YOGITECH

Combining Early Reliability Evaluation with functional safety requirements: a tool suite for safety design and verification

Francesco Sforza – YOGITECH SPA – IOLTS 2014

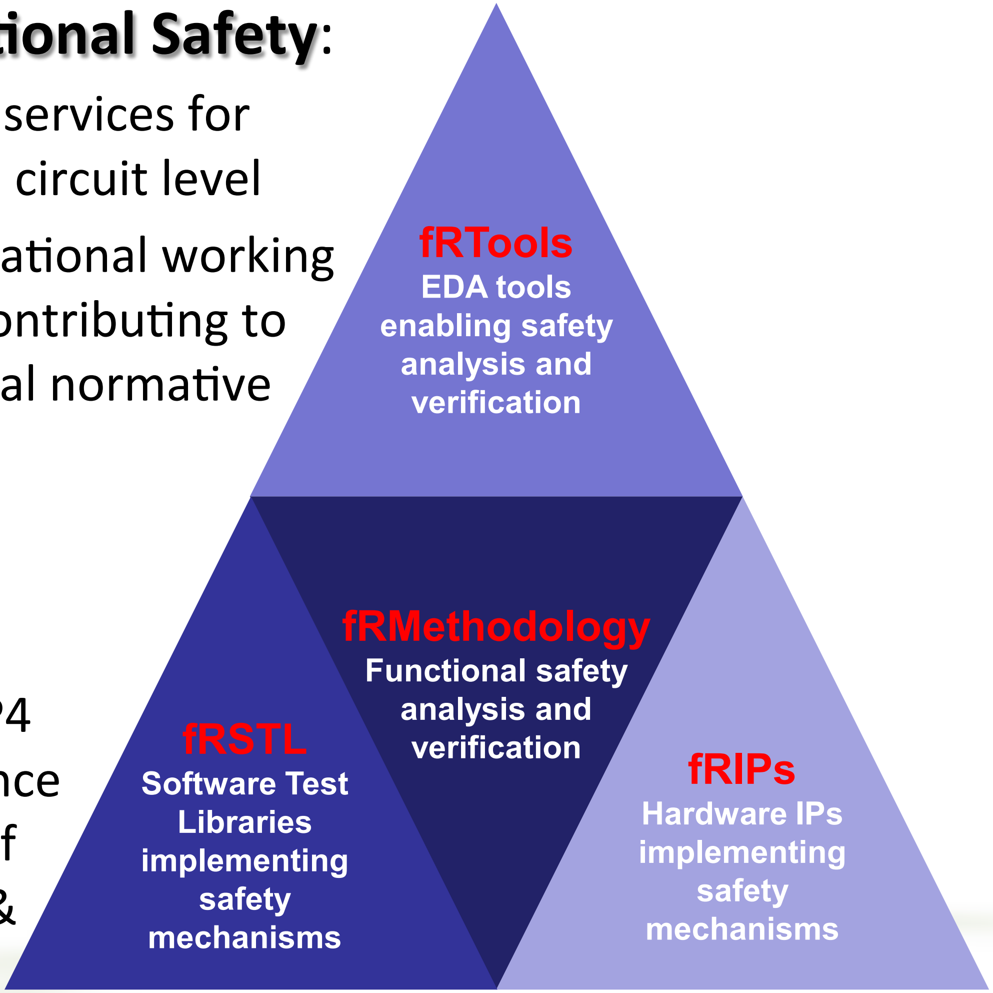
Outline

- About ***Yogitech***
- The ***fault*****Robust** Methodology
- Failure Evaluation
- ***fRTool*** Suites
- Standards vs ***f*****R**Methodology
- Summary

About YOGITECH

- The one-stop-shop for **Functional Safety**:
  - lead provider of products and services for functional safety at integrated circuit level
  - actively participating to international working groups and committees and contributing to the preparation of international normative

- YOGITECH in CLERECO
  - supporting WP2, WP3 and WP4 activities through our experience on tools for characterization of functional safety for systems & components



fRTools
EDA tools enabling safety analysis and verification

fRMethodology
Functional safety analysis and verification

fRSTL
Software Test Libraries implementing safety mechanisms

fRIPs
Hardware IPs implementing safety mechanisms

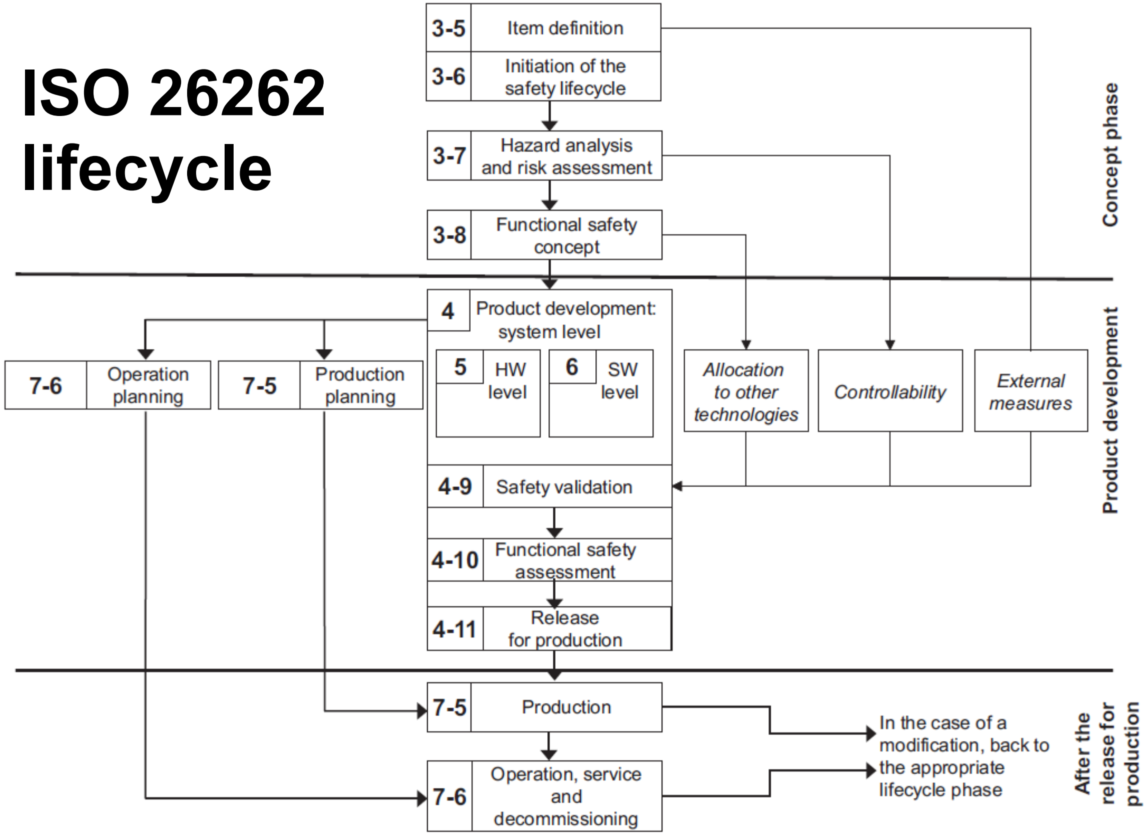
Outline

- About ***Yogitech***
- The ***fault*Robust** Methodology
- Failure Evaluation
- ***fRTool*** Suites
- Standards vs ***f*R**Methodology
- Summary

Requirements from safety standards

- Functional safety standards define a complete “lifecycle”, from concept level to production and operation

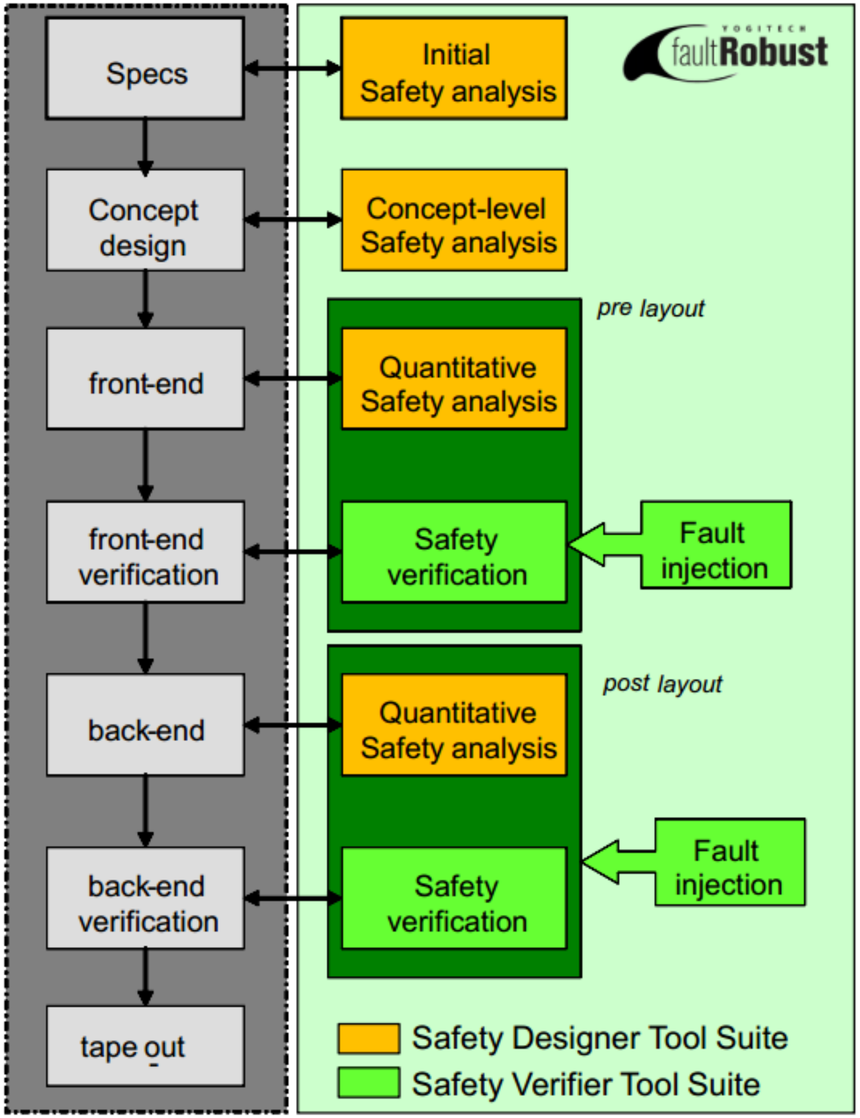
ISO 26262 lifecycle


3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
Concept phase
4 Product development: system level
5 HW level
6 SW level
Allocation to other technologies
Controllability
External measures
7-6 Operation planning
7-5 Production planning
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
Product development
7-5 Production
7-6 Operation, service and decommissioning
In the case of a modification, back to the appropriate lifecycle phase
After the release for production

- Safety lifecycle requires both ***evaluation*** of potential violation of safety goal (e.g. FMEDA) and ***verification*** (e.g. by means of fault insertion)

- With the increasing complexity of new components and applications (e.g. ADAS), **evaluation has a key role in focusing the verification step** – that otherwise would become quickly unaffordable

fRMethodology flow



Specs

Concept design

front-end

front-end verification

back-end

back-end verification

tape out

Initial Safety analysis

Concept-level Safety analysis

pre layout

Quantitative Safety analysis

Safety verification

Fault injection

post layout

Quantitative Safety analysis

Safety verification

Fault injection

faultRobust

🟧 Safety Designer Tool Suite

🟩 Safety Verifier Tool Suite

Key ISO 26262 requirements covered by fRMethodology

- ☑ Review of Functional Safety Management / Process Safety Audit (ISO 26262-2 and -10)
- ☑ Definition of assumed safety requirements with respect to Functional (ISO 26262-3) and Technical (ISO 26262-4) safety concepts
- ☑ Specification / review of HW safety requirements, HW design and HW-SW interface (ISO 26262-5)
- ☑ Computation of the failure rates, preparation / review of FMEA, DFMEA, FMEDA, FTA (ISO 26262-5, -10)
- ☑ Evaluation of HW architectural metrics and safety goal violations due to random HW failures, including providing suggestions & solutions about how to cover the gaps, if any (ISO 26262-5, -10)
- ☑ Preparation / review of Verification and Validation plan (ISO 26262-4, -5, -8)
- ☑ Verification and validation of effectiveness of safety mechanisms, including fault injection (ISO 26262-4 and ISO 26262-5)
- ☑ Specification / review of SW safety requirements with respect to FW and SW units (ISO 26262-6)
- ☑ Review of SW tools confidence in use (ISO 26262-8)
- ☑ Review of ASIL decomposition, FFI and DFA analyses (ISO 26262-9)
- ☑ Review of degree of fulfillment of IC specific recommendations, IC Safety Manual (ISO 26262-10)

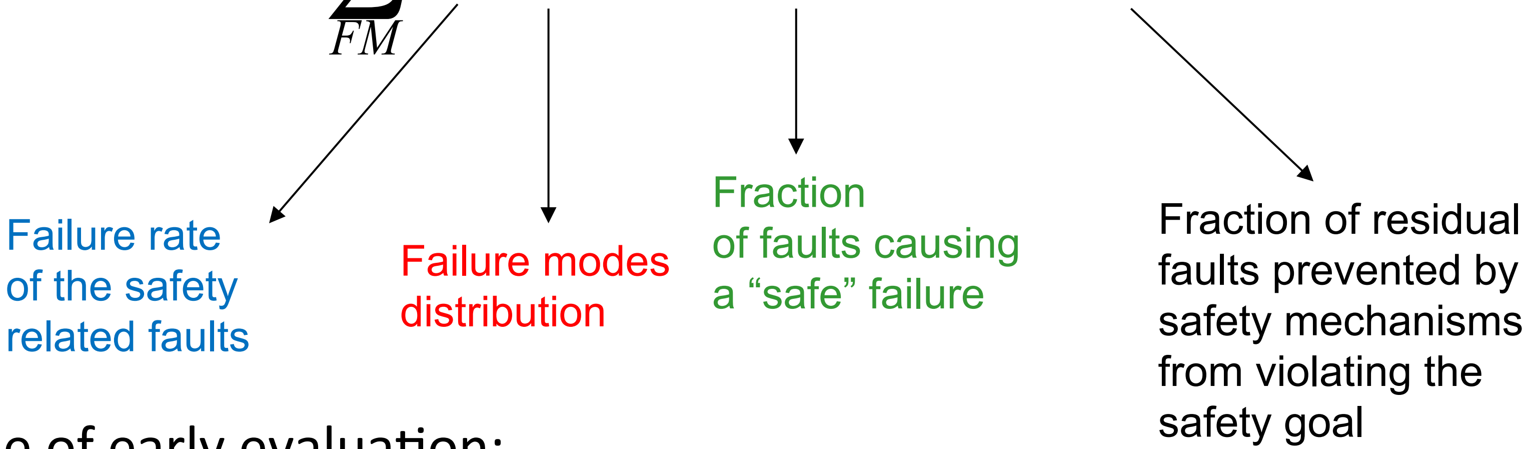
Outline

- About ***Yogitech***
- The ***fault*Robust** Methodology
- Failure Evaluation
- ***fRTool*** Suites
- Standards vs ***fR***Methodology
- Summary

HW random failures evaluation

- In functional safety standards, evaluation of probability of HW random failures can be summarized by a simple formula:

$$\lambda_{DU} = \sum_{FM} \lambda \times \Lambda \times (1 - S) \times (1 - DC)$$



Failure rate of the safety related faults

Failure modes distribution

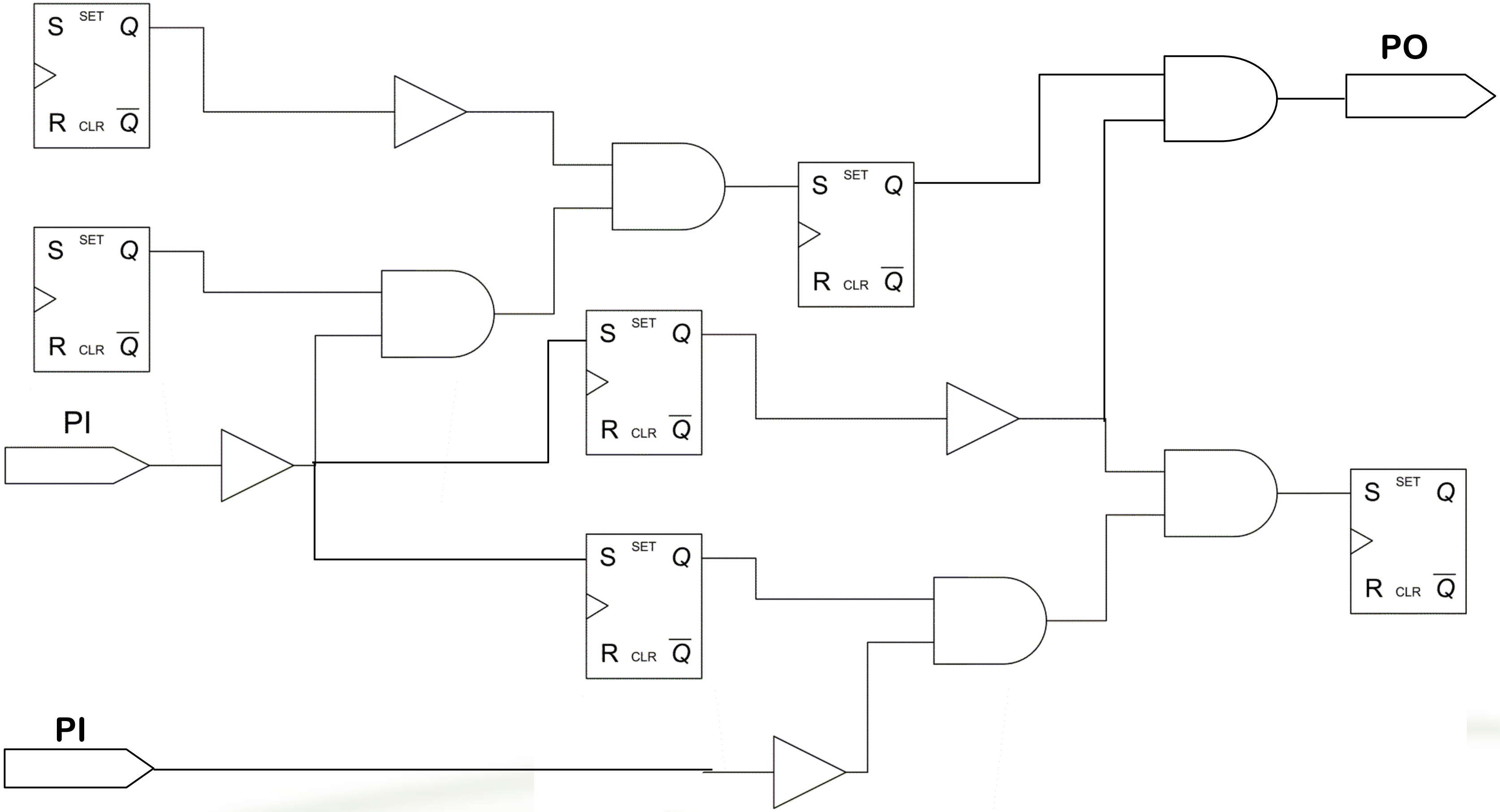
Fraction of faults causing a “safe” failure

Fraction of residual faults prevented by safety mechanisms from violating the safety goal

- Role of early evaluation:
  - provide accurate estimations of λ and Λ
  - provide estimations of S and DC, to be verified with fault injection
- Estimation of Λ is one of the most difficult challenges
  - next slides describe our current approach and highlight improvement areas

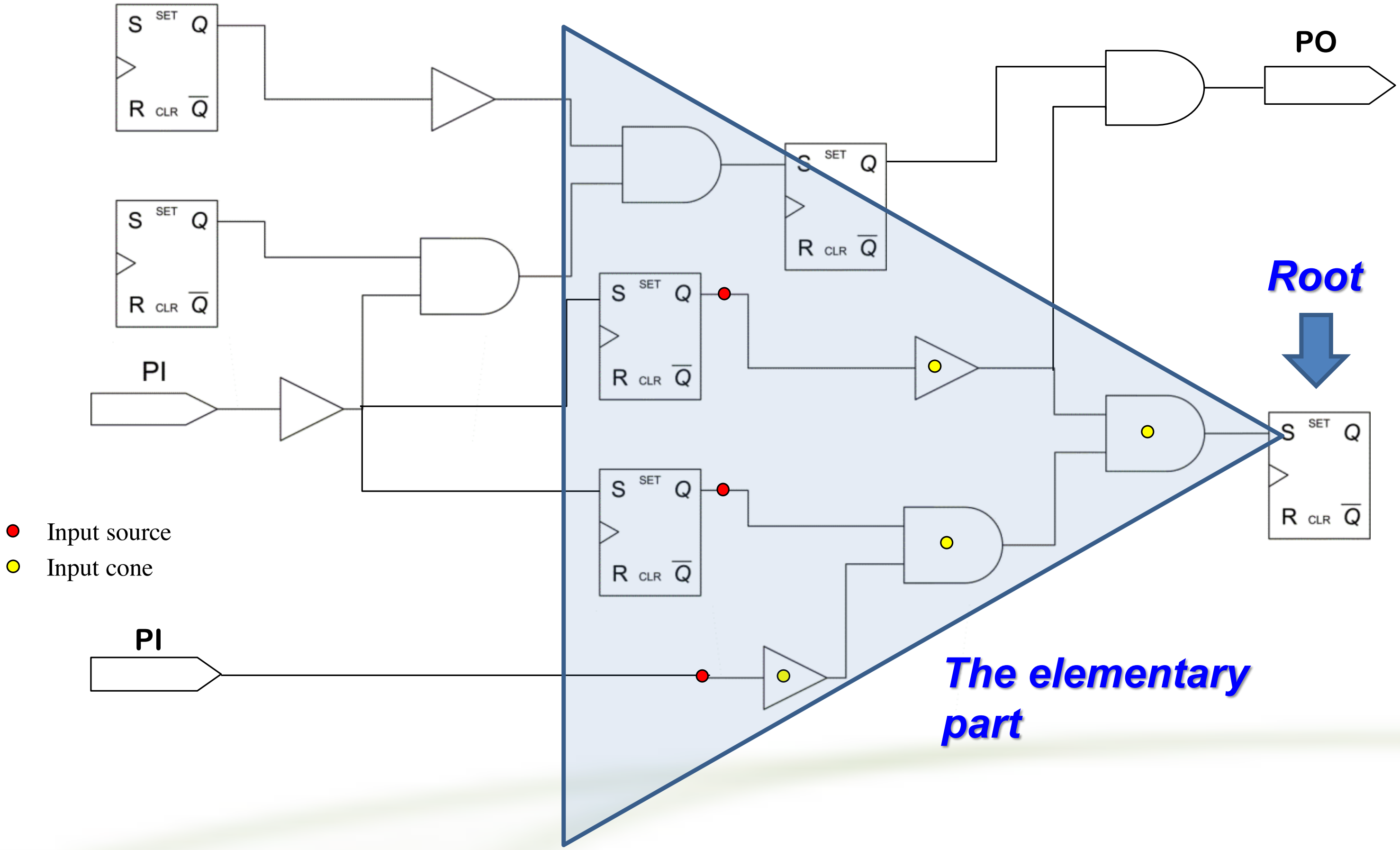
About early evaluation of Λ (0/3)

- Suppose you have some design …



About early evaluation of Λ (1/3)

- Starting point for early evaluation of Λ is to partition the design into “elementary parts” (EP)



Root

The elementary part

About early evaluation of Λ (2/3)

- For each EP, we automatically extract from the design the following information:

1. Elementary Part name

Name associated to the cone

(typically the cone ***Root*** name)

2. Input Cone Area (CAR)

Area of the logic belonging

to the cone (🟡)

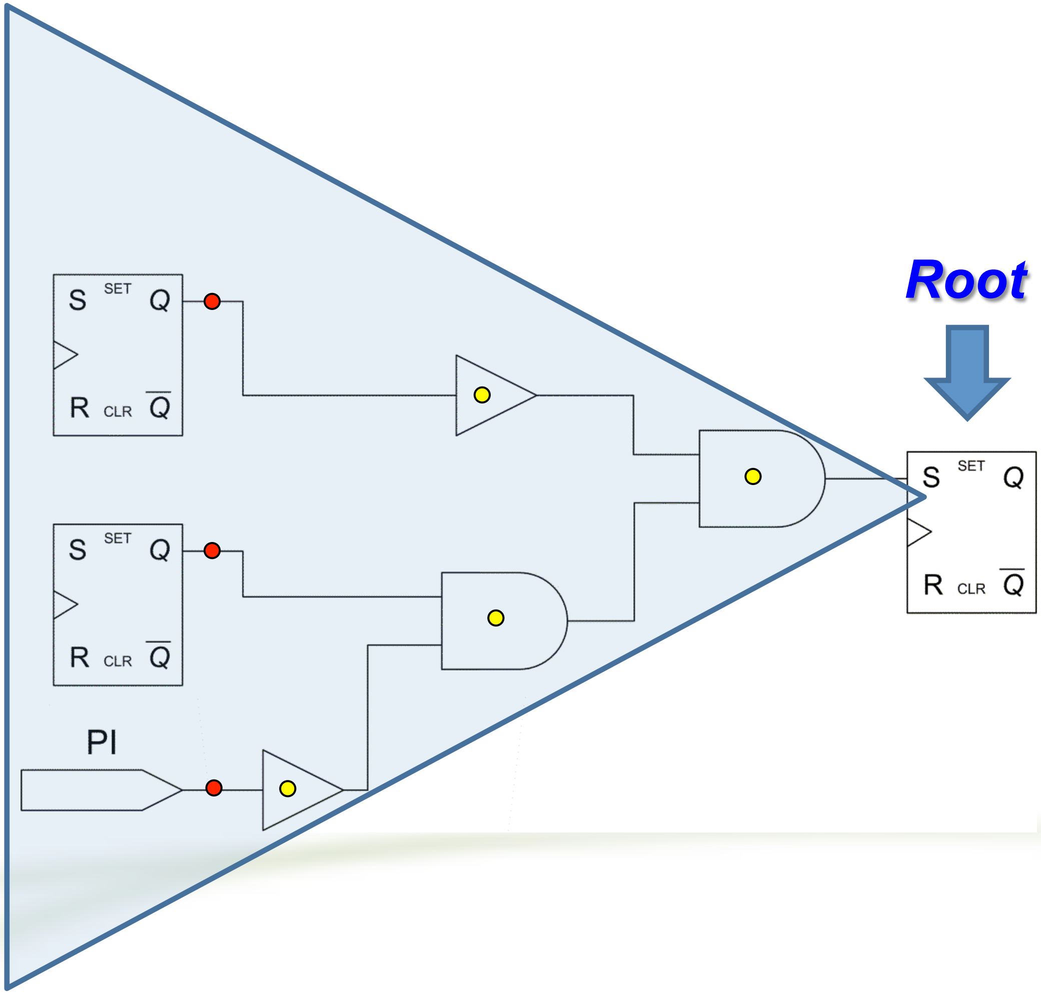
3. Number Sinks

Flip-Flops or Outs

4. Number of Sources

Number of the sources or

Primary Input in the cone (🔴)



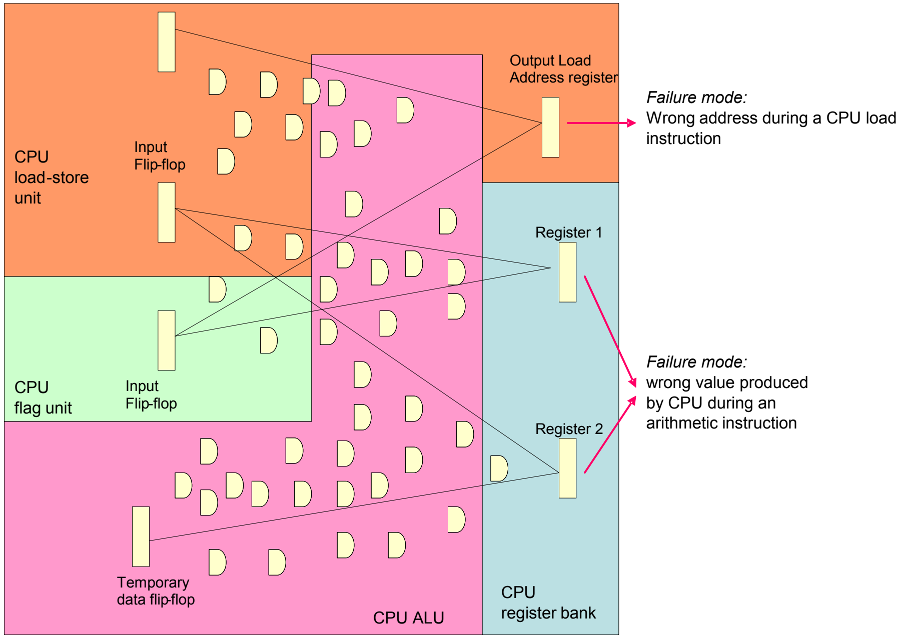
About early evaluation of Λ (3/3)

- Based on:
  a) EP information and
  b) connection between EP and FM

  we estimate the value of Λ

- At present, connection between EP and FM is done:
  - manually or
  - based on hierarchy information

- Current challenge (that we are exploring within CLERECO) is to automatize as much as possible the EP-FM connection



Failure mode: Wrong address during a CPU load instruction

Failure mode: wrong value produced by CPU during an arithmetic instruction

EP	FM	CAR	Λ
Output Load Address Register	Wrong address location during CPU load instruction	44	**44/131 = 33,6%**
Register 1	Wrong value produced by CPU during an arithmetic instruction	38	**(38+49)/131 = 66,4%**
Register 2		49	
	total	**131**	

Outline

- About ***Yogitech***
- The ***fault*Robust** Methodology
- Failure Evaluation
- ***fRTool*** Suites
- Standards vs ***f*R**Methodology
- Summary

YOGITECH *fRTools*

Yogitech's fRTool Suites comprise ...

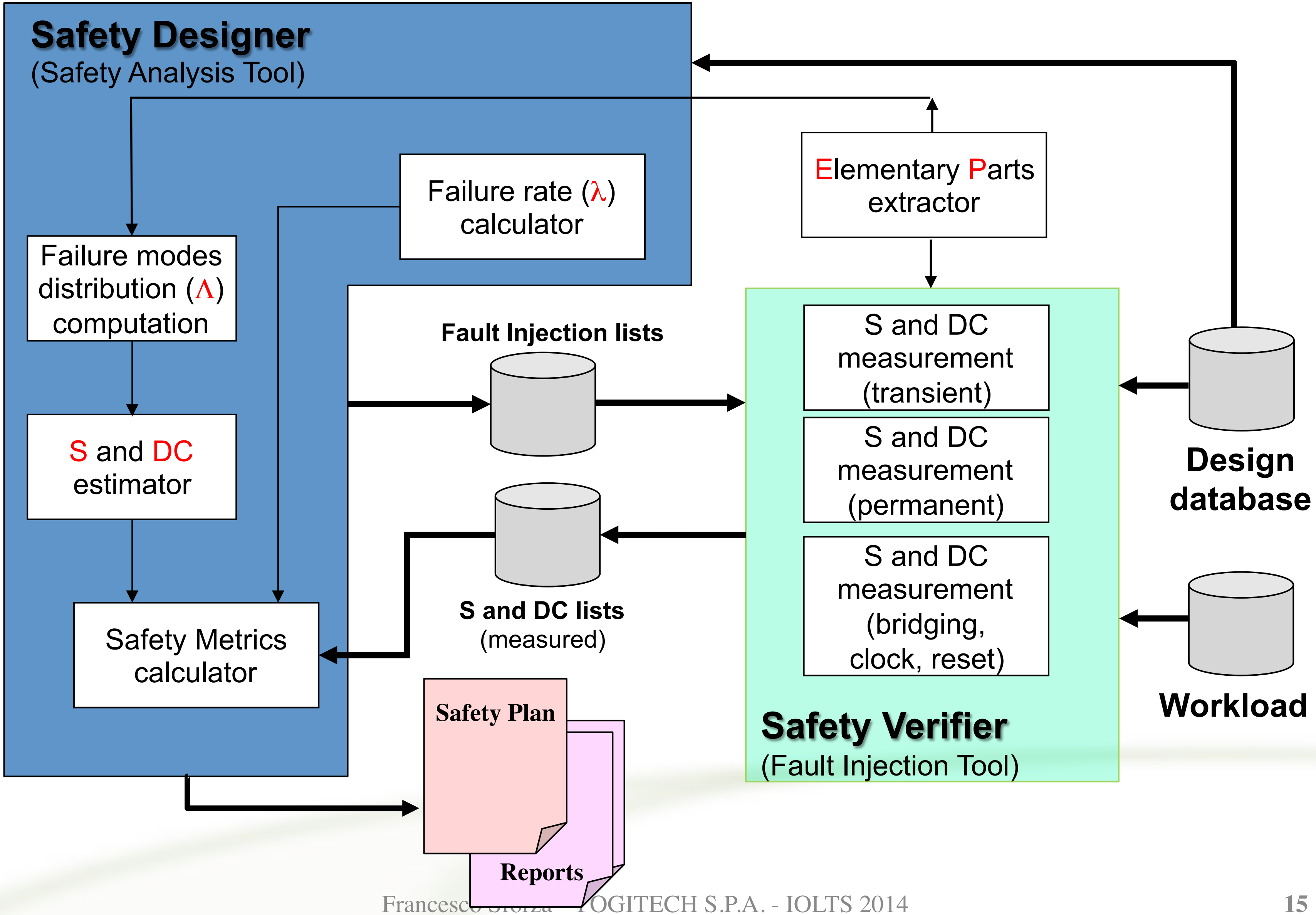
Early Evaluation

- ***Safety Designer tool Suite***:
  - Drives the analysis
  - Elaborates (primary) input data:
    - Design files, Libraries, Technology data, Failure Rates, ...
  - Provides intermediate and final results:
    - Safety metrics estimation and calculation, fault injection lists, Safety Reports, ...

Verification

- ***Safety Verifier tool Suite :***
  - Performs the actual ***fault injection*** so to generate «*real*» (simulation-derived) raw data to be compared against estimated data
  - Uses a 3rd party fault simulator
  - Limited report-generation capabilities

fRTools overview



Safety Designer
(Safety Analysis Tool)

Failure rate (λ) calculator

Failure modes distribution (Λ) computation

S and DC estimator

Safety Metrics calculator

Elementary Parts extractor

Fault Injection lists

S and DC lists
(measured)

S and DC measurement (transient)

S and DC measurement (permanent)

S and DC measurement (bridging, clock, reset)

Safety Verifier
(Fault Injection Tool)

Design database

Workload

Safety Plan

Reports

Safety Designer Main Features

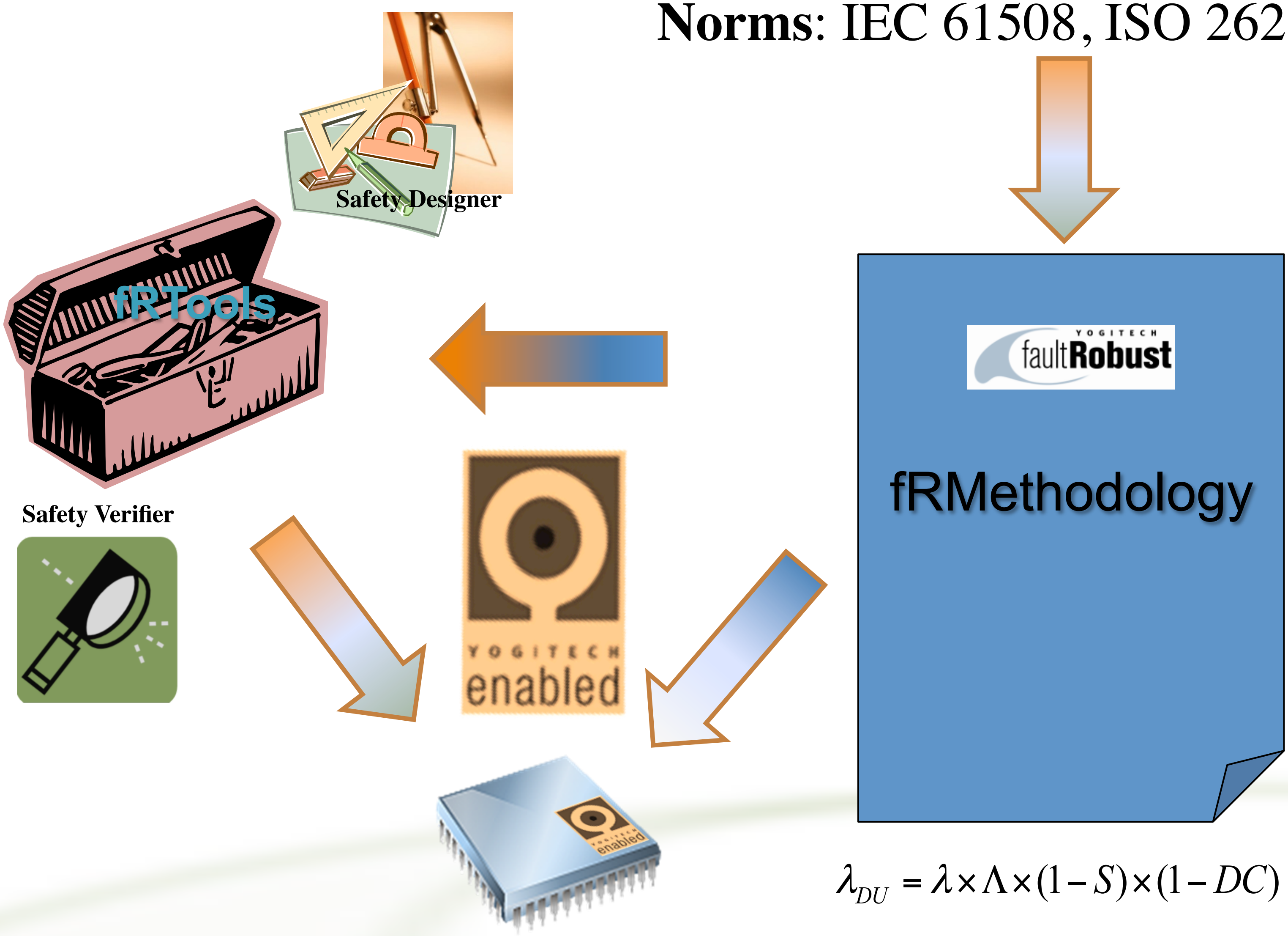
- Design – Elementary Parts representation
- Fault models: Permanent, Transient, Special
- Failure Modes and Safety Mechanisms: built-in and user-defined
- Failure rates computation
- Failure Mode - Elementary Part Association (many to many)
- Operation modes: Estimation, Back-annotation
  - S and DC estimation/computation
  - Safety Metrics computation
- Fault Injection Plan generation: “where” and “how much” to inject
  - Preliminary
  - Refinements (based on fault infos)
- Fault lists generation
- FMEDA
  - High-Level (qualitative)
  - Detailed
- Export (of FMEDA) analysis results

Outline

- About ***Yogitech***
- The ***fault*Robust** Methodology
- Failure Evaluation
- ***fRTool*** Suites
- Standards vs ***f*R**Methodology
- Summary

Standards vs. fRMethodology & fRTools

Norms: IEC 61508, ISO 26262



Safety Designer

fRTools

Safety Verifier

YOGITECH faultRobust

fRMethodology

YOGITECH enabled

$$\lambda_{DU} = \lambda \times \Lambda \times (1-S) \times (1-DC)$$

Summary

- Functional safety standards **mandate** a combination of **early evaluation** and **verification** of reliability & safety
  - YOGITECH has a set of tools (***fRTools***) used in functional safety for years
- <u>Evaluation</u> by itself cannot be the solution, <u>verification</u> will be always required
  - However, evaluation has a key role in focusing the verification on the most critical points, so to reduce the verification effort – especially for the new very complex designs and applications
- There are several challenges in early evaluation
  - the most critical one is <u>how to combine circuit information with function/ application information</u> (e.g. to automatically link EPs to FMs)
- Within CLERECO we are working to address those challenges…..
  - …**YOGITECH** goal is to integrate **CLERECO** results in the roadmap of fRTools

Thank you for your attention
QUESTIONS ?

YOGITECH

Via Lenin 132/P
56017 San Giuliano Terme
loc. San Martino Ulmiano (PI) - ITALY

TEL: +39 050.86351

www.yogitech.com
contactus@yogitech.com