YOGITECH

The One Stop Shop for Functional Safety

Workshop on Early Reliability Modeling for Aging and Variability in Silicon Systems

Panel Session

Mauro Pipponzi – fRTools director - YOGITECH

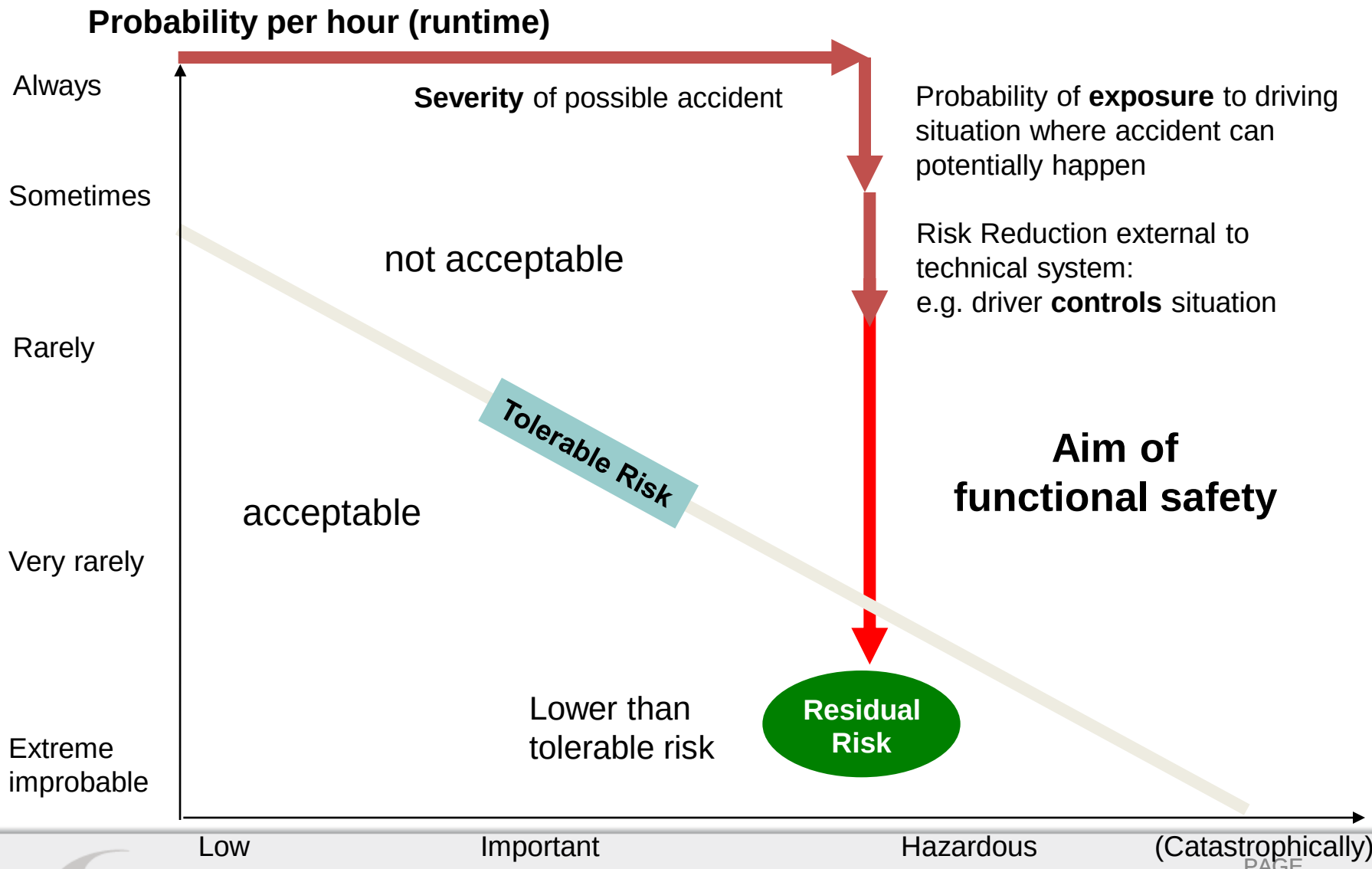
Initial Statement

- We argue that discussing which class of failures poses the most serious threat, it is not a totally well-posed problem

- The dangerousness of a fault – whatever the physical phenomenon causing it – depends from a number of factors, including the type of functionality (i.e. the use case) and the design implementation.

- Safety Standards (and ISO26262 in particular) provide a framework within which to evaluate the whole fault – error – failure chain.

Risk evaluation

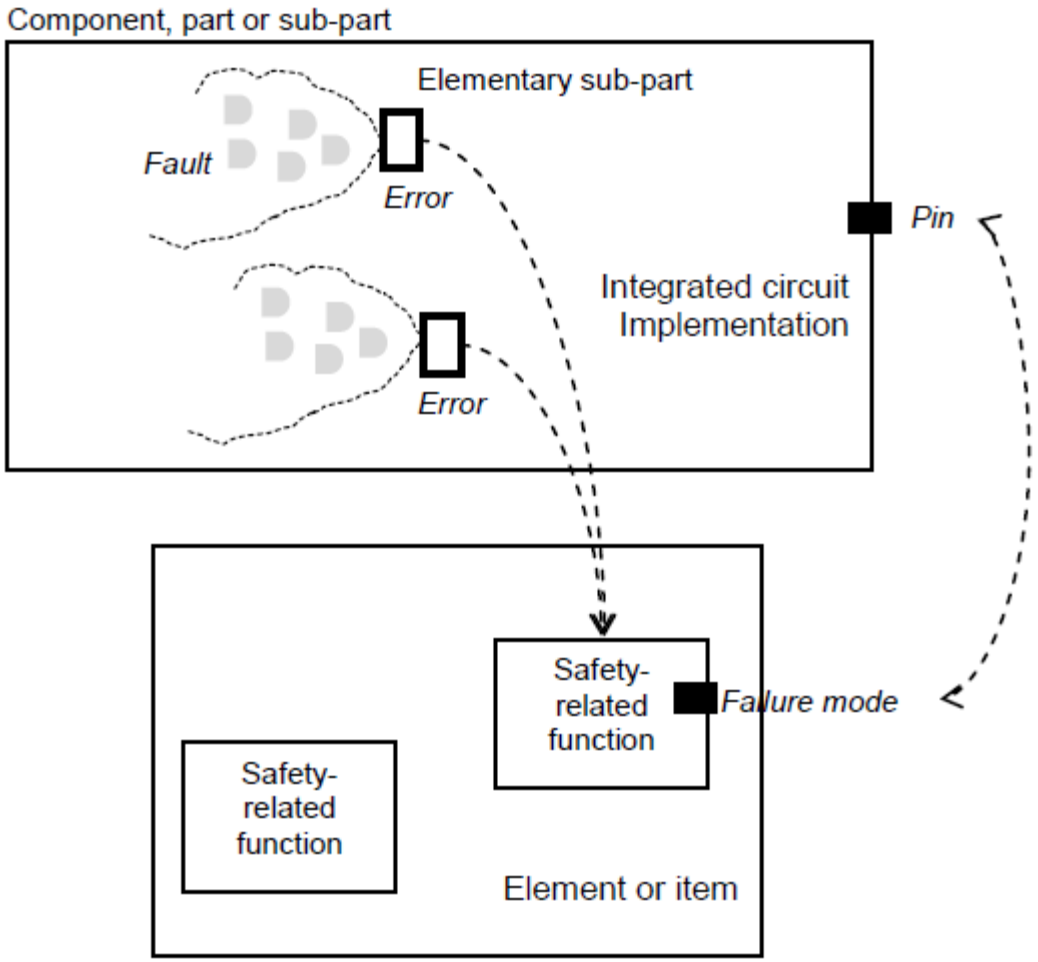


Fault Classification

- The fault classification is affected by
  - Level of risk
  - Probability of occurrence
  - Identification of the failure modes
  - Implementation

- The same fault can in principle be considered safe within one application, acceptable as residual in another, dangerous in a third

The fault must be considered in the context of the failure modes

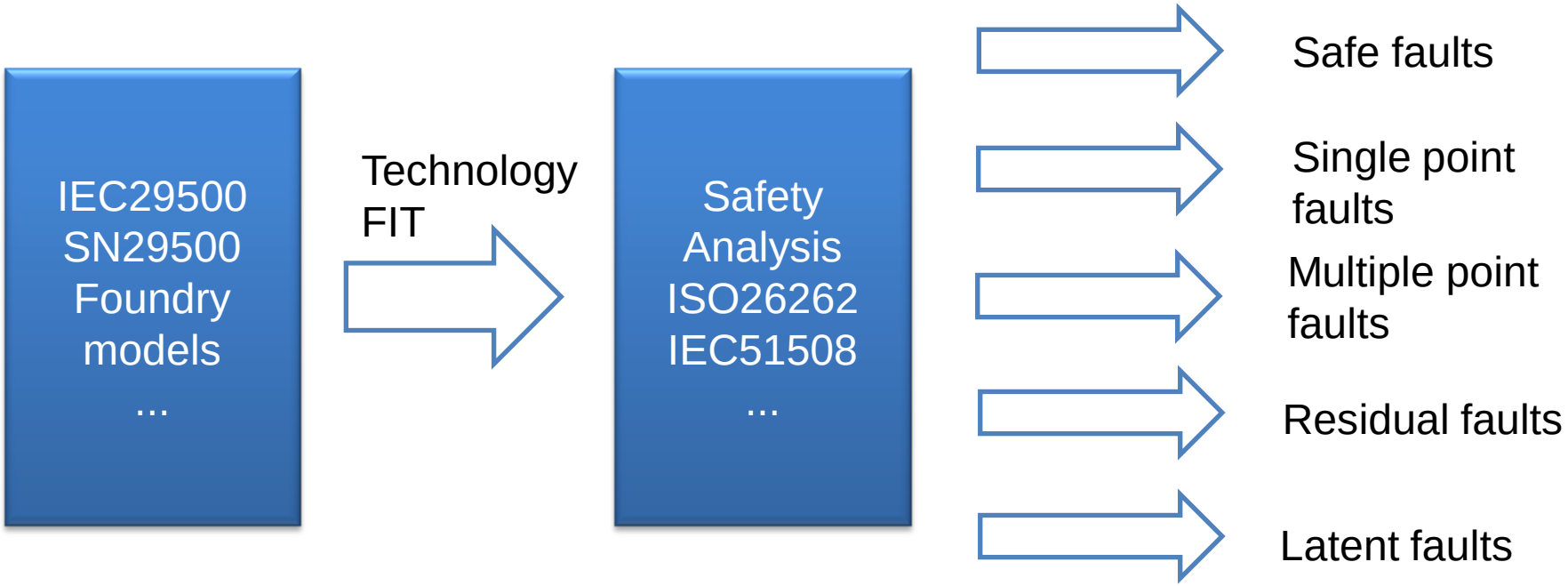


Ref. ISO26262 part 11 (2nd edition)

The functional safety view

$$\lambda_{RF} = \lambda \times \sum_{FM} \Lambda_{FM} \times (1 - F_{safe_{FM}}) \times (1 - K_{FMC,RF_{FM}})$$

- The fault model (λ) is just the first piece of the chain…..



Risk Analysis -> ASIL Classification -> reccomendations about faults

	ASIL			
	A	B	C	D
Permanent faults	No specific recommendation	Stuck-at faults[a]	Stuck-at faults[a], d.c. faults[b], additional fault models if necessary[d]	Stuck-at faults[a], d.c. faults[b], additional fault models if necessary[d]
Transient faults	No specific recommendation	Soft error model[c]	soft error model[c], additional fault models if necessary[d]	soft error model[c], additional fault models if necessary[d]

[a] See Table 30, note a).
[b] See Table 30, note b).
[c] See Table 30, note c).
[d] If necessary based on the fault model pareto or specific component or technology or the specific safety mechanism being considered.
EXAMPLE see Table 31 for additional fault models related to memories.

Ref. ISO26262 part 11 (2nd edition)

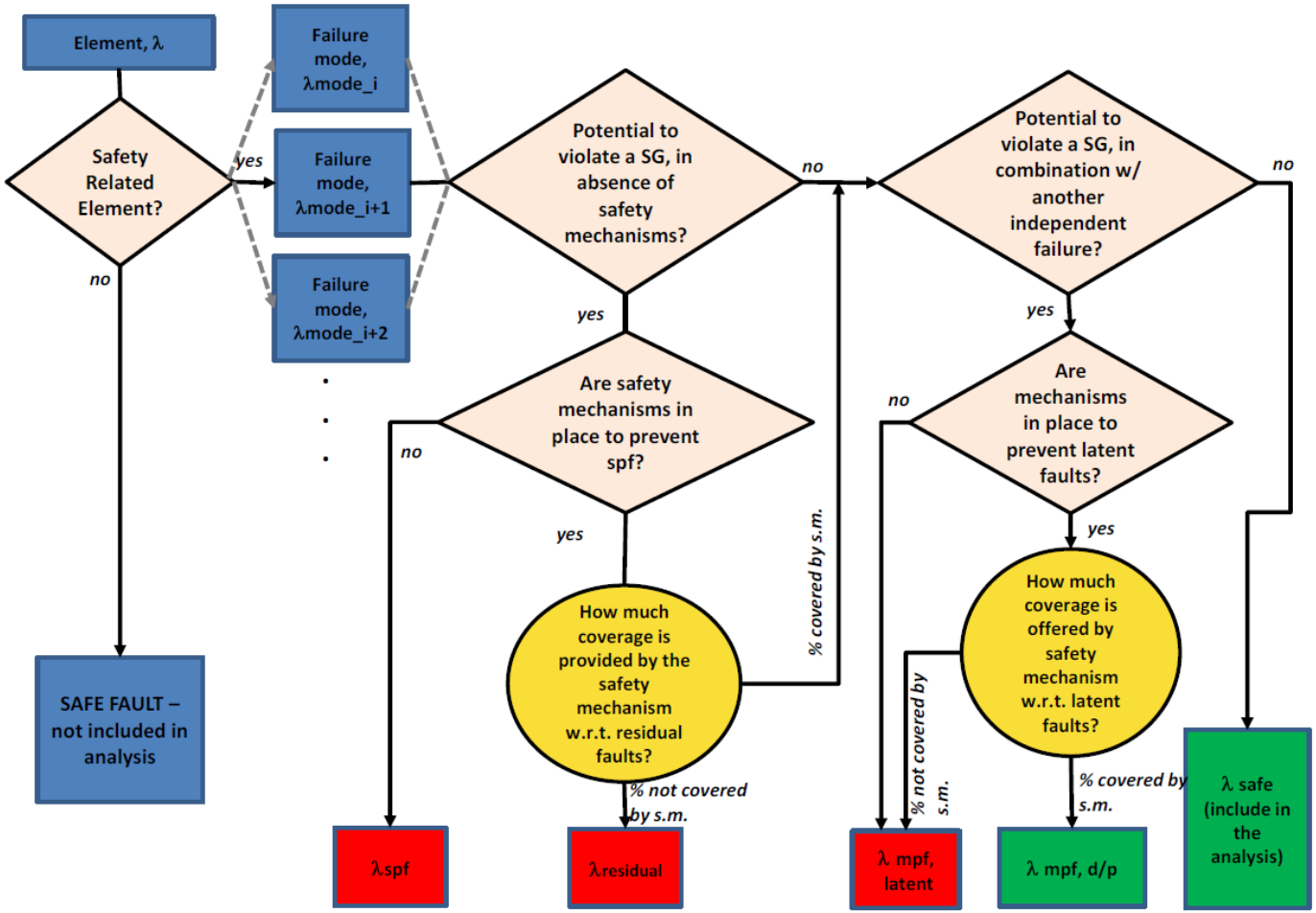
Analogue requires more sophisticated fault models and failure modes

Table 35 — Possible failure modes of analogue and mixed signal parts and sub-parts

Part / sub-part	Short description	Failure modes
Regulators and Power stages		
Voltage regulators (linear, SMPS, etc.)	HW part/sub-part that maintains the voltage of a power source within a prescribed range that can be tolerated by elements using that voltage.	Output voltage higher than a high threshold of the prescribed range (i.e. over voltage – OV) Output voltage lower than a low threshold of the prescribed range (i.e. under voltage – UV) Output voltage affected by spikes[b] Incorrect start-up time (i.e. outside the expected range) Output voltage accuracy too low, including drift[c] Output voltage oscillation[a] within the prescribed range Output voltage affected by a fast oscillation[a] outside the prescribed range but with average value within the prescribed range Quiescent current (i.e. current drawn by the regulator in order to control its internal circuitry for proper operation) exceeding the maximum value
Charge pump, regulator boost	HW part/sub-part that converts, and optionally regulates, voltages using switching technology and capacitive-energy storage elements, and maintains a constant output voltage with a varying voltage input.	Output voltage higher than a high threshold of the prescribed range (i.e. over voltage – OV) Output voltage lower than a low threshold of the prescribed range (i.e. under voltage – UV) Output voltage affected by spikes[b] Incorrect start-up time (i.e. outside the expected range) Quiescent current (i.e. current drawn by the regulator in order to control its internal circuitry for proper operation) exceeding the maximum value

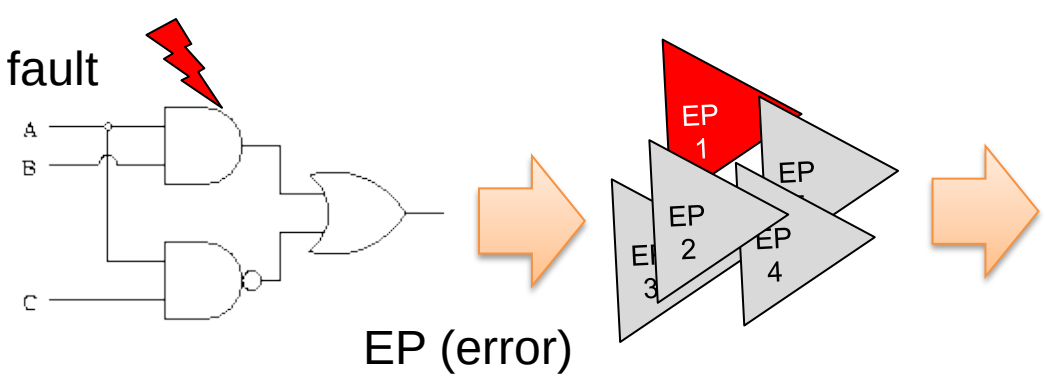
Ref. ISO26262 part 11 (2nd edition)

The Framework for Fault Classification in ISO26262



Ref. ISO26262 part 5 (2nd edition)

The Failure Mode Distribution Drives the Analysis



ISO Summary | IEC Summary | Design | Sub Design List | EP List | MC List | FMEDA List | SVP | SMA List | Associations | Failure Modes | Safety Mechanisms | Settings | Failure Rate

Id	FM Id	FM Name	Target	# Associations	FMD%	Fsafe	Krf	Klat	Fsafe(ba)	Krf(ba)	Klat(ba)	λSR	λsafe	λns	λSPF	λMPF	λRF	λMPF,D	λMPF,L	SPFm	LFm	Comment
FMEDA2	FM_C-17	I2C - Registers	DATA_PATH, REGIF(non-VBUSP)	135	39.11%	0.00%	0.0...	0.00%				1.253E-02	0.0	1.253...	1.253E-02	0.0	0.0	0.0	0.0	0.00%		
FMEDA4	FM_C-19	I2C - Control/Status	REGIF,PINCTRL	130	36.77%	0.00%	0.0...	0.00%				1.178E-02	0.0	1.178...	1.178E-02	0.0	0.0	0.0	0.0	0.00%		
FMEDA3	FM_C-16	I2C - Serial Interface	MASTER_FSM,SLAVE_FSM	48	16.30%	0.00%	0.0...	0.00%				5.224E-03	0.0	5.224...	5.224E-03	0.0	0.0	0.0	0.0	0.00%		
FMEDA5	FM_C-18	I2C - VBUSP interface	REGIF(VBUSP)	15	4.85%	0.00%	0.0...	0.00%				1.555E-03	0.0	1.555...	1.555E-03	0.0	0.0	0.0	0.0	0.00%		
FMEDA1	FM_C-20	I2C - Clock Generator	PRSC	5	2.97%	0.00%	0.0...	0.00%				9.521E-04	0.0	9.521...	9.521E-04	0.0	0.0	0.0	0.0	0.00%		

Thank you!

Mauro Pipponzi
Director - fRTools

Via Lenin 132/P Loc. San Martino Ulmiano
56017 San Giuliano Terme, (PI)
Italy
Tel: +39 050 86351
Fax: +39 050 861870
contactus@yogitech.com
www.yogitech.com