2024
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES
SAN JOSE, CA, USA
MARCH 4-7, 2024

Leveraging Functional Safety Methodologies to Enhance Design Quality in Automotive IC

Gulshan Kumar Sharma - Samsung (SSIR)
Sougata Bhattacharjee - Samsung (SSIR)
James Kim - Siemens Korea

SAMSUNG
SIEMENS
accellera
SYSTEMS INITIATIVE

2024
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SAN JOSE, CA, USA
MARCH 4-7, 2024

Wonil Cho - Samsung Korea
Akshaya Jain - Samsung (SSIR)
Andrey Likhopoy - Samsung Korea
Arun Gogineni - Siemens USA
Ann Keffer - Siemens USA
Sangkyu Park - Samsung Korea
Hyeonuk Noh - Samsung Korea

SAMSUNG

accellera
SYSTEMS INITIATIVE

Introduction to Functional Safety (FuSa)

- ➢Standard for Functional safety → ISO26262 → Automotive
- ➢Harm
- ➢Risk → Probability of occurrence of harm + Severity of that harm
- ➢Safety Types in Automobiles/Car → Passive, Active, Preventive
- ➢What is Functional Safety ?

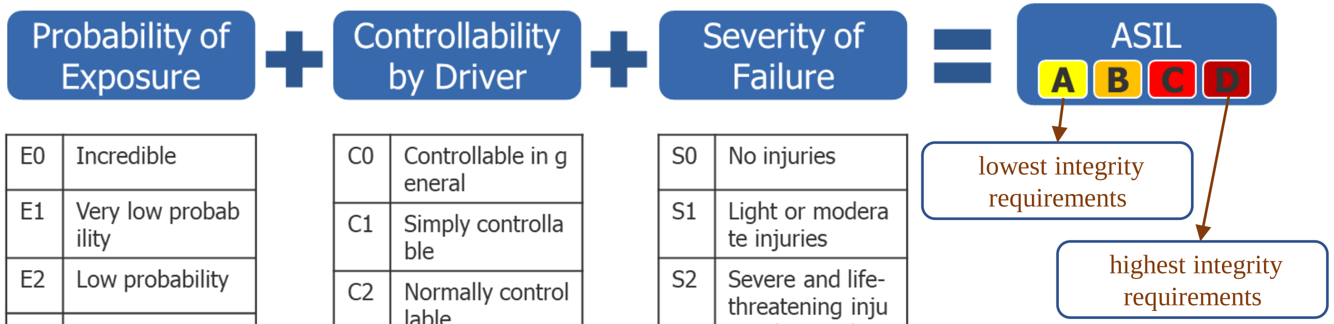
Problem Statement and Motivation

- Problem statement → Functional verification approach and its limitations

- Motivation →
- Introduce functional safety-related flows
- We present several comparisons of optimization techniques while performing fault simulation with full fault list and SRF fault list

ASIL (Automotive Safety Integrity Level)

- Key component of ISO 26262
- Used A risk classification scheme
- Combination of
  - Severity(S)
  - Probability of exposure (E)
  - Controllability (C)



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

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

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

* Source : ISO26262-3:2018, Clause 6.4.3 Classification of hazardous events

Base Failure Rate λ (lambda) – IEC62380

$$\lambda = \lambda_{die} + \lambda_{package}$$

in which

$$\lambda_{die} = \lambda_{thermal\ effects} + \lambda_{EOS\ effects}$$

$$\lambda_{package} = \lambda_{thermomechanical\ effects}$$

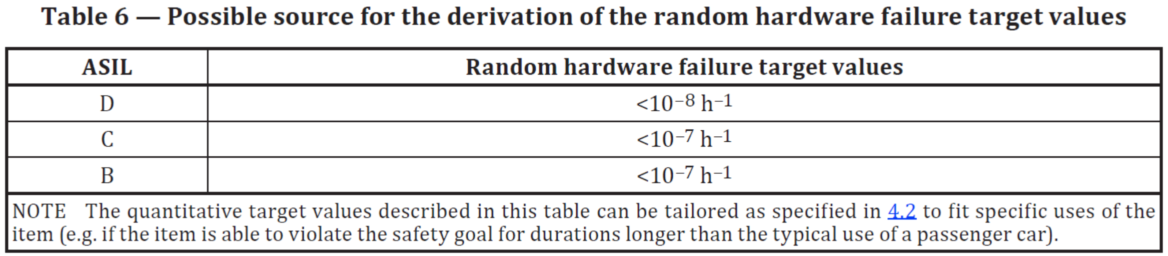


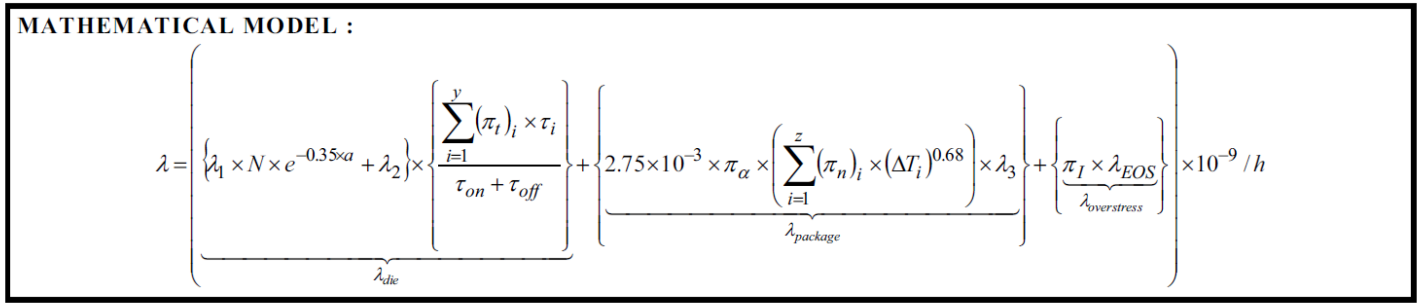
Table 6 — Possible source for the derivation of the random hardware failure target values

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

NOTE The quantitative target values described in this table can be tailored as specified in 4.2 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

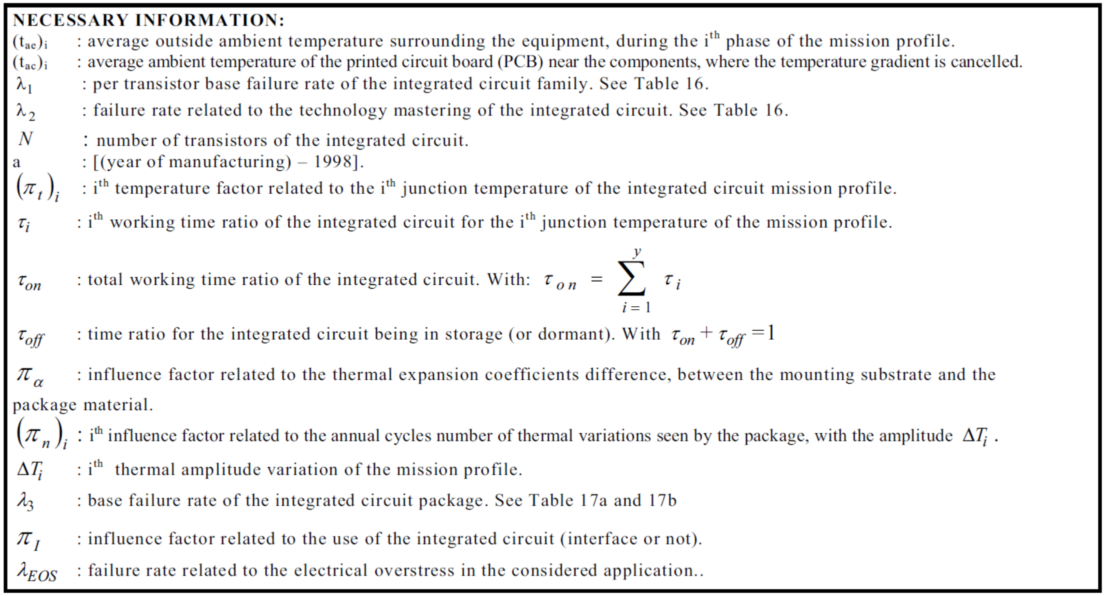
* Source : ISO26262-5:2018, Clause 9.4.2.2, Page 23

* Source : IEC TR 62380, Clause 7.3.1, Page 31



MATHEMATICAL MODEL :

$$\lambda = \left(\underbrace{\left\{ \lambda_1 \times N \times e^{-0.35 \times a} + \lambda_2 \right\} \times \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\}}_{\lambda_{die}} + \left\{ \underbrace{2.75 \times 10^{-3} \times \pi_\alpha \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3}_{\lambda_{package}} \right\} + \left\{ \underbrace{\pi_I \times \lambda_{EOS}}_{\lambda_{overstress}} \right\} \right) \times 10^{-9} / h$$



NECESSARY INFORMATION:

$(t_{ae})_i$: average outside ambient temperature surrounding the equipment, during the ith phase of the mission profile.

$(t_{ac})_i$: average ambient temperature of the printed circuit board (PCB) near the components, where the temperature gradient is cancelled.

λ_1 : per transistor base failure rate of the integrated circuit family. See Table 16.

λ_2 : failure rate related to the technology mastering of the integrated circuit. See Table 16.

N : number of transistors of the integrated circuit.

a : [(year of manufacturing) – 1998].

$(\pi_t)_i$: ith temperature factor related to the ith junction temperature of the integrated circuit mission profile.

τ_i : ith working time ratio of the integrated circuit for the ith junction temperature of the mission profile.

τ_{on} : total working time ratio of the integrated circuit. With: $\tau_{on} = \sum_{i=1}^{y} \tau_i$

τ_{off} : time ratio for the integrated circuit being in storage (or dormant). With $\tau_{on} + \tau_{off} = 1$

π_α : influence factor related to the thermal expansion coefficients difference, between the mounting substrate and the package material.

$(\pi_n)_i$: ith influence factor related to the annual cycles number of thermal variations seen by the package, with the amplitude ΔT_i .

ΔT_i : ith thermal amplitude variation of the mission profile.

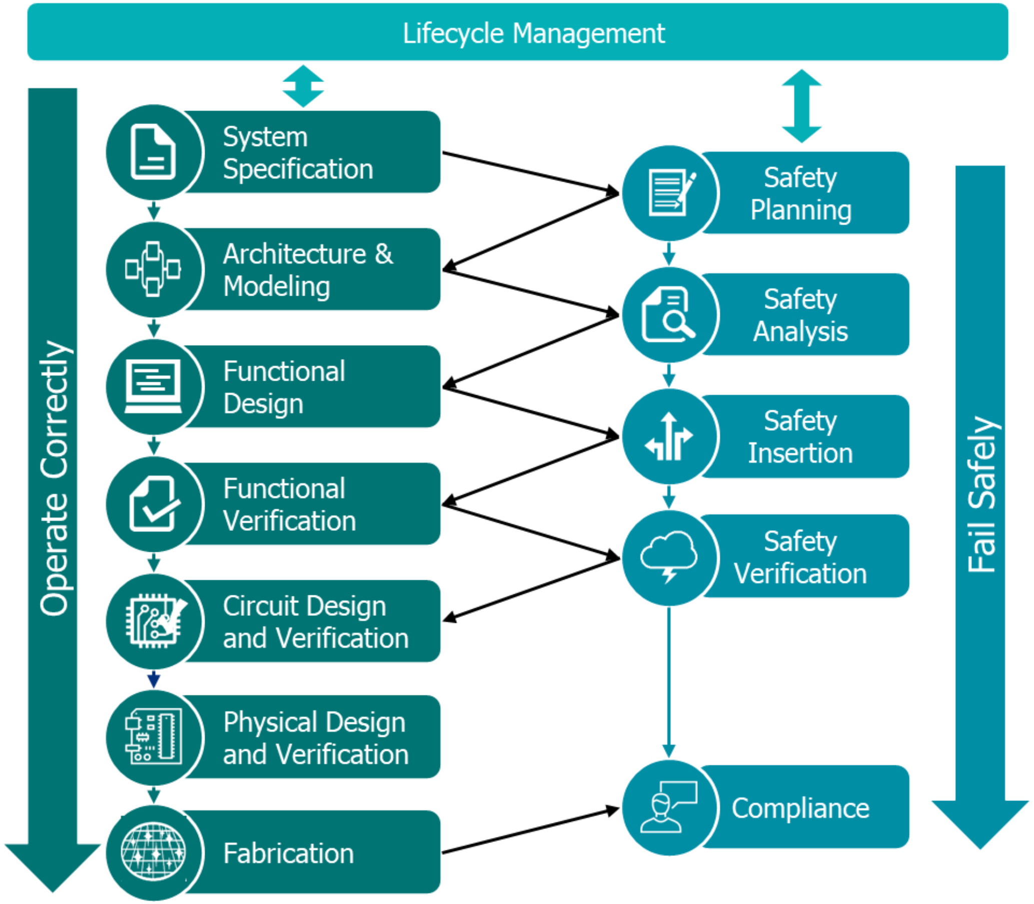
λ_3 : base failure rate of the integrated circuit package. See Table 17a and 17b

π_I : influence factor related to the use of the integrated circuit (interface or not).

λ_{EOS} : failure rate related to the electrical overstress in the considered application..

FuSa Flow

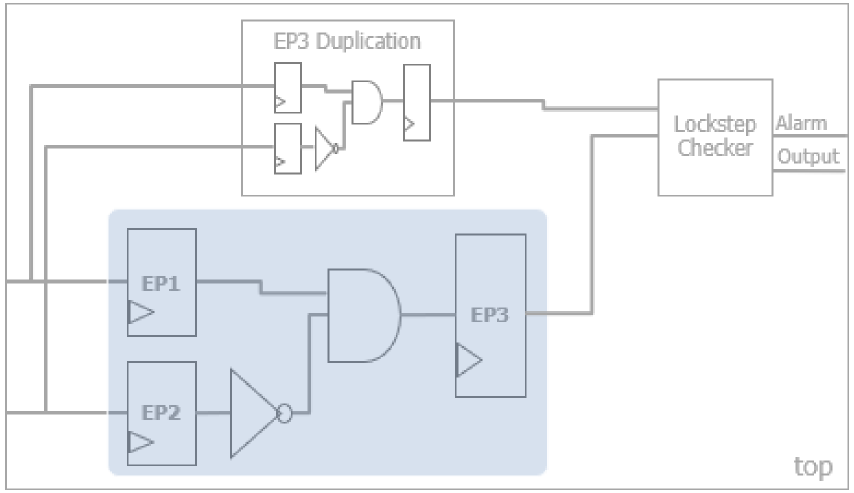
- ➢Should start at early stages of the Architectural cycle
- ➢Multiple Safety Mechanisms can be checked as per the requirement of Safety Standard Metrics at initial stages



Traditional flow vs FuSa flow

Safety Mechanism (SM)

- ➢ Safety Mechanism refers technical solution implemented by E/E functions or elements, or by other technologies, to detect and mitigate or tolerate faults or control or avoid failures in order to maintain intended functionality or achieve or maintain a safe state
- ➢ Different diagnostic coverage can consider achievable by type of Safety Mechanism



HW redundancy implementation Example (Lockstep)

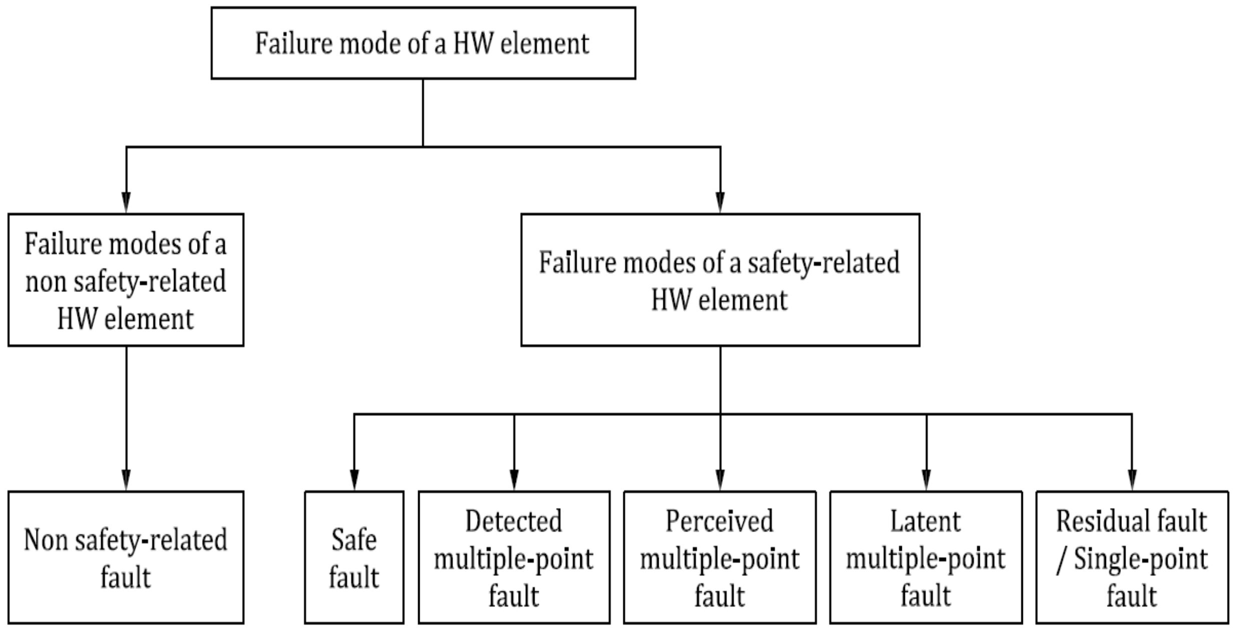
Safety mechanism/measure	Typical diagnostic coverage considered achievable	Example
Multi-bit hardware redundancy	Medium	CRC, Low Density Parity Check code
Self-test supported by hardware (1ch)	Medium	EDC coder/decoder
HW redundancy	High	Dual Core Lock Step, asymmetric redundancy
Timeout monitoring	Medium	Watch Dog Timer

* Source : ISO26262-5:2018, Annex D, Evaluation of the diagnostic coverage

Fault Classification

Fault classification of hardware element per failure mode is as mentioned below:

- Safe fault
- Detected multiple-point fault
- Perceived multiple-point fault
- Latent multiple-point fault
- Residual fault
- Single-point fault



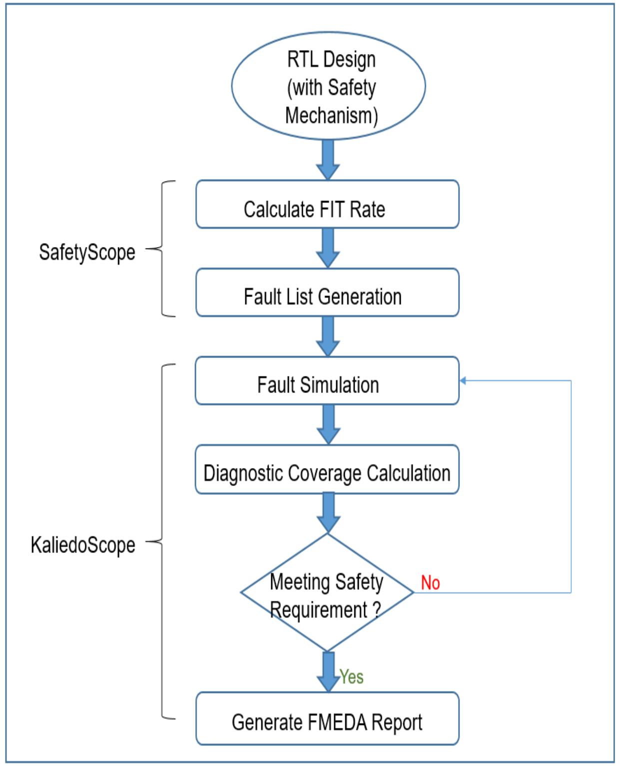
* Source : ISO26262-5:2018, Annex B. Failure mode classification of a hardware element, Page 36

FuSa Fault Injection Flow

Step1 → Fault list creation and Optimization from defined safety architecture

Step2 → Validating estimated coverage by Fault Injection Testing

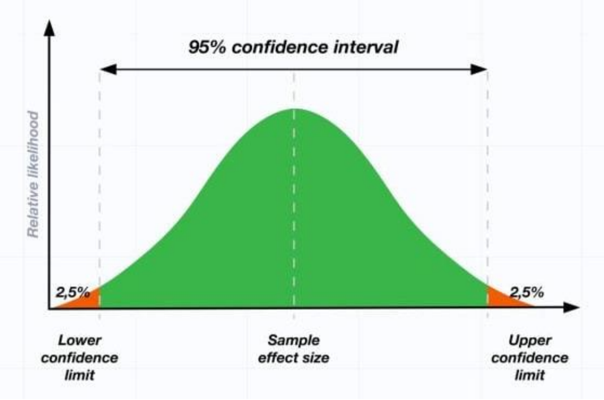
Step3 → Review Fault Injection Testing result and finalize validated metric



Statistical Random Fault (SRF)

- complexity and the number of faults has increased exponentially
- computational time for full fault campaign also increased multifold
- SRF contains the subset of actual fault samples in the design
- Reference: ISO26262-5:2018, Clause 4.8.2
  - A Sampling factor can be used to reduce the fault list, if justified with respect to the specified purpose, confidence level, type/nature of the safety mechanism, selection criteria etc.

* Source : ISO26262-11:2018, Clause 4.8.2 Characteristics or variables of fault injection



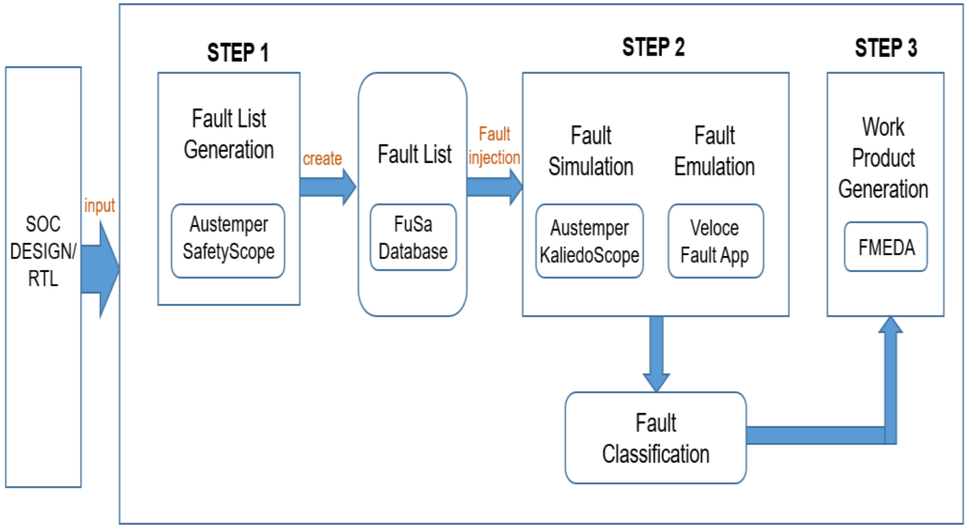
Considered Factor for SRF	Description
N	Population Size
n	Sample Size
Confidence Interval (CI)	Interval which is expected to typically contain the parameter being estimated
Margin Of Error (MOE)	amount of random sampling error in the results

Sampling factors

Fault Campaign Execution

Austemper SafetyScope is used during Safety analysis and KaleidoScope is used for fault simulation. Fault campaign implementation steps are as follows:

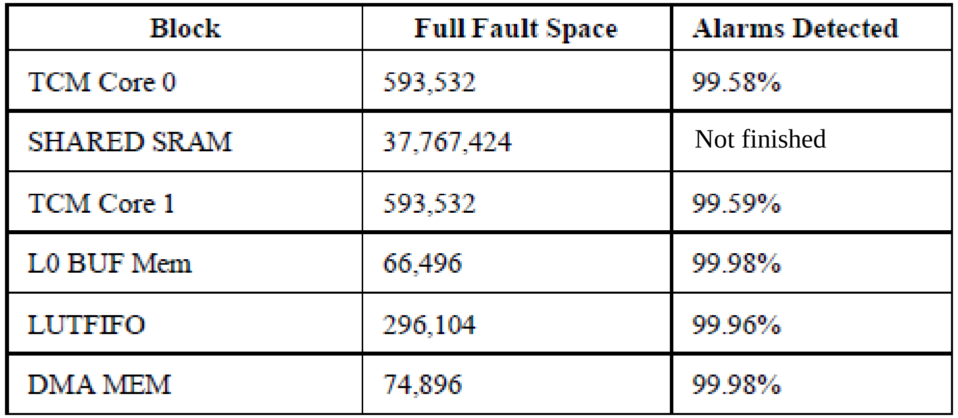
- RTL design is given as input to the tool along with the safety mechanism information implemented for each block under observation.
- Tool generates the FIT values (λ) for both permanent and transient faults analysis.
- The tool analyzes the design and safety mechanism information to generate a fault list for the block. The fault list generated is an optimized fault list.
- The generated fault list along with observation points for the faults and alarm list is provided as input to tool for fault simulation. Faults are injected in fault simulation and output of fault simulation is observed.
- The KaleidoScope will generate the diagnostic coverage (fault coverage) values for the faults.
- Tool will also perform fault classification and the results can be analyzed to improve the DC coverage.
- The final step is the generation of the FMEDA report for ISO26262 automotive standard compliance.



Fault Campaign

Results

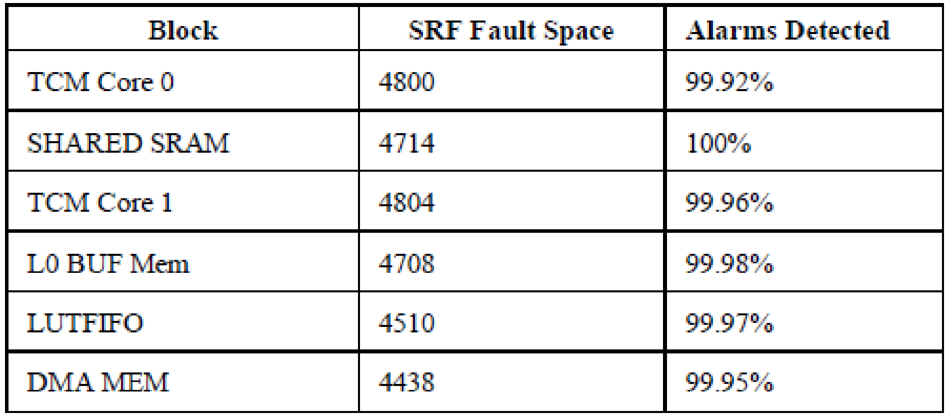
- Results obtained in the analysis are for different memory blocks inside NPU Subsystem block. Memory blocks under analysis were TCM Memory, Shared SRAM, LUTFIFO, DMA Memory. The faults under analysis are single point faults and SPFM (Single point fault metric) is calculated for these faults through fault campaign.



Block	Full Fault Space	Alarms Detected
TCM Core 0	593,532	99.58%
SHARED SRAM	37,767,424	Not finished
TCM Core 1	593,532	99.59%
L0 BUF Mem	66,496	99.98%
LUTFIFO	296,104	99.96%
DMA MEM	74,896	99.98%

ALARMS DETECTED WITH FULL FAULT LIST MEMORY SIMULATION

*MOE : 1.38% ~ 1.43%

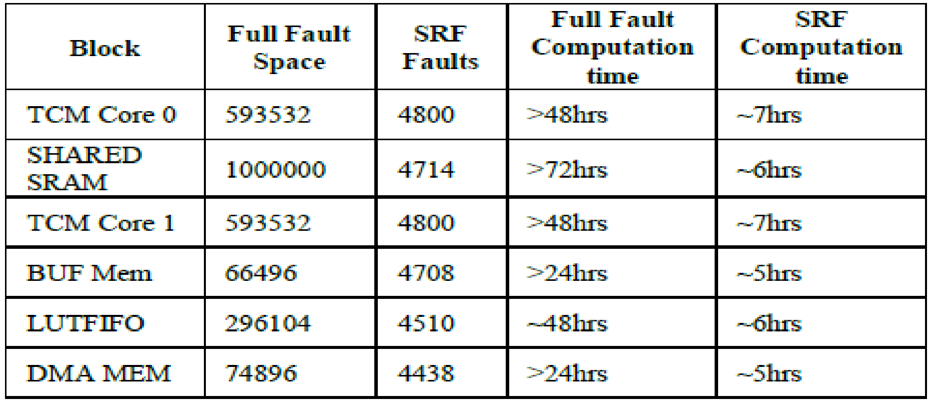


Block	SRF Fault Space	Alarms Detected
TCM Core 0	4800	99.92%
SHARED SRAM	4714	100%
TCM Core 1	4804	99.96%
L0 BUF Mem	4708	99.98%
LUTFIFO	4510	99.97%
DMA MEM	4438	99.95%

ALARMS DETECTED IN SRF FAULT LIST MEMORY SIMULATION

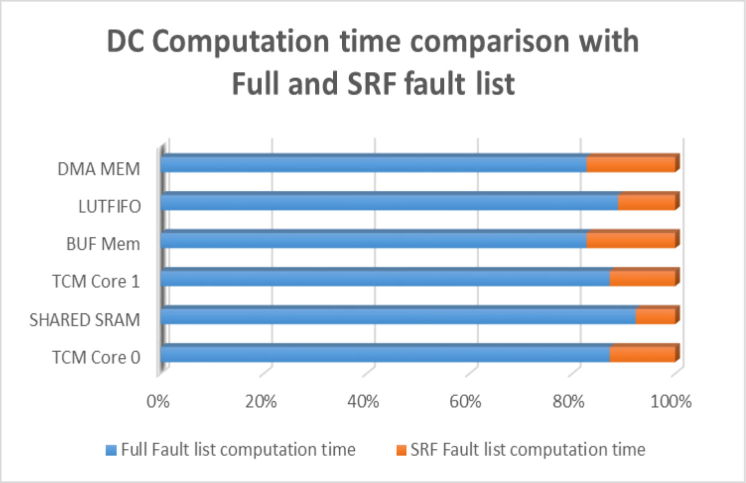
Results

- ➢Simulation time reduction is significant in terms of numbers and percentage for SRF fault list simulations



Block	Full Fault Space	SRF Faults	Full Fault Computation time	SRF Computation time
TCM Core 0	593532	4800	>48hrs	~7hrs
SHARED SRAM	1000000	4714	>72hrs	~6hrs
TCM Core 1	593532	4800	>48hrs	~7hrs
BUF Mem	66496	4708	>24hrs	~5hrs
LUTFIFO	296104	4510	~48hrs	~6hrs
DMA MEM	74896	4438	>24hrs	~5hrs

COMPUTATION TIME REDUCTION IN SRF FOR TCM MEMORY SIMULATION



COMPUTATION TIME COMPARISON

Thank you !!