Next-Generation Automotive Functional-Safety™

Revitalizing Automotive Safety Hard and Soft Error Approaches

Presented as tutorial at DVCon 29, 30 Oct 2019, Munich

www.optima-da.com

Nael Qudsi nael@optima-da.com

Ayman Mouallem ayman@optima-da.com

Agenda

- About Optima
- New challenges in semiconductor land: ISO-26262
- Challenges and solutions for Hard-Errors
- The Optima-Medini/Ansys integration
- Optima-SA™ - for early structural Analysis and fault-model sizing
    - Optima-SA demo
- Optima-HE™ - Hard-Error or permanent faults analysis
    - Optima-HE demo
- Soft-error or transient faults – problem definition
- Optima-SE™ - Soft-error analysis solution
    - Optima-SE demo

Optima Design Automation

OPTIMA

Next-Generation
Automotive Functional Safety

Founded 2014   Nazareth, Israel

- Portfolio of advanced solutions for complex safety scenarios
  - Key challenges addressed with automated, effective safety apps
- Revolutionary, high-performance fault simulation technology
  - Radical, new algorithms drive 1,000X performance improvement
- CoverageMaximizer™ Technology
  - For manual and automated diagnostic Coverage closure
- Well funded* core team of verification & safety experts
  - Substantial EU funding has enabled a world-leading expert team

Optima-SE™
Soft Error Simulation and Selective Hardening

Automated FIT rate reduction to enable ASIL-D with minimal silicon cost

Optima-HE™
Hard Error Coverage Measurement & Boosting

Rapid fault coverage measurement with automated coverage boosting

Optima-SA™
Structural Analysis Solution

Provide accurate FMEDA, for safety setup alternatives size calculation

Optima Fault Injection Engine™ (FIE) Technology Platform: 1,000x faster than competing solutions

*This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 850104.

New Challenges in Semiconductor Land: ISO-26262

Hard-errors: Different Safety Mechanism methodologies

Logic-BIST

Stop the unit, perform

Logic-BIST test on it

Reset it

Put it back in operation

Suitable if you have redundant cores and can stop one or a few of them for testing

STL SW Test Lib

Dedicated STL process that reads and writes to CPU register to check it's lack of permanent-fault

Suitable for CPU designs only, some IP vendors provide it with the CPU IP

Lockstep

Duplicate the IP twice

Both get same inputs

Compare outputs at each cycle

Suitable for mostly for CPUs

But can be used for other designs

Other Methods

Parity bits

ECC, CRC

Hand crafted methods

Watchdog

Etc.

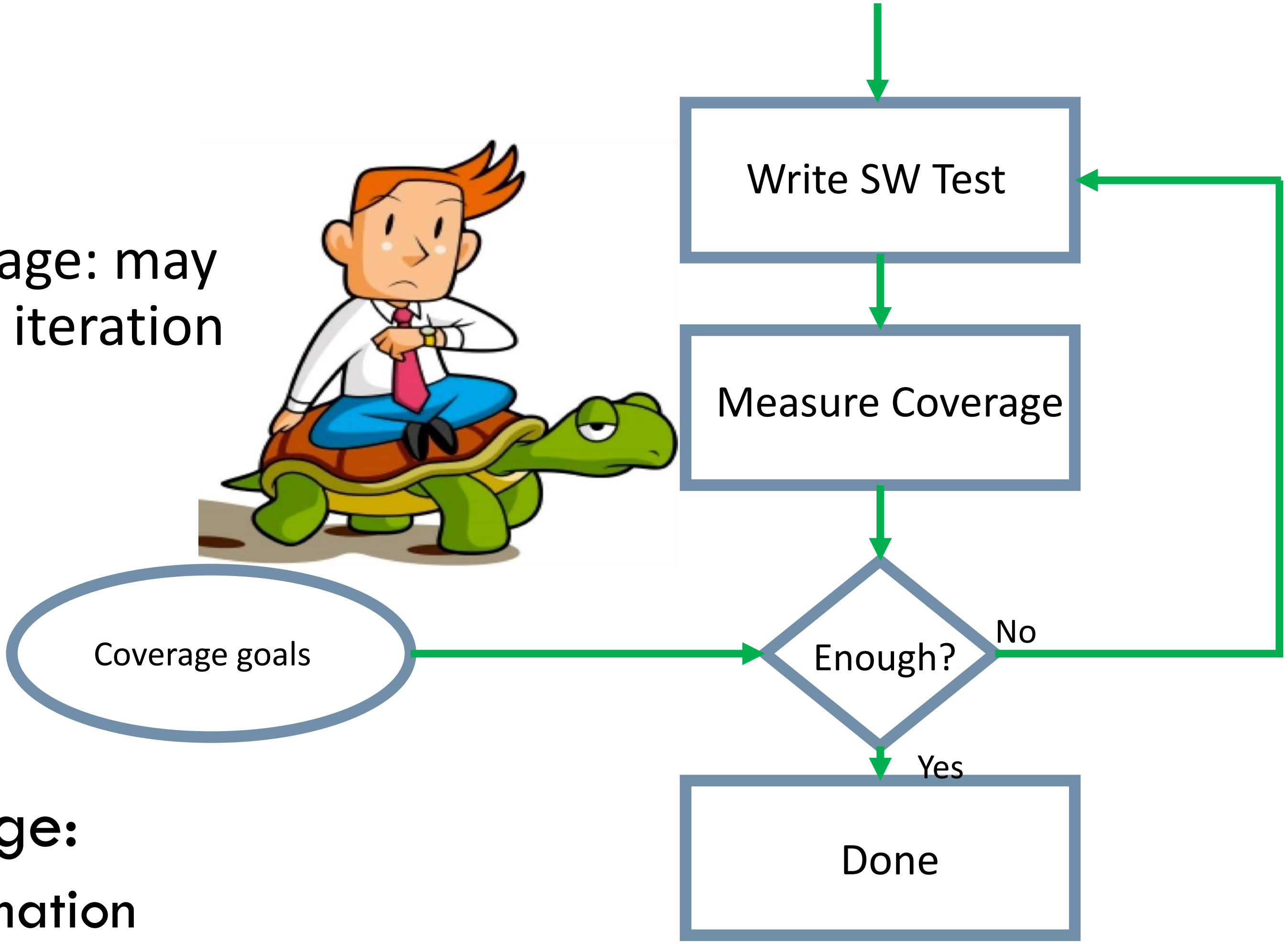
Hard-errors: Measuring SM Coverage

- Whatever the methodology used for a given unit
- Need to measure the Safety Mechanism coverage
  - Perform fault-simulation on all pins of all gates
  - Measure if the SM can detect this fault or not
  - Run all needed fault models
    - Stuck-at-0
    - Stuck-at-1
    - Bridging-fault
    - Etc.
- Need to be done on gate-level
- The task is immense, given the number of gates in the chip X time-per-fault-sim

The General Work-Flow (without Optima)

Challenges:

- Measure coverage: may take weeks per iteration



Write SW Test

Measure Coverage

Coverage goals

Enough?

No

Yes

Done

Challenges:

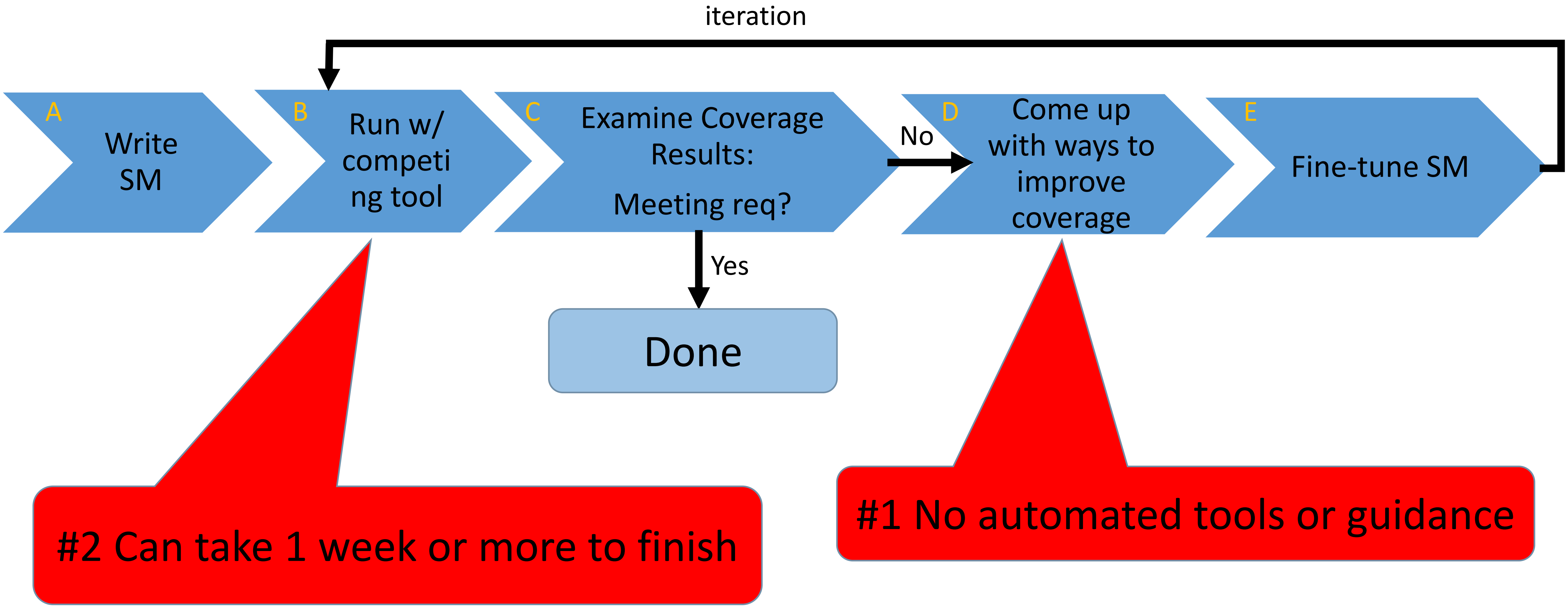
- Lack of visibility to improve coverage

  => very manual process

General challenge:

- Lack of automation

Challenges:


iteration
A
Write SM
B
Run w/ competi ng tool
C
Examine Coverage Results:
Meeting req?
No
D
Come up with ways to improve coverage
E
Fine-tune SM
Yes
Done
#2 Can take 1 week or more to finish
#1 No automated tools or guidance

Challenge 1: Reaching Coverage goal can be very manual and human-resource intensive

- No automated way to improve coverage
- No guidance and information to improve coverage
- No easy way to browse coverage results

- **Optima is changing this with CoverageMaximizer™**

Challenge 2: Run-time to measure SM coverage could become hundreds of compute years problem

- Need to be done at gate-level
- Each gate in the design need to be simulates 2..3 times (for each fault-model)

10 Million gates x 2 x 5 min = 100 million min

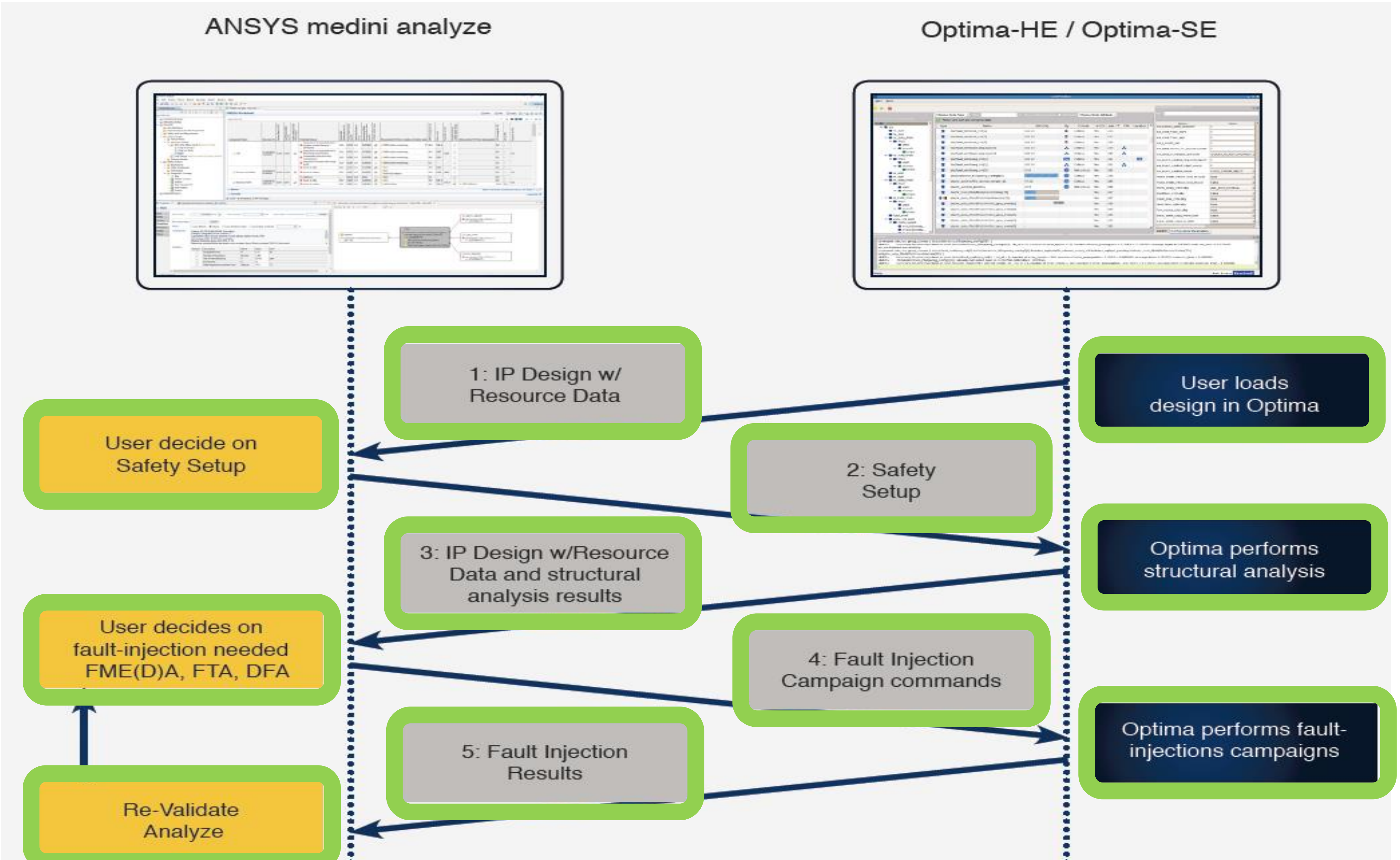
(before fault-pruning reduction)

~190 machine years

- **Optima is changing this with**
  - **Optima’s fault-simulations are over 1,000x faster than competing solutions**

Optima-Ansys flow

Optima Medini Ansys integration



ANSYS medini analyze

Optima-HE / Optima-SE

User loads design in Optima

1: IP Design w/ Resource Data

User decide on Safety Setup

2: Safety Setup

Optima performs structural analysis

3: IP Design w/Resource Data and structural analysis results

User decides on fault-injection needed FME(D)A, FTA, DFA

4: Fault Injection Campaign commands

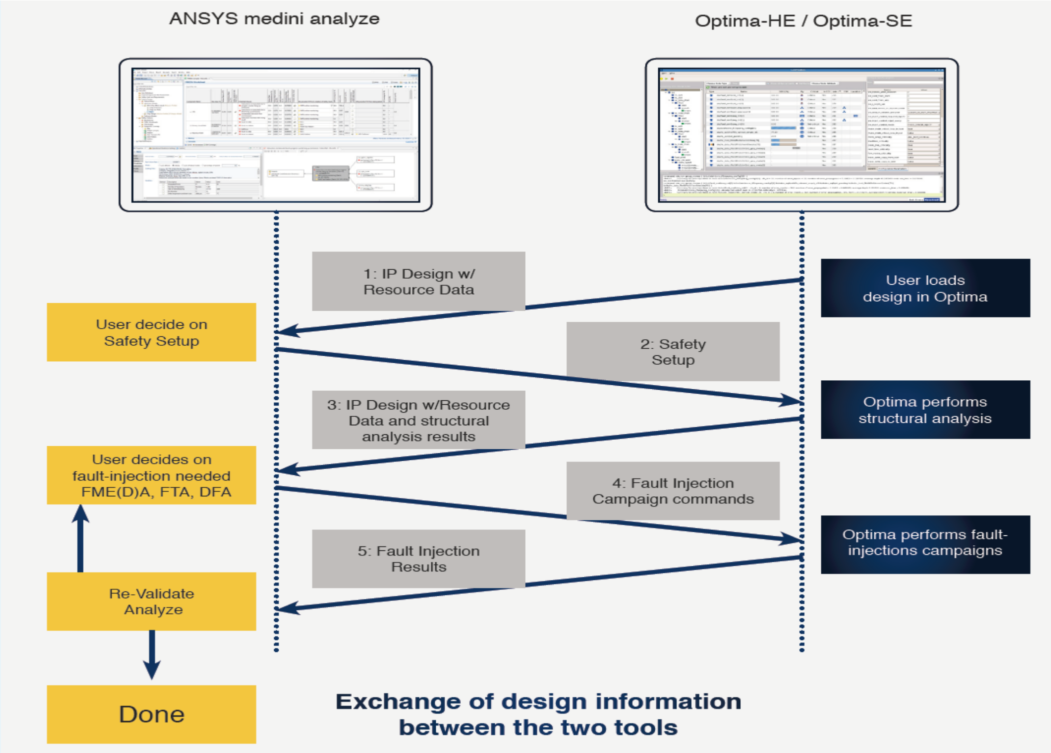
Optima performs fault-injections campaigns

5: Fault Injection Results

Re-Validate Analyze

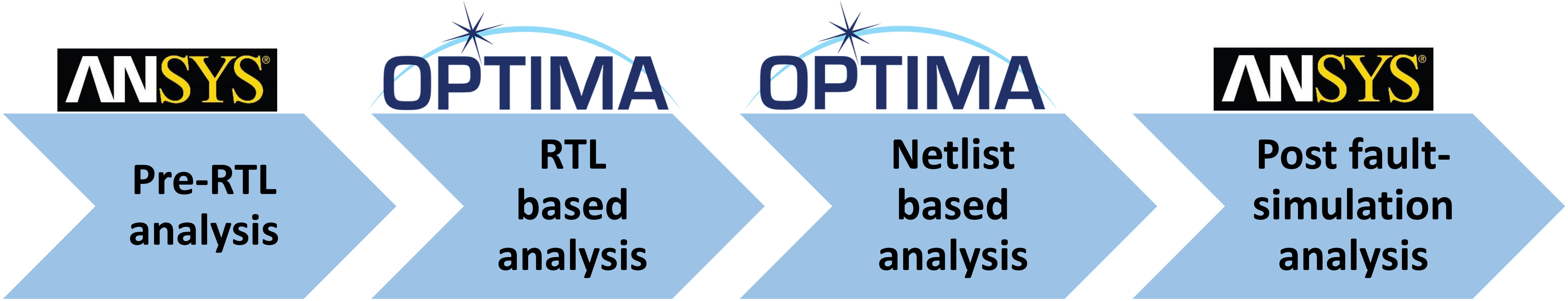
Benefits of the Optima Medini integration

- Formalized communication between the “ASIC world” and “FuSa world”
- Seamless, closed-loop integration
- Fusa management platform
- Safety analyst, FME(D)A
- ASIC fault simulation platform
- 1000X faster fault-simulation


ANSYS medini analyze
Optima-HE / Optima-SE
1: IP Design w/ Resource Data
User loads design in Optima
User decide on Safety Setup
2: Safety Setup
3: IP Design w/Resource Data and structural analysis results
Optima performs structural analysis
User decides on fault-injection needed FME(D)A, FTA, DFA
4: Fault Injection Campaign commands
5: Fault Injection Results
Optima performs fault-injections campaigns
Re-Validate Analyze
Done

Exchange of design information between the two tools

High-level Safety Flow



ANSYS

Pre-RTL analysis

- FMEA/FMEDA
- Estimate

OPTIMA

RTL based analysis

- Structural analysis
- Fault-simulation

OPTIMA

Netlist based analysis

- Structural analysis
- Fault-simulation

ANSYS

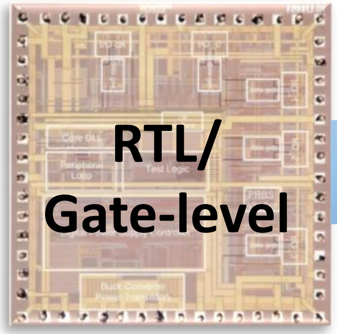
Post fault-simulation analysis

- ASIL calculation
- etc

Optima-SA™

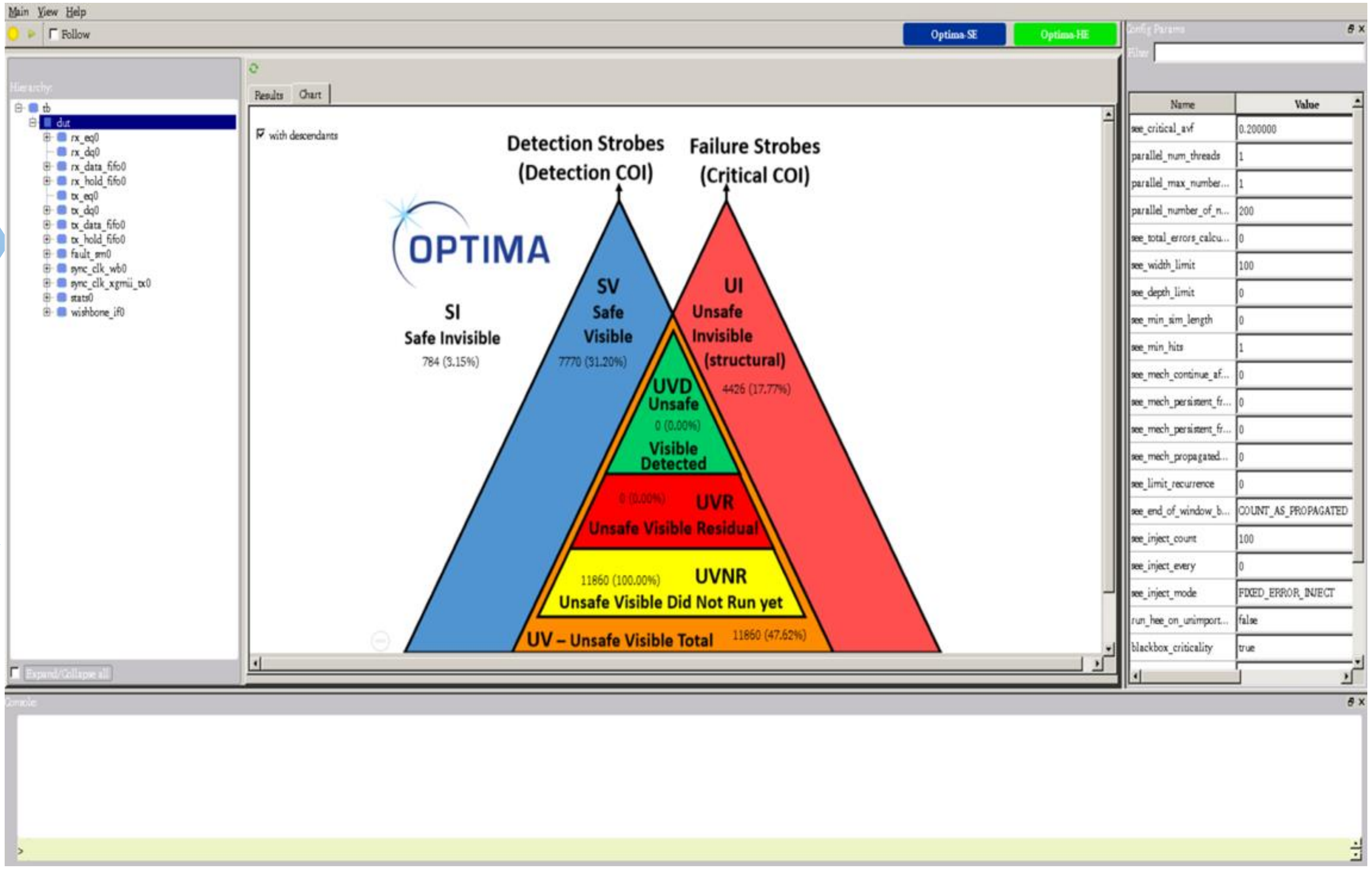
Early structural Analysis and fault-model sizing

Optima-SA™: Early structural analysis and FMEDA sizing



RTL/ Gate-level

Safety setup's



Name	Value
see_critical_avf	0.200000
parallel_num_threads	1
parallel_max_number...	1
parallel_number_of_n...	200
see_total_errors_calcu...	0
see_width_limit	100
see_depth_limit	0
see_min_sim_length	0
see_min_hits	1
see_mech_continue_af...	0
see_mech_persistent_fr...	0
see_mech_persistent_fr...	0
see_mech_propagated...	0
see_limit_recurrence	0
see_end_of_window_b...	COUNT_AS_PROPAGATED
see_inject_count	100
see_inject_every	0
see_inject_mode	FIXED_ERROR_INJECT
run_hee_on_unimport...	false
blackbox_criticality	true

Structural debug

Early FMEDA Parameters for identifying major issues

FMEDA data for Medini or other FMEDA tools

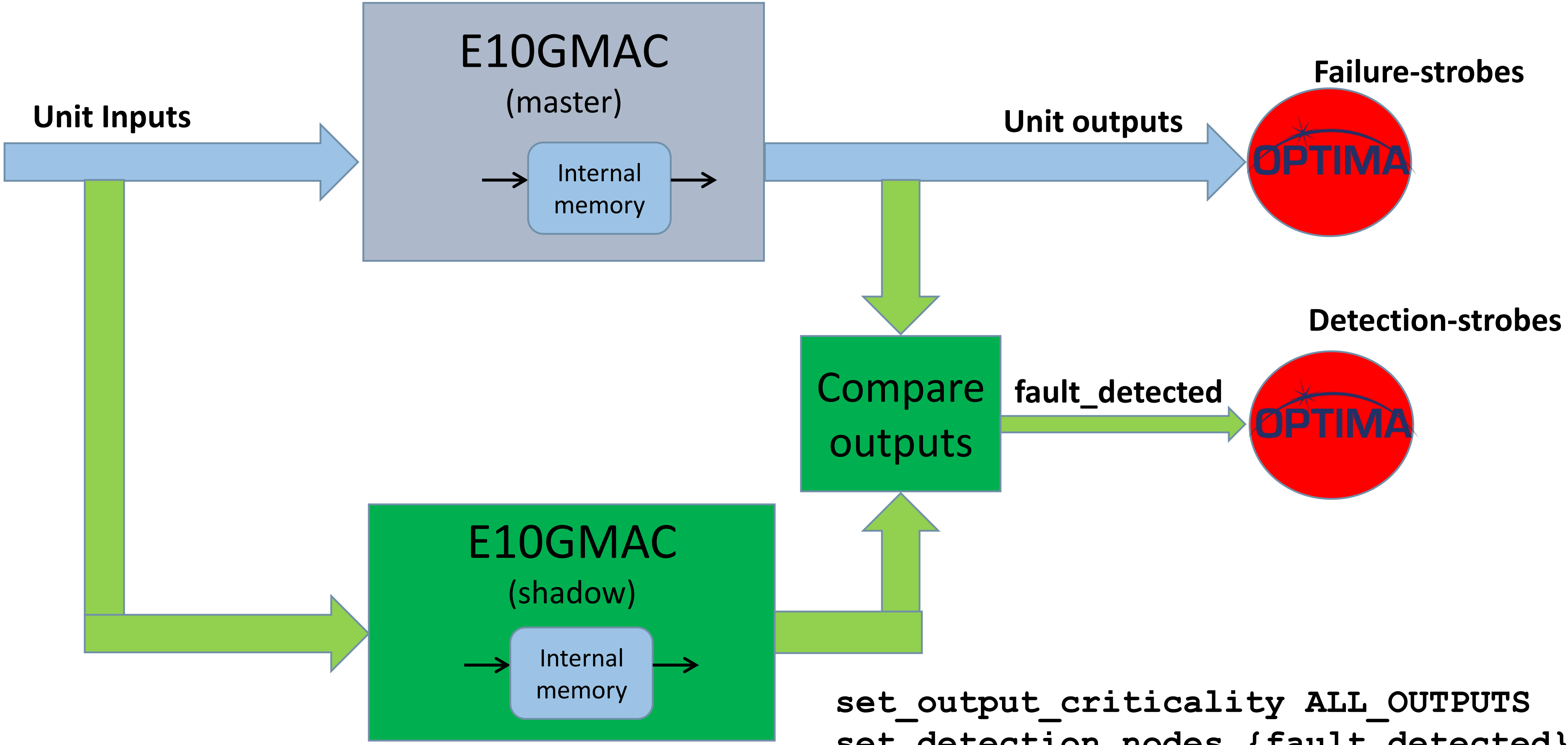
Safety Setup: definition

- Given a design in RTL or GL-netlist, a Safety Setup includes:
  - A given Failure Mode (Safety Goal)
  - and its covering Safety Mechanism

- Need to specify the related signals:

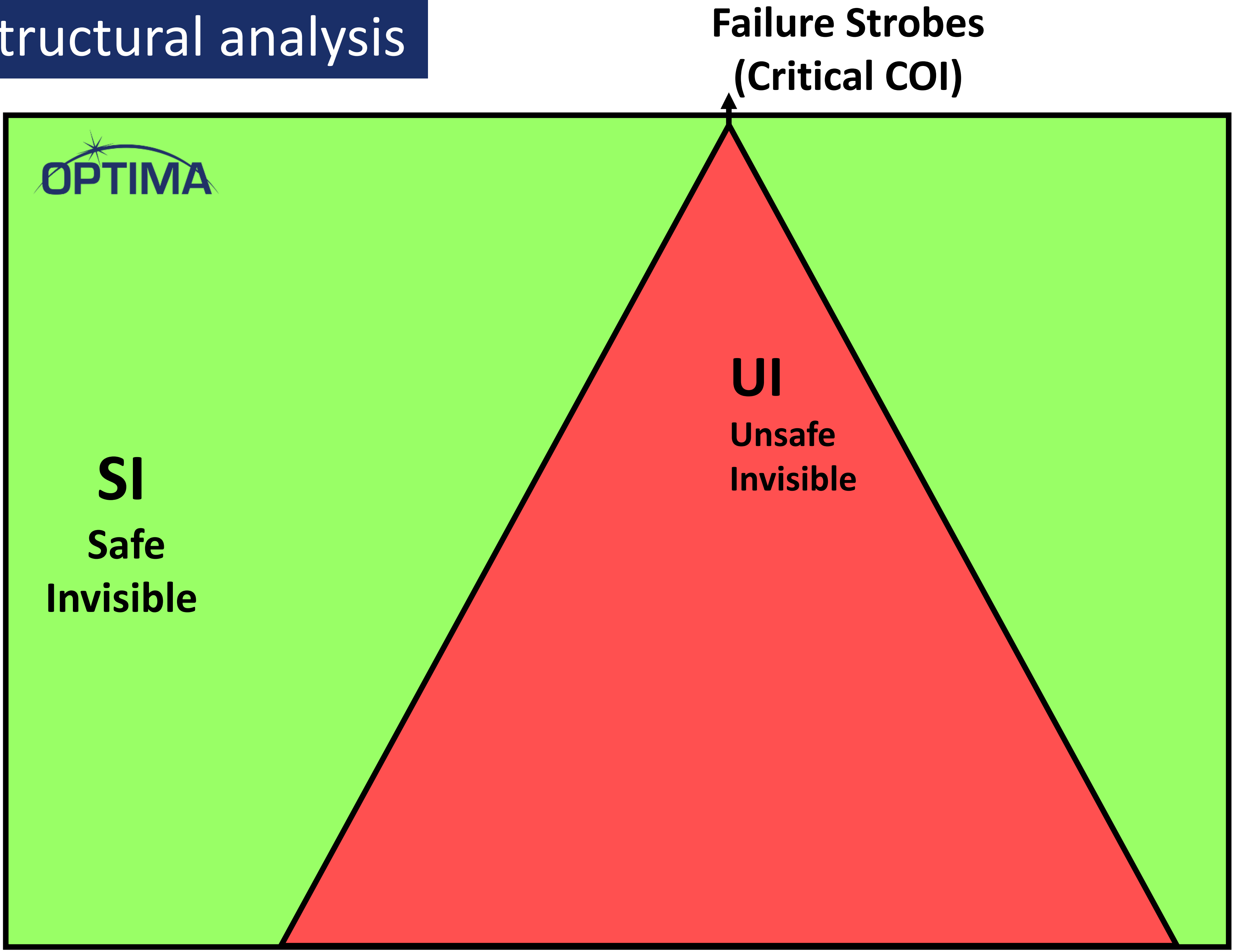
- **Failure-Mode Strobes** of a **Failure-mode** are the hardware signals that if fault arrives to them the Failure-mode is activated
- **Detection strobes** of a **Safety Mechanism** are outputs of the Safety Mechanism, hardware signals or SW variables, that are activated when a fault is detected

Example with Lockstep SM methodology

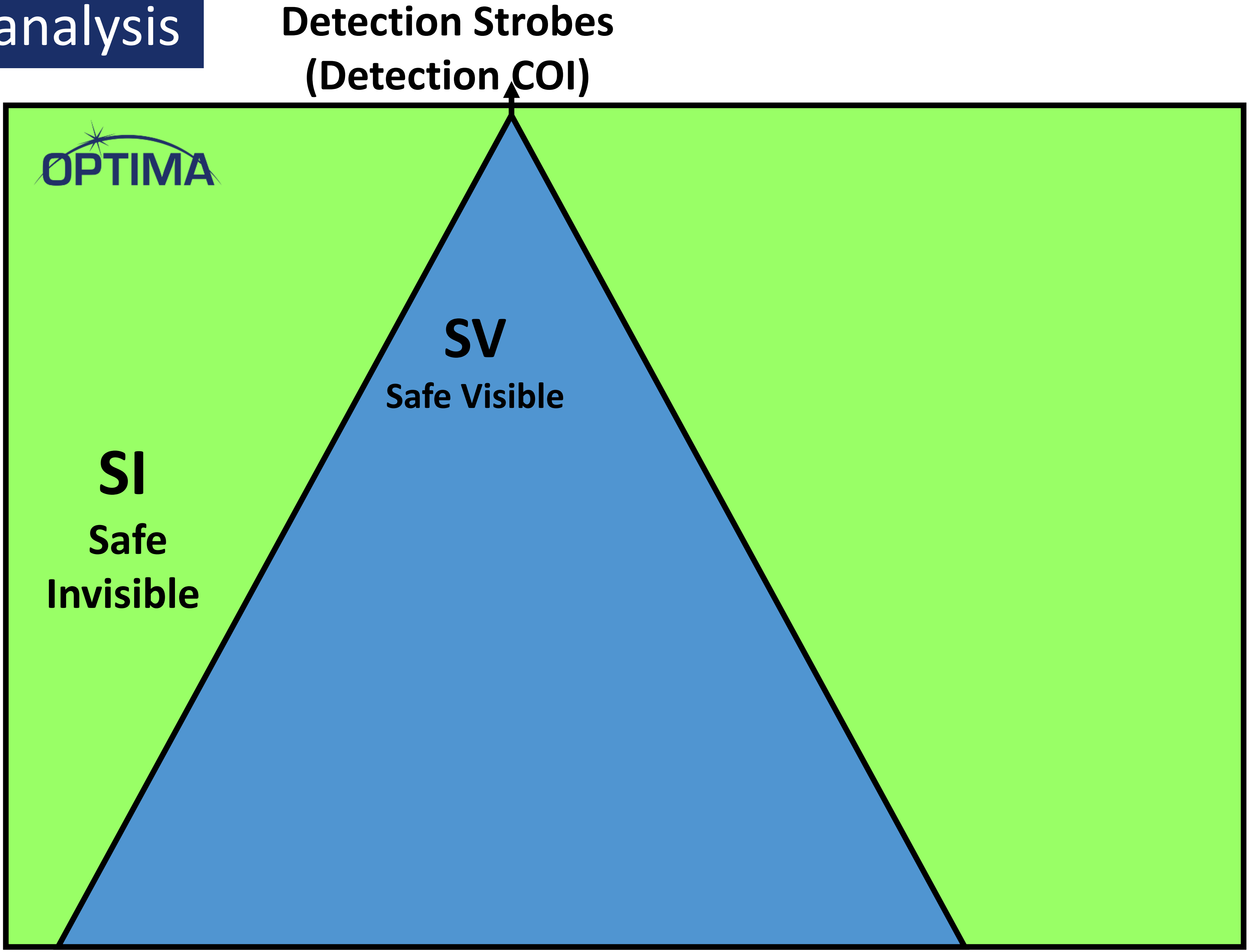


```
set_output_criticality ALL_OUTPUTS
set_detection_nodes {fault_detected}
```

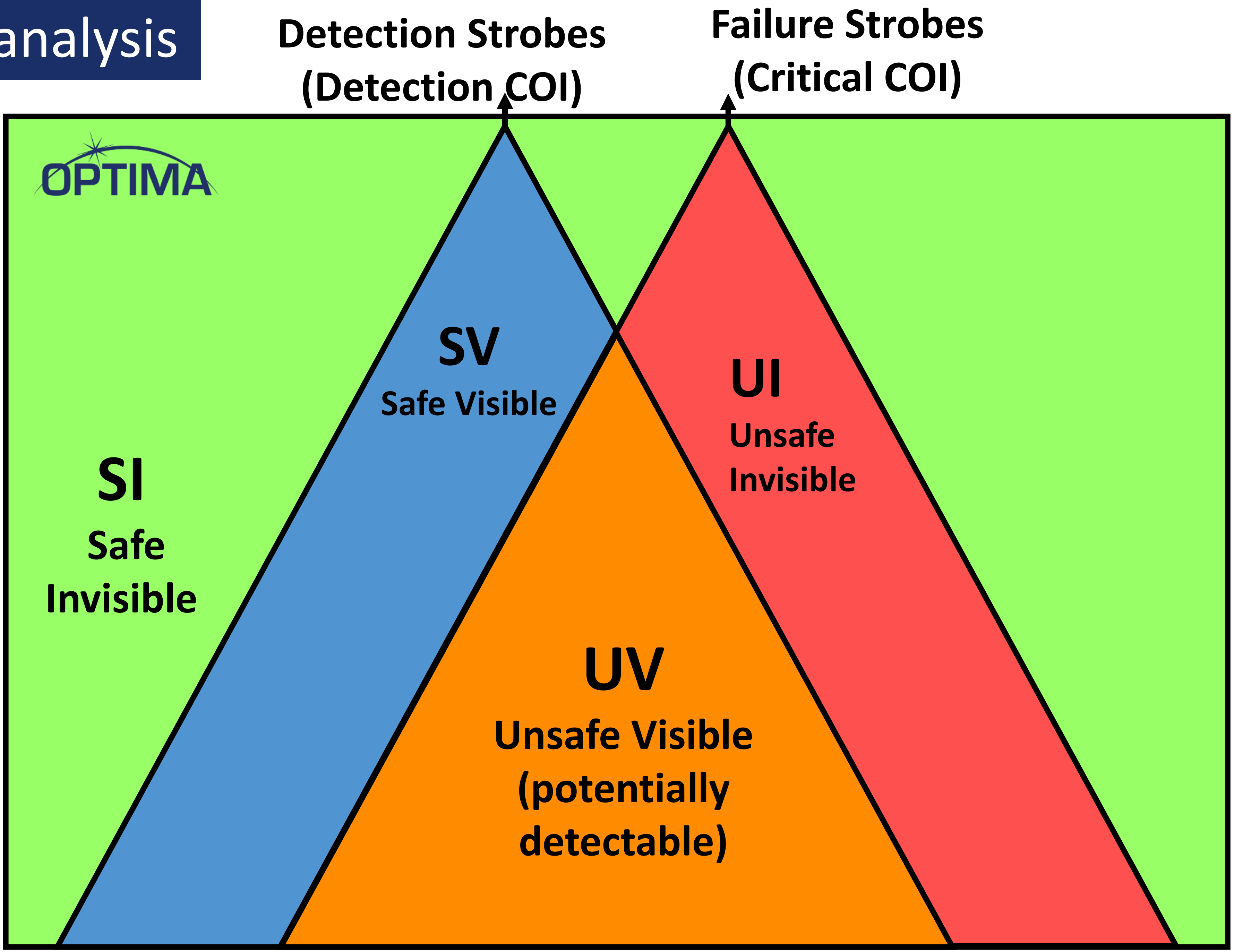
Optima's Structural analysis



Structural analysis



Structural analysis



ISO-26262 FMEDA parameters

Safe faults

- Not in safety relevant parts of the logic
- In safety relevant logic but unable to impact the design function (cannot violate a safety goal)

Single point faults

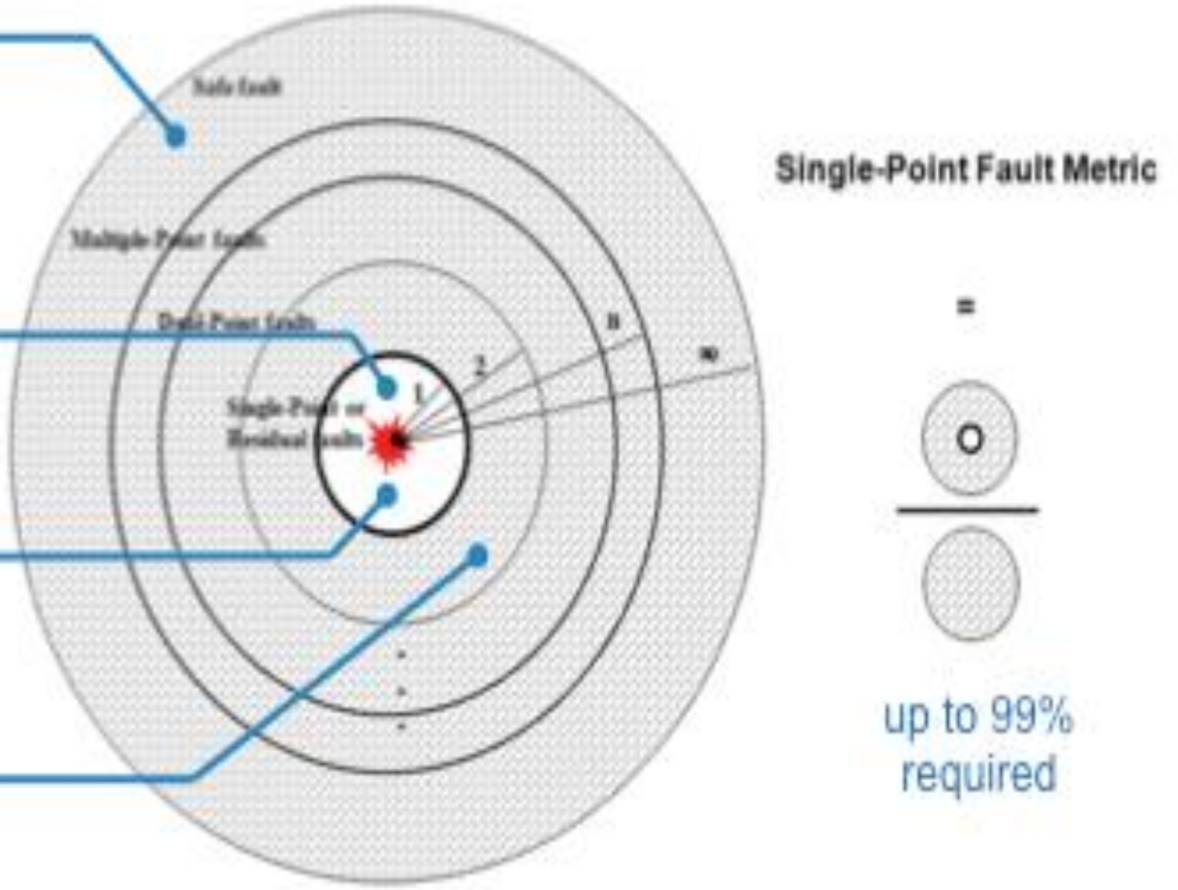
- Dangerous, can violate the safety goal and no safety mechanism

Residual faults

- Dangerous, can violate the safety goal and escape the safety mechanism

Multipoint faults

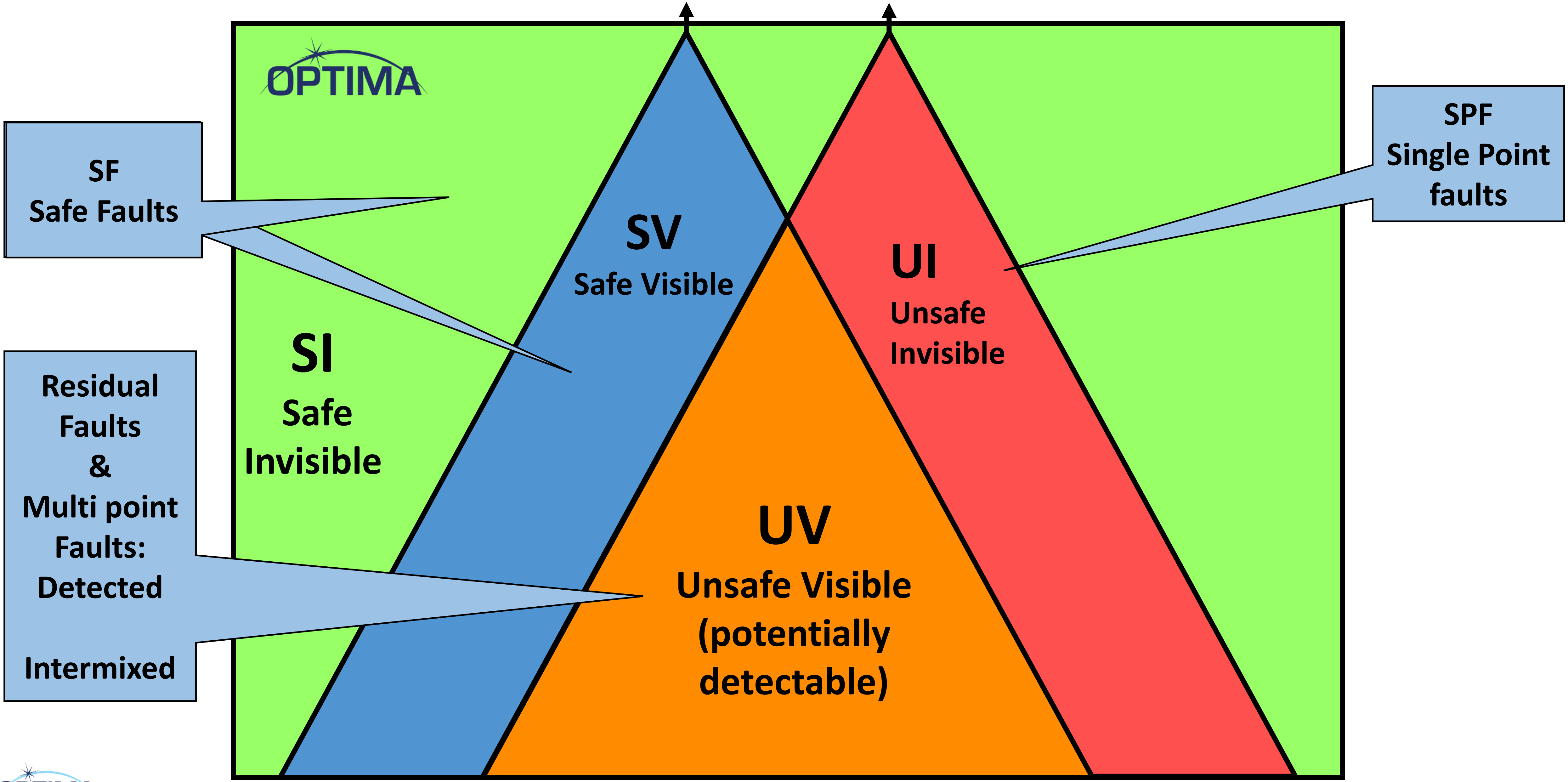
- Can violate the safety goal but are observed by a safety mechanism
- Sub-classified as "detected", "perceived" or "latent"



up to 99% required

Diagram Courtesy International Standards Organization (ISO)

Mapping Optima's Structural analysis to FMEDA terms



Optima-SA™ demo

Optima-SA: Early structural analysis and FMEDA parameters sizing

Features

- Size the FMEDA parameter
- Early detection of major issues:
  - Like SPF is too large
  - Certain areas not covered by any SM
  - Unnecessary overlap between SM’s
- Works on both RTL (early estimation) or gate-level (final results)
- Advanced structural debug capabilities
- Hierarchical based results

Benefits

- 0-effort
- Very fast, results available in minutes to 2 hours
- Identify issues early in the project, based on RTL only
- Analyze each fault-model separately, by groups, or all FM’s combined
- Export your results to your FMEDA tool (Ansys, Excel, or any other)

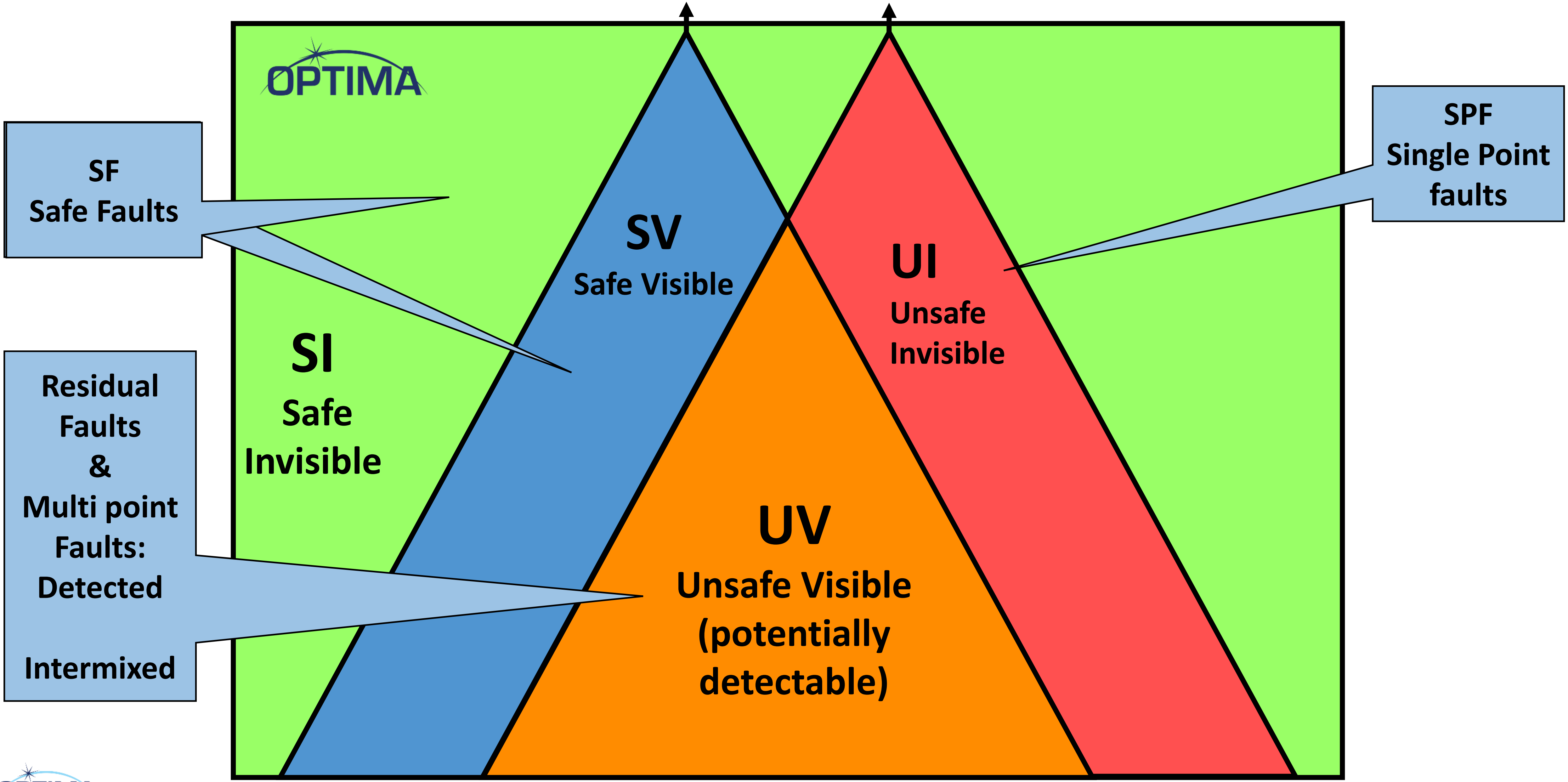
Optima-HE™

Hard Error fault-simulation

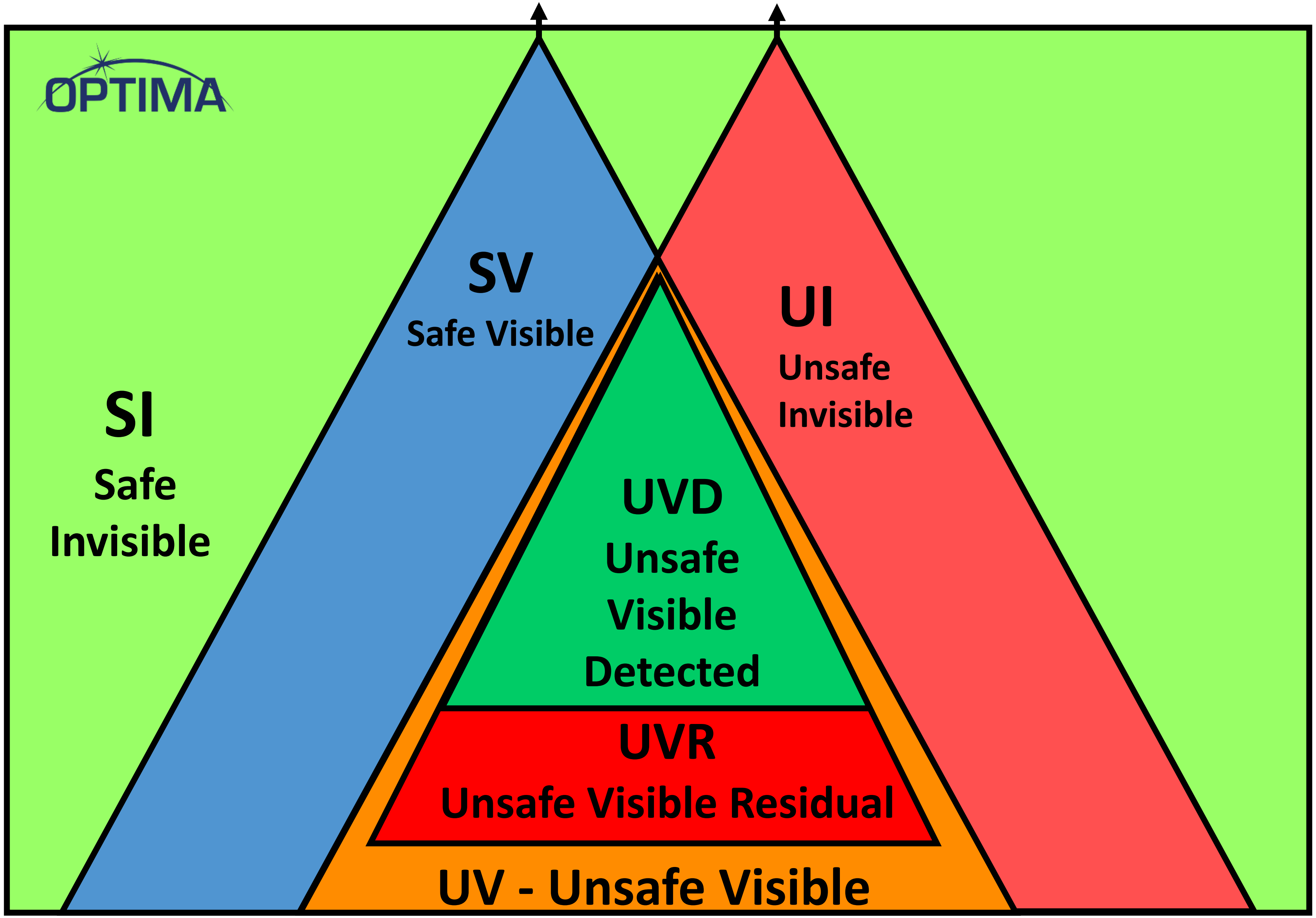
Optima-HE™

- Will take-over after Optima-SA™
- Perform accelerated fault-simulation in the UV area
- Split the UV area into Detected and not Detected

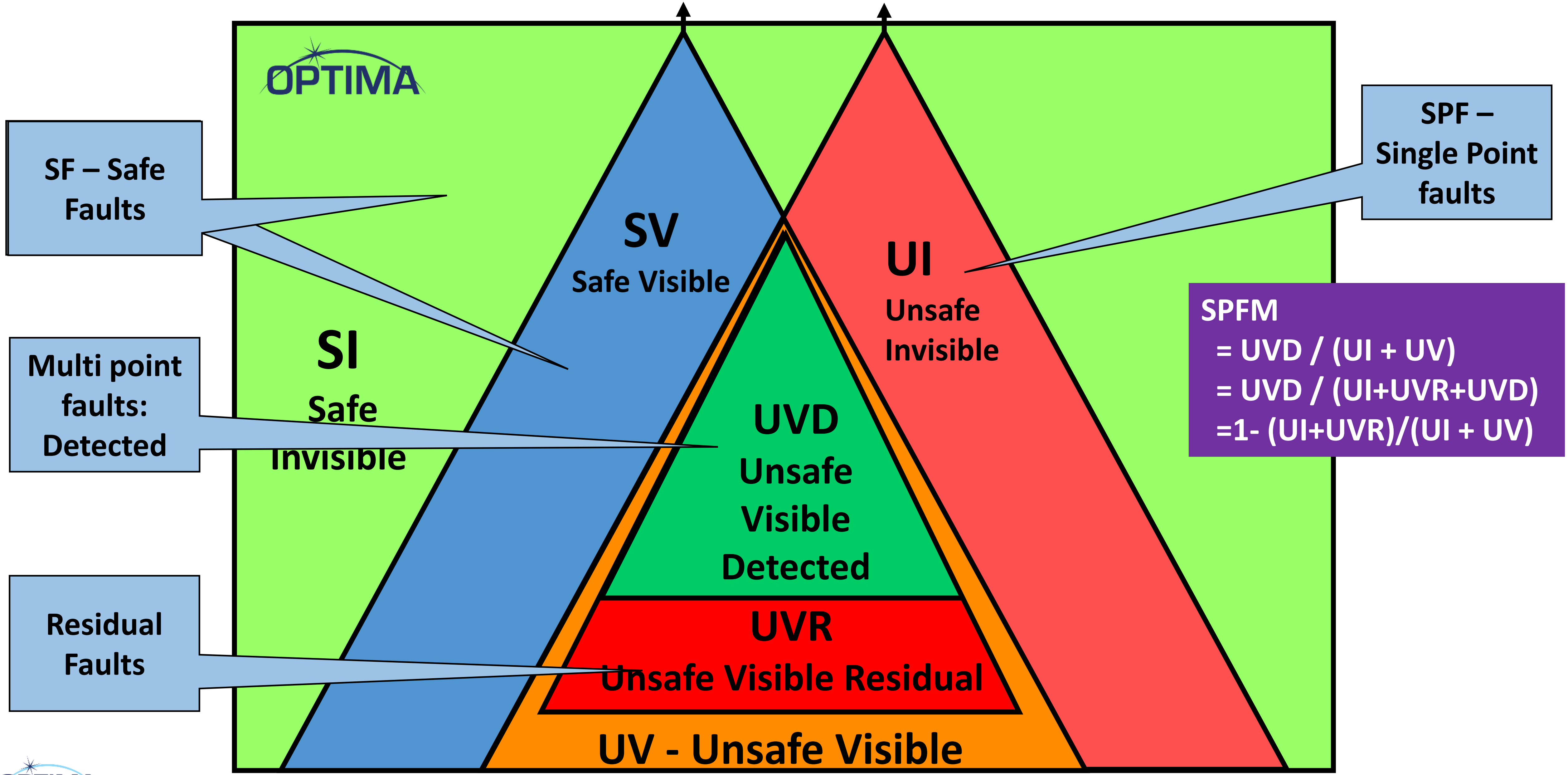
What Optima-SA gave us….



Optima-HE results:

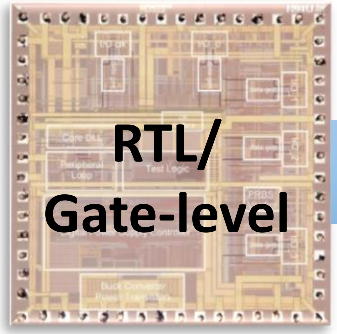


Optima-HE results:



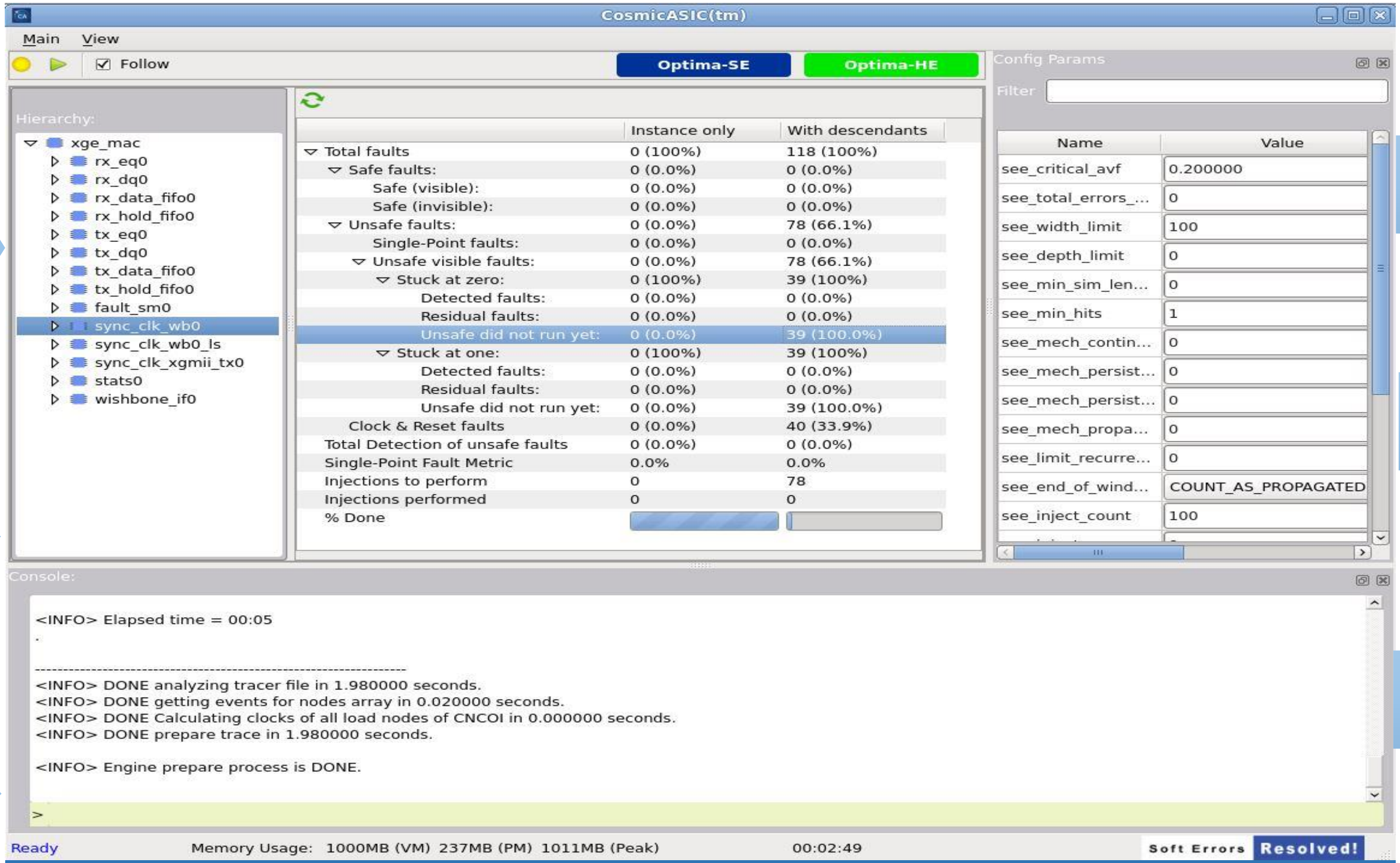
SPFM
= UVD / (UI + UV)
= UVD / (UI+UVR+UVD)
=1- (UI+UVR)/(UI + UV)

Optima-HE™: Complete Hard-errors solution



Safety Setup

Coverage goal



Hierarchy:

```
▽ xge_mac
   ▷ rx_eq0
   ▷ rx_dq0
   ▷ rx_data_fifo0
   ▷ rx_hold_fifo0
   ▷ tx_eq0
   ▷ tx_dq0
   ▷ tx_data_fifo0
   ▷ tx_hold_fifo0
   ▷ fault_sm0
   ▷ sync_clk_wb0
   ▷ sync_clk_wb0_ls
   ▷ sync_clk_xgmii_tx0
   ▷ stats0
   ▷ wishbone_if0
```

	Instance only	With descendants
▽ Total faults	0 (100%)	118 (100%)
▽ Safe faults:	0 (0.0%)	0 (0.0%)
Safe (visible):	0 (0.0%)	0 (0.0%)
Safe (invisible):	0 (0.0%)	0 (0.0%)
▽ Unsafe faults:	0 (0.0%)	78 (66.1%)
Single-Point faults:	0 (0.0%)	0 (0.0%)
▽ Unsafe visible faults:	0 (0.0%)	78 (66.1%)
▽ Stuck at zero:	0 (100%)	39 (100%)
Detected faults:	0 (0.0%)	0 (0.0%)
Residual faults:	0 (0.0%)	0 (0.0%)
Unsafe did not run yet:	0 (0.0%)	39 (100.0%)
▽ Stuck at one:	0 (100%)	39 (100%)
Detected faults:	0 (0.0%)	0 (0.0%)
Residual faults:	0 (0.0%)	0 (0.0%)
Unsafe did not run yet:	0 (0.0%)	39 (100.0%)
Clock & Reset faults	0 (0.0%)	40 (33.9%)
Total Detection of unsafe faults	0 (0.0%)	0 (0.0%)
Single-Point Fault Metric	0.0%	0.0%
Injections to perform	0	78
Injections performed	0	0
% Done		

Name	Value
see_critical_avf	0.200000
see_total_errors_...	0
see_width_limit	100
see_depth_limit	0
see_min_sim_len...	0
see_min_hits	1
see_mech_contin...	0
see_mech_persist...	0
see_mech_persist...	0
see_mech_propa...	0
see_limit_recurre...	0
see_end_of_wind...	COUNT_AS_PROPAGATED
see_inject_count	100

```
<INFO> Elapsed time = 00:05
.

--------------------------------------------------------------------
<INFO> DONE analyzing tracer file in 1.980000 seconds.
<INFO> DONE getting events for nodes array in 0.020000 seconds.
<INFO> DONE Calculating clocks of all load nodes of CNCOI in 0.000000 seconds.
<INFO> DONE prepare trace in 1.980000 seconds.

<INFO> Engine prepare process is DONE.

>
```

Ready Memory Usage: 1000MB (VM) 237MB (PM) 1011MB (Peak) 00:02:49

Optima FAULT INJECTION ENGINE (FIE™)

Over 1,000X faster than competing solutions

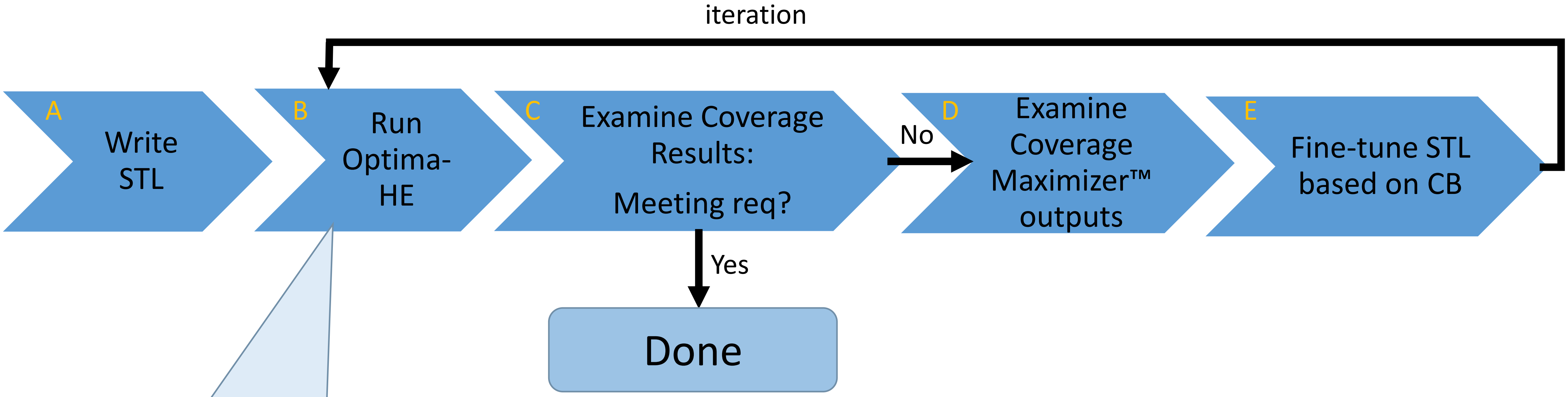
Safety mech. Coverage results

CoverageMaximizer™ recommendations

FMEDA Parameters for ASIL calculations

FMEDA data for Medini

Application Example: Tuning STL – Software Test Library


iteration
A
Write STL
B
Run Optima-HE
C
Examine Coverage Results:
Meeting req?
No
D
Examine Coverage Maximizer™ outputs
E
Fine-tune STL based on CB
Yes
Done

Optima-HE does this step over 1,000 times faster than competing solutions
Reducing this step from weeks to hours

Note:
The same process is used for all types of SM’s for HE detection
STL has the most iterations...

Optima-HE: Features

- Ultra fast fault simulation engine
  - Fast single-thread performance
- Parallel multi-threading, work on as many CPU-Cores available as possible
  - With 64 Cores machine, speedup can reach 64X the single thread performance
- Fault-Pruning
  - Identify only the faults needed for ISO-26262 requirements
  - Do faults only on them
- Fault-Collapsing
  - Identify faults that will produce the same results and do only what is needed
- Works both on RTL and Gate-Level Netlist
  - RTL – for initial estimations etc
  - GL – for final results for the audit report

Optima-HE: Ultra-fast Hard-Error fault simulation

Features

- Exhaustive fault simulation
- Safety-Mechanism coverage
- CoverageMaximizer™:
  - guidance for raising coverage
- For both gate-level and RTL

Benefits

- Faster fault simulation
- High accuracy
- Low effort coverage boosting
- Reduce Time-to-Market
- Reduce design costs
- Reduce needed compute resources

Optima-HE™ demo

CoverageMaximizer™

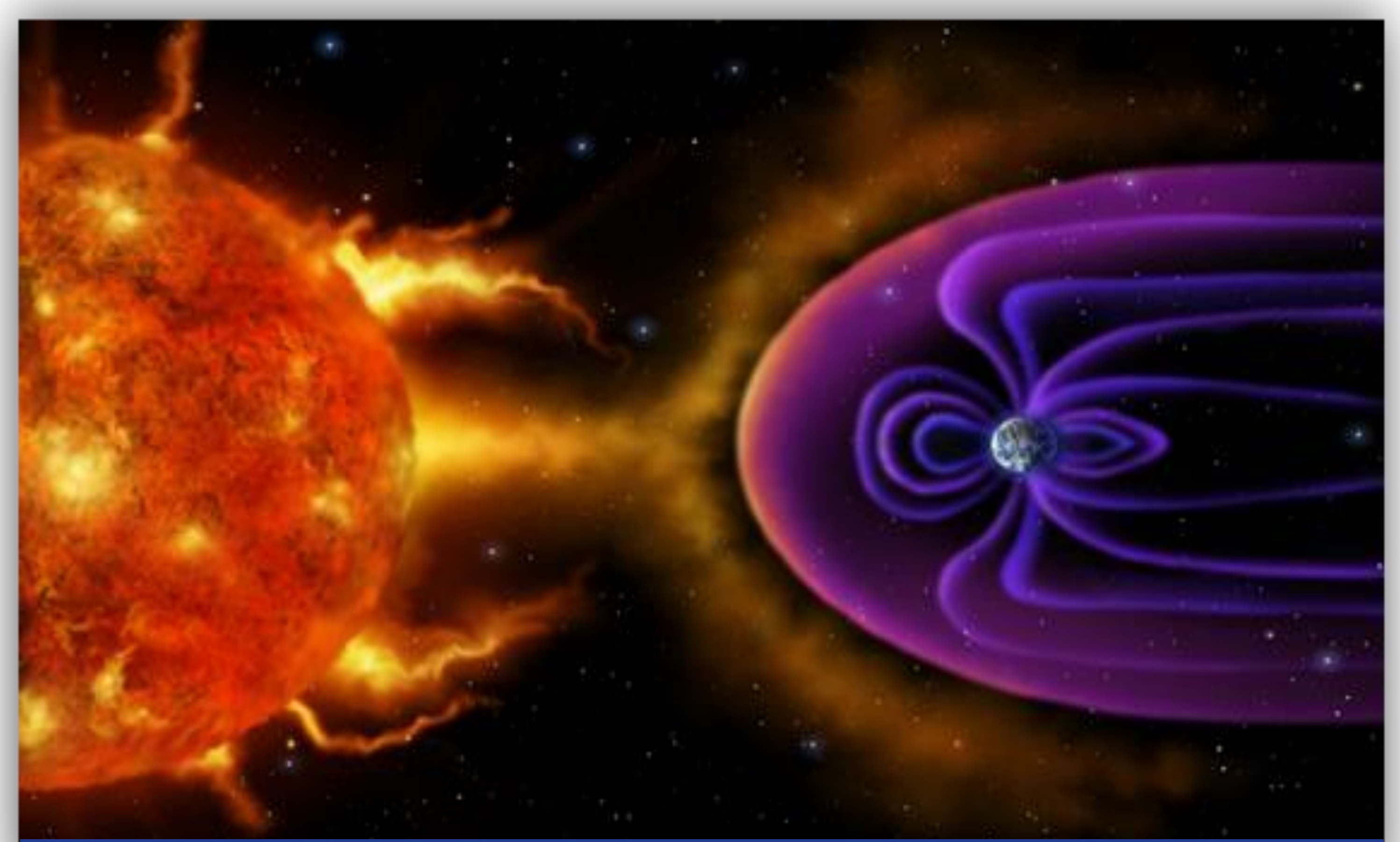
Guided-Manual and automated closure of diagnostic coverage

More details can be delivered under NDA

Transient faults or Soft-Errors

Problem definition

Transient-faults (Soft-errors/SEU/SET): What are they?



Bit-flips caused mostly by cosmic-rays
(radiation coming from the Sun)

Protecting against Transient-faults at the flops:

Unit-level Lockstep mechanism

(cost: 70% more silicon)

Hardening all flops

(cost: 30% more silicon)

Selective flip-flop hardening

(cost: 1-5% more silicon)

Using older silicon nodes (like 180nm)

Using special Rad-Hard silicon technology

Transient-faults (Soft-errors/SEU/SET)

Where do they hit?

Memory bits:

Single or multiple bits

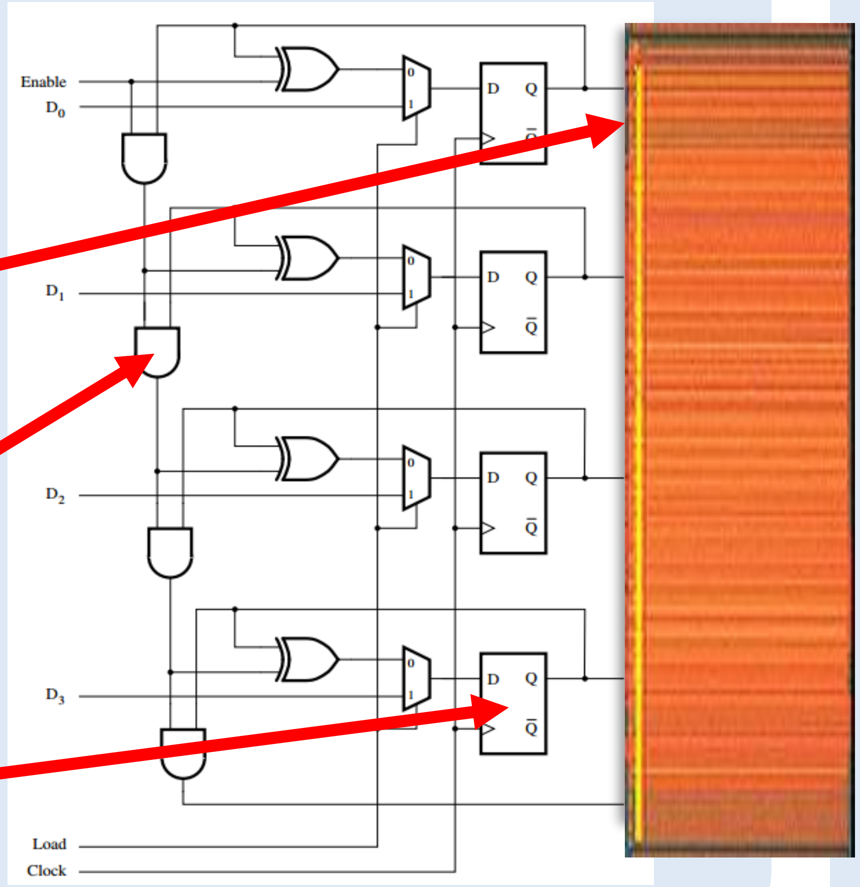
Gates:

Combinatorial logic

SET – Single-Event-Transient

Flip-flops:

Bit-flip in a single flop



Protecting against them

Memory:

ECC and bit dealignment

Gates: Low-probability,

not considered an issue by most experts

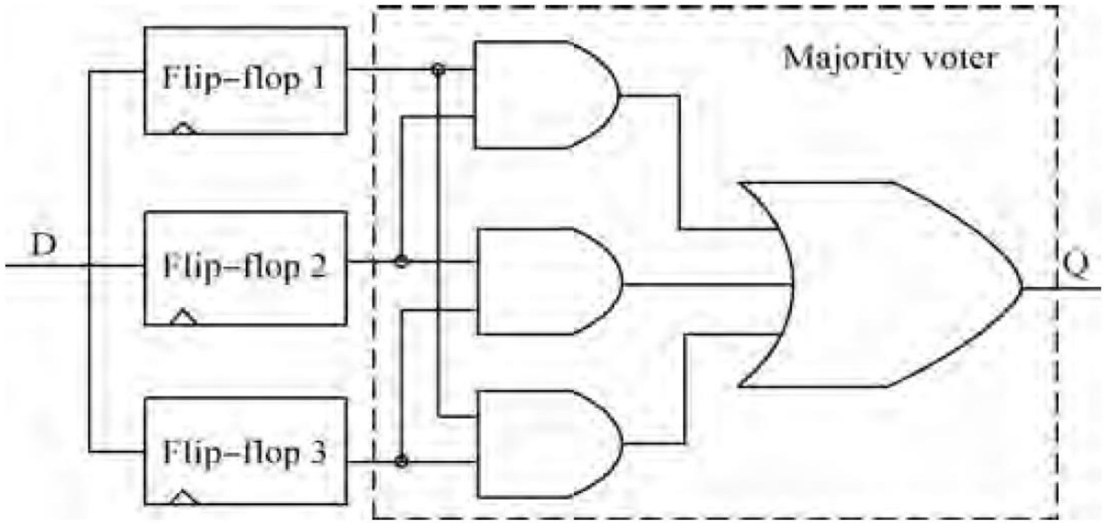
Flops:

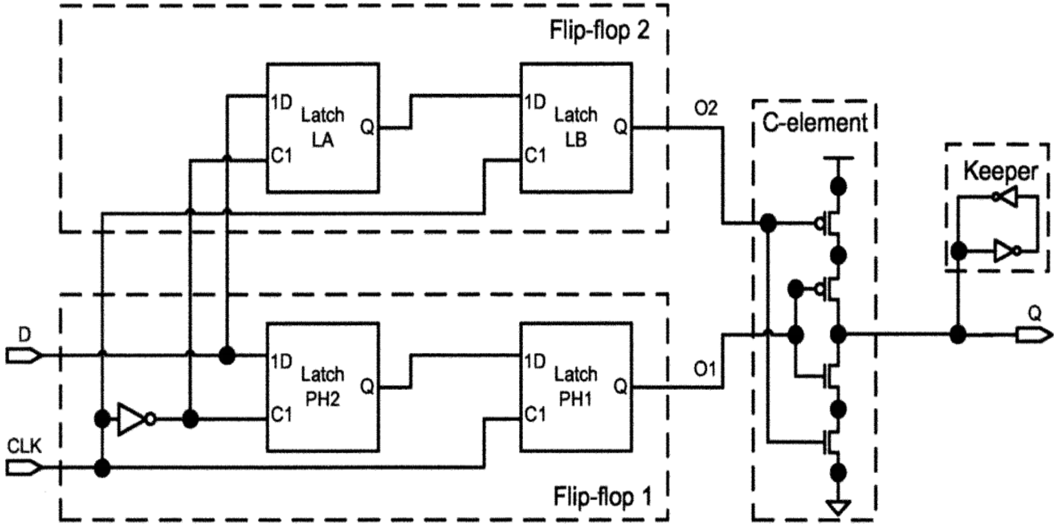
Next slides

Soft-errors: Examples of flip-flop hardening methods:

TMR with Majority voter

DMR with C-element



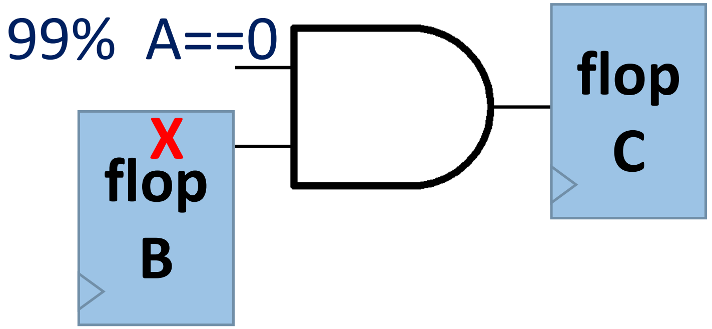


Transient-faults: logical-masking, deration and AVF

- Most flop TF are masked by the “logical masking” phenomena

  if 99% of the time: A== 0

  Then most faults on B or coming from B will be masked



- Some flops are logically masked most of the time

  -> they have low AVF

- Some are not

  -> they have high AVF

AVF :Architectural Vulnerability Factor

AVF of flop_a is:

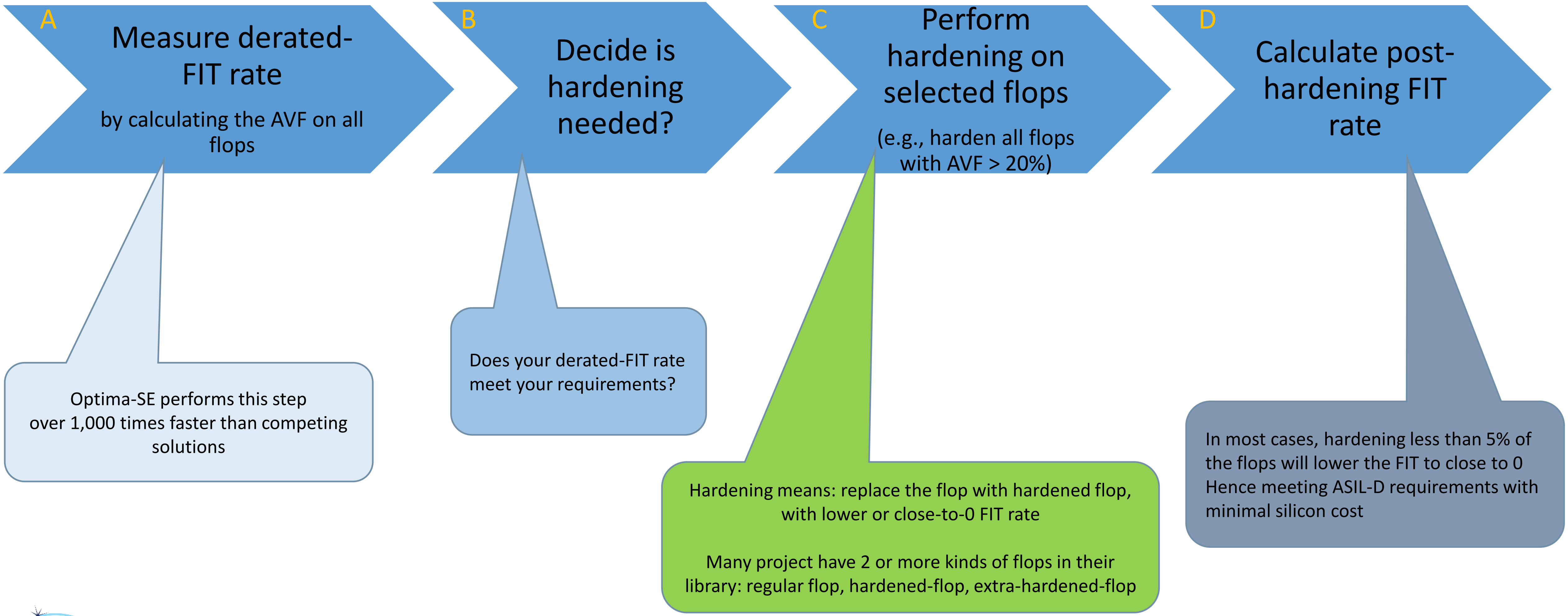
the probability that when a TF (bit-flip) happened on flop_a, then the error will propagate and reach a safety-goal output

Optima-SE: Soft Error: Selective Hardening

- While some designers resolve Soft Errors by complete duplication of full-units, or sometimes even full-CPU (lock-step or TMR), selective-flip-flop hardening is considered to be the most optimal and cost effective method
- Our tools enables selective flip-flop level hardening
- Definition: Find the 5-10% of the flops that contribute the 99% of the FIT, and perform hardening only on them. Reduce the FIT rate to close to 0
- This is an old problem in the industry, but almost has No commercial and accurate solution, all solutions require immense compute resources

  (measured in years and hundreds of years of simulations)

Selective hardening process:



A Measure derated-FIT rate

by calculating the AVF on all flops

B Decide is hardening needed?

C Perform hardening on selected flops

(e.g., harden all flops with AVF > 20%)

D Calculate post-hardening FIT rate

Optima-SE performs this step over 1,000 times faster than competing solutions

Does your derated-FIT rate meet your requirements?

Hardening means: replace the flop with hardened flop, with lower or close-to-0 FIT rate

Many project have 2 or more kinds of flops in their library: regular flop, hardened-flop, extra-hardened-flop

In most cases, hardening less than 5% of the flops will lower the FIT to close to 0
Hence meeting ASIL-D requirements with minimal silicon cost

Challenge: Calculating AVF can take hundred of compute years

- Calculating AVF involves performing fault simulations on all flops
- Each flop needs to be fault-simulated 50 to 1000 times to build reliable statistics
- Historically, this has been “very lengthy and expensive task”

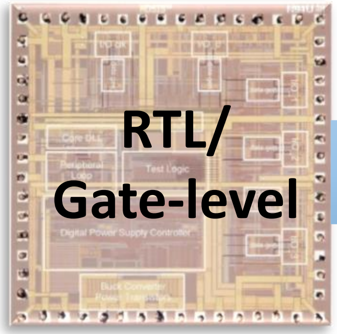
50 sims X 1M flops X 10 min = 500M min =

950 machine years

- **Optima is changing this with**
    - **Optima’s fault-simulations are over 1,000x faster than competing solutions**
    - **Reducing the 950 machine years to ~4 machine days**

Optima-SE
Soft-Error – Transient faults solutions

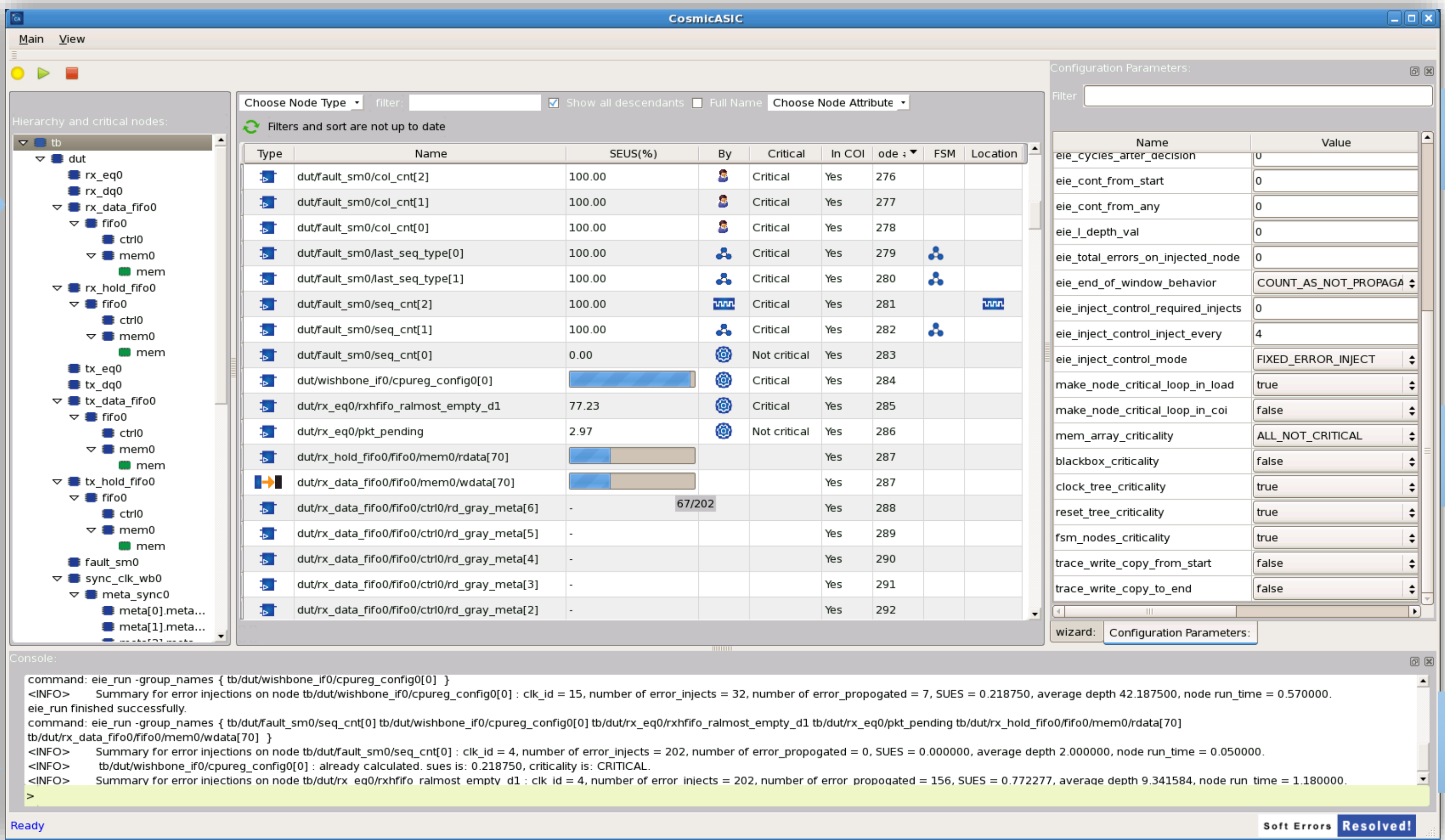
Optima-SE™: Complete Soft-errors solution



RTL/ Gate-level

Safety goal

Coverage goal



Hierarchy and critical nodes:

```
▽ tb
  ▽ dut
      rx_eq0
      rx_dq0
    ▽ rx_data_fifo0
      ▽ fifo0
          ctrl0
        ▽ mem0
            mem
    ▽ rx_hold_fifo0
      ▽ fifo0
          ctrl0
        ▽ mem0
            mem
      tx_eq0
      tx_dq0
    ▽ tx_data_fifo0
      ▽ fifo0
          ctrl0
        ▽ mem0
            mem
    ▽ tx_hold_fifo0
      ▽ fifo0
          ctrl0
        ▽ mem0
            mem
      fault_sm0
    ▽ sync_clk_wb0
      ▽ meta_sync0
          meta[0].meta...
          meta[1].meta...
```

Choose Node Type ▾ filter: ☑ Show all descendants ☐ Full Name Choose Node Attribute ▾

Filters and sort are not up to date

Type	Name	SEUS(%)	By	Critical	In COI	ode ▼	FSM	Location
	dut/fault_sm0/col_cnt[2]	100.00		Critical	Yes	276		
	dut/fault_sm0/col_cnt[1]	100.00		Critical	Yes	277		
	dut/fault_sm0/col_cnt[0]	100.00		Critical	Yes	278		
	dut/fault_sm0/last_seq_type[0]	100.00		Critical	Yes	279		
	dut/fault_sm0/last_seq_type[1]	100.00		Critical	Yes	280		
	dut/fault_sm0/seq_cnt[2]	100.00		Critical	Yes	281		
	dut/fault_sm0/seq_cnt[1]	100.00		Critical	Yes	282		
	dut/fault_sm0/seq_cnt[0]	0.00		Not critical	Yes	283		
	dut/wishbone_if0/cpureg_config0[0]			Critical	Yes	284		
	dut/rx_eq0/rxhfifo_ralmost_empty_d1	77.23		Critical	Yes	285		
	dut/rx_eq0/pkt_pending	2.97		Not critical	Yes	286		
	dut/rx_hold_fifo0/fifo0/mem0/rdata[70]				Yes	287		
	dut/rx_data_fifo0/fifo0/mem0/wdata[70]				Yes	287		
	dut/rx_data_fifo0/fifo0/ctrl0/rd_gray_meta[6]	-			Yes	288		
	dut/rx_data_fifo0/fifo0/ctrl0/rd_gray_meta[5]	-			Yes	289		
	dut/rx_data_fifo0/fifo0/ctrl0/rd_gray_meta[4]	-			Yes	290		
	dut/rx_data_fifo0/fifo0/ctrl0/rd_gray_meta[3]	-			Yes	291		
	dut/rx_data_fifo0/fifo0/ctrl0/rd_gray_meta[2]	-			Yes	292		

67/202

Configuration Parameters:

Filter

Name	Value
eie_cycles_after_decision	0
eie_cont_from_start	0
eie_cont_from_any	0
eie_l_depth_val	0
eie_total_errors_on_injected_node	0
eie_end_of_window_behavior	COUNT_AS_NOT_PROPAGA
eie_inject_control_required_injects	0
eie_inject_control_inject_every	4
eie_inject_control_mode	FIXED_ERROR_INJECT
make_node_critical_loop_in_load	true
make_node_critical_loop_in_coi	false
mem_array_criticality	ALL_NOT_CRITICAL
blackbox_criticality	false
clock_tree_criticality	true
reset_tree_criticality	true
fsm_nodes_criticality	true
trace_write_copy_from_start	false
trace_write_copy_to_end	false

Console:

```
command: eie_run -group_names { tb/dut/wishbone_if0/cpureg_config0[0]  }
<INFO>       Summary for error injections on node tb/dut/wishbone_if0/cpureg_config0[0] : clk_id = 15, number of error_injects = 32, number of error_propogated = 7, SUES = 0.218750, average depth 42.187500, node run_time = 0.570000.
eie_run finished successfully.
command: eie_run -group_names { tb/dut/fault_sm0/seq_cnt[0] tb/dut/wishbone_if0/cpureg_config0[0] tb/dut/rx_eq0/rxhfifo_ralmost_empty_d1 tb/dut/rx_eq0/pkt_pending tb/dut/rx_hold_fifo0/fifo0/mem0/rdata[70]
tb/dut/rx_data_fifo0/fifo0/mem0/wdata[70]  }
<INFO>       Summary for error injections on node tb/dut/fault_sm0/seq_cnt[0] : clk_id = 4, number of error_injects = 202, number of error_propogated = 0, SUES = 0.000000, average depth 2.000000, node run_time = 0.050000.
<INFO>        tb/dut/wishbone_if0/cpureg_config0[0] : already calculated. sues is: 0.218750, criticality is: CRITICAL.
<INFO>       Summary for error injections on node tb/dut/rx_eq0/rxhfifo_ralmost_empty_d1 : clk_id = 4, number of error_injects = 202, number of error_propogated = 156, SUES = 0.772277, average depth 9.341584, node run_time = 1.180000.
>
```

Ready

Soft Errors **Resolved!**

Optima FAULT INJECTION ENGINE (FIE™)

Over 1,000 faster than competing solutions

AVF report

(for selective hardening)

FMEDA Parameters for ASIL calculations

Audit trail

(for certification)

Another way to look at it: FIT rate calculation

Without knowing the "personal" AVF of each flip-flop

FIT_chip=

$$n \ast \mathrm{fit\_unhard}$$

With knowing the "personal" AVF of each flop

(using Optima-SE or other methods)

Without hardening

FIT_chip=

$$\sum_{k=0}^{n} (AVF(k) \ast \ fit\_unhard)$$

With knowing the "personal" AVF of each flop

(using Optima-SE or other methods)

With selective hardening of m flops

FIT_chip=

$$\sum_{k=0}^{m-1} (AVF(k) \ast fit\_hard)$$

$$+$$

$$\sum_{i=m}^{n} (AVF(i) \ast \ fit\_unhard)$$

n = Number of flops in the chip/IP/unit
AVF(k) = The "personal" AVF of specific flop k
m= number of hardened flops

FIT_chip = FIT Rate for the chip/IP/unit from flop from soft-error
fit_unh = FIT Rate of a single flop, unhardened regular flop
fit_hard = FIT Rate of a single flop, for hardened flop

Pre-silicon application of Optima-SE

- All 4 steps are possible
  - Lower the FIT rate to achieve the required ASIL level
  - Easley balance silicon hardening cost with lower-FIT rate

- Fault-simulations can be performed multiple times during the project
  - Early RTL for estimation
  - Re-run after different version and different hardening decisions or Safety-Mechanism changes
  - At RTL-freeze as close-to-final results
  - At Gate-Level for final results and certification
  - Etc..

- Optima's Fault-simulation speed

  -> increased fault-capacity

  -> raise the accuracy of measurements

Post-silicon (Post-Software) application of Optima-SE

- Only steps A is possible (calculate derated FIT rate), however:

- In many projects, due to the limited fault-simulation capacity
  - Derated-FIT rate is not calculated
  - No deration is taken in the ASIL and FIT calculations
  - Over-estimation and safe-guards are used
  - Resulting in higher FIT rate and lower ASIL than the chip really is

- Measuring deration with Optima-SE allows:
  - Accurate measurement of actual derated FIT rate
  - The measurement can lower the previously calculated FIT rate
  - Hence, raise the ASIL level
  - In some cases, tweaking the SW can also lower the derated-FIT rate (post-silicon)

- Value proposition to our customers:
  - Re-certify your chip to higher ASIL
  - Raise the price/value of the chip
  - Bid on projects closed to you before, due to low ASIL

Another option:
Combine selective hardening with planned re-spin to improve FIT rate

Optima-SE: Value proposition:

- Industries only:
    - Automated and complete solution for soft-errors
    - RTL based solution
- Lower the FIT rate to close to 0 at low silicon cost => Meet ASIL-D requirements
- Hardening results can either be inserted to RTL or to Gate-Level
- Ultra-fast fault simulator allows accurate results
- Vast savings in:
    - Silicon cost
    - Compute power
    - Engineering time and costs

Optima-SE™ demo

Optima-SE: Ultra-fast Soft-error Fault Simulation

Features

Calculate derated FIT rate

Selective-hardening

Lower FIT rate to close to 0

Measure SM effectiveness

1,000x faster than competing solutions

Benefits

- High accuracy
- Improve ASIL
- Reduce:
  - Time-To-Market
  - Silicon and power
  - Compute-resources needs

OPTIMA

Next Generation Automotive Functional Safety

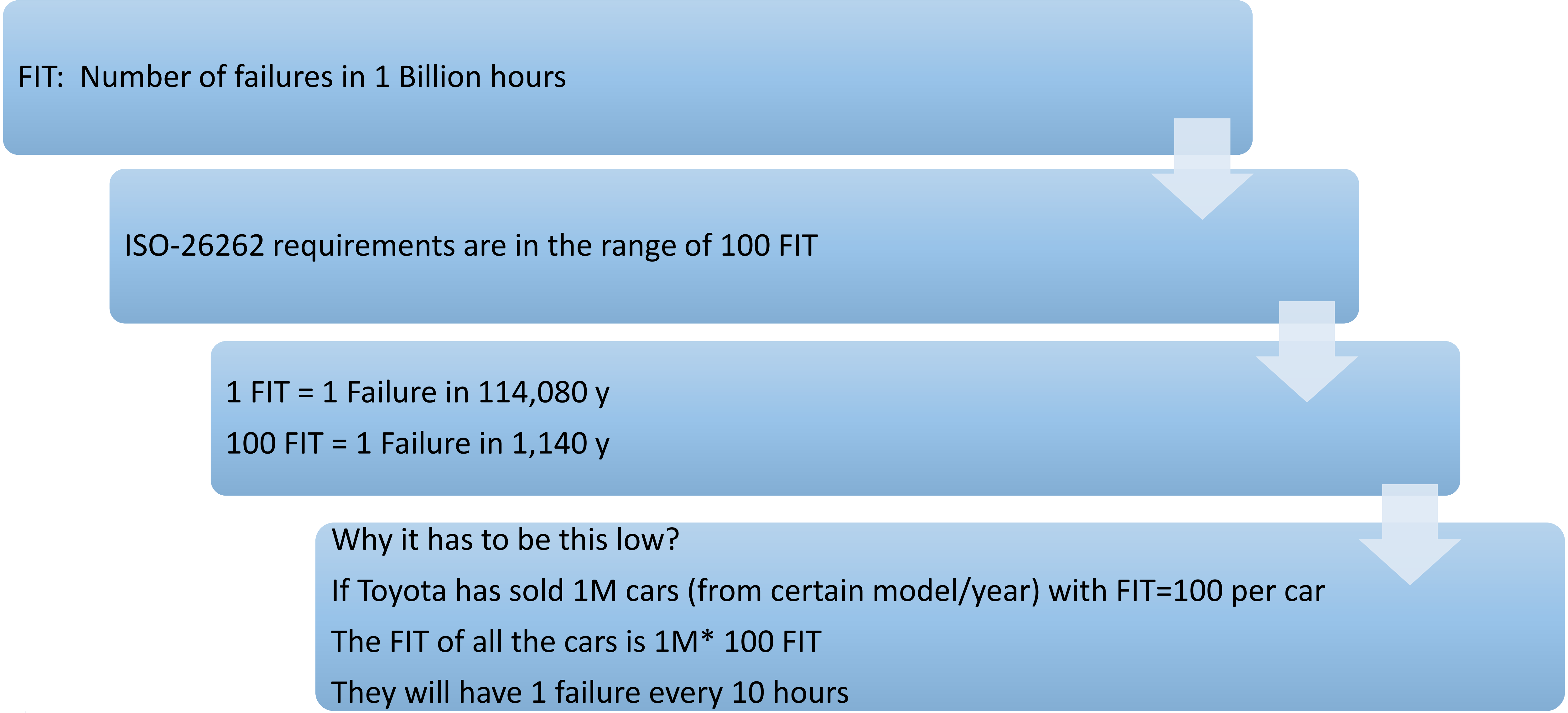
www.optima-da.com
info@optima-da.com
+972-4-619-4602

Terminology

Glossary (key confusing terms)

"Old" Scientific term	ISO-26262 term	Meaning
SEU Single Event Upset **SE** Soft-Error	**TF** Transient-fault	Bit-flip at a storage element: • memory bit • latch • flop Soft: No hardware damage happened
SET Single Event Transient	**TF** Transient-fault	Particle hitting a gate, causing a glitch that travels through the combinatorial logic It may be latched at flip-flop ➔ become SEU Mostly, it will not be latched and dissipate
HE Hard-Error	Permanent Fault	Physical damage in the chip. A burnout of a transistor. Seen as stuck-at-0, stuck-at-1, bridging fault etc.

Measuring failure: FIT – Failure in Time



FIT: Number of failures in 1 Billion hours

ISO-26262 requirements are in the range of 100 FIT

1 FIT = 1 Failure in 114,080 y

100 FIT = 1 Failure in 1,140 y

Why it has to be this low?

If Toyota has sold 1M cars (from certain model/year) with FIT=100 per car

The FIT of all the cars is 1M* 100 FIT

They will have 1 failure every 10 hours