## Making ISO26262 Functional Safety Verification a Natural Extension of Functional Verification

Andrew Betts, Verification Engineer, Arm Ann Keffer, Product Management Director, Functional Safety, Cadence Design Systems









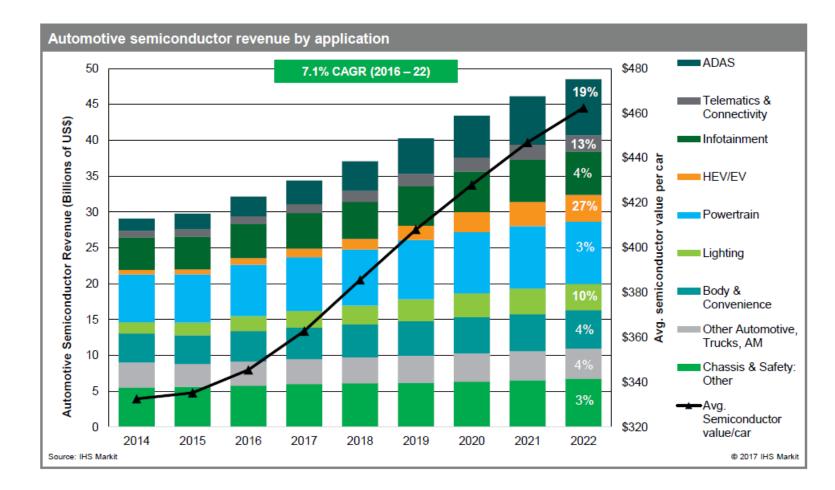
# Agenda

- Market landscape
- Introduction into functional safety
- Why the FMEDA is important
- Functional verification and Safety verification
- Arm<sup>®</sup> processor design description
- Arm Safety Package
- FMEDA Methodology
- Importance of safety campaigns for Arm's STL
- Validation of the FMEDA
- Arm's safety flow
- Q&A





### **Automotive Semiconductor Growth**



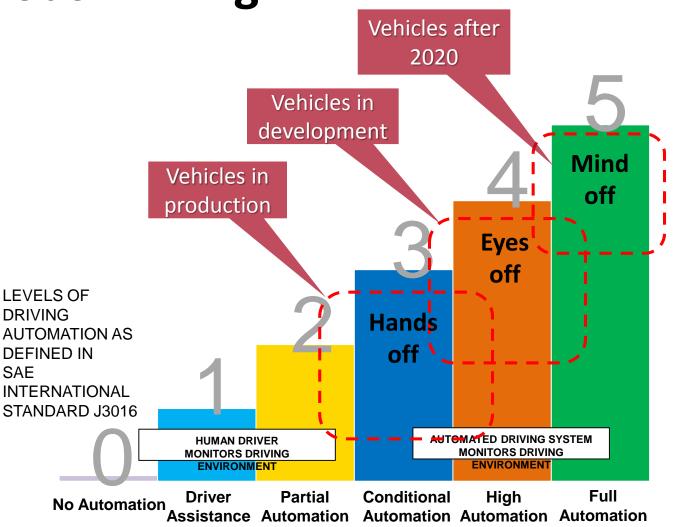




#### **Autonomous Driving**

SAE

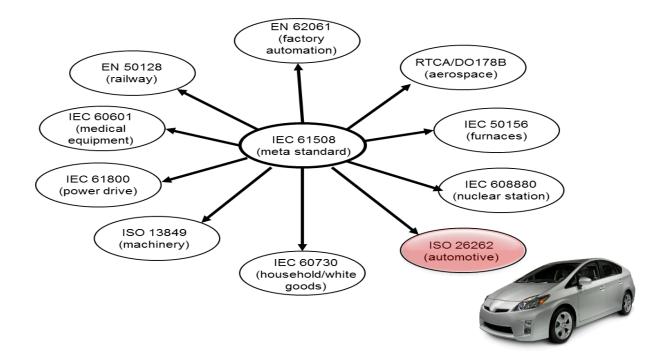
- Amount of electronics is growing fast ullet
- (ADAS) based on complex SoCs to ulletenable high-performance computing
- Safety critical ADAS applications have stringent requirements on
  - Functional safety
  - Security
  - Reliability







### **Functional Safety Standards**



#### ISO 26262 defines

- Processes to follow
- Hardware/software performance to achieve
- Safety documentation to produce
- Software tools compliance process

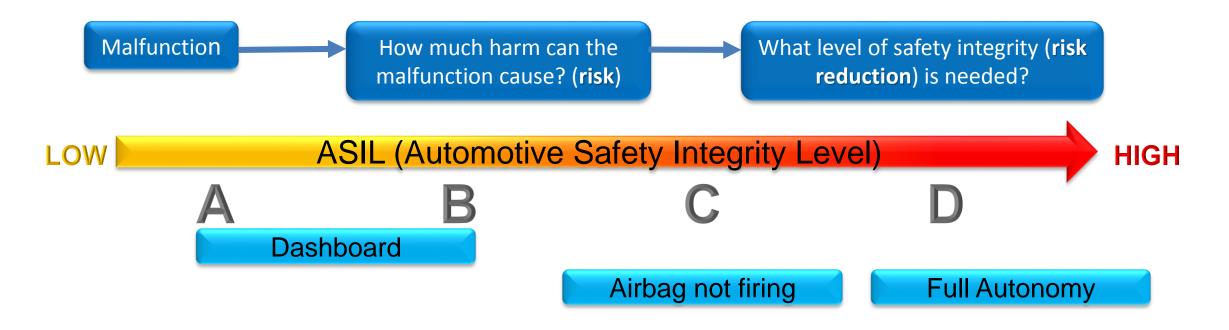
2-5 Overall safety management	2-6 Safety management and the product develop	renent during the concept phase 2-7 Safety management after the item's release for production							
3. Concept phase     3.5 Item definition     3.6 Initiation of the safety lifecycle     3.7 Hazard analysis and risk     assessment     3.8 Functional safety     concept	4. Product develop 45 Initiation of product development at the system level 4-6 Specification of the technical sefety requirements 4-7 System design 5-2 Initiation of product development at the hardware level 5-3 Initiation of product development at the hardware level 5-4 Sington of the order level 5-5 Sington of the nardware safety requirements 5-7 Hardware design 5-8 Evaluation of the hardware architectural netroics 5-8 Evaluation of the safety goal volutions due to random hardware singtone due t		(maintenance and repair), and decommissioning						
	8. Supporti	ng processes							
8-5 Interfaces within distributed develop 8-6 Specification and management of s 8-7 Confguration management 8-8 Change management 8-9 Verification		8-10 Documentation 8-11 Confidence in the use of soft 8-12 Qualification of software cor 8-13 Qualification of hardware co 8-14 Proven in use argument	mponents						
9-5 Requirements decomposition with r 9-6 Criteria for coexistence of elements		afety-oriented analyses 9-7 Analysis of dependent failure 9-8 Safety analyses	\$						





# Functional Safety Definition—ISO 26262

"Absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical and/or electronic systems" (ISO 26262)

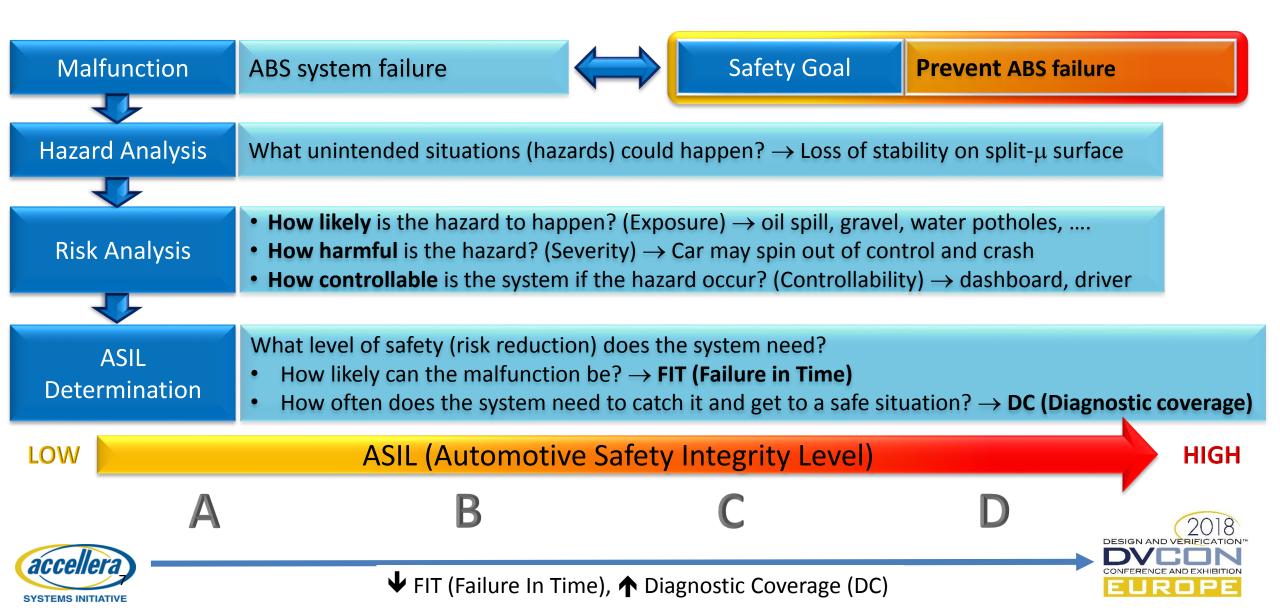


ASIL examples for illustration purposes only

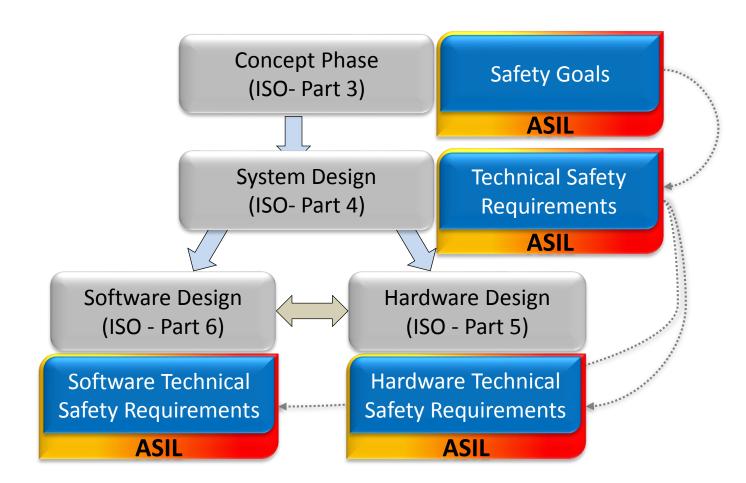




## ASIL Determination Example—ISO 26262



#### Design and Safety Flow ISO 26262









#### Failures Relevant to Functional Safety ISO26262—Functional Safety Principles

#### **Systematic Failures**

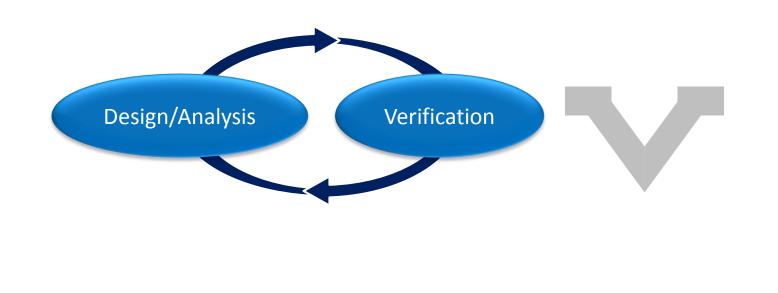
(e.g., software bug)

- Addressed by processes (planning, traceability, documentation, specs)
- Strictness of processes are dependent on the ASIL level

#### **Random Failures**

(e.g., component malfunction, noise injection)

- Considers permanent failure and transient effects
- Includes **safety mechanisms** design and integration to handle faults
- Demonstrated by calculations of Reliability/verification of failure rates
- Failure rates and diagnostic coverage requirement depend on ASIL





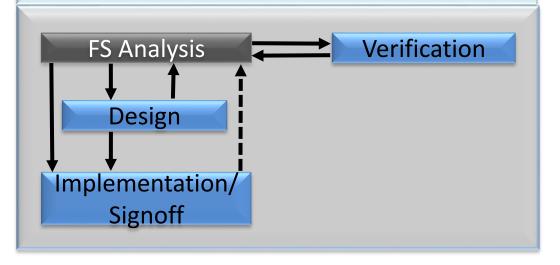


# What is Functional Safety Analysis?

- Define Failure Modes (FM)
- Determine Safety Mechanisms (SM)
- Validate Single Point Failure Metric (SPFM) and Latent Failure Metric (LFM)

How to improve your HW metric (to achieve the target ASIL):

- Better component
- Better/Additional Safety Mechanism



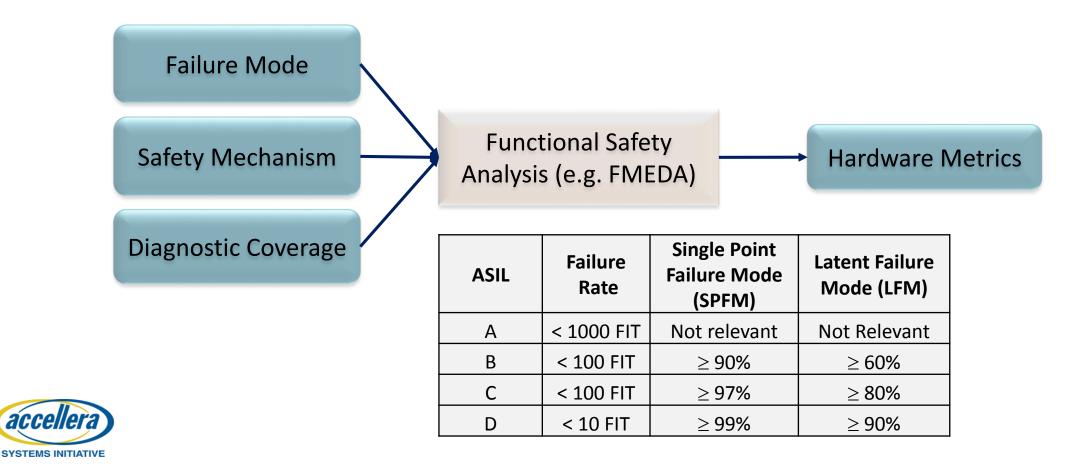




#### **Defining Functional Safety**

#### **Structured Approach to Measure the ASIL HW Metrics**

Safety is the freedom from unacceptable risk of physical injury or damage due to unplanned or undesired events



accel



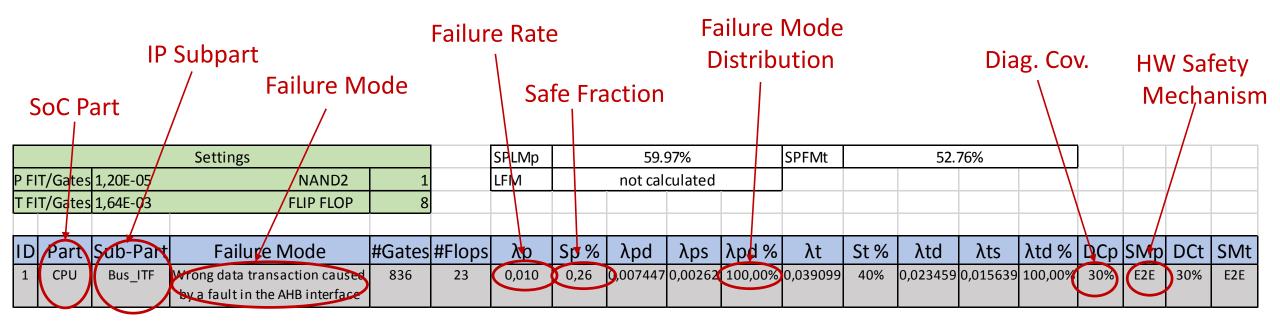
#### Importance of Failure Mode Effects and Diagnositc Analysis (FMEDA)

- The FMEDA is safety analysis required by ISO26262
  - Other analysis are FMEA, FTA, DFA,....
- FMEDA is needed to:
  - Verify the number of Safety Mechanisms and their claimed diagnostic coverage properties are enough to reach the required ASIL level calculating the architectural safety metrics: SPFM, LFM
  - Validates the Safety Architecture (collection of safety mechanisms) and calculates the performance of the system (SPFM, LFM)





#### FMEDA – Capture and Analyze Safety Goals

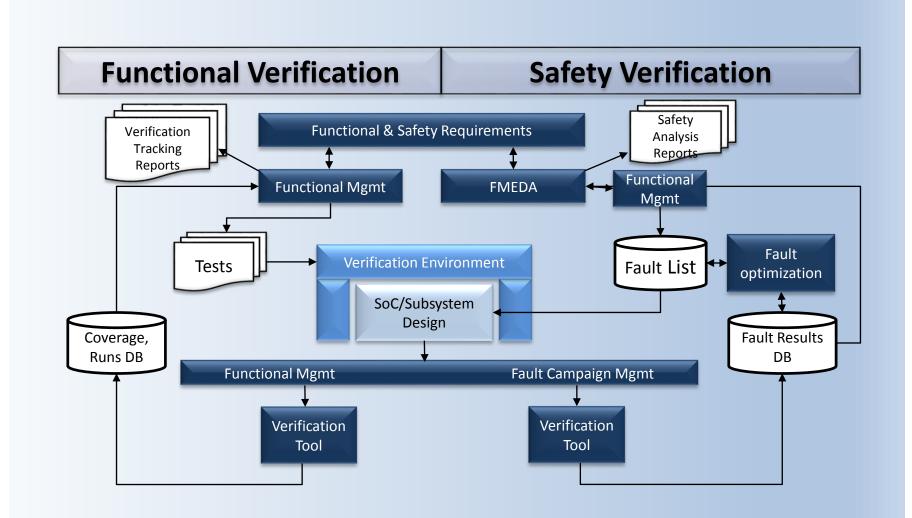




DESIGN AND VERIE

CONFERENCE AND EXHIBIT

#### **Safety Verification Flow**







# **Arm Functional Safety Design Description**

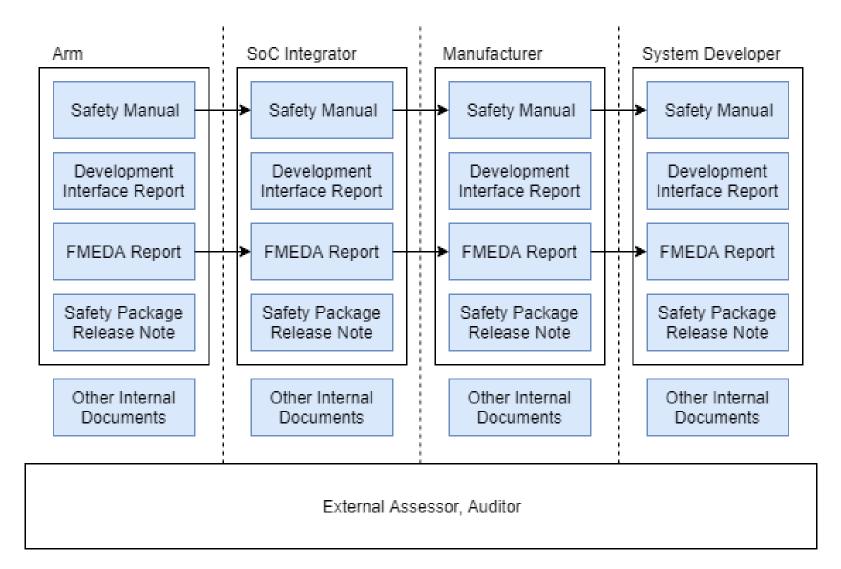
• Functional Safety is critical to many Arm products, especially those targeting automotive segment

- Arm has many safety packages already:
  - Arm Cortex<sup>®</sup>-A53, A57, A72, A75, A76, A35, A32, A34, A55, R5F, R52, M3, M4, M0+, M7, M33, M23
- Arm's safety analysis is for a Safety Element out of Context (SEooC)





## **Arm Safety Documentation Package**

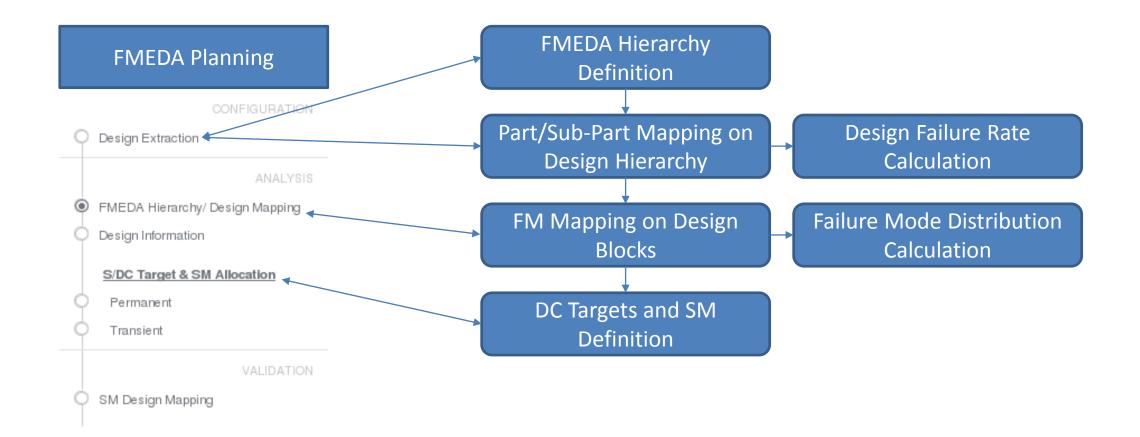








## **FMEDA Methodology**





© Accellera Systems Initiative

DESIGN AND VERIE

CONFERENCE AND EXHIBITION

R

#### **FMEDA Analytics**

🗲 🖉 🍋   https://euvclo40:8889/web/	(99%) C 9, Search 🛧 🛍 🕴
	/ FMEDA_DEMO / Configuration
	Project Setup
Architectural FMEDA	
Not created	Project Name FMEDA_DEMO
. Step (4)	
	Safety Requirements
Detailed FMEDA	ASI, Requirement A B C D Tanget Metrics
Not created	Transiest Exable SPFM P: 90% - SPFM T: 90% - LFM: 60% - PMHF
Ó 5kgr- (4)	Transient Enable EPFM P: 90% - 5PFM T: 90% - LPM: 60% - PMMF:
	Technology Information
	Tech Na ] Type ] P Pe Tr ] Tra Tr ] Tra R ] Unit
	DigLib Digital 1.0 FIT/ 1.6 FIT/ 1.6 FIT/FF 0.72 µm2
	New Tech



2018
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
EUROPE

#### **FMEDA Methodology**

🗲 ) 🛈 🕰   https://euvclo	40:8889/web/vmgr	/fmeda/index.html#/project/setu 🥨 🤇 🗘 🔍 Search 🟠 🖨 🖡 🏫	
			ferlini
		Project Setup	
Not created Step: -	•	Project Name FMEDA_DEMO	
<i>о</i> ююр.		Safety Requirements	
Detailed FMEDA		ASIL Requirement A B C D Target Metrics	
<ul> <li>Not created</li> <li>Step: -</li> </ul>	<b>± O</b>	Transient Enable SPFM P: 90% - SPFM T: 90% - LFM: 60% - PMHF: 100	
		Technology Information	
		Tech Na         Σтуре         P         Pe         Tr         Tra         Tra         R         Unit           DigLib         Digital         1.0         FIT/         1.6         FIT/         1.6         FIT/         0.7.2         µm2	
		New Technology	





### **Design Mapping**

CONFIGURATION       FMEDA Hierarchy / Design       Upload Mapping         Design Extraction       ANALYSIS         P FMEDA Hierarchy / Design Mapping       Design Information         S/DC Target & SM Allocation       FETCH         P Fermanent       OECODER         P Fermanent       OFLOORE REGS         P CORE REGS       OFLOORE REGS         WR-BACK LOGIC       OFLOORE REGS         WR-BACK LOGIC       OFLOORE REGS         FPU Fromp       Floating point std       DigLib         FPU Fromp       Floating point std       DigLib         FPU Int Flot       Integer and foati       DigLib       Ofl200_fpu.fpu_arthin.         FPU Int Flot       Integer and foati       DigLib       Ofl200_fpu.fpu_arthin.       1/1         ALUDANON       FREEZE       Ofl200_fpu.fpu_arthin.       1/1       1/1	CONFIGURATION       FMEDA Hierarchy / Design       C Upload Mapping         Design Extraction       ANALYSIS         ANALYSIS       ANALYSIS         P FMEDA Hierarchy / Design Mapping       a: CDNS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.xlsx         Design Information       SUDC Target & SM Allocation         S/DC Target & SM Allocation       FETCH         P ermanent       of 200_ of 1200_ge         Transient       OCORE REGS         VALIDATION       FPU Arita =         FMEDA Plan       FPU FCmp         FNUMAC       DigLib for 07200_gfu,         Parmanent       FPU FCmp         Fault Injection Campaign Configuration       FPU FCmp         Parmanent       FPU FCmp         FRUE A Plan       FPU FCmp         Parmanent       FPU FCmp         FRUMAC       DigLib for 07200_gfu, untfu, 10/11         FPU FCmp       Floating point co       DigLib for 07200_gfu, untfu, 10/11         FPU FCmp       Floating point co       DigLib for 07200_gru, 01/100_gru, 01/10         FPU FCmp       Floating point co       DigLib for 07200_gru, 01/10_gru, 01/10         AUMAC       FPU FCmp       FREEZE       Or1200_gru, 01/10_gru, 01/10         AUMAC       FREEZE       Or1200_gru, 01/10_gru,	CONFIGURATION   Design Extraction     ANALYSIS     PMEDA Hierarchy/Design Mapping   Bosign Information   SPOC Target & SM Allocation   Permanent   Parmanent   Transient   VALIDATION   PMEDA Plan   Permanent   Prov Allpeaton   Prov Allpeaton   PU Int Flot   Pormanent   Configuration   Prov Annage   Parmanent   Configuration   Parmanent   Configuration   Parmanent   Configuration   Parmanent   Configuration   Parmanent   Configuration   Parmanent   Configuration   Parmanent   Parmanent   Configuration   Parmanent   Parmanent <	CONFIGURATION   Design Extraction     ANALYSIS   ANALYSIS   PMEDA Hierarchy/ Design Mapping   Design Information   SIDE Target & SM Allocation   Permanent   Transient   VALIDATION   VALIDATION   VALIDATION   Permanent   Transient   Permanent   Ord Design Mapping   Permanent   Pru Int Flot   Pru From   Flaoting point sc   Diglub 1   ord 2000 (pu.fpu.gruth   PU From   Flaoting point sc   Diglub 2   ord 2000 (pu.fpu.gruth   Pru Int Flot   Integer and foat   Diglub 2   ord 2000 (pu.fpu.gruth   Pru Int Flot   Prezeution   Pauti Infection Campaign   Configuration   Praining   Execution Configuration   Planing   Execution Configuration   Planing   Execution Configuration   Planing   Execution Configuration   Planing   Execution Configuration <		ጽ / 🌣 FMEDA	_DEMO / Detail	ed FMEDA 👻		¢	ferlir
Design Extraction       FMEDA Hierarchy / Design       © Upload Mapping         ANALYSIS       ArcDNS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.xlsx         P FMEDA Hierarchy / Design Mapping       Name       Subpart Descri       Technology       Mapping         S/DC Target & SM Allocation       - FETCH       - DECODER       - or1200       or1200_ge       - FM #         Permanent       - CORE REGS       - or1200       or1200_ge       - or1200       or1200_ge       - FPU         SM Design Mapping       FM URBACK LOGIC       - or1200       or1200_fpu       10/11       -         Permanent       - FPU       Floating point std       Diglub       or1200_fpu.fpu_arith       10/11       -         SM Design Mapping       FPU Fcmp       Floating point std       Diglub       or1200_fpu.fpu_arith       10/11       -         Permanent       - FPU Int Flot       Integer and foati       Diglub       or1200_fpu.fpu_arith       10/11       -         Permanent       - ALUMAC       - Or1200_fmu_arith       0/1200_fmu_arith       1/1       -         - ALUMAC       - Or1200_fmu_arith       Or1200_fmu_arith       0/1200_fmu_arith       1/1       -         - Planning       - FREEZE <t< th=""><th>Design Extraction     ANALYSIS     ANALYSIS     Name   Subpart Descri   Technology   Mapping     * CDNS:Design:Mapping   Design Information   S/DC Target &amp; SM Allocation   Permanent   Transient     VALIDATION     VALIDATION   Permanent   O SM Design Mapping   Permanent   Pulaning   Permanent   Permanent </th></t<> <th>Pesign Extraction     ANALYSIS     ANALYSIS     PAEDA Hierarchy / Design Mapping   Design Information   SIDE Target &amp; SM Allocation   Permanent   Transient     VALIDATION   Permanent   Transient   VALIDATION   Permanent   CORF REGS   PEDA Plan   Permanent   Configuration   PENDA Plan   Permanent   Configuration   Panning   Panning   Panning     Panning     Planning     Planni</th> <th>Pesign Extraction       Mapping       Image: CDNS-Design-Mapping         ANALYSIS       ANALYSIS         P MEDA Hierarchy/ Design Mapping       Image: CDNS-Design-Mapping       Image: CDNS-Design-Mapping         P MEDA Hierarchy/ Design Mapping       Image: CDNS-Design-Mapping       Image: CDNS-Design-Mapping         SIDC Target &amp; SM Allocation       FETCH       Image: CDNS-Design Mapping         Permanent       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         Permanent       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         PMEDA Plan       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         Permanent       FPU Form plate in Floating point std       Diglub 1 or1200 (pu.fpu.garth, 10/11 )         FPU Form plating       Floating point std       Diglub 2 or1200 (pu.fpu.garth, 10/11 )         FPU Form planing       FREEZE       Image: CDNS-Design (pu.fpu.garth, 10/11 )         Parmaning       Execution Configuration       Image: CDNS-DEsign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.ga</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Design Extraction     ANALYSIS     ANALYSIS     Name   Subpart Descri   Technology   Mapping     * CDNS:Design:Mapping   Design Information   S/DC Target & SM Allocation   Permanent   Transient     VALIDATION     VALIDATION   Permanent   O SM Design Mapping   Permanent   Pulaning   Permanent	Pesign Extraction     ANALYSIS     ANALYSIS     PAEDA Hierarchy / Design Mapping   Design Information   SIDE Target & SM Allocation   Permanent   Transient     VALIDATION   Permanent   Transient   VALIDATION   Permanent   CORF REGS   PEDA Plan   Permanent   Configuration   PENDA Plan   Permanent   Configuration   Panning   Panning   Panning     Panning     Planning     Planni	Pesign Extraction       Mapping       Image: CDNS-Design-Mapping         ANALYSIS       ANALYSIS         P MEDA Hierarchy/ Design Mapping       Image: CDNS-Design-Mapping       Image: CDNS-Design-Mapping         P MEDA Hierarchy/ Design Mapping       Image: CDNS-Design-Mapping       Image: CDNS-Design-Mapping         SIDC Target & SM Allocation       FETCH       Image: CDNS-Design Mapping         Permanent       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         Permanent       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         PMEDA Plan       Image: CDNS-Design Mapping       Image: CDNS-Design Mapping         Permanent       FPU Form plate in Floating point std       Diglub 1 or1200 (pu.fpu.garth, 10/11 )         FPU Form plating       Floating point std       Diglub 2 or1200 (pu.fpu.garth, 10/11 )         FPU Form planing       FREEZE       Image: CDNS-Design (pu.fpu.garth, 10/11 )         Parmaning       Execution Configuration       Image: CDNS-DEsign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.garth, 10/11 )         Planning       Execution Configuration       FREEZE       Image: CDNS-DESign (pu.fpu.ga							
Mapping       L CDNS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.xlsx         ANALYSIS       Name       Subpart Descri       Technology       Mapping       FM #         P FMEDA Hierarchy/ Design Mapping       EXCEPT       of1200_except       of1200_except       of1200_except       interplate-v1.0-OpenRISC- 01072018.xlsx         S/DC Target & SM Allocation       EXCEPT       of1200_except       of1200_except       interplate-v1.0-OpenRISC- 01200_except       interplate-v1.0-OpenRISC- 01200_except         Permanent       CORE REGS       of1200_except       of1200_except       interplate-v1.0-OpenRISC- 01200_fpu       interplate-v1.0-OpenRISC- 01200_except         SM Design Mapping       FPU Arits       Floaiting point std       Diglub       of1200_except       interplate-v1.0-OpenRISC- 01200_fpu         PMEDA Plan       FPU Fcmp       Floaiting point co       Diglub       of1200_fpu.fpu_intflo       1 / 1         PHI Int Flot       Integer and foati       Diglub       of1200_fpu.fpu_intflo       1 / 1       integer and foati       Diglub       of1200_fpu.fpu_intflo       1 / 1       integer and foati       Diglub       of1200_frue_rex       integer and foati       Diglub       of1200_frue_rex       integer and foati       Diglub       of1200_frue_rex       integer and foati <th>ANALYSIS       ANALYSIS         ANALYSIS       Name       Subpart Descri       Technology       Mapping       FM #         Design Information       SiDC Target &amp; SM Allocation       PETCH       Orl 200_ge       Orl 200_ge</th> <th>ANALYSIS       A CDNS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.stax         P FMEDA Hieranchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target &amp; SM Allocation       -       FETCH       or1200_ge       <td< th=""><th>ANALYSIS       A CONS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.slax         P FMEDA Hieranchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target &amp; SM Allocation       -       FETCH       or1200_op       <td< th=""><th>Design Extraction</th><th>FMEDA Hierarc</th><th>hy / Design</th><th>🖞 Upload Map</th><th>ping</th><th></th><th></th></td<></th></td<></th>	ANALYSIS       ANALYSIS         ANALYSIS       Name       Subpart Descri       Technology       Mapping       FM #         Design Information       SiDC Target & SM Allocation       PETCH       Orl 200_ge	ANALYSIS       A CDNS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.stax         P FMEDA Hieranchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target & SM Allocation       -       FETCH       or1200_ge       or1200_ge <td< th=""><th>ANALYSIS       A CONS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.slax         P FMEDA Hieranchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target &amp; SM Allocation       -       FETCH       or1200_op       <td< th=""><th>Design Extraction</th><th>FMEDA Hierarc</th><th>hy / Design</th><th>🖞 Upload Map</th><th>ping</th><th></th><th></th></td<></th></td<>	ANALYSIS       A CONS-Design-Mapping-Template-v1.0-OpenRISC- 01072018.slax         P FMEDA Hieranchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target & SM Allocation       -       FETCH       or1200_op       or1200_op <td< th=""><th>Design Extraction</th><th>FMEDA Hierarc</th><th>hy / Design</th><th>🖞 Upload Map</th><th>ping</th><th></th><th></th></td<>	Design Extraction	FMEDA Hierarc	hy / Design	🖞 Upload Map	ping		
NALEYSIS         FMEDA Hierarchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         Design Information       -	ANALYSIS         PARLYSIS         P MEDA Hierarchy/ Design Mapping       Name       Subpart Descri       Technology       Mapping       FM #         S/DC Target & SM Allocation       PETCH       Or120       Or1200_get       FM #         Permanent       OCORE REGS       Or1200_ort200_get       FM #         CORE REGS       Or1200_ort200_get       Or1200_ort1200_get       Io/11         SM Design Mapping       FPU Arit@ I       Floating point std       DigUb< for or1200_fpu.fpu_arith	ANALYSIS         P MEDA Hierarchy/ Design Mapping         Design Information         S/DC Target & SM Allocation         Permanent         Transient         VALIDATION         SM Design Mapping         FMEDA Plan         Pormanent         SM Design Mapping         FMEDA Plan         Parmanent         FMEDA Plan         Parmaning         Fault Injection Campaign Configuration         Execution         Transient         Fault Injection Campaign Configuration         Paraning         Planning               Planni	PARALYSIS         PAREDA Hierarchy/ Design Mapping         Design Information         SIDC Target & SM Allocation         Permanent         Transient         VALIDATION         VALIDATION         VALIDATION         Permanent         Transient         VALIDATION         VALIDATION         Permanent         FMEDA Plan         Permanent         FRU Frup         Floating point sch         Diglub       orl200_fpu.fpu_arith         Image: Prup Frup         Permanent         Configuration         PHanning         Execution         Pault injection Campaign         Configuration         Planning         Execution Configuration         Planning	- Booign Extraorion	Mapping		Ju CDNS-Desig	n-Mapping-Template-v1.0-Ope	enRISC-	
Design Information       FFTCH       FETCH       of1200of1200.ge       of1200_ctrl       of1200_ctrl.	Design Information       FM #         S/DC Target & SM Allocation <ul> <li>FETCH</li> <li>DECODER</li> <li>EXCEPT</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> <li>FW</li> <li>FULDATION</li> <li>SM Design Mapping</li> <li>FMEDA Plan</li> <li>Permanent</li> <li>FAult Injection Campaign Configuration</li> <li>Planning</li> <li>Execution</li> <li>Freeze</li> <li>FREEZE</li></ul>	Design Information       FM #         S/DC Target & SM Allocation       - FETCH         Permanent       - DECODER         Transient       - CORE REGS         WABPDING       - FPU         FMEDA Plan       - FPU Formp         FMEDA Plan       - FPU Int Flot         Permanent       - FPU Formp         FAult Injection Campaign       - FREEZE         Configuration       - FREEZE	Design Information       FRECH       iccnnology       Mapping       FM #         S/DC Target & SM Allocation       - FETCH       orl200       orl200.get       orl200.get       orl200.get       iccnnology       Mapping       FM #         Permanent       - DECODER       - EXCEPT       - Orl200.get       orl200.get       orl200.get       - FETCH       - Orl200.get       - Orl200.get       - FETCH       - Orl200.get       - Orl200.get       - Orl200.get       - FETCH       - Orl200.get       - Orl	ANALYSIS						
Design Information <ul> <li>FETCH</li> <li>DECODER</li> <li>DECODER</li> <li>DECODER</li> <li>EXCEPT</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> ofl 200_cort ofl 200_cort	besign Information   S/DC Target & SM Allocation   S/DC Target & SM Allocation   Permanent   Transient   VALIDATION   VALIDATION   VALIDATION   Permanent   SM Design Mapping   FMEDA Plan   Permanent   FMEDA Plan   Permanent   Configuration   Parming   Execution Configuration   Planning   Execution Configuration   Planning   Execution Configuration   Planning   FREEZE	<ul> <li>Design Information</li> <li>SIDC Target &amp; SM Allocation</li> <li>Permanent</li> <li>Transient</li> <li>VALIDATION</li> <li>SM Design Mapping</li> <li>FMEDA Plan</li> <li>Permanent</li> <li>FPU Int Flot</li> <li>FPU Fcmp</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>10/11</li> <li>FPU Frup</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>10/11</li> <li>FPU Frup</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>10/11</li> <li>FPU Frup</li> <li>Floating point co</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>11/1</li> <li>FPU Int Flot</li> <li>Integer and foati</li> <li>Diglib</li> <li>or1200_frue.fpu_arith</li> <li>11/1</li> <li>FREEZE</li> </ul>	<ul> <li>Design Information</li> <li>S/DC Target &amp; SM Allocation</li> <li>Permanent</li> <li>Transient</li> <li>VALIDATION</li> <li>SM Design Mapping</li> <li>FMEDA Plan</li> <li>Parmanent</li> <li>FAULT Injection Campaign Configuration</li> <li>Planning</li> <li>Execution Configuration</li> </ul>	FMEDA Hierarchy/ Design Mapping	Namo	Subpart Descri	Technology	Manning	FM #	
S/DC Target & SM Allocation <ul> <li>DecodeR</li> <li>ExcEPT</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> <ul> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> <ul> <li>FPU Arite</li> <li>Floating point std</li> <li>DigUb</li> <li>of1200_fpu.fpu.garth</li> <li>10/11</li> </ul> <li>FPU Formp</li> <li>Floating point std</li> <li>DigUb</li> <li>of1200_fpu.fpu.garth</li> <li>10/11</li> <li>FPU Int Flot</li> <li>Integer and foati</li> <li>DigUb</li> <li>of1200_fpu.fpu.garth</li> <li>1/1</li> <li>ALUMAC</li> <ul> <li>ALUMAC</li> <li>LOAD-STORE</li> <li>FREEZE</li> <li>Integer and foati</li> <li>DigUb</li> <li>of1200_fpu.fpu.garth</li> <li>1/1</li> </ul>	S/DC Target & SM Allocation <ul> <li>Permanent</li> <li>Transient</li> </ul> <ul> <li>DECODER</li> <li>EXCEPT</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> SM Design Mapping <ul> <li>FPU Arita</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpu</li> <li>or1200_ffu</li> <li>or1200_ffu</li> <li></li></ul>	S/DC Target & SM Allocation <ul> <li>Permanent</li> <li>Transient</li> </ul> <ul> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> of 1200_except of 1200_encept of 1200_encept	S/DC Target & SM Allocation <ul> <li>Permanent</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> <ul> <li>FPU Arita</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>10/11</li> </ul> <li>FPU Femp</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpufpu_arith</li> <li>10/11</li> <li>FPU Femp</li> <li>Floating point std</li> <li>Diglib</li> <li>or1200_fpu.fpu_arith</li> <li>10/11</li> <li>FPU Femp</li> <li>Floating point co</li> <li>Diglib</li> <li>or1200_fpu.fpu_arith</li> <li>11/1</li> <li>ALJMAC</li> <li>LOAD-STORE</li> <li>LOAD-STORE</li> <li>FREEZE</li> <li>Or1200_freeze</li> <li>Or1200_freeze</li> <li>Or1200_freeze</li> <li>FREEZE</li>	Design Information		Subpart Deserim	icennology		11-1 1/	
Side Target & SM Allocation <ul> <li>Permanent</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> <ul> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> <ul> <li>FPU Arite</li> <li>Floating point std</li> <li>Diglib</li> <li>orl200_epu.goute</li> <li>orl200_fpu.goute</li> <li>orl200_frue</li> <li>orl200_frue</li> <li>orl200_freeze</li> </ul> <ul> <li>orl200_freeze</li> <li>orl200_freeze</li></ul>	SUCC Target & SM Allocation <ul> <li>Permanent</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> orl 200_except             orl.orl.orl.orl.orl.orl.orl.orl.orl.orl.	Side Target & SM Allocation <ul> <li>Permanent</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> of 1200_except             of             of 1200_encept             of             of 1200_encept             of             of	Side Target & SM Allocation <ul> <li>Permanent</li> <li>CORE REGS</li> <li>WR-BACK LOGIC</li> <li>FPU</li> </ul> of 1200_except             of             of 1200_encept             of             of 1200_encept             of             of							
<ul> <li>Transient</li> <li>Transient</li> <li>VALIDATION</li> <li>SM Design Mapping</li> <li>FMEDA Plan</li> <li>Permanent</li> <li>Fault Injection Campaign Configuration</li> <li>Planning</li> <li>Execution Configuration</li> </ul>	Transient       VALIDATION         VALIDATION         SM Design Mapping         FMEDA Plan         Permanent         FAult Injection Campaign         Configuration         Planning         Execution         Transient         Fault Injection Campaign         Configuration         Configuration	Transient       FCORE REGS       WR-BACK LOGIC       Off       Off <td< td=""><td>Transient       FCORE REGS       WR-BACK LOGIC       Off       <td< td=""><td></td><td>► EXCEPT</td><td></td><td></td><td></td><td></td><td></td></td<></td></td<>	Transient       FCORE REGS       WR-BACK LOGIC       Off       Off <td< td=""><td></td><td>► EXCEPT</td><td></td><td></td><td></td><td></td><td></td></td<>		► EXCEPT					
VALIDATION       FPU         SM Design Mapping       FPU Arits       Floating point std       Diglub       orl200_fpu.fpu_arith       10/11       >         FMEDA Plan       FPU Int Flot       Integer and foati       Diglub       orl200_fpu.fpu_fmu_mtflo       1/1       >         Fault Injection Campaign Configuration       ALUMAC       FREEZE       orl200_frueze       orl200_frueze       1/1       >         Planning       Execution Configuration       Execution Configuration       Configuration       orl200_frueze       orl200_frueze       orl200_frueze       Integer       Integer       orl200_frueze       Integer       Integer       orl200_frueze       Integer       Integer       Integer       orl200_frueze       Integer       Integer       orl200_frueze       Integer       I	VALIDATION       FPU       Floating point std       DigLib       or1200_fpu.fpu_arith       10/11       Image: std. ima	VALIDATION       FPU       Floating point std       Diguib       or1200_fpufw1200_gp       10/11       Image: state s	VALIDATION       VALIDATION         SM Design Mapping       FPU Arita •       Floating point std       Diglib •       orl 200 fpu.fpu.garith       10 / 11       )         FMEDA Plan       FPU Int Flot       Integer and foati       Diglib •       orl 200 fpu.fpu.garith       10 / 11       )         FMEDA Plan       FPU Int Flot       Integer and foati       Diglib •       orl 200 fpu.fpu.garith       11 / 1       )         Fault Injection Campaign       Configuration       LOAD-STORE       orl 200 fpu.fpu.garith       11 / 1       )         Planning       Execution Configuration       FREEZE       orl 200 fpu.fpu.garith       11 / 1       )         Fault Injection Campaign       Configuration       FREEZE       orl 200 fpu.fpu.garith       10 / 11       )         Planning       Execution Configuration       FREEZE       orl 200 fpu.fpu.garith       10 / 11       )         Planning       Fault Injection Campaign       Configuration       Configuration       Integer and foati       Integer and fo	Permanent	► CORE REGS			or or o or		
YALLDATION       FPU Arits       Floaitng point std       DigLib       Iorl 200 [pu.fpu_fu_arith       10/11         FMEDA Plan       FPU Fcmp       Floating point co       DigLib       Iorl 200 [pu.fpu_fu_fu_arith       10/11         Permanent       FPU Int Flot       Integer and foati       DigLib       Iorl 200 [pu.fpu_fu_fu_intflo       1/1         ALUMAC       FPU Int Flot       Integer and foati       DigLib       Iorl 200 [pu.fpu_fu_intflo       1/1         ALUMAC       FREZZE       Iorl 200 [su]       Iorl 200 [su]       Iorl 200 [reeze]       Iorl 200 [reeze]         Planning       FREZZE       Iorl 200 [reeze]       Iorl 200 [reeze]       Iorl 200 [reeze]       Iorl 200 [reeze]	VALUATION       FPU Arita       Floating point std       Diglib       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Flaating point co       Diglib       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Int Flot       Integer and foati       Diglib       or1200 fpu.fpu_arith       1/1         Permanent       ALUMAC       LOAD-STORE       FREEZE       or1200 fpu.fpu_arith       1/1         Planning       Execution Configuration       FREEZE       or1200 fpu.eze       or1200 fpe.eze       Image: State	VALUATION       FPU Arita       Floating point std       Diglub       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Flaating point co       Diglub       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Int Flot       Integer and foati       Diglub       or1200 fpu.fpu_infpu_arith       1/1         Permanent       ALUMAC       Diglub       or1200 fpu.fpu_infpu_arith       1/1       )         Planning       Execution Configuration       FREEZE       or1200 fpu.fpu_arith       1/1       )         Planning       Fault Injection Campaign Configuration       or1200 fpu.fpu_arith       1/1       )         Planning       Fault Injection Campaign Configuration       FREEZE       or1200 fpu.fpu_arith       1/1       )         Planning       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration       Free Planning       Fault Injection Campaign       Free Planning       Fault Injection Campaign       Free Planning       Fault Injection Campaign       Fault Injection       F	VALUATION       FPU Arita       Floating point std       Diglub       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Flaating point co       Diglub       or1200 fpu.fpu_arith       10/11         FMEDA Plan       FPU Int Flot       Integer and foati       Diglub       or1200 fpu.fpu_arith       1/1         Permanent       ALUMAC       FPU Int Flot       Integer and foati       Diglub       or1200 fpu.fpu_arith       1/1         Planning       Execution Configuration       FREEZE       or1200 fpu.fpu_arith       1/1       Planing         Planning       Fault Injection Campaign Configuration       FREEZE       or1200 fpu.fpu_arith       1/1       Planing         Planning       Execution Configuration       Execution Configuration       FREEZE       or1200 fpu.execution       Integer         Planning       Execution Configuration       Planning       Execution Configuration       Integer       Integer       Integer       Integer         Planning       Execution Configuration       Planning       Integer       Integer       Integer       Integer       Integer         Planning       Execution Configuration       Integer       Integer       Integer       Integer       Integer       Integer	) Transient	► WR-BACK LOGIC			or120 or1200_op		
SM Design Mapping       FPU Arite •       Floating point std       DigLib       •       orl200_fpu.fpu_anth       10 / 11         FMEDA Plan       FPU Fcmp       Flaoting point co       DigLib       •       orl200_fpu.fpu_fnu_fncmp       1 / 1       )         Permanent       FPU Int Flot       Integer and foati       DigLib       •       orl200_fpu.fpu_fnu_intflo       1 / 1       )         Parmanent       Configuration       Onl200_fmu.fpu_intflo       0 / 1200_ffeeze       orl200_fmu.fpu_intflo       1 / 1       )         Planning       FREEZE       Integer and foati       orl200_freeze       Integer and foati       orl200_freeze       Integer and foati       orl200_freeze       Integer and foati       Integer and foati       orl200_freeze       Integer and foat	SM Design Mapping       FPU Arite       Floating point std       Diglib       cr1200_fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Flaating point co       Diglib       cr1200_fpu.fpu_fcmp       1/1         FMEDA Plan       FPU Int Flot       Integer and foati       Diglib       cr1200_fpu.fpu_intflo       1/1         Permanent       FPU Int Flot       Integer and foati       Diglib       cr1200_fpu.fpu_intflo       1/1         ALUMAC       LOAD-STORE       LOAD-STORE       or1200_freeze       or1200_freeze       1/1         Planning       Execution Configuration       FREEZE       or1200_freeze       or1200_freeze       0         Transient       Fault Injection Campaign Configuration       Fault	SM Design Mapping       FPU Arita       Floating point std       Diglib       or1200_fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Flaating point co       Diglib       or1200_fpu.fpu_fmm.s       1/1         FMEDA Plan       FPU Int Flot       Integer and foati       Diglib       or1200_fpu.fpu_infm.s       1/1         Permanent       FPU Int Flot       Integer and foati       Diglib       or1200_fpu.fpu_infm.s       1/1         Fault Injection Campaign       Configuration       or1200_ffu.fpu_infm.s       1/1       +         Planning       Execution       FREEZE       or1200_ffeezes       or1200_ffeezes       -         Planning       Fault Injection Campaign       Configuration       or1200_ffeezes       -       -         Planning       Fault Injection Campaign       Configuration       -       -       -       -         Planning       Planning       -       -       -       -       -       -         Planning       Planning       -       -       -       -       -       -	SM Design Mapping       FPU Arita       Floating point std       Diglub       or1200_fpu.fpu_arith       10/11         FMEDA Plan       FPU Fcmp       Floating point co       Diglub       or1200_fpu.fpu_fmu_mtm       10/11         Permanent       FPU Int Flot       Integer and foati       Diglub       or1200_fpu.fpu_infmu_mtm       1/1         Parmanent       ALUMAC       Diglub       or1200_fpu.fpu_infmu_mtm       1/1       +         Pault Injection Campaign       Configuration       or1200_ffue.eze       or1200_ffue.eze       1/1       +         Planning       Execution Configuration       Fault Injection Campaign       or1200_ffue.eze       -       -       -         Planning       Fault Injection Campaign       Configuration       -       <	VALIDATION	▼ FPU			or1200_fpu		
FMEDA Plan       FPU Frmp       Flaating point co       Diglub       of 1200_fpu.fpu_fpu_fmcmp       1/1         Permanent       FPU Int Flot       Integer and foati       Diglub       of 1200_fpu.fpu_intflo       1/1         ALUMAC       LOAD-STORE       Integer and foati       of 1200_fpu.fpu_intflo       1/1         Planning       FREEZE       of 1200_freeze       of 1200_freeze       Integer and foati	FMEDA Plan       FPU Fcmp       Flaoting point co       DigLib       orl 200 fpu.fpu_itmp       1/1         Permanent       FPU Int Flot       Integer and foatl       DigLib       orl 200 fpu.fpu_itmlio       1/1         Fault Injection Campaign Configuration       FREEZE       orl 200 fpu.fpu_itmlio       1/1       1/1         Planning       Execution Configuration       FREEZE       orl 200 freeze       orl 200 freeze       0/1         Transient       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration       Image: Configuration	FMEDA Plan       FPU Ecmp       Flaoting point co       Digub       orl 200 fpu.fpu.femp       1/1         Permanent       FPU Int Flot       Integer and foati       Digub       orl 200 gru.fpu.itfbu       1/1         Fault Injection Campaign Configuration       FPU Ecmp       Flaoting point co       Digub       orl 200 gru.fpu.itfbu       1/1         Planning       Execution Configuration       FREEZE       orl 200 frueeze       orl 200 frueeze       1/1         Fault Injection Campaign Configuration       Freeze       orl 200 frueeze       orl 200 frueeze       1/1         Fault Injection Comfiguration       Freeze       orl 200 frueeze       orl 200 frueeze       1/1         Fault Injection Compaign Configuration       Fault Injection Campaign Configuration       orl 200 frueeze       1/1       1/1         Planning       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration       Integer and foat i       Integer and foat i       Integer and foat i       Integer and foat i         Planning       Fault Injection Campaign Configuration       Integer and foat i       Integer and foat i       Integer and foat i       Integer and foat i	FMEDA Plan       FPU Fcmp       Flaoting point co       Digub       orl 200 fpu.fpu.fcmp       1/1         Permanent       FPU Int Flot       Integer and foati       Digub       orl 200 gru.fpu.ftml.ntlot       1/1         Fault Injection Campaign Configuration       FPU Ecmp       Flaoting point co       Digub       orl 200 gru.fpu.ftml.ntlot       1/1         Planning       Execution Configuration       FREEZE       orl 200 freeze       orl 200 freeze       1/1         Fault Injection Campaign Configuration       Freeze.       orl 200 freeze       orl 200 freeze       1/1         Fault Injection Configuration       Freeze.       orl 200 freeze       orl 200 freeze       1/1         Fault Injection Configuration       Execution Configuration       Freeze.       orl 200 freeze       1/1         Planning       Execution Configuration       Planning       Freeze       orl 200 freeze       Image: Freeze         Planning       Execution Configuration       Planning       Image: Freeze       Image: Freeze       Image: Freeze       Image: Freeze         Planning       Execution Configuration       Freeze       Image: Freeze       Image: Freeze       Image: Freeze       Image: Freeze		FPU Arit	Floaitng point std	DigLib 🗾	or1200_fpu.fpu_arith	10/11	•
Permanent <ul> <li>ALUMAC</li> <li>LOAD-STORE</li> <li>Configuration</li> <li>Planning</li> <li>Execution Configuration</li> <li>Execution Configuration</li></ul>	Permanent <ul> <li>ALUMAC</li> <li>IOAD-STORE</li> <li>IOAD-STORE</li> <li>FREEZE</li> <li>Orl 200_freeze</li> </ul> Planning     FREEZE <ul> <li>Orl 200_freeze</li> <li>Orl 200_freeze</li> <li>FREEZE</li> </ul>	Permanent <ul> <li>ALUMAC</li> <li>LOAD-STORE</li> <li>Configuration</li> </ul> or1200_fsu             or1200_freeze             Planning              FREEZE                or1200_freeze            Transient              Fault Injection Campaign             Configuration               FREEZE            Planning              Freeze               or1200_freeze            Planning              Freeze               or1200_freeze            Planning              Pault Injection Campaign             Configuration               Pault Injection Campaign             Configuration            Planning              Planning	Permanent <ul> <li>ALUMAC</li> <li>LOAD-STORE</li> <li>Configuration</li> </ul> or1200_fsu             or1200_freeze             Planning              FREEZE                or1200_freeze            Planning              Freeze               or1200_freeze            Planning              Freeze               or1200_freeze            Planning              Freeze              Planning              Freeze               Freeze            Planning                Freeze               Freeze            Planning                   Planning                   Planning                   Planning                   Planning                   Execution Configuration	Sim Design Mapping	FPU Fcmp	Flaoting point co	· _		1/1	•
Permanent     > LOAD-STORE       Fault Injection Campaign Configuration     > FREEZE       ) Planning     > Execution Configuration	Permanent     LOAD-STORE     or1200_lsu       Fault Injection Campaign Configuration     FREEZE     or1200_freeze       Planning     Execution Configuration       Execution     Frault Injection Campaign Configuration       Fault Injection Campaign Configuration	Permanent     > LOAD-STORE     or1200_lsu       Fault Injection Campaign Configuration     > FREEZE       Planning     > Execution Configuration       Execution       Transient Configuration       Fault Injection Campaign Configuration       Planning       Planning	Permanent       LOAD-STORE       of1200_lsu         Fault Injection Campaign Configuration       FREEZE       of1200_freeze         Planning       Freezetion       of1200_freeze         Execution       Freezetion       Freezetion         Transient       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration         Planning       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration         Planning       Fault Injection Configuration       Fault Injection Configuration         Planning       Fault Injection Configuration       Fault Injection Campaign Configuration	FMEDA Plan		Integer and foati	DigLib 🝷		1/1	
Fault Injection Campaign Configuration     FREEZE     Or1200_freeze       Planning     Execution Configuration	Fault Injection Campaign Configuration     FREEZE     01200_fteeze       Planning     Execution Configuration       Execution       Transient Configuration       Fault Injection Campaign Configuration	Fault Injection Campaign Configuration     FREEZE     01200_titles       Planning     FREEZE     01200_freeze	Fault Injection Campaign Configuration     FREEZE     or1200_tdum       Planning       Execution Configuration       Fault Injection Campaign Configuration       Fault Injection Campaign Configuration       Planning       Planning       Execution Configuration       Planning       Execution Configuration       Planning       Execution Configuration	Permanent						
Configuration     FREEZE     OFFZOU_FREEZE       )     Planning       )     Execution Configuration	Configuration     FREEZE     OrlZOU_treezes       Planning     Execution Configuration       Execution     Fault Injection Campaign Configuration	Configuration     FREEZE     Ch200_treeze       Planning     Execution Configuration       Execution     Fault Injection Campaign Configuration       Planning     Planning	Configuration     FREEZE     Ch200_treeze       Planning     Execution Configuration       Execution     Fault Injection Campaign Configuration       Planning       Planning       Execution Configuration							
) Execution Configuration	Execution Configuration Execution Transient Fault Injection Campaign Configuration	Execution Configuration       Execution       Transient       Fault Injection Campaign Configuration       Planning	Execution Configuration       Execution       Transient       Fault Injection Campaign       Configuration       Planning       Execution Configuration       Execution Configuration		► FREEZE			or1200_freeze		
	) Execution Transient ) Fault Injection Campaign Configuration	Execution       Transient       Fault Injection Campaign       Configuration       Planning	Execution       Transient       Fault Injection Campaign Configuration       Planning       Execution Configuration	) Planning						
	Transient Fault Injection Campaign Configuration	Transient       Fault Injection Campaign       Configuration       Planning	Transient       Fault Injection Campaign       Configuration       Planning       Execution Configuration	) Execution Configuration						
) Execution	) Fault Injection Campaign Configuration	Fault Injection Campaign       Configuration       Planning	Fault Injection Campaign         Configuration         Planning         Execution Configuration	) Execution						
Transient	Configuration	Configuration Planning	Configuration       Planning       Execution Configuration	Transient						
		) Planning	Planning       Execution Configuration							
	Planning Planning		Execution Configuration							
	Execution Configuration									
			) Execution	Execution Configuration						
Fault Injection Campaign     Configuration     Planning	Execution Configuration			Fault Injection Campaign Configuration						





#### S/CD Target and SM Allocation

				FMEDA_DEMO/Detailed/DetailedSDcTargetAndSm CDN_MAPS 🗢 IT 🛅 FTP 🕒 CCMSutil 💥			S> Home - 2017 SVG	GTn 📙 Other	Bookmarks 🚺	) Jabber 🗋	Q3Meeting17 💥	JabRef ன ncls		) 🔍 🖒
		MEDA_DEM	O / Detailed FMEDA	•										e fer
CONFIGURATION Design Extraction	S/DC Tar	get & SM Allo	cation - Permanent								SM	I Allocation 🚺 λ Values 🚺		SM Definitions
	FM ID	Part	Subpart	Failure Mode	λр 🎼	Sp% Target 🏢	Sp% Annotated	Apd 📄	λр% [	DCp% Target	DCp% Annotated	SM Permanent		λpr 🔺
	FM_1	FETCH	Instruction Fetch	Incorrect Instruction Flow caused by a fault the bran	1.34e-3		4.97% (+4.97%) 🔀	1.27e-3	1.33%		100% (+1%) 🔀	SM_3		_
MEDA Hierarchy/ Design Mapping	FM_2	FETCH	GenPC	Incorrect Instruction Flow caused by a fault in the fe	1.13e-3	0%		1.13e-3	1.12%	0%		Select	•	1.13e
esign Information	FM_3	FETCH	GenPC	Incorrect fetch address generation caused by a fault	1.23e-4	0%		1.23e-4	0.12%	0%		Select		1.23e
DC Target & SM Allocation	FM_4	DECODER	DecodCtrl	Incorrect Instruction Flow caused by a fault in the d	2.57e-3	0%		2.57e-3	2.55%	0%		Select	•	2.57e
Permanent	FM_5	DECODER	DecodCtrl	Incorrect Instruction sequence caused by a fault in $t \ldots % \left( f_{1} \right) = 0$	3.10e-4	0%		3.10e-4	0.31%	0%		Select	•	3.10e
Transient	FM_6	EXCEPT	Except	Un-intended execution/not executed interrupt request	4.37e-3	0%		4.37e-3	4.35%	0%		Select	•	4.37e
Tanoich	FM_7	CORE REGS	Special Regs	Processor deadlock caused by system register corr	1.60e-3	0%		1.60e-3	1.6%	0%		Select	•	1.60e
VALIDATION	FM_8	CORE REGS	Special Regs	Processor memory protection error caused by fault i	4.92e-5	0%		4.92e-5	0.05%	0%		Select	-	4.92e
M Design Mapping	FM_9	CORE REGS	Register File	Corrupt data or value caused by a fault in the regist	3.58e-2		9.25% (+9.25%) 🔀	0.03	35.67%			SM_2	•	0.1
													~	
MEDA Plan														
Permanent	FM_12	FPU	FPU top logic	Incorrect result caused by fault in the FPU state ma	8.52e-4	0%		8.52e-4	0.85%	70%		Select	•	2.56e
Fault Injection Campaign	FM_13	FPU	FPU Arithmetic	Incorrect result caused by fault in the FPU-Arith stat	2.19e-3	0%		2.19e-3	2.18%	70%		Select	•	6.57e
Configuration	FM_14	FPU	FPU Arithmetic	FPU Adder produces incorrect data due to fault into	1.30e-3	0%		1.30e-3	1.29%	70%		Select	•	3.89e
Planning	FM_15	FPU	FPU Arithmetic	FPU Incorrect division data due to fault into the FPU	2.63e-3	0%		2.63e-3	2.62%	70%		Select	•	7.90e
Execution Configuration	FM_16	FPU	FPU Arithmetic	FPU Incorrect multiplication data due to fault into th	3.22e-3	0%		3.22e-3	3.2%	70%		Select	•	9.65e
Execution	FM_17	FPU	FPU Arithmetic	FPU Incorrect post-division data due to fault into the	4.23e-3	0%		4.23e-3	4.21%	70%		Select	•	1.27e
Transient	FM_18	FPU	FPU Arithmetic	FPU Incorrect post-normalization multiplication data	5.97e-3	0%		5.97e-3	5.94%	70%		Select	•	1.79e
Fault Injection Campaign	FM_19	FPU	FPU Arithmetic	FPUpost-normalized AdderSubtracter produces inc	2.18e-3	0%		2.18e-3	2.17%	70%		Select	•	6.53e
Configuration	FM_20	FPU	FPU Arithmetic	FPU Incorrect pre-division data due to fault into the	1.47e-3	0%		1.47e-3	1.47%	70%		Select	•	4.42e
Planning	FM_21	FPU	FPU Arithmetic	FPU Incorrect multiplication data due to fault into th	2.52e-4	0%		2.52e-4	0.25%	70%		Select	•	7.56e
Execution Configuration	FM_22	FPU	FPU Arithmetic	FPU Adder produces incorrect data due to fault into	1.89e-3	0%		1.89e-3	1.88%	70%		Select	•	5.67e
Execution	FM_23	FPU	FPU Fcmp	FPU Incorrect comparing result due to fault into the	3.73e-4	0%		3.73e-4	0.37%	50%		SM_1	•	1.87e
DEGUNZ	FM_24	FPU	FPU Int Float	FPU Incorrect floating integer data result due to faul	6.23e-3	0%		6.23e-3	6.2%	40%		SM_1	•	3.74e
RESULT	FM_25	ALUMAC	Arith. Logic	Incorrect result caused by fault in the ALU state ma	1.43e-3	0%		1.43e-3	1.42%	0%		Select	•	1.43e
MEDA	FM_26	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the	3.42e-4	0%		3.42e-4	0.34%	0%		Select	•	3.42e
afety Mechanisms	FM_27	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the i	1.32e-4	0%		1.32e-4	0.13%	0%		Select	•	1.32e
	FM_28	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the	1.06e-3	0%		1.06e-3	1.06%	0%		Select	•	1.06e
	FM_29	ALUMAC	Multiplier Accumulator	Incorrect result caused by fault in the MAC state ma	4.52e-3	0%		4.52e-3	4.5%	0%		Select	•	4.52e
	FM_30	ALUMAC	Multiplier Accumulator	Incorrect Instruction Result caused by a fault in the	2.40e-3	0%		2.40e-3	2.38%	0%		Select	•	2.40e
	FM_31	ALUMAC	Multiplier Accumulator	Incorrect Instruction Result caused by a fault in the	9.60e-3	0%		9.60e-3	9.55%	0%		Select	•	9.60e
	FM_32	LOAD-STORE	Load Store	Wrong address addressing load/store data caused	5.11e-4	0%		5.11e-4	0.51%	0%		Select	-	5.11e



cādence

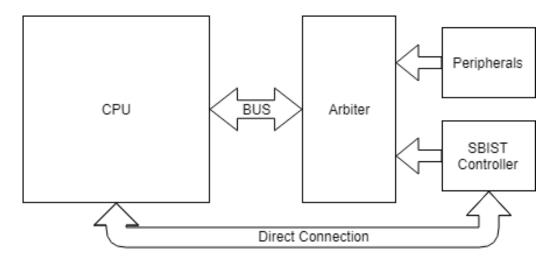
21



9 Parts / 16 Sub-Parts / 35 Failure Modes SPFMp: 25.53% SPFM: DISABLED LFM: 100% PMHFp: 0.07 PMHFI: DISABLED PMHFifm: 0 Fault Campaigns: 2 / 2 / 35 👀 🎓

#### STL and Safety Mechanisms The Importance of Fault Injection Campaigns on the STL

- Software Test Library (STL)
- It is intended to be run on a safety critical processor, and attempt to detect any errors
  - This can allow the system to fail safely
- The design of the processor is created with the STL in mind
  - Optimisations enable software to test certain parts and be deterministic



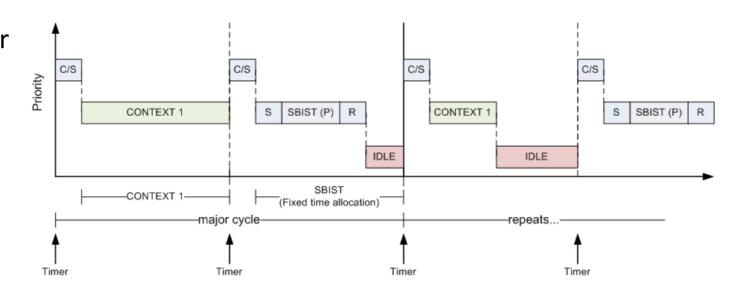




# **STL and Safety Mechanisms**

The Importance of Fault Injection Campaigns on the STL (continued)

- STL is very low level
  - Written in C and assembly
  - Contains a number of functions for testing the "health" of the processor
- Requirements are strict on size and execution time
  - They can be "online" as well as "offline"
- Fault injection used to measure the effectiveness of STL







## **Example: FMEDA**

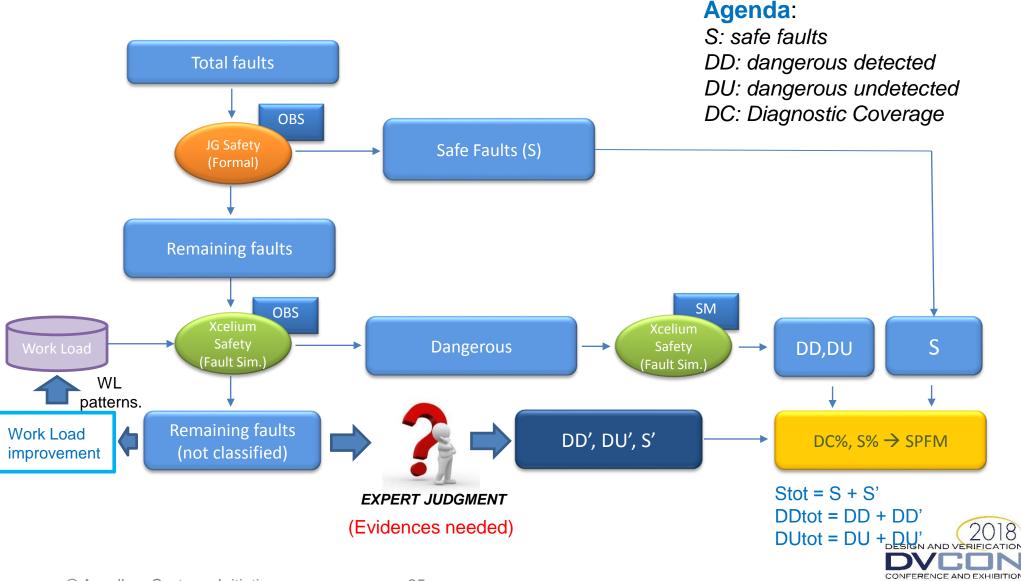
FMEDA reports are done for the processor with the STL, and also for the SBIST controller.

			Permanent fa	ults				
FM distribution	Failure rate	Fsafe	Fault detection and control mechanism	Diagnostic coverage (Krf)	Residual / single point failure rate	Multiple point failure rate	Diagnostic coverage for latent faults (Klat)	Latent multiple point failure rate
0.000%	3.57E-04	0.000%	STL	89.240%	3.84E-05	3.19E-04	100.00%	0.00E+00





#### How to Validate an FMEDA



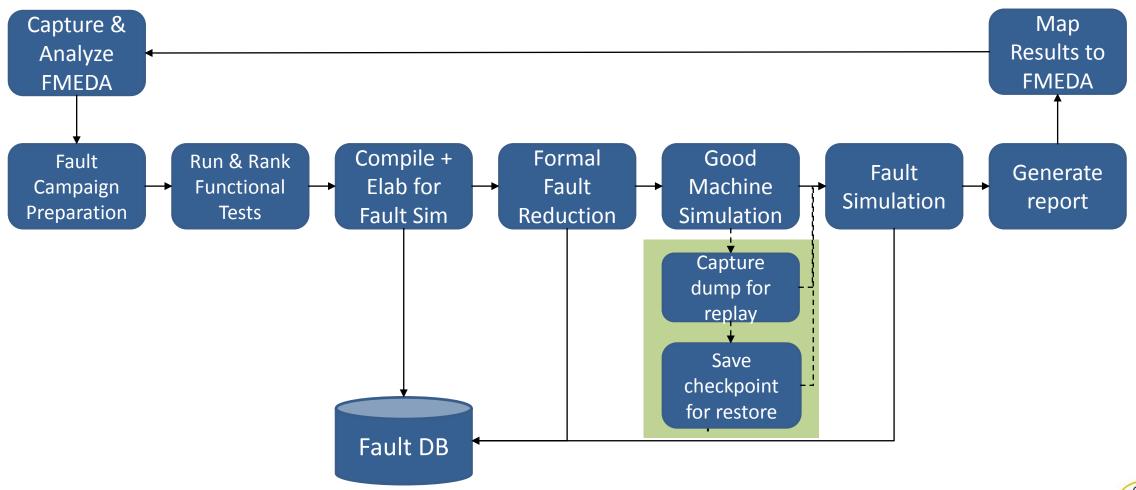
IROP

accellera

SYSTEMS INITIATIVE

© Accellera Systems Initiative

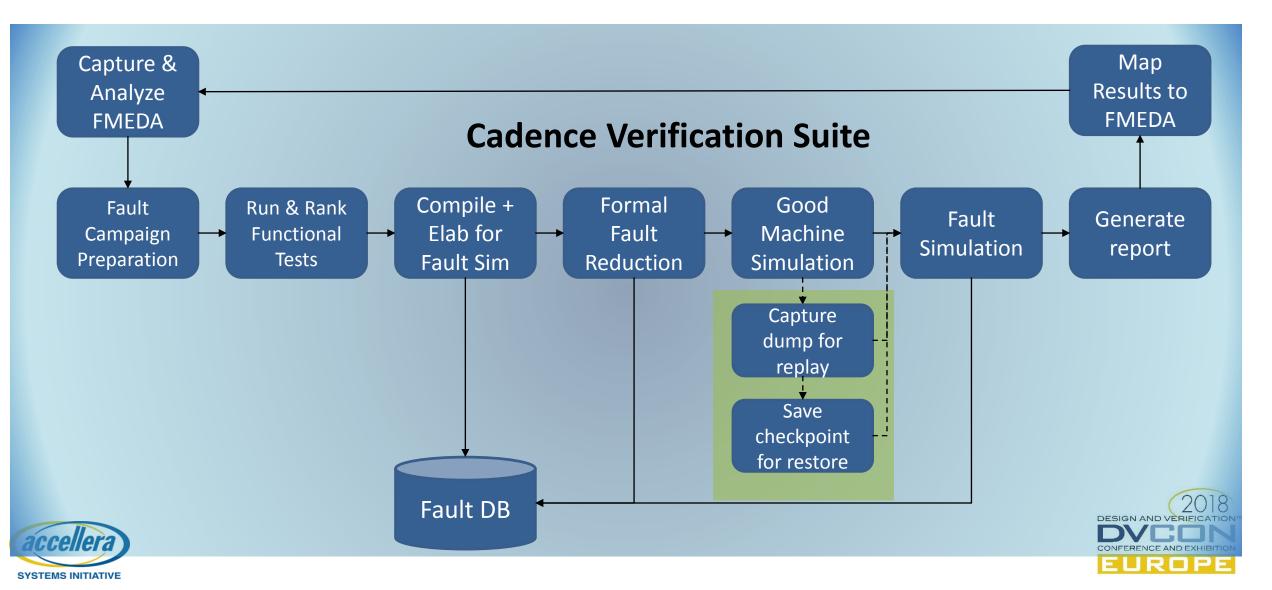
#### **Functional Safety Flow**







### **Cadence Functional Safety Flow**



### **Questions?**





#### Demo





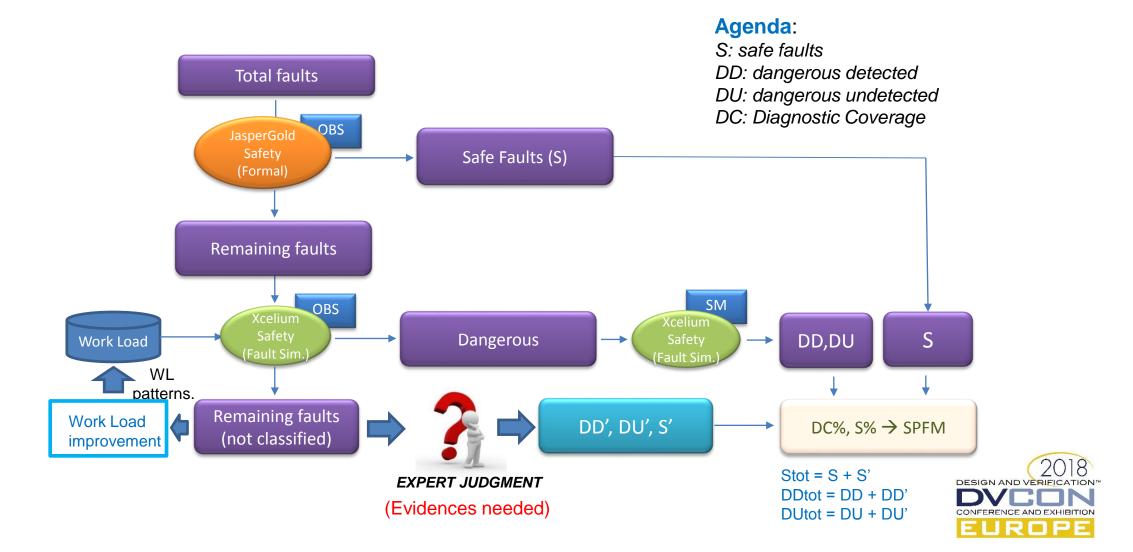
#### FMEDA Demo





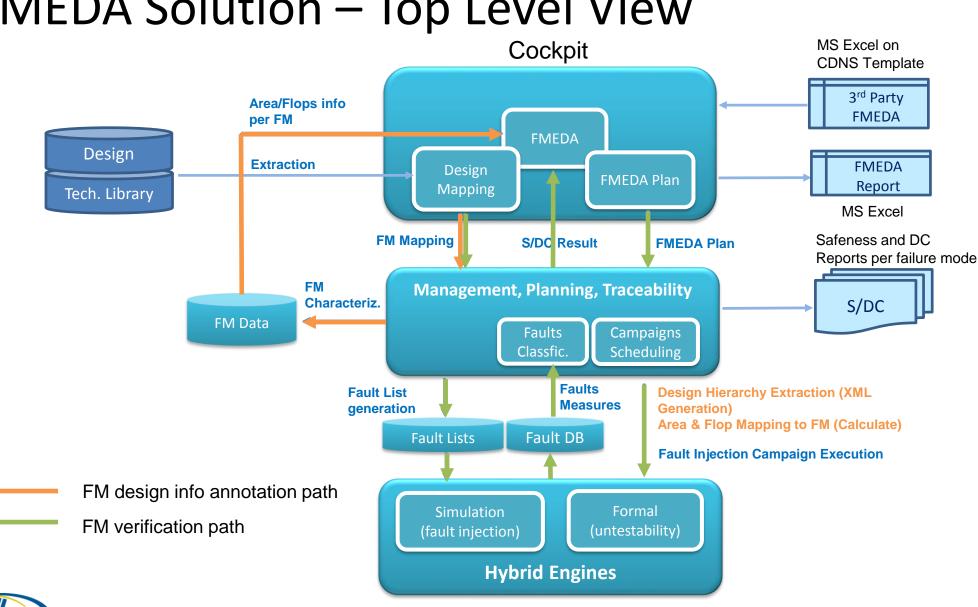
#### How to Validate an FMEDA – Fault Classification Flow

 Fault classification can't be ideal in practice, not classified faults (NC) can be exposed to user expert judgment to be further classified



Compliant DC/S Calculation SO26262 accellera

SYSTEMS INITIATIVE

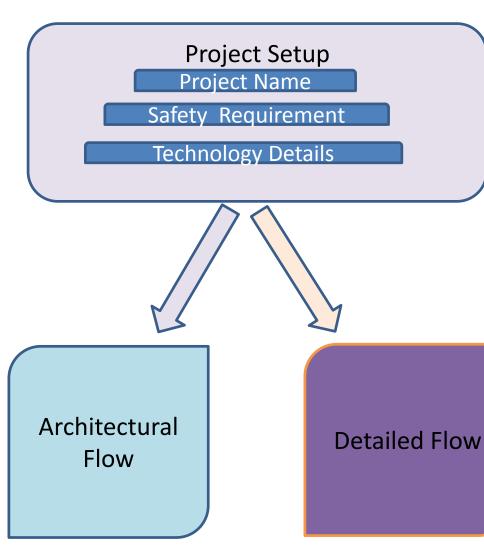


#### FMEDA Solution – Top Level View





## Flow support



Architectural FMEDA Flow:

- Rough estimation of the overall metrics
  - Course grained FMEDA
- Metrics evaluation before RTL/design information availability
- Analysis is to address feasibility study
- Analysis aimed to figure out primary SM requirements.

#### Detailed FMEDA Flow:

- Accurate estimation of the overall metrics
  - Fine grained FMEDA
- Metrics evaluation using actual design & assumed DC targets
- Evidence to prove the achieved safety goals
  - Data for ASIL certification
- Validation of metrics Fault Injection, Formal Analysis



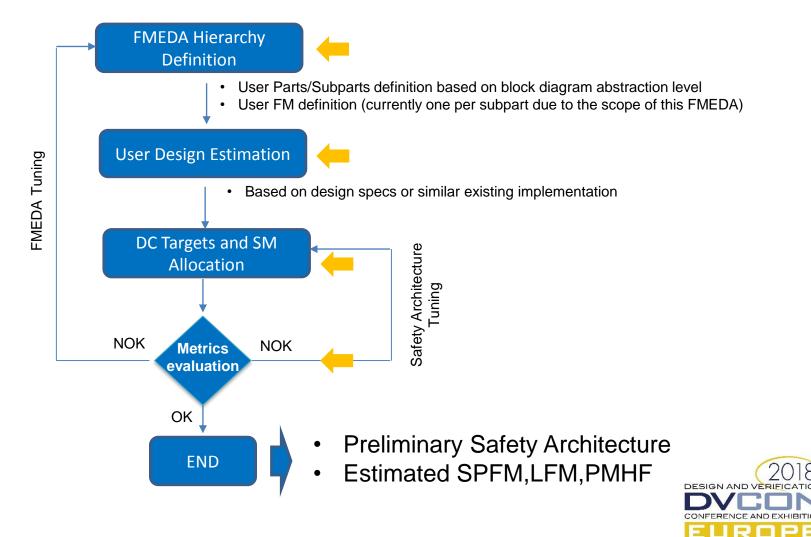


#### **FMEDA Solution**

#### Architectural FMEDA: based on Design Estimation (before RTL availability)

#### SCOPE:

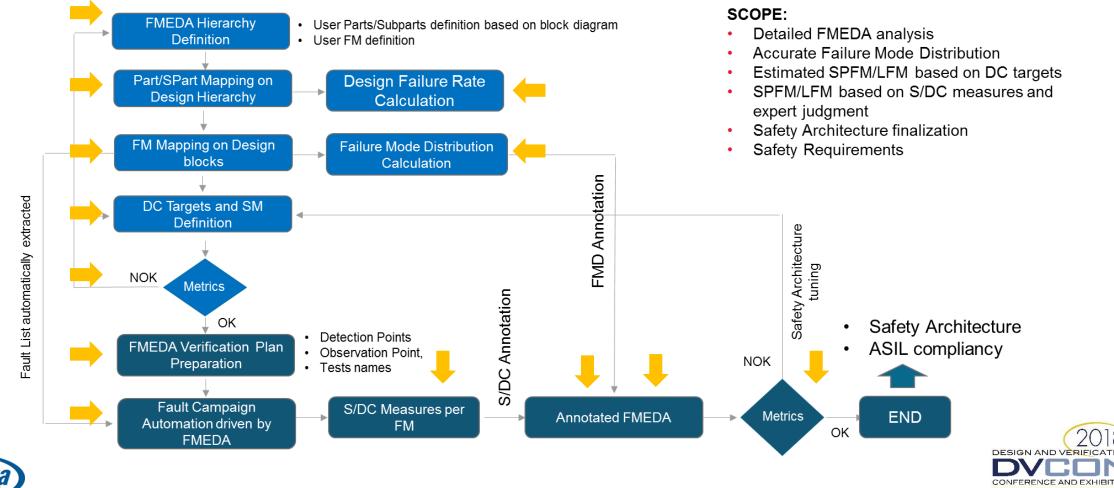
- Course grained FMEDA analysis
- Preliminary Safety Architecture
- Preliminary Safety Requirements
  - S, DC associated with mapped Safety Mechanism
- Estimated SPFM,LFM, PMHF
  - For Permanent and Transient



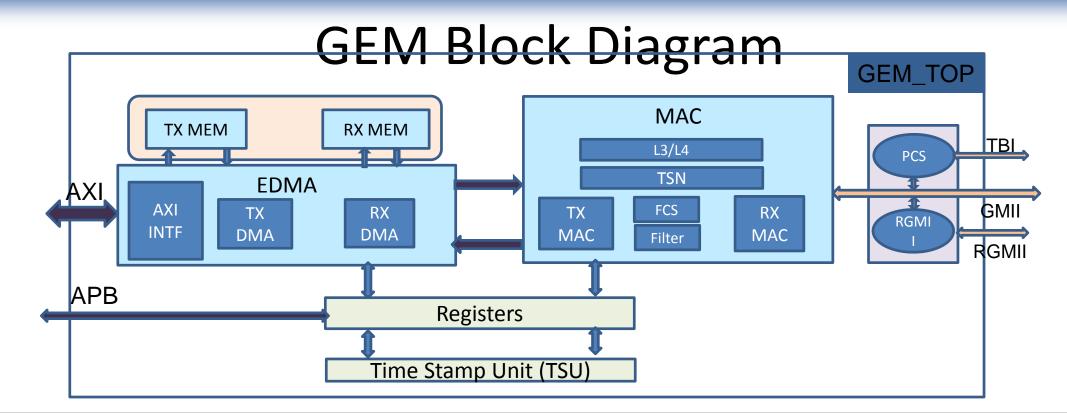


#### **FMEDA Solution**

Detailed FMEDA: based an actual design information (after RTL, Netlist availability)



SYSTEMS INITIATIVE



Safety Relevant

1

1

1

1

gem\_gxl.i\_gem\_ss.i\_gem\_top.gen\_tsu\_i\_gem\_tsu

Mission

Mission

Mission

Mission

Туре

v

v

v

w

Memory Bits

#### 

Failure Mode

TX/RX timestamp is corrupted, output TSU timer value to local s...

The timer value may not be captured or captured incorrectly

The TSU seconds interrupt is incorrect

TSU compare interrupt is incorrect

gen\_tsu\_i\_gem\_tsu

ID

.

#### FMEDA Hierarchy / Design Mapping

FM\_1

FM\_2

FM\_3

FM\_4

#### 🖞 Upload Mapping

4/4

admin

Design Extraction

FMEDA Hierarchy/ Design Mapping

O Design Information

S/DC Target & SM Allocation

Permanent

Transient

VALIDATIO





Mapping

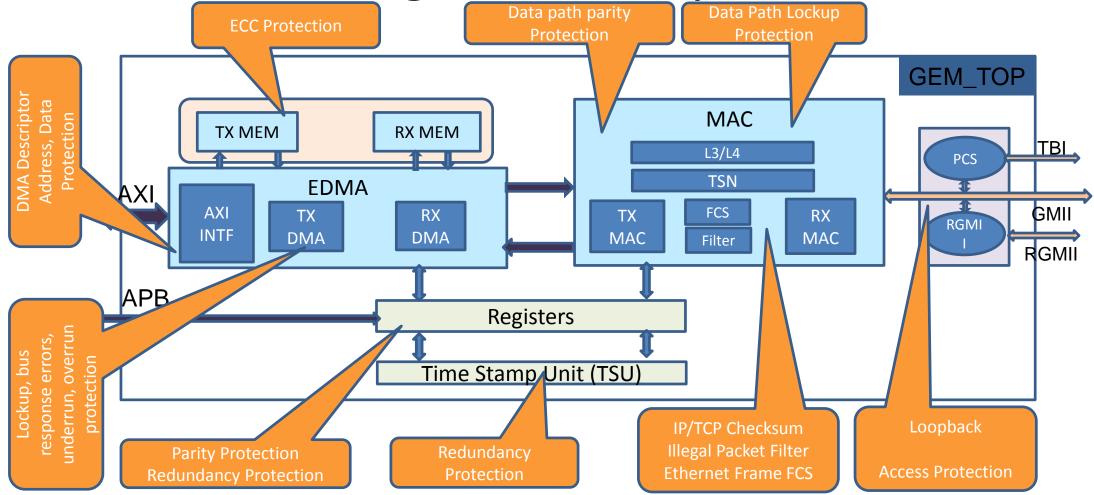
gem\_gxl.i\_gem\_ss.i\_gem\_top.gen\_tsu\_i\_gem\_tsu..

em\_gxl.i\_gem\_ss.i\_gem\_top.gen\_tsu\_i\_gem\_tsu

gem\_gxl.i\_gem\_ss.i\_gem\_top.gen\_tsu\_i\_gem\_tsu

gem\_gxl.i\_gem\_ss.i\_gem\_top.gen\_tsu\_i\_gem\_tsu

### GEM Block Diagram - Safety mechanism view







#### FMEDA Template – Instance Mapping Formats

#### DESIGN MAPPING INFORMATION

			1			
Part (Block)	Part Instances mapping	Subpart (Sub-block)	Description	Subpart Instances mapping	Failure Mode	Failure Mode Instances mapping
	gem_gxl.i_gem_ss.i_ gem_top	gen_tsu_i_gem_tsu	Time Stamp Unit	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i gem_tsu	The timer value may not be captured or captured incorrectly	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
					The TSU seconds interrupt is incorrect	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
					TSU compare interrupt is incorrect	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
					TX/RX timestamp is corrupted, output TSU timer value to local system will be invalid, Timer value read back in registers is also invalid. May also cause TX lockup for time based scheduling.	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
		i_gem_reg_top.i_g em_registers	Etherent IP Registers	gem_gxl.i_gem_ss.i_gem_top.i_gem_reg _top.i_gem_registers		gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.gen_axi_i_gem_parity_gen_dma_config_burst _len; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_dma_config_byte_1; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_default; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_int_mask_disable
a !a	.b.c.d -> In	clude only -> Exclude	Submod all the su	ubmodules instances		<ul> <li>em_ss.i_gem_top.i_gem_reg_top.i_gem_registers;!gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_t op.i_gem_registers.gen_axi_i_gem_parity_gen_dma_config_burst_len;</li> <li>'gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_dma_config_byte_1; m_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_default;</li> <li>d.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_int_mask_disable</li> </ul>
	allara				Fault in dynamic control outputs from the registers	gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers;
aci						CONFERENCE AND EXHIBITION

SYSTEMS INITIATIVE

EUROPE

#### Architectural Flow

Controls visibility

ANALYSIS	_															
O FMEDA Hierarchy	F	MEDA Res	ult									Des	ign Informatio	n 💽 FN	1 Туре 🌑	Generate Report
O Design Estimation		ID 🗄	Part	Subpart	Technology	Area 📄	#G	[1	#bit	λр []=	Sp 🎼	λpd 📄	λρ %	DCp % 🗎	λpr	SM ID Perma
	F	M_ARCH_16	gem_gxl	TX _Data_Memory	MEM_LIB	4505.6			4096	4.92e-2	2%	0.05	2.77%	99%	4.82e-4 \$	M_11
S/DC Target & SM Allocation	F	M_ARCH_15	gem_gxl	RX_Data_Memory	MEM_LIB	9011.2			8192	9.83e-2	2%	0.1	5.54%	99%	9.63e-4	M_11
O Permanent	F	M_ARCH_14	gem_gxl	TSU_Comparator .	Generic_SS_LIB	513	500	64		2.91e-3	2%		0.16%			
O Transient	F	M_ARCH_13	gem_gxl	Register_Parity_Logic .	Generic_SS_LIB	1026	1000	0		5.82e-3	2%		0.33%			
RESULT	F	M_ARCH_12	gem_gxl	PHY Interface .	Generic_SS_LIB	5130	5000	100		2.91e-2	2%	0.03	1.64%	90%	2.85e-3	M_13
	F	M_ARCH_11	gem_gxl	MISC .	Generic_SS_LIB	3078	3000	200		1.75e-2	2%	0.02	0.98%	90%	1.71e-3	M_12
• FMEDA	F	M_ARCH_10	gem_gxl	ECC_protection .	Generic_SS_LIB	2872.8	2800	50		1.63e-2	2%	0.02	0.92%	95%	7.99e-4	M_11
Safety Mechanisms	F	M_ARCH_9	gem_gxl	CSR_Space	Generic_SS_LIB	51300	50000	4500		2.91e-1	2%	0.29	16.41%	95%	0.01	M_5 ; SM_6
	F	M_ARCH_8	gem_gxl	TSU .	Generic_SS_LIB	12312	12000	300		6.99e-2	2%	0.07	3.94%	98%	1.37e-3	M_10
	F	M_ARCH_7	gem_gxl	TX_MAC .	Generic_SS_LIB	41040	40000	1500		2.33e-1	2%	0.23	13.13%	97%	6.85e-3	M_7 ; SM_9 ; SM_12 ; \$
	F	M_ARCH_6	gem_gxl	RX_MAC .	Generic_SS_LIB	34884	34000	22		1.98e-1	2%	0.19	11.16%	97%	5.82e-3	M_8 ; SM_12 ; SM_13 ;
	F	M_ARCH_5	gem_gxl	AXI_RD_WR	Generic_SS_LIB	61560	60000	4600		3.49e-1	2%	0.34	19.7%	95%	0.02	M_3 ; SM_4 ; SM_7 ; SI
	F	M_ARCH_4	gem_gxl	DMA_RX_RD	Generic_SS_LIB	30780	30000	1400		1.75e-1	2%	0.17	9.85%	95%	8.56e-3	M_2 ; SM_4
	F	M_ARCH_3	gem_gxl	DMA_RX_WR	Generic_SS_LIB	5130	5000	250		2.91e-2	2%	0.03	1.64%	95%	1.43e-3	M_4
	F	M_ARCH_2	gem_gxl	DMA_TX_RD .	Generic_SS_LIB	14364	14000	1200		8.15e-2	2%	0.08	4.6%	92%	6.39e-3	M_3
	F	M_ARCH_1	gem_gxl	DMA_TX_WR	Generic_SS_LIB	22572	22000	1350		1.28e-1	2%	0.13	7.22%	96%	5.02e-3	M_1; SM_3

cādence



1 Parts / 16 Sub-Parts / 16 Failure Modes SPFMp: 95.85% SPFMt: 95.14% LFM: 99.95% PMHFp: 0.07 PMHFt: 6.9 PMHFlfm: 8.56e-4



Report

#### **Detailed Flow**

Option: Safety Relevant	IS	$\rightarrow$	Design Inform	mation 🔵 FM Typ	De 🔵 🔒 (	Generate Report
true	λp					
true true true true true true	8.49e-3 8.44e-3 8.44e-3 8.44e-3 4.72e-4 1.84e-1 1.74e-1	6.38% 2% 2% 2%	7.90e-3 8.27e-3 8.27e-3 4.62e-4 0.18 0.17	2.15% 2.15% 0.12% 46.83% 44.43%		
						Generate Re in Excel For

cādence accelera systems initiative

1 Parts / 2 Sub-Parts / 7 Failure Modes SPFMp: 95.43% SPFMt: 96.61% LFM: 100% PMHFp: 0.02 PMHFt: 1.8 PMHFlfm: 0 Fault Campaigns: 2 / 0 / 7 🙍



#### **Detailed Flow**

Design Extraction	FME	DA Result		Filter	Options	S	$\rightarrow$	Design Informa	tion 🔵 FM Type		enerate Report
ANALYSIS		ID 📑 Part	Subpart	Failure Mode	Safety Relevant	λр []	Sp %	λpd 🎼	λp %	DCp %	λpr
MEDA Hierarchy/ Design Mapping	FM_1	i_gem_top	gen_tsu_i_gem_tsu	The timer value may not be captured or captured incorrectly	true	8.49e-3	6.49%	7.94e-3	2.16%	1009	
	FM_2	i_gem_top	gen_tsu_i_gem_tsu	The TSU seconds interrupt is incorrect	true	8.44e-3	6.38%	7.90e-3	2.15%	99.769	1.926
esign Information	FM_3	i_gem_top	gen_tsu_i_gem_tsu	TSU compare interrupt is incorrect	true	8.44e-3	2%	8.27e-3	2.15%	989	1.65e
DC Target & SM Allocation	FM_4	i_gem_top	gen_tsu_i_gem_tsu	TX/RX timestamp is corrupted, output TSU timer value to local system will be	true	8.44e-3	2%	8.27e-3	2.15%	989	1.65e
Permanent	FM_5	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in Parity Generators of Registers	true	4.72e-4	2%	4.62e-4	0.12%	959	2.31e
Transient	FM_6	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in static configuration outputs from the registers	true	1.84e-1	2%	0.18	46.83%	959	9.00e
ransient	FM_7	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in dynamic control outputs from the registers	true	1.74e-1	2%	0.17	44.43%	959	8.54e
Fault Injection Campaign Configuration Planning Execution Configuration Execution	<							in	Exce	l Fori	mat
Transient											
Fault Injection Campaign Configuration											
Planning											
Execution Configuration											



1 Parts / 2 Sub-Parts / 7 Failure Modes SPFMp: 95.43% SPFMt: 96.61% LFM: 100% PMHFp: 0.02 PMHFt: 1.8 PMHFlfm: 0 Fault Campaigns: 2 / 0 / 7 👩



#### Summary

- Integrated functional + safety verification flow and engines
  - Reduce effort of developing & maintaining different environments
  - Highest performance native fault simulation
- vPlan-based requirements traceability, with FMEDA plan based metrics analysis
  - Use FMEDA user strategy to reduce amount of required fault simulation
  - Integrate design data for accurate analysis
- Automate the functional safety verification tool flow
  - Reduce the human effort whenever possible, automate all possible steps
  - Minimize the Fault Injection Campaign Set-up time
  - Reuse of Functional Verification Environment
- Execution core
  - Optimized flow to improve the TAT and optimized usage of each involved feature
  - Use coverage data to reduce the number of test to be executed
  - Utilization of formal techniques to reduce the fault space
  - Intelligent algorithms to minimize the number of fault to be injected and executed
- Cadence provides the most comprehensive solution for Functional Safety





#### Thanks



