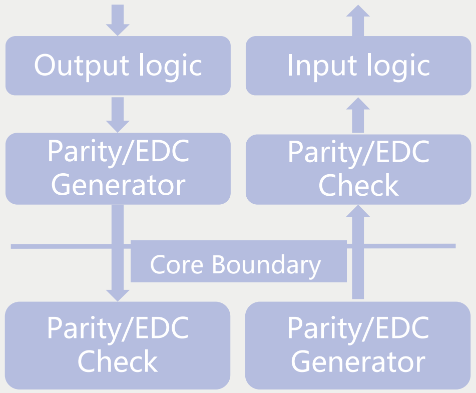
Implementing error detection code (EDC) on critical DFF. Selective coverage of architectural, pipeline or all DFF.

SRAM ECC



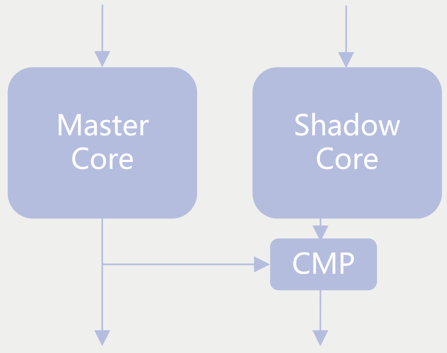
Implementing error correction code (ECC) on ILM, DLM, I/D-Cache with enhanced address and multi-bit error coverage

IO Parity/EDC

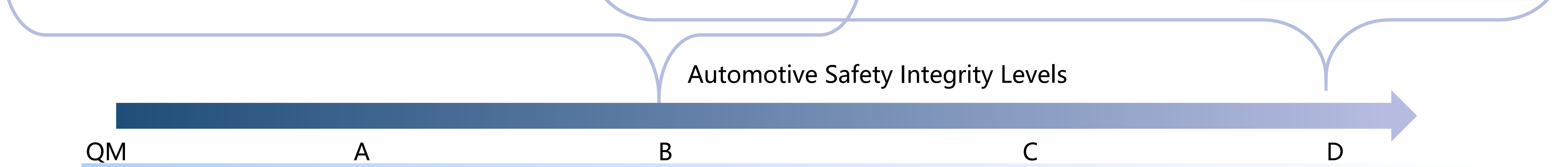


Implementing error detection code (EDC) on core boundary IO

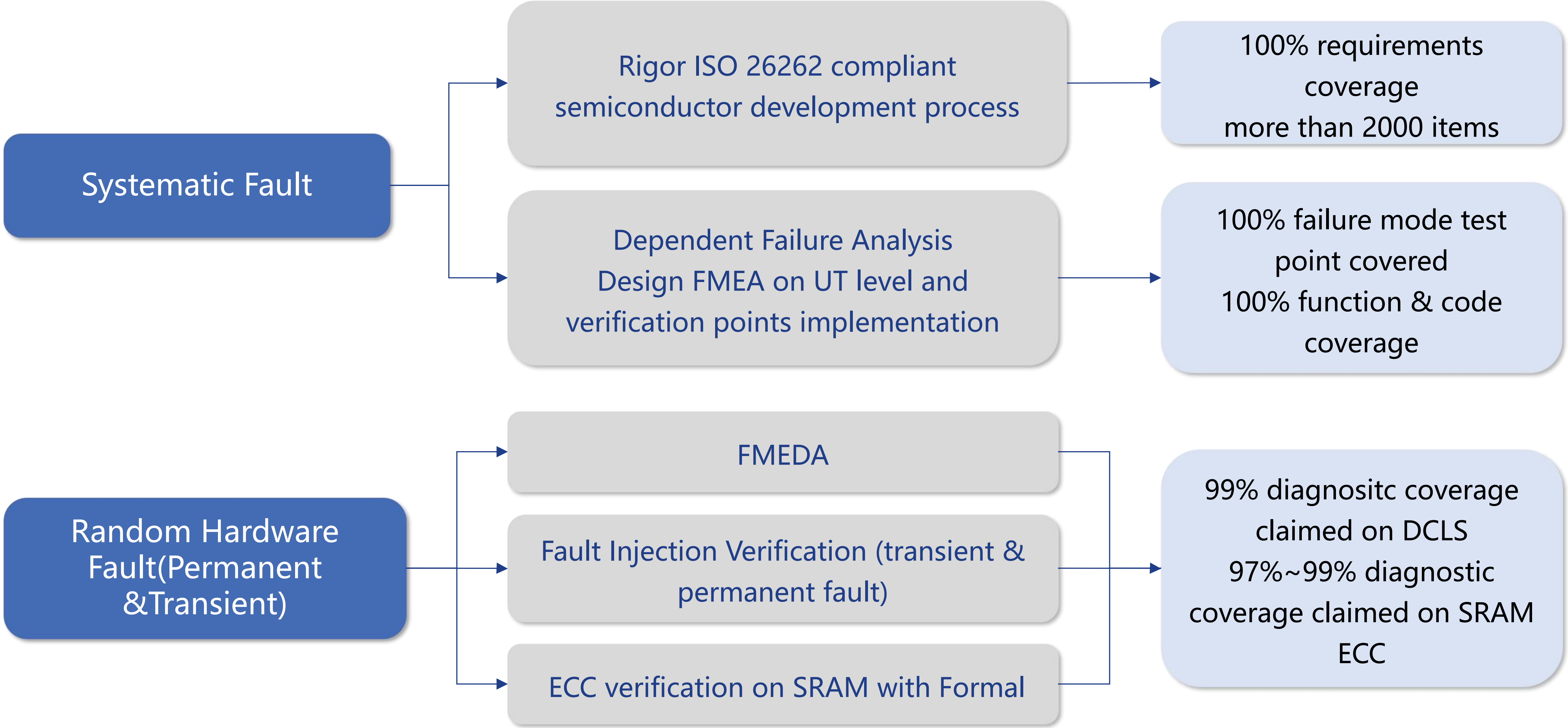
Dual-Core Lockstep



The Dual-core lockstep cores executing the same code, then their outputs and key internal states are compared every cycle; Any mismatch will generate a fault by the comparison unit



ISO 26262 Compliance



Systematic Fault

Rigor ISO 26262 compliant semiconductor development process

100% requirements coverage
more than 2000 items

Dependent Failure Analysis
Design FMEA on UT level and verification points implementation

100% failure mode test point covered
100% function & code coverage

Random Hardware Fault(Permanent &Transient)

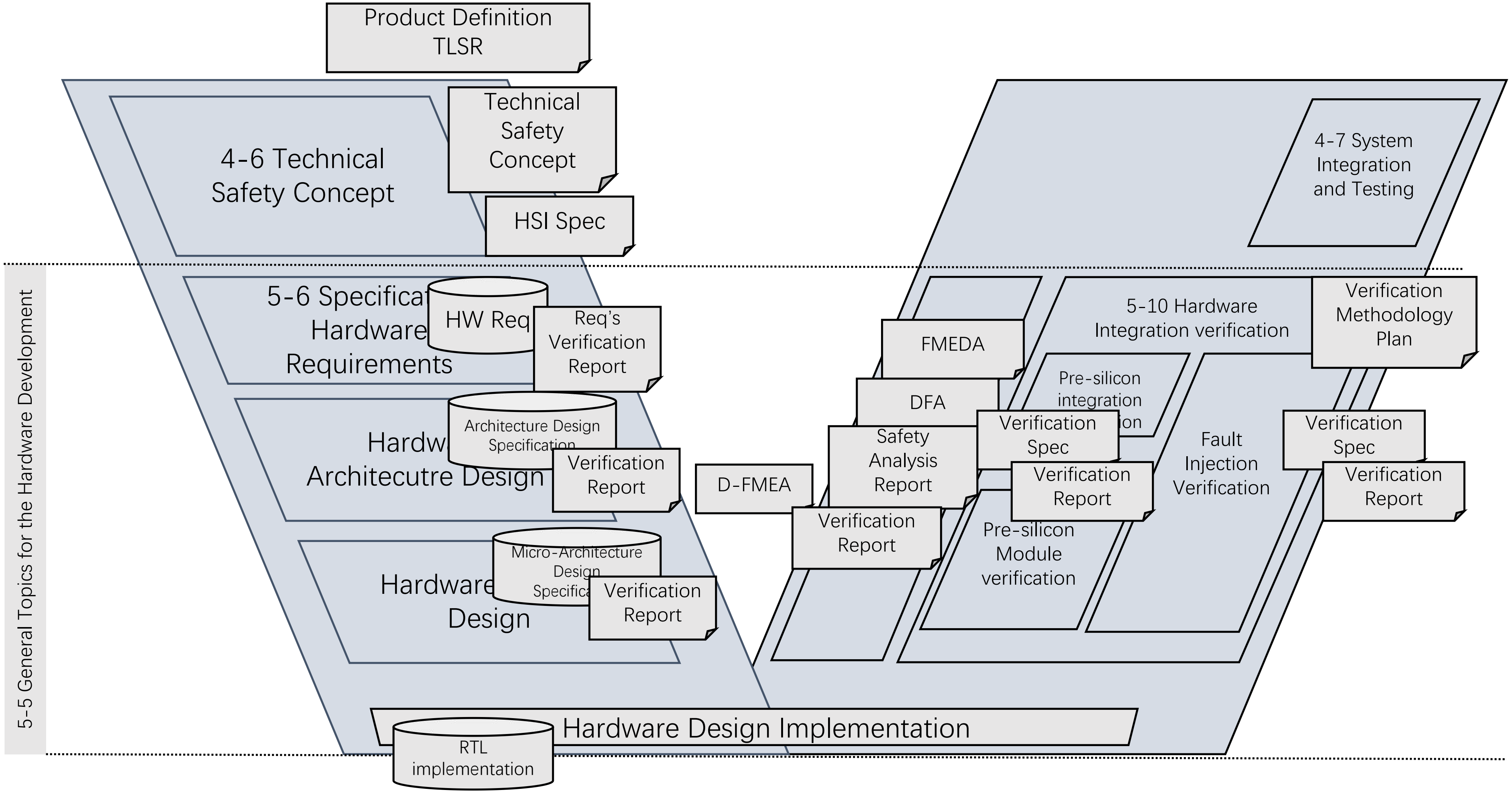
FMEDA

Fault Injection Verification (transient & permanent fault)

ECC verification on SRAM with Formal

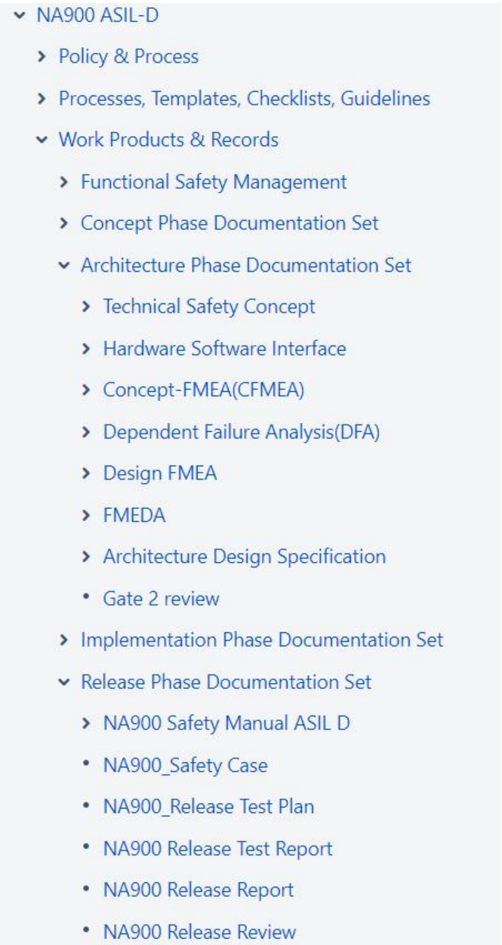
99% diagnositc coverage claimed on DCLS
97%~99% diagnostic coverage claimed on SRAM ECC

V-Model for CPU IP Design


Product Definition
TLSR
4-6 Technical Safety Concept
Technical Safety Concept
HSI Spec
5-6 Specificat
Hardware Requirements
HW Req
Req's Verification Report
Hardw
Architecutre Design
Architecture Design Specification
Verification Report
Hardware
Design
Micro-Architecture Design Specifica
Verification Report
D-FMEA
RTL implementation
Hardware Design Implementation
5-5 General Topics for the Hardware Development
4-7 System Integration and Testing
FMEDA
DFA
Safety Analysis Report
Verification Report
5-10 Hardware Integration verification
Verification Methodology Plan
Pre-silicon integration
ion
Verification Spec
Verification Report
Pre-silicon Module verification
Fault Injection Verification
Verification Spec
Verification Report

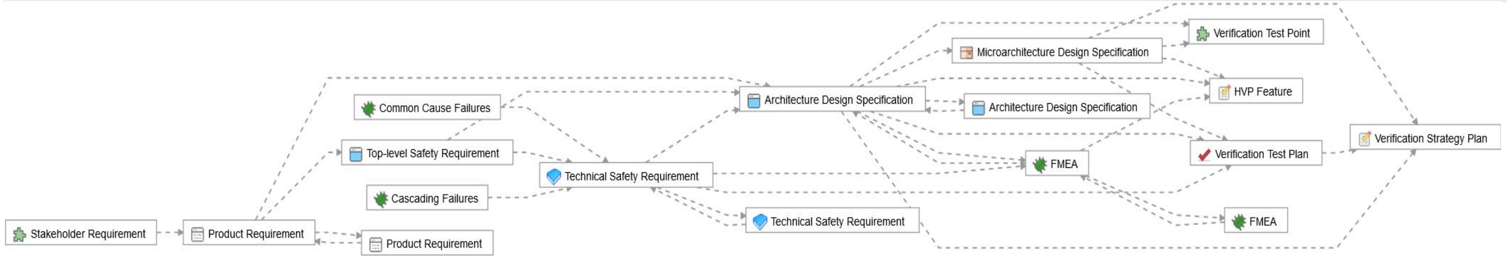
Functional Safety Management

Documentation Management(in wiki)

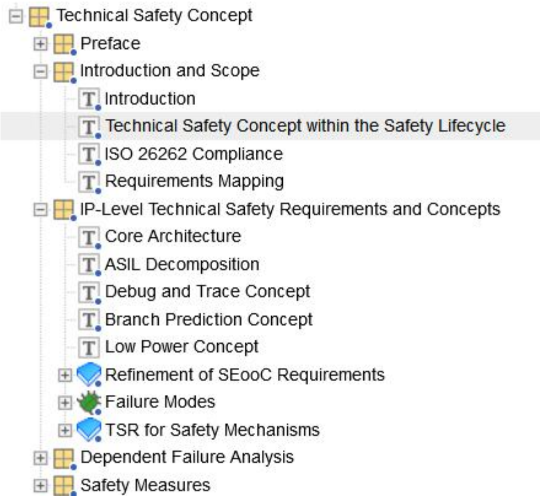


- NA900 ASIL-D
  - Policy & Process
  - Processes, Templates, Checklists, Guidelines
  - Work Products & Records
    - Functional Safety Management
    - Concept Phase Documentation Set
    - Architecture Phase Documentation Set
      - Technical Safety Concept
      - Hardware Software Interface
      - Concept-FMEA(CFMEA)
      - Dependent Failure Analysis(DFA)
      - Design FMEA
      - FMEDA
      - Architecture Design Specification
      - Gate 2 review
    - Implementation Phase Documentation Set
    - Release Phase Documentation Set
      - NA900 Safety Manual ASIL D
      - NA900_Safety Case
      - NA900_Release Test Plan
      - NA900 Release Test Report
      - NA900 Release Report
      - NA900 Release Review

Requirements Management(in JAMA)

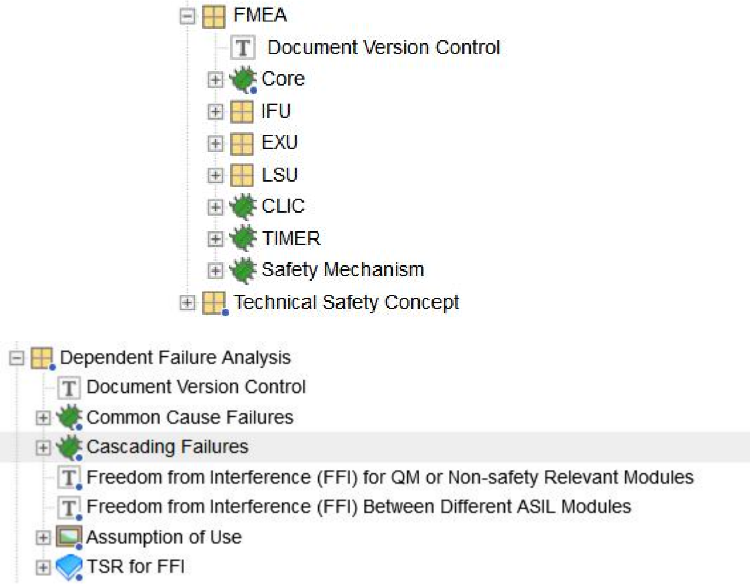

Verification Test Point
Microarchitecture Design Specification
HVP Feature
Common Cause Failures
Architecture Design Specification
Architecture Design Specification
Verification Strategy Plan
Top-level Safety Requirement
FMEA
Verification Test Plan
Technical Safety Requirement
Cascading Failures
Technical Safety Requirement
FMEA
Stakeholder Requirement
Product Requirement
Product Requirement

Technical Safety Concept(in JAMA)



- Technical Safety Concept
  - Preface
  - Introduction and Scope
    - Introduction
    - Technical Safety Concept within the Safety Lifecycle
    - ISO 26262 Compliance
    - Requirements Mapping
  - IP-Level Technical Safety Requirements and Concepts
    - Core Architecture
    - ASIL Decomposition
    - Debug and Trace Concept
    - Branch Prediction Concept
    - Low Power Concept
    - Refinement of SEooC Requirements
    - Failure Modes
    - TSR for Safety Mechanisms
  - Dependent Failure Analysis
  - Safety Measures

Safety Analysis(FMEA&DFA) (in JAMA)

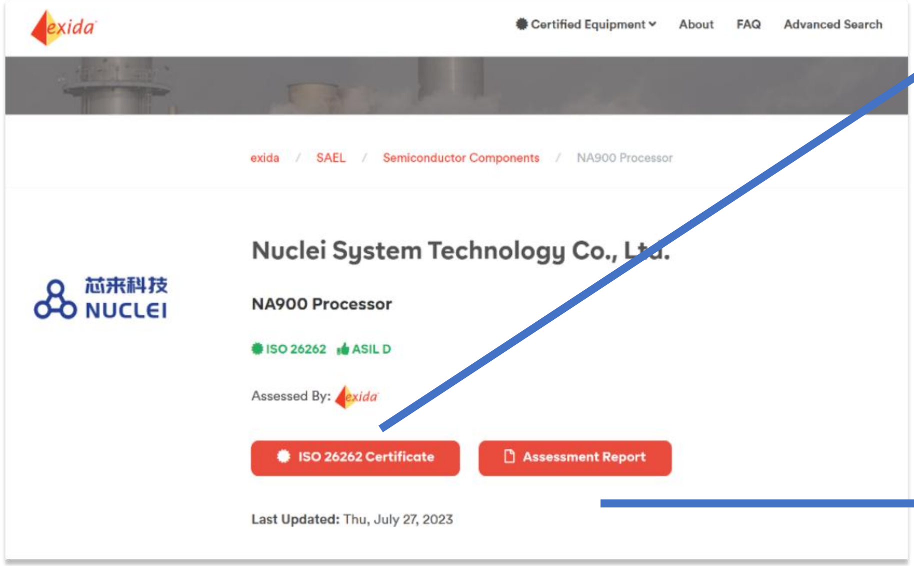


- FMEA
  - Document Version Control
  - Core
  - IFU
  - EXU
  - LSU
  - CLIC
  - TIMER
  - Safety Mechanism
  - Technical Safety Concept

- Dependent Failure Analysis
  - Document Version Control
  - Common Cause Failures
  - Cascading Failures
  - Freedom from Interference (FFI) for QM or Non-safety Relevant Modules
  - Freedom from Interference (FFI) Between Different ASIL Modules
  - Assumption of Use
  - TSR for FFI

NA900 ISO26262 Product Certification

https://www.exida.com/SAEL-Safety/nuclei-system-technology-co.-ltd.-na900-processor



exida / SAEL / Semiconductor Components / NA900 Processor

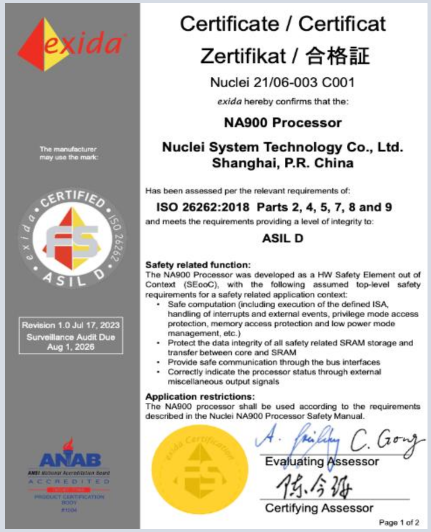
Nuclei System Technology Co., Ltd.

NA900 Processor

ISO 26262 ASIL D

Assessed By: exida

Last Updated: Thu, July 27, 2023



Certificate / Certificat
Zertifikat / 合格証

Nuclei 21/06-003 C001

exida hereby confirms that the:

NA900 Processor

**Nuclei System Technology Co., Ltd.
Shanghai, P.R. China**

Has been assessed per the relevant requirements of:

ISO 26262:2018 Parts 2, 4, 5, 7, 8 and 9

and meets the requirements providing a level of integrity to:

ASIL D

Safety related function:
The NA900 Processor was developed as a HW Safety Element out of Context (SEooC), with the following assumed top-level safety requirements for a safety related application context:

- Safe computation (including execution of the defined ISA, handling of interrupts and external events, privilege mode access protection, memory access protection and low power mode management, etc.)
- Protect the data integrity of all safety related SRAM storage and transfer between core and SRAM
- Provide safe communication through the bus interfaces
- Correctly indicate the processor status through external miscellaneous output signals

Application restrictions:
The NA900 processor shall be used according to the requirements described in the Nuclei NA900 Processor Safety Manual.

The manufacturer may use the mark:

CERTIFIED exida ISO 26262 ASIL D

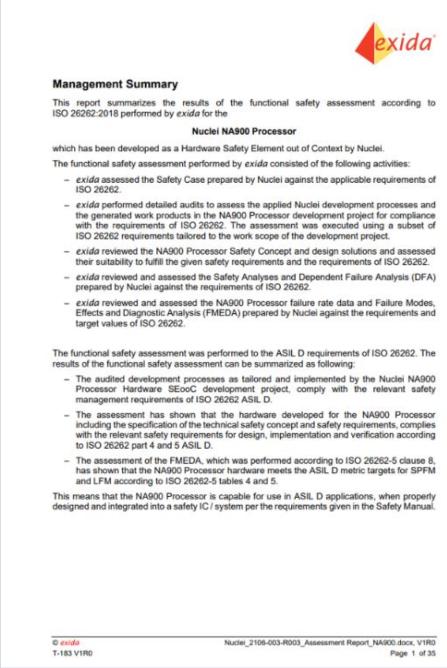
Revision 1.0 Jul 17, 2023
Surveillance Audit Due
Aug 1, 2026

ANAB
ANSI National Accreditation Board
ACCREDITED
PRODUCT CERTIFICATION BODY
#1004

C. Gong
Evaluating Assessor

Certifying Assessor

Page 1 of 2



Management Summary

This report summarizes the results of the functional safety assessment according to ISO 26262:2018 performed by *exida* for the

Nuclei NA900 Processor

which has been developed as a Hardware Safety Element out of Context by Nuclei.

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the Safety Case prepared by Nuclei against the applicable requirements of ISO 26262.
- *exida* performed detailed audits to assess the applied Nuclei development processes and the generated work products in the NA900 Processor development project for compliance with the requirements of ISO 26262. The assessment was executed using a subset of ISO 26262 requirements tailored to the work scope of the development project.
- *exida* reviewed the NA900 Processor Safety Concept and design solutions and assessed their suitability to fulfill the given safety requirements and the requirements of ISO 26262.
- *exida* reviewed and assessed the Safety Analyses and Dependent Failure Analysis (DFA) prepared by Nuclei against the requirements of ISO 26262.
- *exida* reviewed and assessed the NA900 Processor failure rate data and Failure Modes, Effects and Diagnostic Analysis (FMEDA) prepared by Nuclei against the requirements and target values of ISO 26262.

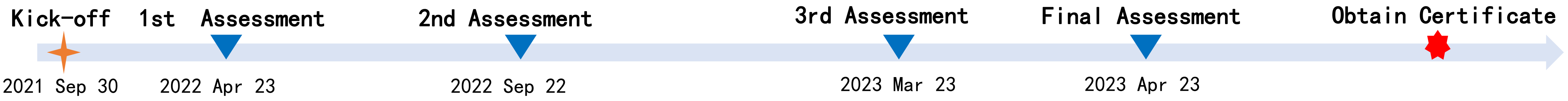
The functional safety assessment was performed to the ASIL D requirements of ISO 26262. The results of the functional safety assessment can be summarized as following:

- The audited development processes as tailored and implemented by the Nuclei NA900 Processor Hardware SEooC development project, comply with the relevant safety management requirements of ISO 26262 ASIL D.
- The assessment has shown that the hardware developed for the NA900 Processor including the specification of the technical safety concept and safety requirements, complies with the relevant safety requirements for design, implementation and verification according to ISO 26262 part 4 and 5 ASIL D.
- The assessment of the FMEDA, which was performed according to ISO 26262-5 clause 8, has shown that the NA900 Processor hardware meets the ASIL D metric targets for SPFM and LFM according to ISO 26262-5 tables 4 and 5.

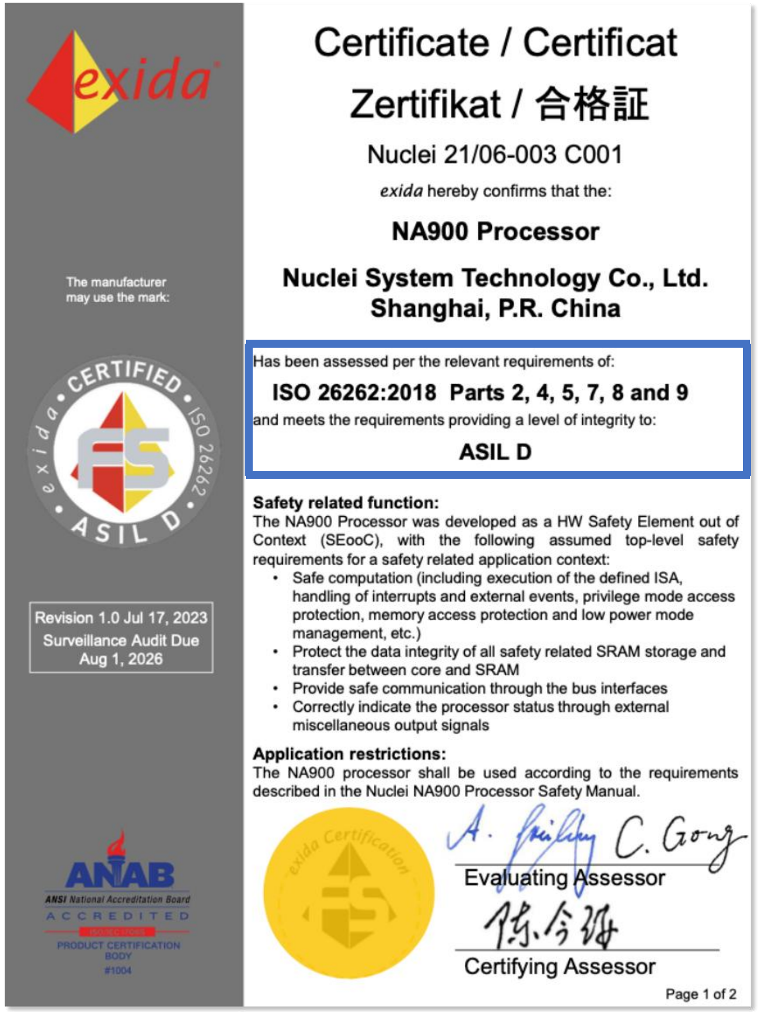
This means that the NA900 Processor is capable for use in ASIL D applications, when properly designed and integrated into a safety IC / system per the requirements given in the Safety Manual.

© exida
T-183 V1R0

Nuclei_2106-003-R003_Assessment Report_NA900.docx, V1R0
Page 1 of 35



NA900 — 1st ASIL D RISC-V CPU IP Product Certification with exida



exida

The manufacturer
may use the mark:

CERTIFIED • ISO 26262 • ASIL D • exida

Revision 1.0 Jul 17, 2023
Surveillance Audit Due
Aug 1, 2026

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17065
PRODUCT CERTIFICATION
BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

Nuclei 21/06-003 C001

exida hereby confirms that the:

NA900 Processor

Nuclei System Technology Co., Ltd.
Shanghai, P.R. China

Has been assessed per the relevant requirements of:

ISO 26262:2018 Parts 2, 4, 5, 7, 8 and 9

and meets the requirements providing a level of integrity to:

ASIL D

Safety related function:
The NA900 Processor was developed as a HW Safety Element out of Context (SEooC), with the following assumed top-level safety requirements for a safety related application context:

- Safe computation (including execution of the defined ISA, handling of interrupts and external events, privilege mode access protection, memory access protection and low power mode management, etc.)
- Protect the data integrity of all safety related SRAM storage and transfer between core and SRAM
- Provide safe communication through the bus interfaces
- Correctly indicate the processor status through external miscellaneous output signals

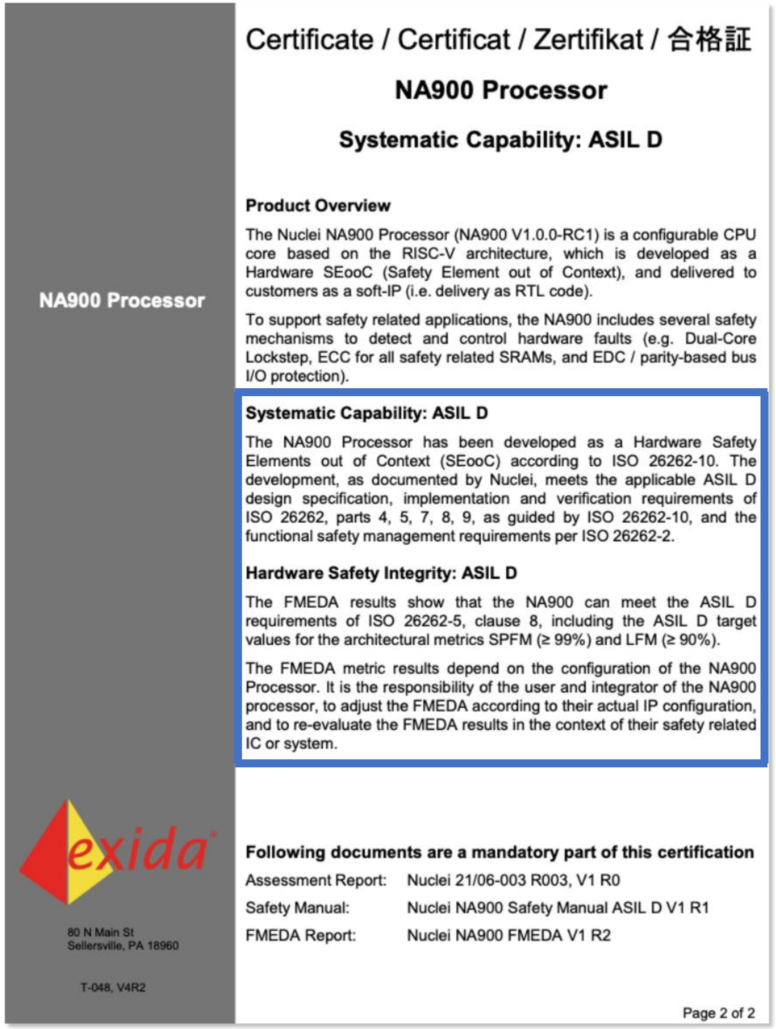
Application restrictions:
The NA900 processor shall be used according to the requirements described in the Nuclei NA900 Processor Safety Manual.

exida Certification

C. Gong
Evaluating Assessor

Certifying Assessor

Page 1 of 2



NA900 Processor

exida

80 N Main St
Sellersville, PA 18960

T-048, V4R2

Certificate / Certificat / Zertifikat / 合格証

NA900 Processor

Systematic Capability: ASIL D

Product Overview

The Nuclei NA900 Processor (NA900 V1.0.0-RC1) is a configurable CPU core based on the RISC-V architecture, which is developed as a Hardware SEooC (Safety Element out of Context), and delivered to customers as a soft-IP (i.e. delivery as RTL code).

To support safety related applications, the NA900 includes several safety mechanisms to detect and control hardware faults (e.g. Dual-Core Lockstep, ECC for all safety related SRAMs, and EDC / parity-based bus I/O protection).

Systematic Capability: ASIL D

The NA900 Processor has been developed as a Hardware Safety Elements out of Context (SEooC) according to ISO 26262-10. The development, as documented by Nuclei, meets the applicable ASIL D design specification, implementation and verification requirements of ISO 26262, parts 4, 5, 7, 8, 9, as guided by ISO 26262-10, and the functional safety management requirements per ISO 26262-2.

Hardware Safety Integrity: ASIL D

The FMEDA results show that the NA900 can meet the ASIL D requirements of ISO 26262-5, clause 8, including the ASIL D target values for the architectural metrics SPFM (≥ 99%) and LFM (≥ 90%).

The FMEDA metric results depend on the configuration of the NA900 Processor. It is the responsibility of the user and integrator of the NA900 processor, to adjust the FMEDA according to their actual IP configuration, and to re-evaluate the FMEDA results in the context of their safety related IC or system.

Following documents are a mandatory part of this certification

Assessment Report:	Nuclei 21/06-003 R003, V1 R0
Safety Manual:	Nuclei NA900 Safety Manual ASIL D V1 R1
FMEDA Report:	Nuclei NA900 FMEDA V1 R2

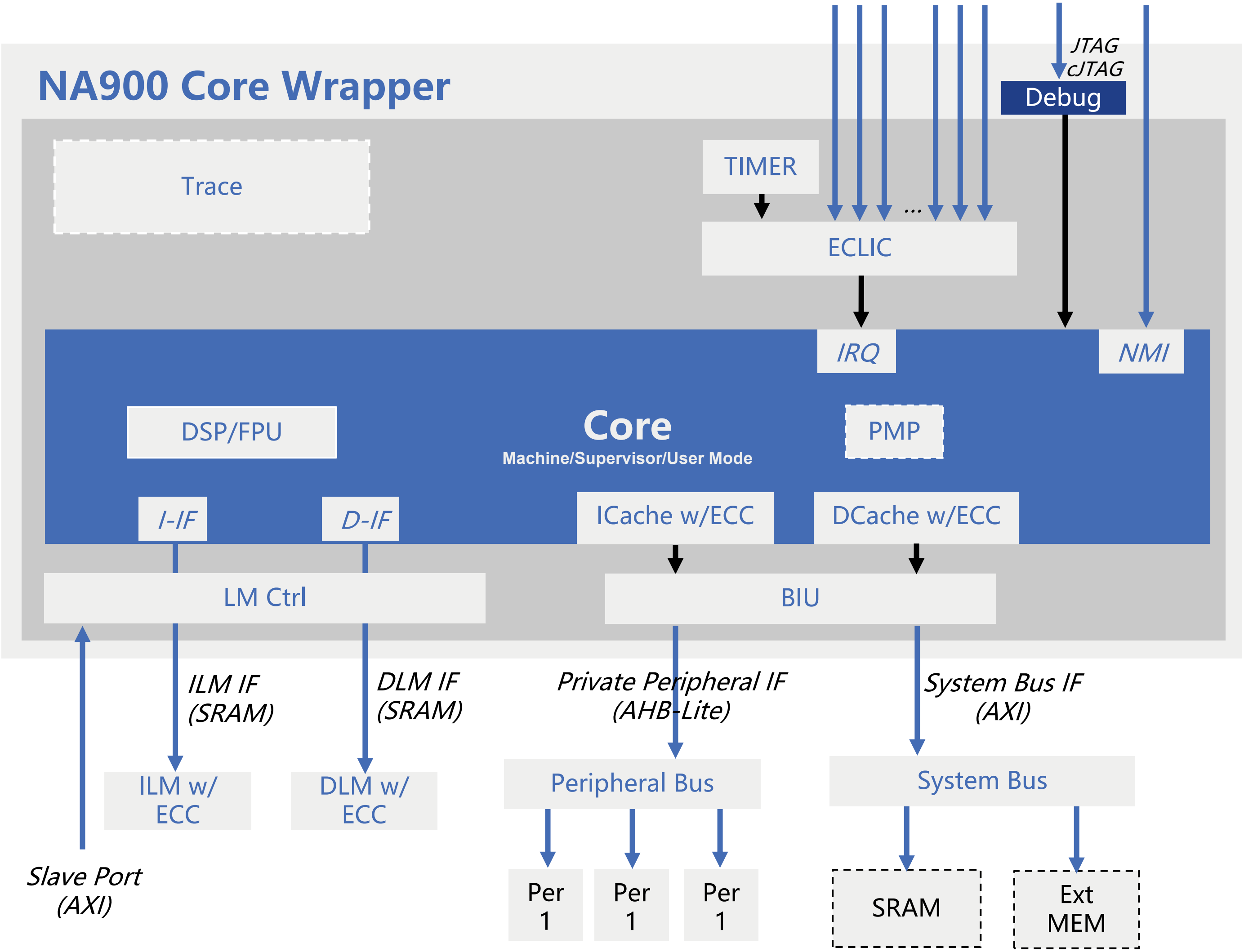
Page 2 of 2

NA900 Micro-Architecture Diagram

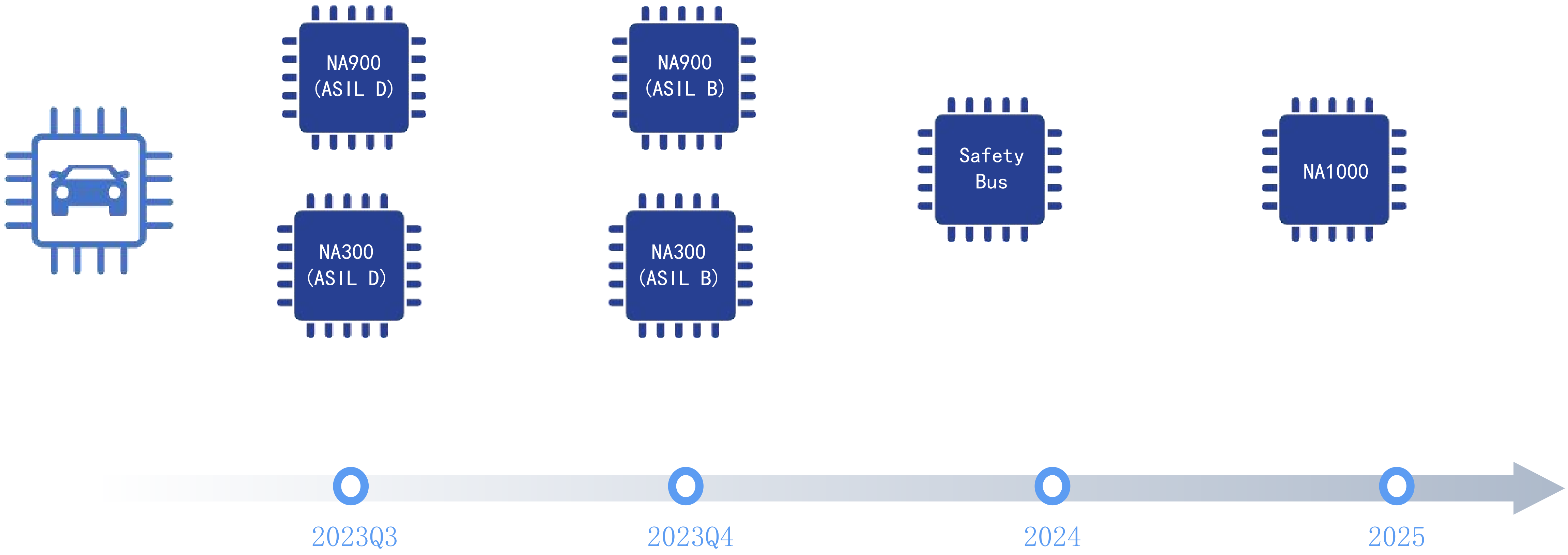
芯来科技
NUCLEI

- RISC-V RV32IMACFDPB ISA supported
- Dual Issue, in-order 9 stage Harvard Pipeline
- Single precision floating point, double prevision configurable
- ILM & DLM0/DLM1 with ECC, 512KB
- I-Cache & D-Cache with ECC, 32/64KB
- 64/128-bit AXI system bus, configurable 64-bit AXI slave port
- Besides Machine mode & User mode, Supervisor mode is supported for TEE (Trust Execution Environment)
- Configurable Trace module
- Full Standard Debug Function with JTAG/cJTAG Port
- Configurable in lockstep or split mode

Safety Mechanism	Description
HWSM-DCLS	Dual Core Lockstep
HWSM-SRAM-PROT	ECC Protection on SRAM
HWSM-I/O Protection	Input.Output signal protection
HWSM-NSI-ISO	Non-safety isolation
HWSM-DCLS-TSC	Total-self-check comparator
HWSM-EXT-WDG	External watchdog timer



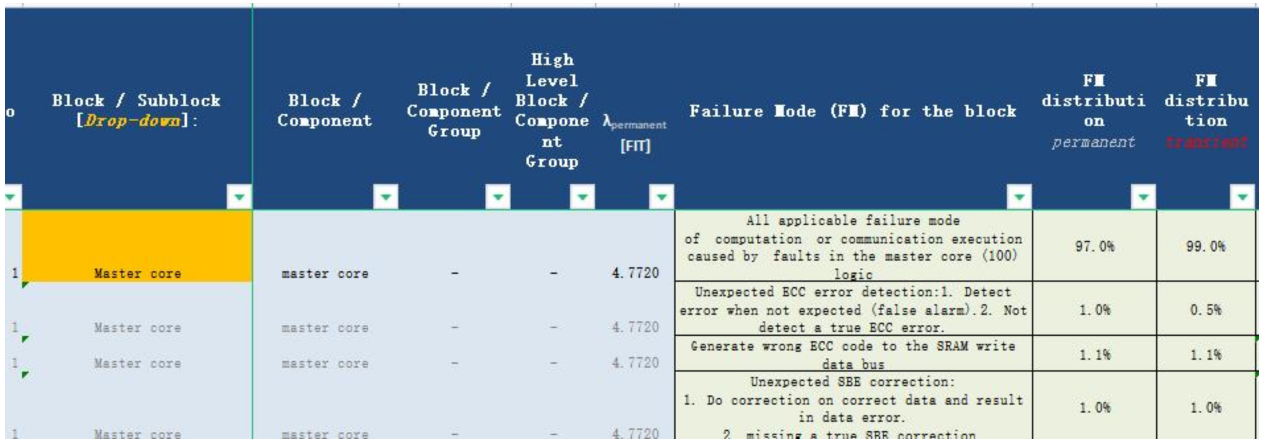
Safety critical SoC with Nuclei



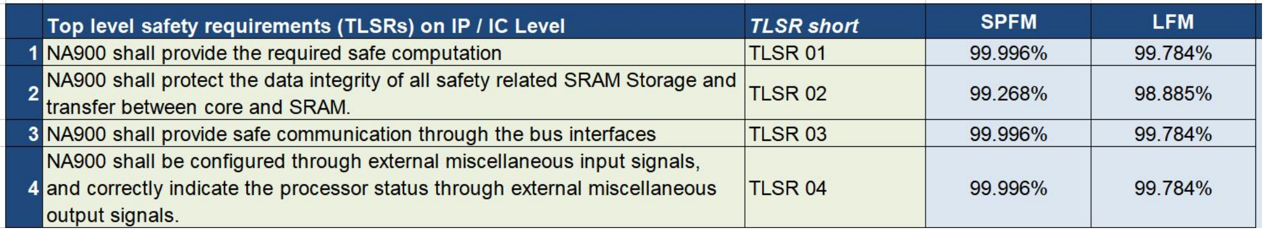
Safety Package

芯来科技 NUCLEI

FMEDA

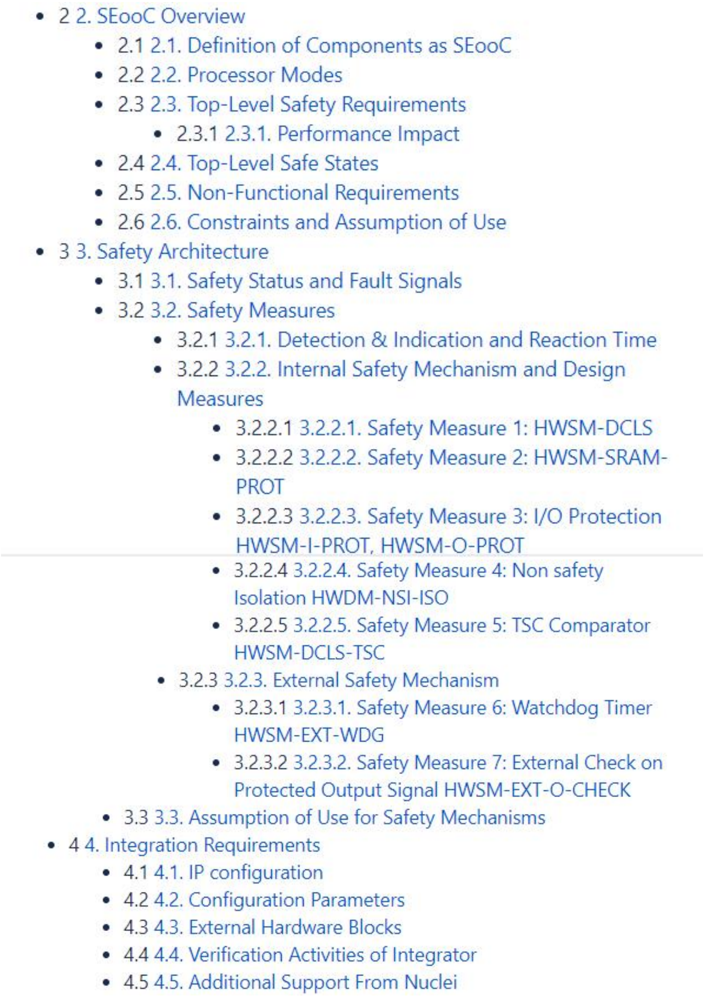


o	Block / Subblock [*Drop-down*]:	Block / Component	Block / Component Group	High Level Block / Component Group	$\lambda_{permanent}$ [FIT]	Failure Mode (FM) for the block	FM distribution *permanent*	FM distribution *transient*
1	Master core	master core	-	-	4.7720	All applicable failure mode of computation or communication execution caused by faults in the master core (100) logic	97.0%	99.0%
1	Master core	master core	-	-	4.7720	Unexpected ECC error detection:1. Detect error when not expected (false alarm).2. Not detect a true ECC error.	1.0%	0.5%
1	Master core	master core	-	-	4.7720	Generate wrong ECC code to the SRAM write data bus	1.1%	1.1%
1	Master core	master core	-	-	4.7720	Unexpected SBE correction: 1. Do correction on correct data and result in data error. 2. missing a true SBE correction	1.0%	1.0%



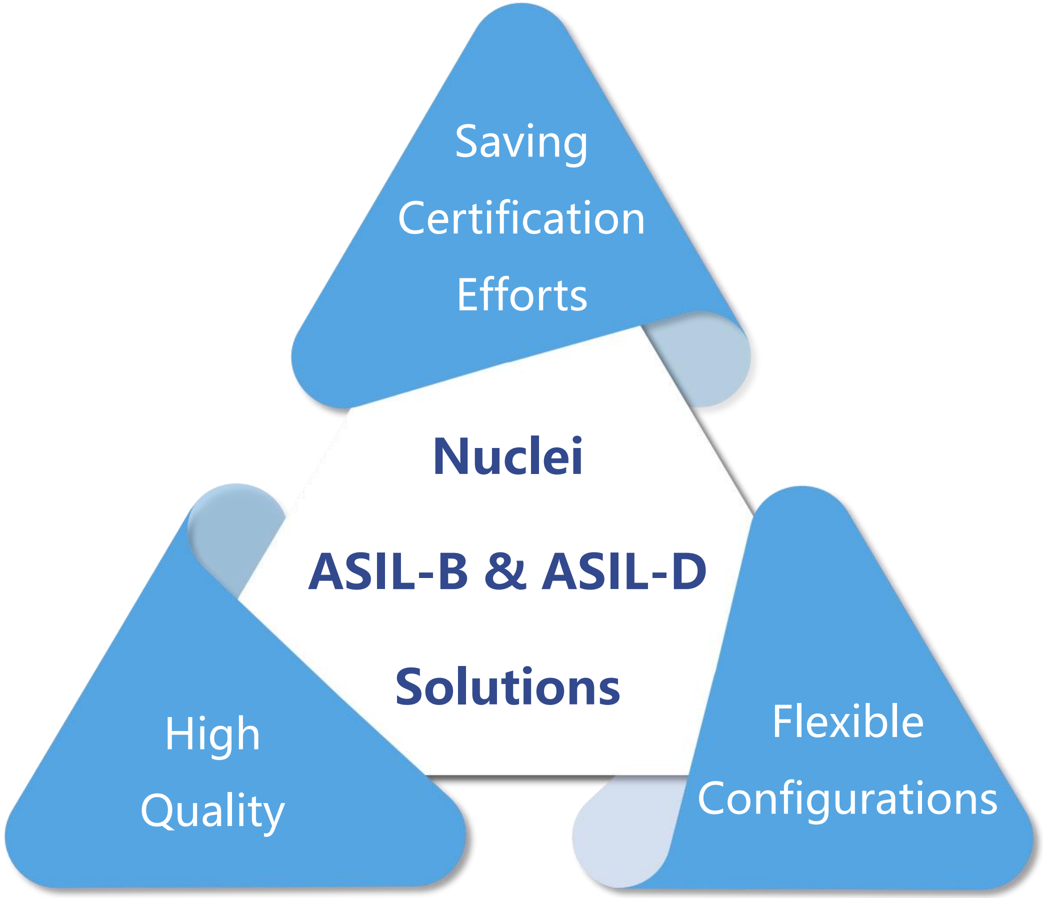
	Top level safety requirements (TLSRs) on IP / IC Level	*TLSR short*	SPFM	LFM
1	NA900 shall provide the required safe computation	TLSR 01	99.996%	99.784%
2	NA900 shall protect the data integrity of all safety related SRAM Storage and transfer between core and SRAM.	TLSR 02	99.268%	98.885%
3	NA900 shall provide safe communication through the bus interfaces	TLSR 03	99.996%	99.784%
4	NA900 shall be configured through external miscellaneous input signals, and correctly indicate the processor status through external miscellaneous output signals.	TLSR 04	99.996%	99.784%

Safety Manual



Summary for Nuclei Automotive FuSa Solutions

- ASIL-B & ASIL-D solutions are both available
- Rich configurations to fit variable automotive SoC requirements
- Competitive PPA with ASIL B&D
- Comprehensive safety package
  - Adaptable Safety Manual
  - Adaptable Safety Analysis Report
    - FMEDA
    - FMEA
  - Supporting Evidence



芯来科技 NUCLEI

THANK YOU