NUCLEI

A Leading RISC-V CPU IP and Solution Vendor

芯来科技 NUCLEI

NA900-ISO 26262 ASIL-D Product Certified RISC-V CPU IP

exida

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.

Evaluating Assessor

Certifying Assessor

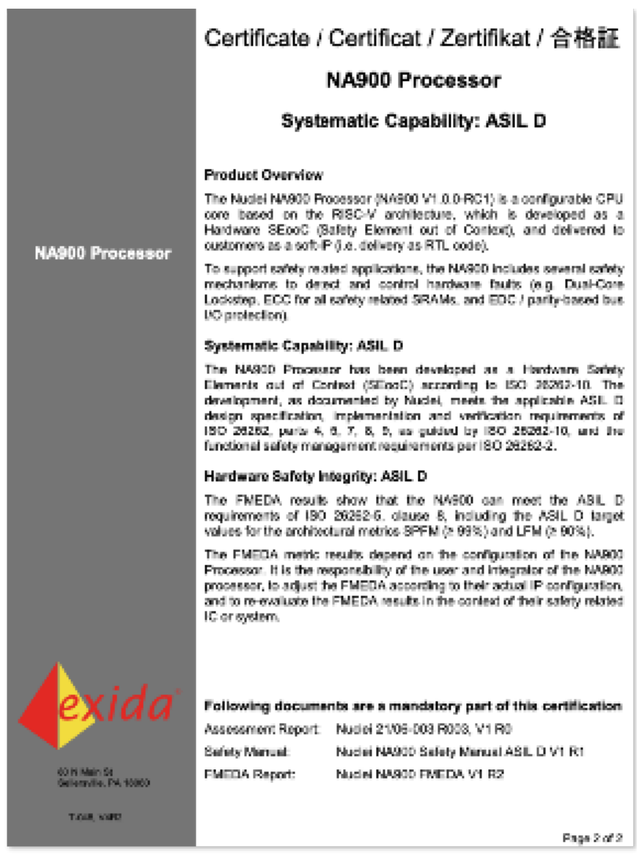
Page 1 of 2

The manufacturer may use the mark.

ASIL D

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

ANAB ACCREDITED



NA900 Processor

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, 6, 7, 8, 5, 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

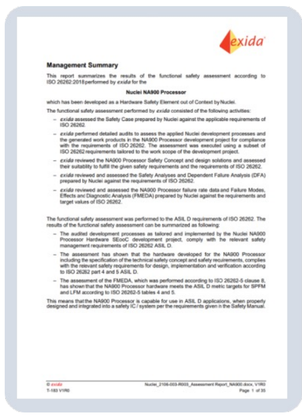
Assessment Report:	Nuclei 21/06-003 R003, V1 R0
Safety Manual:	Nuclei NA900 Safety Manual ASIL D V1 R1
FMEDA Report:	Nuclei NA900 FMEDA V1 R2

exida
63 N Main St
Sellersville, PA 18960

Page 2 of 2

ASIL-D level for Both
Systematic Capability and
Hardware Safety Integrity

Assessment Report Link



exida

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:

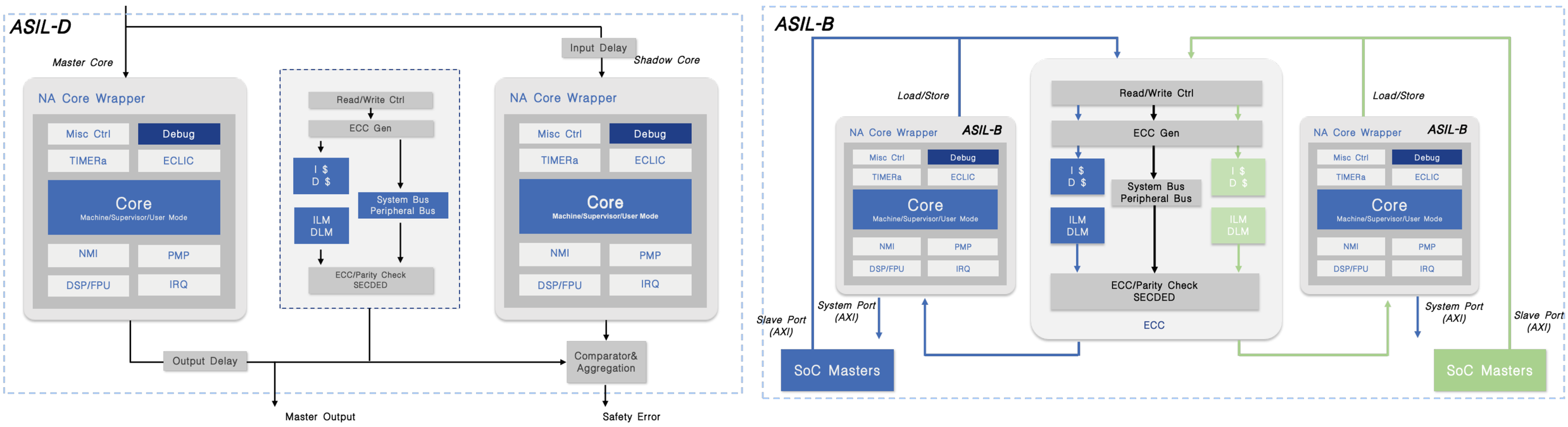
- exida assessed the Safety Case prepared by Nuclei against the applicable requirements of ISO 26262.
- exida performed detailed audits to assess the applied Nuclei development processes and the generated work products in the NA900 Processor development project for compliance with the requirements of 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.

Automotive Application with ASIL-B&D



Safety Package and Real Use Cases

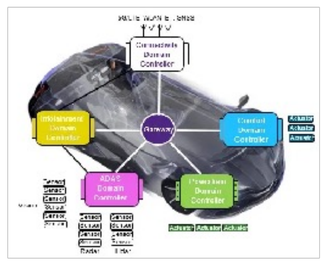
FMEDA

	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%

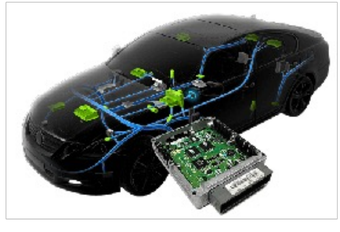
	Top level safety requirements (TLSRs) on IP / IC Level	*TLSR short*	SPFM	LFM
1	NA900 shall provide the required safe computation	TLSR 01	99.996%	99.784%
2	NA900 shall protect the data integrity of all safety related SRAM Storage and transfer between core and SRAM.	TLSR 02	99.268%	98.885%
3	NA900 shall 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

Lidar
ASIL-B



Gateway
ASIL-D



Domain Controller
ASIL-D

ADAS
ASIL-D

Contact： neil@nucleisys.com