FMEDA-Driven Safety Verification

DVCon China

Xinwei Wu September 2023



Outline

- Automotive Trends and ISO 26262
- FMEDA Creation and Safety Analysis
- Safety Verification
- Summary





Automotive Market and Key Trends

- Still strong Automotive Semiconductor Growth
 - o CAGR of 11.1%, 2021-2027 (Source: YOLE Intelligence, 10/2022)
 - Main drivers are SW-defined vehicles, Autonomous Driving, EVs
- Drive towards leading-edge technology nodes
 - 3D-IC design, Chiplets
 - 5nm, 3nm gate-all-around (GAA)
- Industry Responding to Supply Chain Disruption
 - OEM and Tier-1s initiating SoC designs
 - Traditional semiconductor companies entering the automotive market
 - Startup companies developing autonomous driving platforms and sensors

Semi (8.1%) \rightarrow Auto Semi (11.1%) \rightarrow AD (19%) \rightarrow EVs (22%) \rightarrow Lidar (71%)





Electrification Hybrid & EVs



cādence

3 © 2023 Cadence Design Systems, Inc. All rights reserved

Automotive Challenges



FMEDA-Driven Digital Safety Analysis and Verification ISO 26262 Functional Safety

ISO 26262 Functional Safety



FMEDA-Driven Digital Safety Analysis and Verification ISO 26262 Functional Safety

ISO 26262 Functional Safety



Failure Modes Effects and Diagnostic Analysis

- Verify that the Safety Mechanisms and their diagnostic coverage reach the required ASIL level by calculating the architectural safety metrics: SPFM, LFM
- FMEDA validates the Safety Architecture (collection of safety mechanisms) and the safety performance of the system (SPFM, LFM).

ASIL	ASIL A	ASIL B	ASIL C	ASIL D
SPFM	n.d	≥90%	≥97%	≥99%
LFM	n.d	≥60%	≥80%	≥90%
PMHF (FIT)	< 1000	< 100	< 100	< 10
1FIT = 1E-9				

Closing the Gap Between FMEDA and Safety Verification

	Abstraction	Safety Step	User			
Functional Safety Concept	Functional	FMEA	Safety Architect (System level)		Safety Requirements	
Technical Safety Concept SoC	Block Diagram	FMEDA (architectural)	Safety Architect (SoC level)	alysis	Estimation	
SoC Design	RTL/netlist	FMEDA (detailed)	Safety Engineer (RTL/gate level)	Safety Ana		
SoC Safety Verification	Netlist	Safety Verification (Formal/Fault Injection)	Safety Verification Engineer	Verification	Verification	
Safety Metrics	Verification Result	FMEDA backannotation	Safety Verification Engineer	Safety	More accurate safety metrics	



FMEDA Creation and Safety Analysis



Cadence Functional Safety Solution



Unified Midas Safety Platform for FMEDA-Driven Functional Safety

- Midas[™] Safety Platform driving analog and digital flows for FMEDA-based functional safety
- Early phase safety analysis and architecture exploration
- Automated safety mechanism insertion and verification
- Native chip design data for accuracy and detailed safety analysis
- Unified Safety Format (USF) support

adence	a Mirdas Safety Platform = CPU								- 0
lence	File Edit Project Help								
	a anna a shine as satariya a santara Santa								
	CPU .	FMEDA Parts SubParts	SM Mappings	Attributes Configurat	ons				
	~ 🖿 CPU	Columns Configuration					E	T 2 xport Calculate	Summary Crea
	V Core								
	> FETCH	Failure Mode	Part	SubPart	SubPart Description	FM description	Safety Relevant	FM Type	Technolog
	> DECODER	FM_ARCH_1	Core	FETCH	Instruction Fetch Unit	Any failures of FETCH su	on	Mission	DigLib
	> EXCEPT	FM_ARCH_2	Core	DECODER	Instruction Decoder	Any failures of DECODE	on	Mission	DigLib
	CORE REGS	FM_ARCH_3	Core	EXCEPT	Exception Stage and	Any failures of EXCEPT	on	Mission	DigLib
	> WR BACK	FM_ARCH_4	Core	CORE_REGS	Core Registers Banks	Any failures of	on	Mission	DigLib
	> • FPU	FM_ARCH_5	Core	WR_BACK	Write-Back Logic	Any failures of WR_BACK	on	Mission	DigLib
	> ALU MAC	FM_ARCH_6	Core	FPU	Floating Point Unit	Any failures of FPU sub	on	Mission	DigLib
	> LOAD STORE	FM_ARCH_7	Core	ALU_MAC	Pipelined Arith Logic wit	Any failures of ALU_MAC	on	Mission	DigLib
		FM_ARCH_8	Core	Summary Report					
	Search Select	FM_ARCH_9	Core			Source Incomercian			Lib
	Juice	FM_ARCH_10	Core	Summa	ry of the CP	U FMEDA			Lib
	🛩 🛅 Design Hierarchy			Generated	on: Fri Oct 8 20	021 13:04:31			
	✓ ■ or1200_сри								^
	cmp_if_insn0	Shell			Counts		1 Parts / 10 Sub-Parts	/ 10 Failure Modes	
	cmp_if_pc_sm0	Warning + USE [USE-1]			SPFMp		87.85	96	
	cmp_saving_if_insn0	: Passive Failure Mode	e - Permanent D	Da	SPEMI		85.18	96	
	cmp_if_stall0	Warning : USF [USF-1]	2						- 11
	cmp_genpc_refetch0	: Passive Failure Mode : Midas USF WARNING	e - Permanent E G	Da	LFM		99.58	%	
	cmp_except_itlbmiss0	Warning : USF [USF-1] : Passive Failure Mode	e - Permanent E	Da	PMHFp		1.042e	-02	
	cmp_except_immufault0	: Midas USF WARNING Warning : USF [USF-1]	5		04405		1 0050		
	cmp_except_ibuser/0	: Passive Failure Mode : Midas USE WARNING	e - Residual FIT	Б.	PMHPt		1.0008		
	sm_if_obs0	Warning : USF [USF-1]	- Permanent F	Da	PMHFifm		3.146e	-04	
	cmp_cy_we_rf0	: Midas USE WARNING)		Design Failure Rate Permanent	t (FIT)	λtot(P): 8.5	81e-02	
	sm_rf_obs0	: Passive Failure Mode	e - Residual FIT	8			14-477- C 7		
	> 🛅 or1200_alu	Warning : USF [USF-1]			Design Failure Rate Transient	uni	AtO((1): 6.7	906-00	
	or1200_cfgr	Passive Failure Mode Midas USF WARNING	e - Permanent E G	Ja	Technologies		DigLi	b	
	✓ ■ Shared Library	Warning : USF [USF-1] : Passive Failure Mode	e - Permanent E	Da	Dealers Inform 1		Total Area:	134678.6	
	> 📘 Technologies	: Midas USF WARNING Warning : USF [USF-1]	3		Design information		#Flops: 6	563.0	~
	> Safety Mechanisms	: Passive Failure Mode : Midas USF WARNING	e - Transient Da	an					
	Base Failure Rate Templates	Warning : USF [USF-1]	- Residual CTT	at Zero					177
		: Midas USF WARNING	s - Nesidudi FII	0(20)					



Architectural FMEDA Setup

Create FMEDA					×	FN	MEDA Report									Х
						FMEDA										
FMEDA Project Name:	Chakra_SOC					Columns										Group
Mode: ISO26262 ~	ASIL: C ~	Architectural	Entity:	SoC	~)	Part count	SubPart count	Failure Mode count	SPFMp	SPFMt	LFM	РМНБр	РМНІ
Bota Eactor:		○ Detailed	Poporto	Transiont and parmanar	.+ .		Chakra	SOC	14	38	60	95.10%	95.10%	100.00%	1.187e+01	1.187e+
	51L. L •		Reports.	mansient and permaner			Drink_Mac	hine_IP_1		15	18	98.88%	98.67%	94.27%	1.419e-04	1.970e
							RC_FME	DA_IP_1	10	17	36	83.99%	84.20%	99.97%	1.613e-02	1.146e+
				OK Ca	ncel		Memory	_fmeda		6	6	95.10%	95.10%	100.00%	1.186e+01	1.186e+



BFR calculation engine (IEC TR 62380)

Safety Hierarchy (Parts/Subparts)

Failure Mode Creation

Safety Mechanisms Mapping



Metrics & Reports

Queries

Rule Checks

Project Setup

Device Safety (IP / SoC)

FMEDA Creation

- FMEDA hierarchy only (no IC design)
- Failure Mode Distribution based on user estimation

cādence

Analysis and Reporting



Safety Design and Analysis at System/SoC/IP Level



Refining FMEDA Leveraging Design and Simulation Data

Architectural FMEDA

Summary Report (on sjfhw626)

Summary of the RISC_CORE_ARCH FMEDA Generated on: Tue May 3 2022 23:12:43

Counts	10 Parts / 17 Sub-Parts / 36 Failure Modes
Total FIT (Raw FIT) Permanent - λ	8.582e+00
Total FIT (Raw FIT) Transient - λ	3.931e+01
Safety related FIT Permanent - Asr	7.929e+00
Safety related FIT Transient - λ sr	3.624e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - in FIT	1.087e+00
Probabilistic Metric for random Hardware Failures PMHF Transient - in FIT	5.312e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - in FIT	1.573e-03
Single Point Fault Metric - SPFM Permanent	86.29%
Single Point Fault Metric - SPFM Transient	85.34%
Latent Fault Metric - LEM	99.98%

- No design data available
- FMEDA hierarchy only
- Failure rates and distribution solely based on early estimations



Detailed FMEDA Summary Report (on sjfdcl1247)

Summary of the RISC_CORE_DETAILED FMEDA Generated on: Wed May 4 2022 21:41:28

Counts	10 Parts / 17 Sub-Parts / Failure Modes
Total FIT (Raw FIT) Permanent - λ	1.057e+01
Total FIT (Raw FIT) Transient - λ	4.733e+01
Safety related FIT Permanent - Asr	9.873e+00
Safety related FIT Translent - λsr	4.381e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - In FIT	1.433e+00
Probabilistic Metric for random Hardware Fallures PMHF Transient - in FIT	6.662e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - In FIT	1.499e-03
Single Point Fault Metric - SPFM Permanent	85.49%
Single Point Fault Metric - SPFM Transient	84.79%
	99.98%

- With design data
- Design/FMEDA hierarchy mapping
- Failure rates based on area, gates, and flops
- Safety metrics based on estimated DC, S numbers

Detailed FMEDA (annotated)

Summary Report (on sjfdcl1247)	
Summary of the RISC_CORE_DETAILE Using annotated values Generated on: Tue May 3 2022 23:35:40	D FMEDA
Counts	10 Parts / 17 Sub- Parts / 36 Failure
Total FIT (Raw FIT) Permanent - λ	1.057e+01
Total FIT (Raw FIT) Transient - λ	4.733e+01
Safety related FIT Permanent - λsr	9.873e+00
Safety related FIT Transient - Asr	4.381e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - in FIT	7.097e-01
Probabilistic Metric for random Hardware Failures PMHF Transient - In FIT	2.345e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - in FIT	0.000e+00
Single Point Fault Metric - SPFM Permanent	92.81%
Single Point Fault Metric - SPFM Transient	94.65%
Latent Fault Metric - LFM	100.00%

- With design data
- Design/FMEDA hierarchy mapping
- Failure rates based on area, gates, and flops
- Safety metrics based on simulation-based DC, S numbers

SPFM = 92.81%

Detailed FMEDA Using USF

FMEDA Project (IP and SoC)

BFR calculation engine (IEC TR 62380)

Technologies (Digital, Analog)

Safety Hierarchy (Parts/Subparts)

Failure Mode Creation

Mapping Safety Mechanisms

Mapping Design Hierarchy to FMEDA Hierarchy

Metrics and Reports

11

set_fmeda myFMEDA -ASIL B -t -p -detailed

create_technology DigLib -type Digital -fitperm 1.07e-6 -fittrans_gate
1.64e-6 -fitbit 1.64e-6 -refarea 1.026

create_part "OpenRISC Core" -fmeda myFMEDA -instances
{hinst:or1200_cpu/or1200_if hinst:or1200_cpu/or1200_genpc}
create_subpart FETCH -desc "Instruction Fetch Unit" -part "OpenRISC Core" fmeda myFMEDA -instances {hinst:or1200_cpu/or1200_if}

create_failure_mode FM_ARCH_1 -desc "Any failures of FETCH sub-block" -type
Mission -technology DigLib -subpart FETCH -safe_perm 1 -safe_trans 0 -fmeda
myFMEDA -instances {hinst:or1200_cpu/or1200_if}

create_safety_mechanism SM-IF -desc "Instruction Fetch redundancy" -type
Custom -class HW
apply_safety_mechanism SM-IF -to FM_ARCH_1 -fmeda myFMEDA -dcperm 95 dctrans 0 -dclat 100

report_safety -fmeda myFMEDA permanent csv OpenRISC_Permanent.csv
report_safety -fmeda myFMEDA transient csv OpenRISC_Transient.csv
report_safety -fmeda myFMEDA report html OpenRISC_Report.html

save usf

→ load usf



14 © 2023 Cadence Design Systems, Inc. All rights reserved.

Queries



Safety Verification



Optimizing Throughput Across the Full Verification Flow



* Cadence® Joint Enterprise Data and AI (JedAI) Platform

Digital Safety Verification

Fault analysis and simulation

- ✓ Fault Campaign Management Verisium[™] Manager Safety
 - Unified campaign management across all engines
 - Backannotation of DC results into Midas
 - Requirements traceability
 - Reporting for safety documentation

✓ Fault Analysis – Jasper[™] FSV App

- Applies formal techniques to fault analysis
- Significantly reduces the simulation fault list
- Increases safety verification performance

✓ Fault Simulation – Xcelium[™] Safety

- Native serial and concurrent fault verification
- Same simulator for functional verification (GOOD machine) and fault simulation (BAD machine)





Fault Campaign Management – Automation and Optimization



- Test selection and ranking
 - Coverage-based test selection
 - Customizable ranking criteria
 - Test Dropping
- Fault list reduction
 - Fault collapsing
 - Testability analysis
 - Fault sampling



cādence

- Fault campaigns execution
 - Measured Diagnostic Coverage and Safeness
 - Back-annotation of results to FMEDA
 - Generate reports and analyze fault metric
 - FMEDA, fault classification, campaign summary

18 © 2023 Cadence Design Systems, Inc. All rights reserved.

Xcelium Safety App

- Integrated Xcelium[™] Safety flow with Midas[™],
 Verisium[™] Manager, and Jasper[™] FSV
- Native fault simulation
 - Integration of functional and safety engines
 - Xcelium: a single simulator for functional and fault simulation
 - Superior traceability and debug visibility
- Covers all digital safety verification use cases and provides comparable quality results
- Supports reactive TBs and various abstractions



Xcelium Safety – Fault Simulation



- Native fault simulation
 - Integration of functional and safety verification engines
- Support reactive TBs, various abstractions
 - Integrated serial and concurrent engines
 - Serial support for VHDL and Verilog, RTL, and gatelevel
 - Concurrent support for untimed gate-level and RTL
- Congruency flow between two modes
 - Serial mode: Strength in debuggability, generally used in flow setup and faults debug
 - Concurrent mode: Strength in performance throughput, generally used for whole fault campaign mass runs

cādence

 Two modes use identical flow and can easily switch back and forth

Jasper FSV Integration with Xcelium Safety Simulator



- FSV Structural annotates untestable faults in database \rightarrow safe faults will be ignored
- FSV annotates fault relations \rightarrow equivalent faults will be skipped
- FSV TC annotates faults as unobservable by a particular test \rightarrow pruned faults will be dropped
- Xcelium Safety simulates and annotates all remaining DD/DU faults in the database
- FSV Formal provides interactive propagation analysis for unobservable faults by test

Simulation Verification IP (VIP) for Automotive

VIP for Ethernet TSN (MAC)

- Mature, highly capable compliance verification solution
- TSN protocol stack incl. bus functional model (BFM), integrated protocol checkers, and coverage
- Easy integration in test benches at IP and system levels

VIP for Ethernet Base-T1 (PHY)

• Supports all Base-T1 speeds: 10Mbps, 100Mbps, 1Gps

VIP for MIPI A-PHY

- MIPI A-PHY support for sensor applications (CSI2, I2C)
- Compliance to MIPI A-PHY v1.0 and v1.1 specifications

VIP for PCIe 3.0 / 4.0 / 5.0

Best-in-class PCI Express® Verification IP for IP, SoC

VIP for all CAN standards

• Supports CAN, CAN-FD, and CAN-XL specifications

Automotive Ethernet





Sensor Simulation Verification: A-PHY with CSI2 and I2C VIPs

Helium Virtual Platforms

Virtual digital electronics designed to test full software binaries



Controllability, Observability, Repeatability

Digital Twin elements provided by the *methodology:*



Instruction Accurate

•Target software runs without changes

Full programmers view

•Memory, registers, and interrupts



Loosely Timed •Fast enough for OS Boot

Available Early •6-12 months before silicon

> All in Software •Run on standard x86 workstations

Hybrid Platforms: Helium with Palladium or Protium Combining pre-silicon verification with v-model verification and validation

Digital Twin elements provided by the methodology:



• Circuits for design under test • Abstract for context



Full Programmers' View
• Memory, registers, interrupts, and pins



Mixed Abstraction

Fast enough for OS Boot
Detailed enough verification



Available Early • As soon as the design is ready



Integrated with Hardware • Palladium[®] and Protium[™] platforms for capability and performance



Balance of Speed and Accuracy



Analog / Mixed-Signal Safety Verification

Automated fault identification and simulation

- Developed in alignment with IEEE P2427
 - Standard for Analog Defect Modeling and Coverage
- Fault assistant for rule-based fault identification
 - Fault models: DC short/open, resistive bridge, AC coupling
- Integrates Spectre Simulation Platform and Legato Reliability Solution
 - New Spectre fault analysis simulation modes
- Automates launching of fault simulations for different failure modes
- Back-annotation of safety coverage into the Midas[™] Safety Platform



cādence[®]



Summary



ISO 26262 Tool Qualification

- First EDA supplier to achieve "Fit for Purpose -Tool Confidence Level 1 (TCL1)" for the full solution
- Status for medium/high-level confidence (TCL2/3):

Product	Release	Date
Midas	22.03	Available
vManager Safety	20.09, 21.03, 21.09, 22.03	Available
Xcelium Safety	22.03	Available
Jasper Safety	22.03	Applied for

CER No. Z10 0	RTIFI 097905 0019	CATE Rev. 00		Product Service			
Holder of	f Certificate:	Cadence Design Sys 2655 Seely Avenue San Jose CA 95134 USA	tems Inc				
Certificat	tion Mark:					思新早	
		Andread gr		ICAT			
Product:		Software Tool for Sa	rety Related Development	E			P
Paramete	: ers:	The tool is qualified to be u according to ISO 26262 for is a mandatory part of this	sed in safety-related developmen any ASIL. The test report listed b certificate.	CER	CERII No. Z10 097905 (- I C A I E 1012 Rev. 02	
Tested accordin	g to:	ISO 26262-8:2018		CADO -	Holder of Certific	cate: Cadence Design Systems Inc 2655 Seely Avenue San Jose CA 95134 USA	
The product v	was tested on a vo	oluntary basis and complies with	the essential requirements.	E	Factory(ies):	004603	
to third requirer For deti	ICAT					k:	
Test re	Ē		CATE		Product Service	Foredamily gr	
Valid u	CE N	No. Z10 097905 0020 F	Rev. 00			Software Tool for Safety Related Developmen	it
G Date,	•					vManager Safety	
	CADO	Holder of Certificate:	Cadence Design Systems 2655 Seely Avenue San Jose CA 95134 USA	s inc		The tool is qualified to be used in satety-related developm according to ISO 26262 for any ASIL and suitable to be us safety-related development according to IEC 61508. The t report listed below is a mandatory part of this certificate.	ed in est
	TIFI	Certification Mark:	11 ° 11			ISO 26262-8:2018 IEC 61508-3:2010	
Page 1 (◆ CER					n a voluntary basis and complies with the essential requirements. The bove can be affixed on the product, it is not permitted to alter the ray. In addition the certification holder must not transfer the certification holder must not transfer the certification for the certification holder must not transfer the certification h	e to
TÜV SÜ	E AT	Product:	Software Tool for Safety	Related Dev	elopment	in an and a stand on the instead date, unless it is cancelled earlier. All applie g and certification regulations of TUV SUD Group have to be compli- com/ps-cert	ed. For
	N N	Model(s):	Xcelium Safety			00044500	
	ЪИТ	Parameters:	The tool is qualified to be used in according to ISO 26262 for any is a mandaton part of this careful	n safety-related ASIL. The test r	development eport listed below	2025-07-22	
	E U	Tested	ISO 26262-8:2018	cate.		RL I 110	
	♦ a	according to:				(Poter Weiß)	
	書語語に	The product was tested on a voli the certification mark shown abo- certification mark in any way. In . to third parties. This certificate is equirements of the testing and co- or details see: www.tuvsud.com	untary basis and complies with the vue can be affixed on the product. I addition the certification holder mus valid until the listed date. unless it vertification regulations of TUV SUE v/ps-cert	essential requin t is not permitte at not transfer th is cancelled ear 0 Group have to	ements. d to alter the e certificate tier. All applicable be complied.		
	<u>.</u> т	est report no.:	CS100599C				
	CAT	/alid until:	2028-04-12			mbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany	
	E P	Date, 2023-04-14	Peter 1	' Ilik			
	E		(Peter Weiß)	and a			
	(AT + C						
	ERTIFIK						
	2	age 1 of 1 'UV SUD Product Service GmbH • (Certification Body - Ridierstraße 65 - 80	0339 Munich • Ge	many TUV*		
_							•

Functional Safety Services Achieve ISO26262 compliance

- Support in Safety Architecture definition
 - o Architectural/Detailed FMEDA using Midas[™] Safety Platform
 - Creation of a Technical Safety Concept
 - Safety Analysis and reporting
- Functional Safety Verification
 - Safety Verification flow definition
 - Generation of fault injection campaigns and execution using
 - Midas Safety Platform
 - ▷ Verisium[™] Manager Safety
 - ▷ Jasper[™] FSV
 - ▷ Xcelium[™] Safety Simulator
 - Test bench re-use and qualification
- Support in Safety Manual creation (ISO 26262) based on Cadence[®] safety manuals



Advantages of the Cadence Functional Safety Solution



cadence

© 2023 Cadence Design Systems, Inc. All rights reserved worldwide. Cadence, the Cadence logo, and the other Cadence marks found at <u>www.cadence.com/go/trademarks</u> are trademarks or registered trademarks of Cadence Design Systems, Inc. Accellera and SystemC are trademarks of Accellera Systems Initiative Inc. All Arm products are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All MIPI specifications are registered trademarks or trademarks of PCI-SIG. All other trademarks are the property of their respective owners.