ISO 26262 Fault Analysis in Safety Mechanisms

Considering the impact of residual and latent faults in hardware safety mechanisms

Jörg Grosse[1], Mark Hampton[1], Sergio Marchese[1], Jörg Koch[2], Neil Rattray[1], Alin Zagardan[2]

[1]OneSpin Solutions, Munich, Germany

{joerg.grosse | mark.hampton | sergio.marchese | neil.rattray}@onespin.com

[2]Renesas Electronics Europe, Düsseldorf, Germany

{joerg.koch | alin.zagardan}@renesas.com

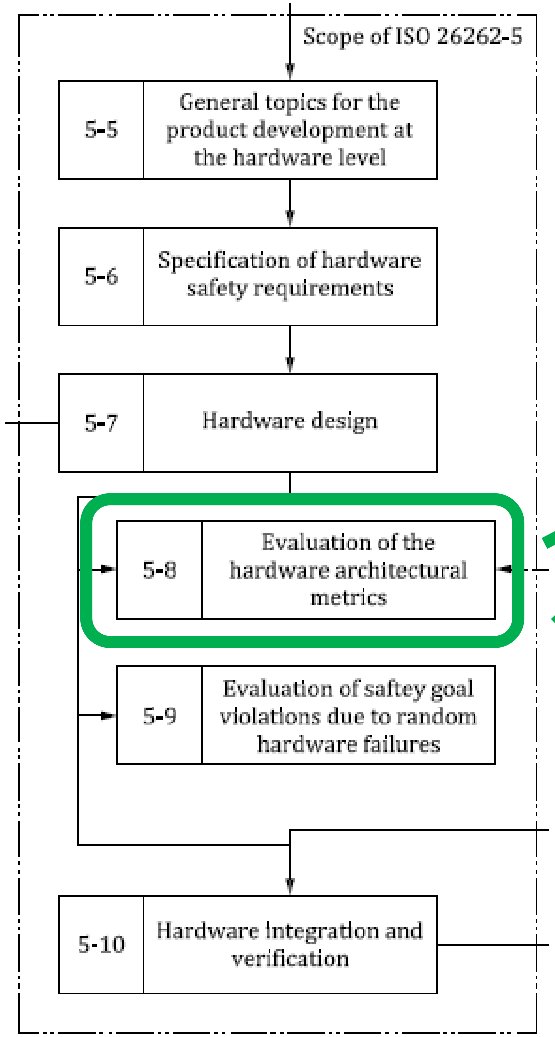
accellera SYSTEMS INITIATIVE

RENESAS

onespin

2019 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

ISO 26262 – Hardware Safety Metrics



Scope of ISO 26262-5

5-5 General topics for the product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Evaluation of the hardware architectural metrics

5-9 Evaluation of saftey goal violations due to random hardware failures

5-10 Hardware integration and verification

- **Evidence that the hardware safety architecture adequately prevents/controls random failures**

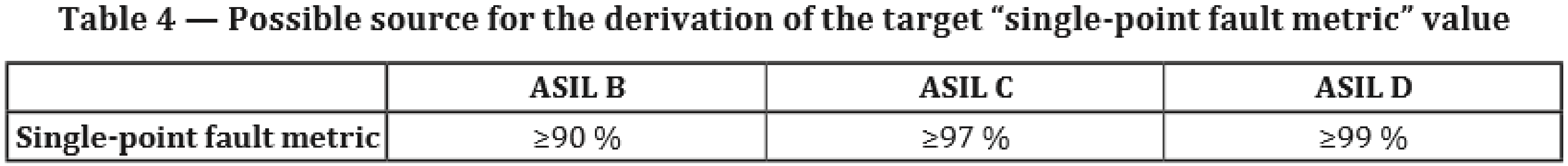


Table 4 — Possible source for the derivation of the target “single-point fault metric” value

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

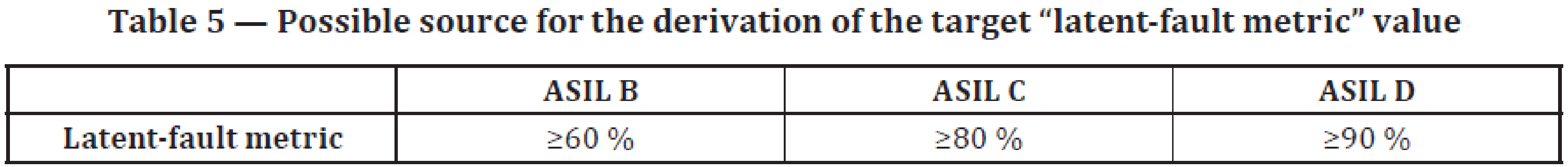
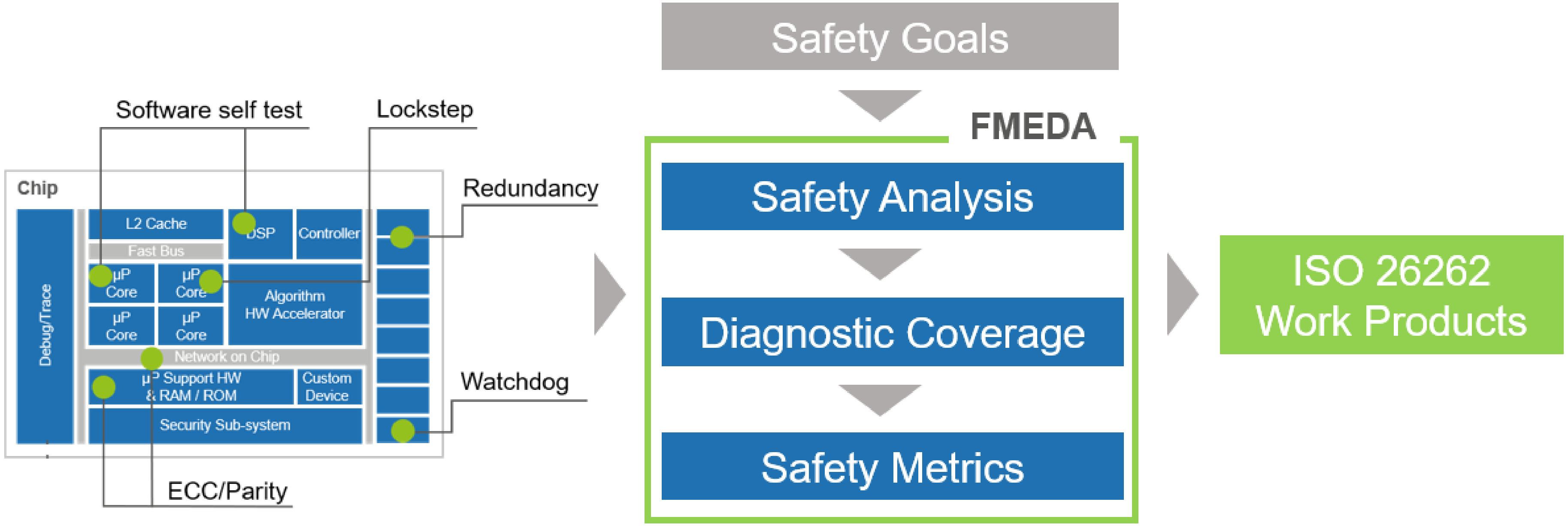


Table 5 — Possible source for the derivation of the target “latent-fault metric” value

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

Efficient and Scalable FMEDA Process



Safety Goals

FMEDA

Safety Analysis

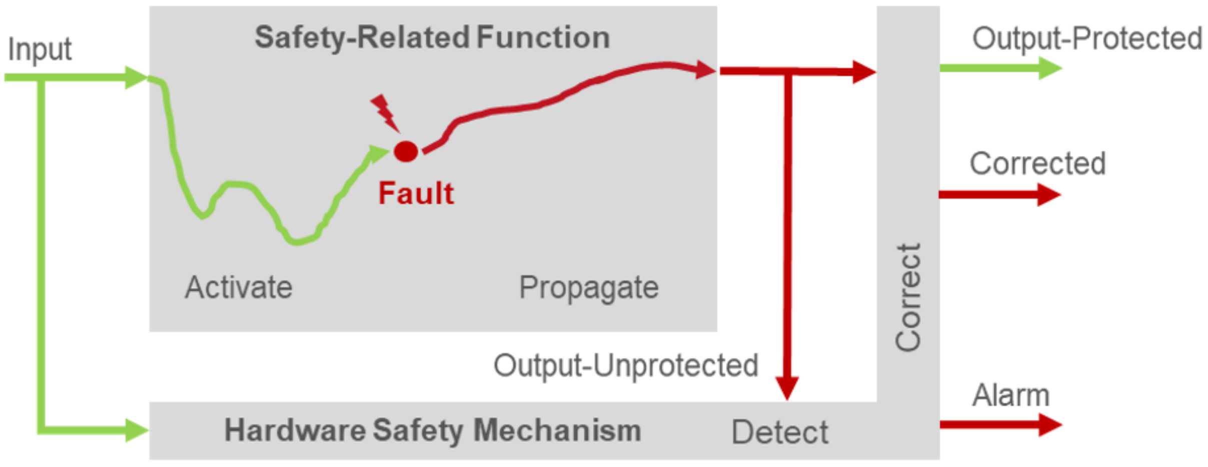
Diagnostic Coverage

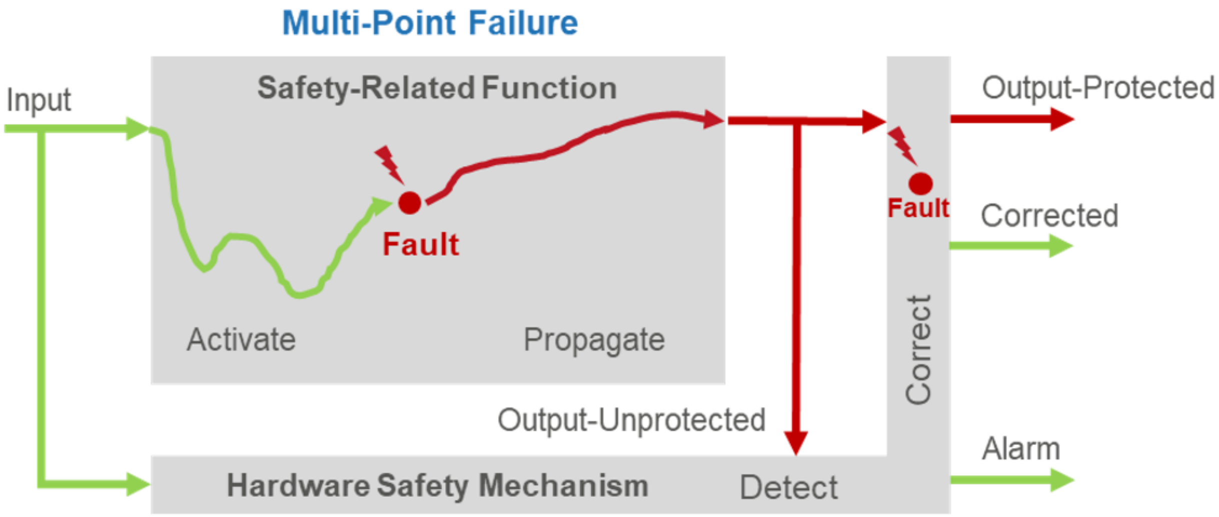
Safety Metrics

ISO 26262 Work Products

- **Safety analysis: Safety-aware hardware partitioning (parts/subparts)**
- **Diagnostic coverage**
  - **Derive initial conservative estimates for each subpart**
  - **Refine/improve results with accurate fault analysis (where necessary)**
- **Safety metrics**
  - **Combine results of parts/subparts, compute SPFM, LFM, PMHF**

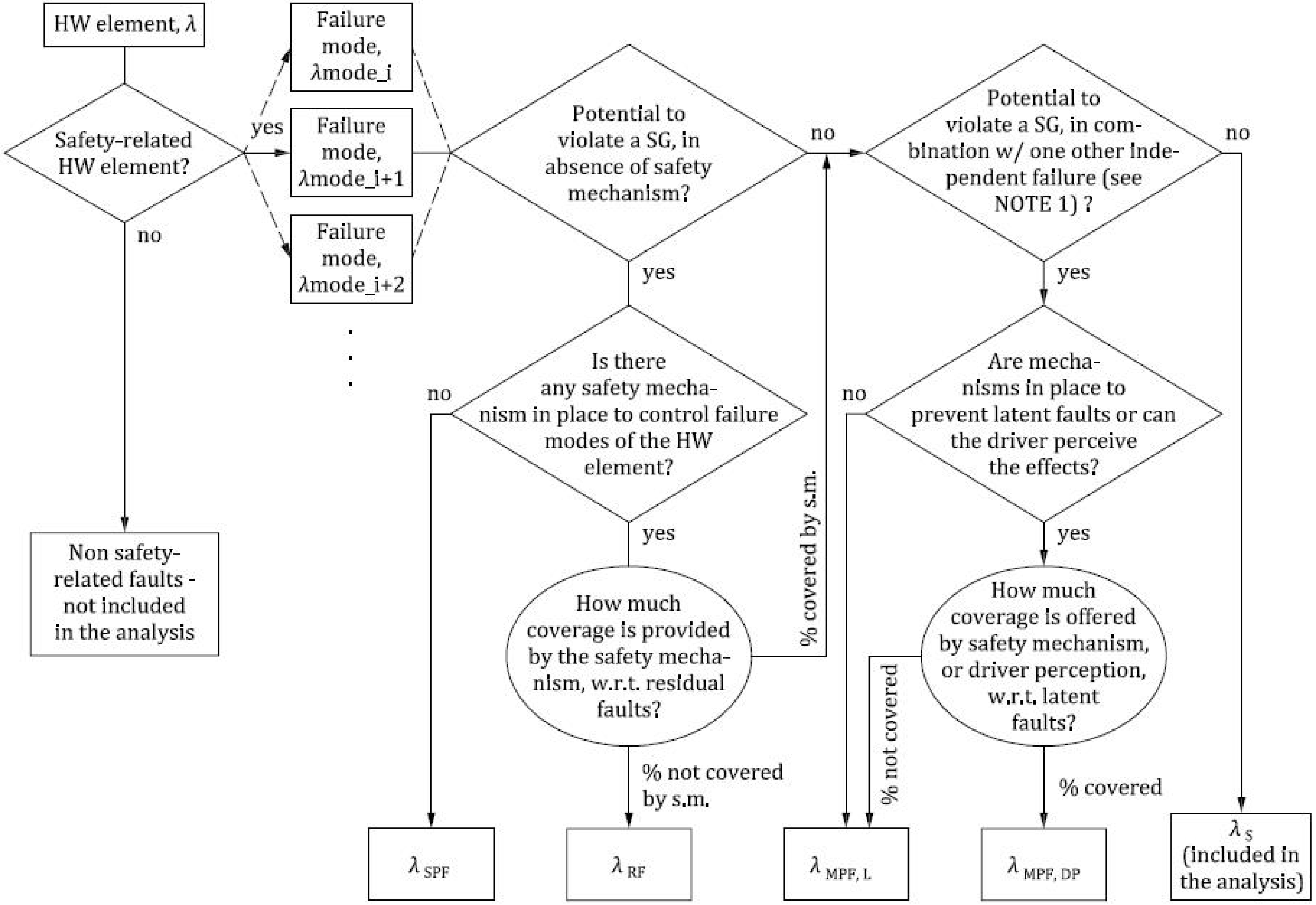
Hardware Safety Mechanisms (SMs)





- **SMs prevent/control failures**
- **Faults in SM logic - active part - may also cause a violation of safety goals**
- **Faults in SM logic – passive part – can only cause a violation of a safety goal in combination with another fault (multi-point)**

Computing Metrics According to ISO 26262

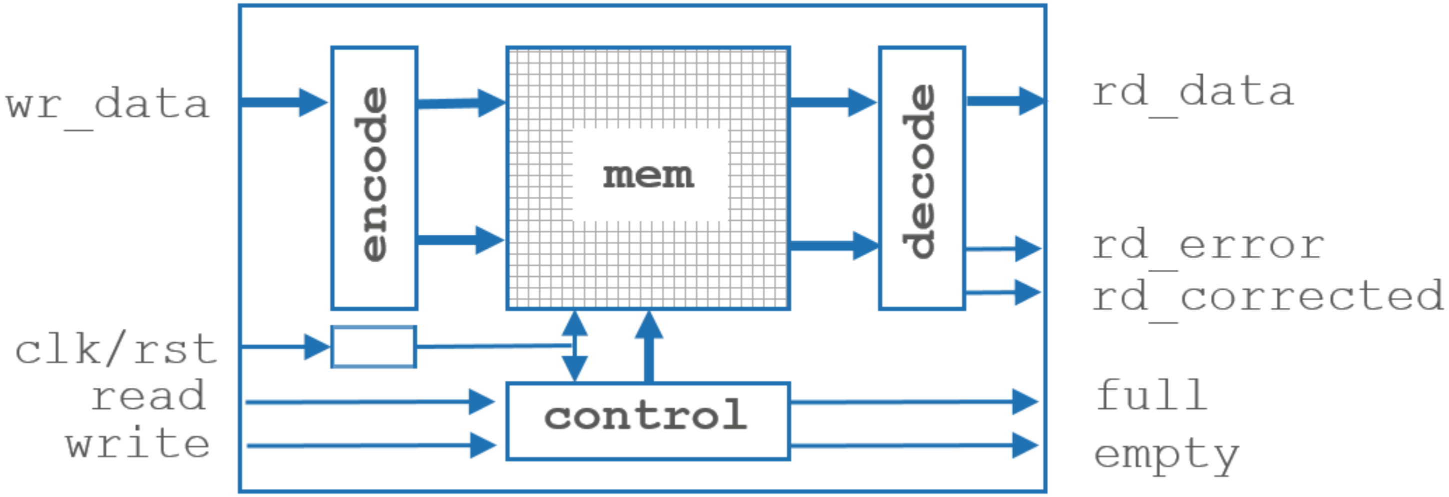

HW element, λ
Safety-related HW element?
yes
no
Failure mode, λmode_i
Failure mode, λmode_i+1
Failure mode, λmode_i+2
Non safety-related faults - not included in the analysis
Potential to violate a SG, in absence of safety mechanism?
no
yes
Is there any safety mechanism in place to control failure modes of the HW element?
no
yes
How much coverage is provided by the safety mechanism, w.r.t. residual faults?
% covered by s.m.
% not covered by s.m.
Potential to violate a SG, in combination w/ one other independent failure (see NOTE 1) ?
no
yes
Are mechanisms in place to prevent latent faults or can the driver perceive the effects?
no
yes
How much coverage is offered by safety mechanism, or driver perception, w.r.t. latent faults?
% not covered
% covered
λ_{SPF}
λ_{RF}
$\lambda_{MPF, L}$
$\lambda_{MPF, DP}$
λ_{S} (included in the analysis)

- F_{SAFE}: safe fault fraction
- F_{PVSG}: fraction of faults that potentially violate a safety goal

- $K_{FMC,RF}$: failure mode coverage in regards to residual faults
- $K_{FMC,MPF}$: failure mode coverage in regards to multi-point faults

Case Study 1: ECC-protected FIFO (FPGA Netlist)

- **FIFO has 16 entries (32-bit data, 7-bit syndrome)**
- **Treated as a SEooC**



Subpart	Protected	Faults
memory	Yes	9752
control	No	658
clk/rst tree	No	16
encoder-active	Yes	270
decoder-active	No	986
decoder-passive	n/a *	54

* Cannot violate safety goal

- **Active subparts: faults can propagate to outputs of intended function**
- **Passive subparts: faults can propagate only to diagnostic outputs**
- **Automated partitioning with OneSpin's Fault Contribution Analysis (FCA) app**

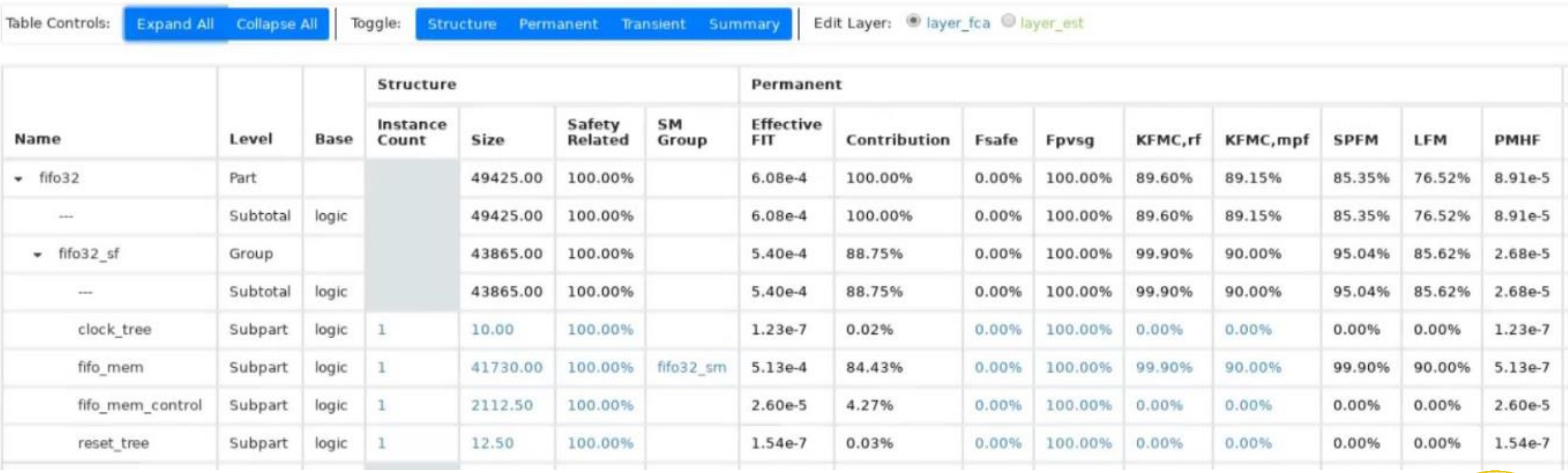
Diagnostic Coverage and Metrics Estimates

Subpart	Protected	Faults	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
memory	Yes	9752	0%	100%	99.9%	90%
control	No	658	0%	100%	0%	n/a
clk/rst tree	No	16	0%	100%	0%	n/a
encoder-active	Yes	270	0%	100%	99.9%	90%
decoder-active	No	986	0%	100%	0%	0%
decoder-passive	n/a *	54	0%	0%	n/a	0%
SPFM			**LFM**			
85.35%			76.52%			

* Cannot violate safety goal

Hardware Metrics Computation (HMC) App

- **Computation of SPFM, LFM, and PMHF**
- **Integrate results of parts/subparts**



Edit Layer: ● layer_fca ○ layer_est

			Structure				Permanent								
Name	Level	Base	Instance Count	Size	Safety Related	SM Group	Effective FIT	Contribution	Fsafe	Fpvsg	KFMC,rf	KFMC,mpf	SPFM	LFM	PMHF
▾ fifo32	Part			49425.00	100.00%		6.08e-4	100.00%	0.00%	100.00%	89.60%	89.15%	85.35%	76.52%	8.91e-5
---	Subtotal	logic		49425.00	100.00%		6.08e-4	100.00%	0.00%	100.00%	89.60%	89.15%	85.35%	76.52%	8.91e-5
▾ fifo32_sf	Group			43865.00	100.00%		5.40e-4	88.75%	0.00%	100.00%	99.90%	90.00%	95.04%	85.62%	2.68e-5
---	Subtotal	logic		43865.00	100.00%		5.40e-4	88.75%	0.00%	100.00%	99.90%	90.00%	95.04%	85.62%	2.68e-5
clock_tree	Subpart	logic	1	10.00	100.00%		1.23e-7	0.02%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	1.23e-7
fifo_mem	Subpart	logic	1	41730.00	100.00%	fifo32_sm	5.13e-4	84.43%	0.00%	100.00%	99.90%	90.00%	99.90%	90.00%	5.13e-7
fifo_mem_control	Subpart	logic	1	2112.50	100.00%		2.60e-5	4.27%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	2.60e-5
reset_tree	Subpart	logic	1	12.50	100.00%		1.54e-7	0.03%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	1.54e-7

Refinement Through Accurate Analysis

Subpart	Protected	Faults	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
memory	Yes	9752	0%	100%	99.9%	90%
control	No	658	0%	100%	0%	n/a
clk/rst tree	No	16	0%	100%	0%	n/a
encoder-active	Yes	270	0%	100%	97%	90%
decoder-active	No	986	0%	49.6%	37.4%	0%
decoder-passive	n/a	54	7.4%	0%	n/a	20%
SPFM			**LFM**			
90.60%			76.62%			

- **Significant improvement in SPFM**
- **85.35% → 90.60%**

- **Automated fault classification - no testbench required**
- **OneSpin's**
  - **Fault Propagation Analysis (FPA) app**
  - **Fault Detection Analysis (FDA) app**

Impact of FIFO Size

FIFO has

16 entries

Subpart	Protected	Faults	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
memory	Yes	9752	0%	100%	99.9%	90%
control	No	658	0%	100%	0%	n/a
clk/rst tree	No	16	0%	100%	0%	n/a
encoder-active	Yes	270	0%	100%	97%	90%
decoder-active	No	986	0%	49.6%	37.4%	0%
decoder-passive	n/a	54	7.4%	0%	n/a	20%
SPFM			**LFM**			
90.60%			76.62%			

FIFO has

1024 entries

Subpart	Protected	Faults	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
memory	Yes	613054	0%	100%	99.9%	90%
control	No	17466	0%	100%	0%	n/a
clk/rst tree	No	20	0%	100%	0%	n/a
encoder-active	Yes	270	0%	100%	97%	90%
decoder-active	No	986	0%	49.6%	37.4%	0%
decoder-passive	n/a	54	7.4%	0%	n/a	20%
SPFM			**LFM**			
97.17%			87.45%			

- **Much bigger memory**
- **As memory is protected, SPFM and LFM increase**
- **But control subpart also gets bigger**
- **Control is unprotected**

Case Study 2: ECC Decoder (Gate-level Netlist)

- **Part of ECC SM integrated in general purpose MCU**
- **Used in automotive and other applications**
- **Input signals to disable error detection/correction**
- **Multiple diagnostic outputs**

Port	Direction	Description
eccdis	input	0: ECC SM is enabled 1: ECC SM is disabled (diagnostic outputs and possible error correction are inactive)
secdis	input	0: ECC single-error correction is enabled 1: ECC single-error correction is disabled (single-errors are still reported)
error	output	0: no error detected 1: error (single or double) detected
err_sed	output	0: no single-error detected 1: single-error detected
err_ded	output	0: no double-error detected 1: double-error detected

Impact of Configuration

- **Correction enabled**
- **Diagnostic: *err_ded***

Subpart	**Protected**	**Faults**	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
decoder-active	no	1250	0%	31%	32.4%	15,7%
decoder-passive	n/a	214	2.3%	0%	n/a	40%

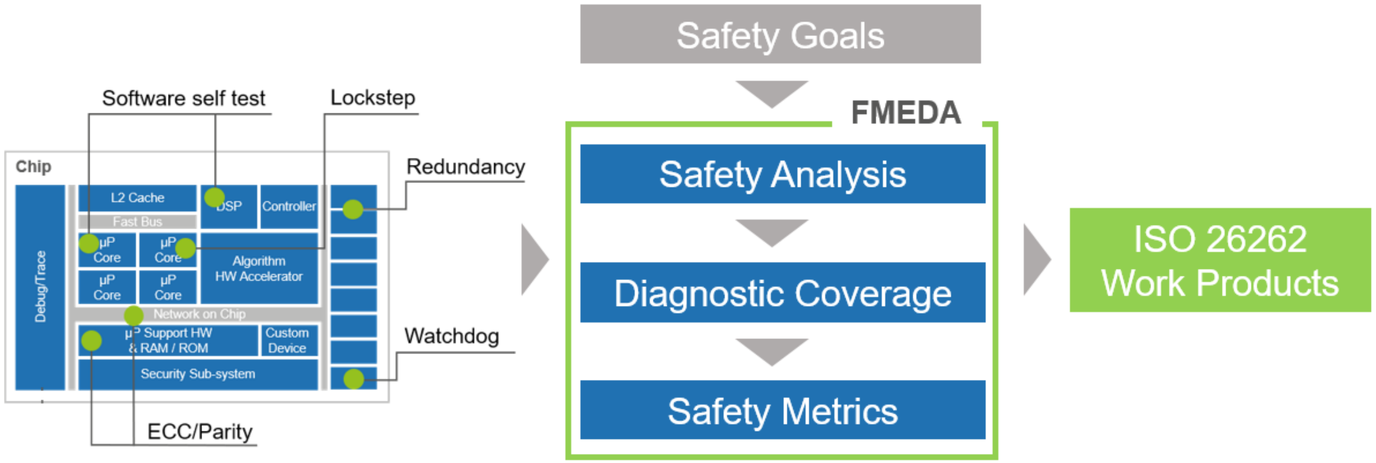
- **Correction enabled**
- **Diagnostic: *err_ded* and *err_sed***

Subpart	**Protected**	**Faults**	F_{SAFE}	F_{PVSG}	$K_{FMC,RF}$	$K_{FMC,MPF}$
decoder-active	no	1250	0%	31%	42.2%	47,7%
decoder-passive	n/a	214	2.3%	0%	n/a	89.5%

- **Much higher $K_{FMC,MPF}$ compared to the decoder subparts in previous case study**

Conclusion

- **Achieving ISO 26262 SPFM and LFM targets is challenging and time consuming**
- **Efficient and scalable FMEDA process**
  - **Divide-and-conquer approach (parts/subparts)**
  - **Easy to derive conservative diagnostic coverage and SPFM/LFM estimates**
  - **Additional fault analysis applied only where/when necessary**
  - **Reduce/eliminate need for fault simulation and testbench**



Thank you!

Questions?