2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION CHINA

accellera SYSTEMS INITIATIVE

DESIGN AND VERIFICATION™ CONFERENCE AND EXHIBITION

Shanghai | September 20, 2023

Facilitating the Advanced Fault Campaign Strategies with Austemper KaleidoScope

Functional Safety Verification

Victor Arribas, Rambus Inc.
Pierre Bayon, Rambus Inc.
Ann Keffer, Siemens EDA
Jacob Wiltgen, Siemens EDA
Kara Liu, Siemens EDA

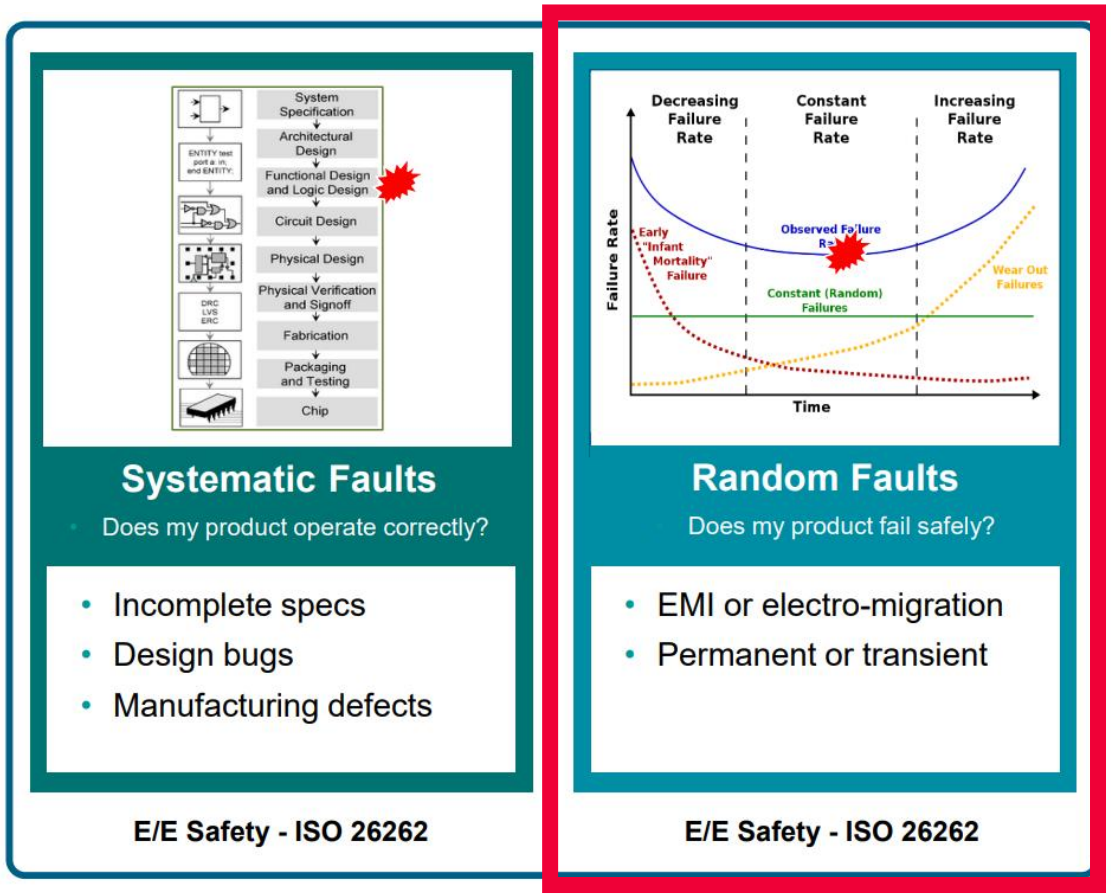
SIEMENS

Agenda

Demonstrate the Achievement of Safety for Random Failures in ISO 26262
Efforts Required to Complete Safety Verification using Fault Injection
KaleidoScope Fault Injection Basics and Result Classification
Fault Campaign Acceleration Strategies for Fault Injection Simulation

SIEMENS

ISO 26262 Provides Specific Safety Targets for Random Failures



- An IC must fail safely in the presence of a random failure
- A sufficient safety architecture protecting against random failures is required

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

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

ASIL	Random hardware failure target values
D	$<10^{-8}$ h^{-1}
C	$<10^{-7}$ h^{-1}
B	$<10^{-7}$ h^{-1}

NOTE The quantitative target values described in this table can be tailored as specified in 4.2 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).

SIEMENS

Safety Verification using Fault Injection

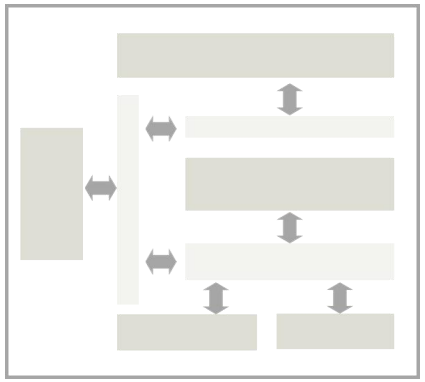
Table 11 — Hardware integration tests to verify the completeness and correctness of the implementation of the hardware safety requirements

	Methods	ASIL			
		A	B	C	D
1	Functional testing[a]	++	++	++	++
2	Fault injection testing[b]	+	+	++	++
3	Electrical testing[c]	++	++	++	++

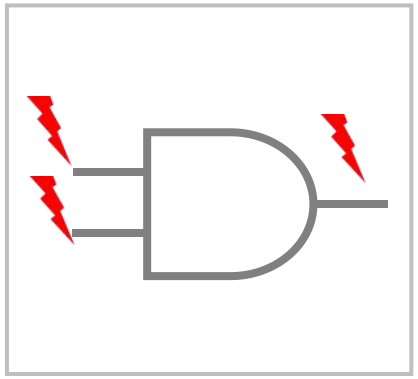
Fault Injection is highly recommended for ASIL-C and D in ISO 26262

- Faults are injected and propagated in the design to verify that the safety mechanisms implemented are functioning correctly.
- Each fault is classified.
- Traditional functional simulator and basic scripting were used to approach fault campaign in the past

Effort Required for Fault Campaign



Millions or billions of gates

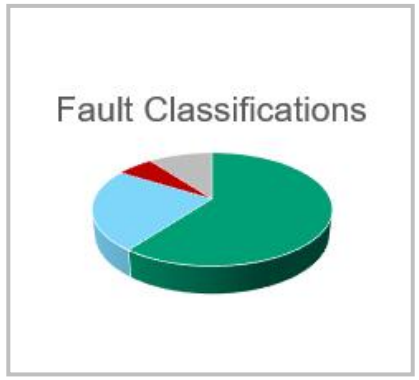


Multiple fault sites or nodes for each gate

More than one fault model at one fault site or node

ASIL-B
vs
ASIL-D

Higher fault coverge for certain ASIL

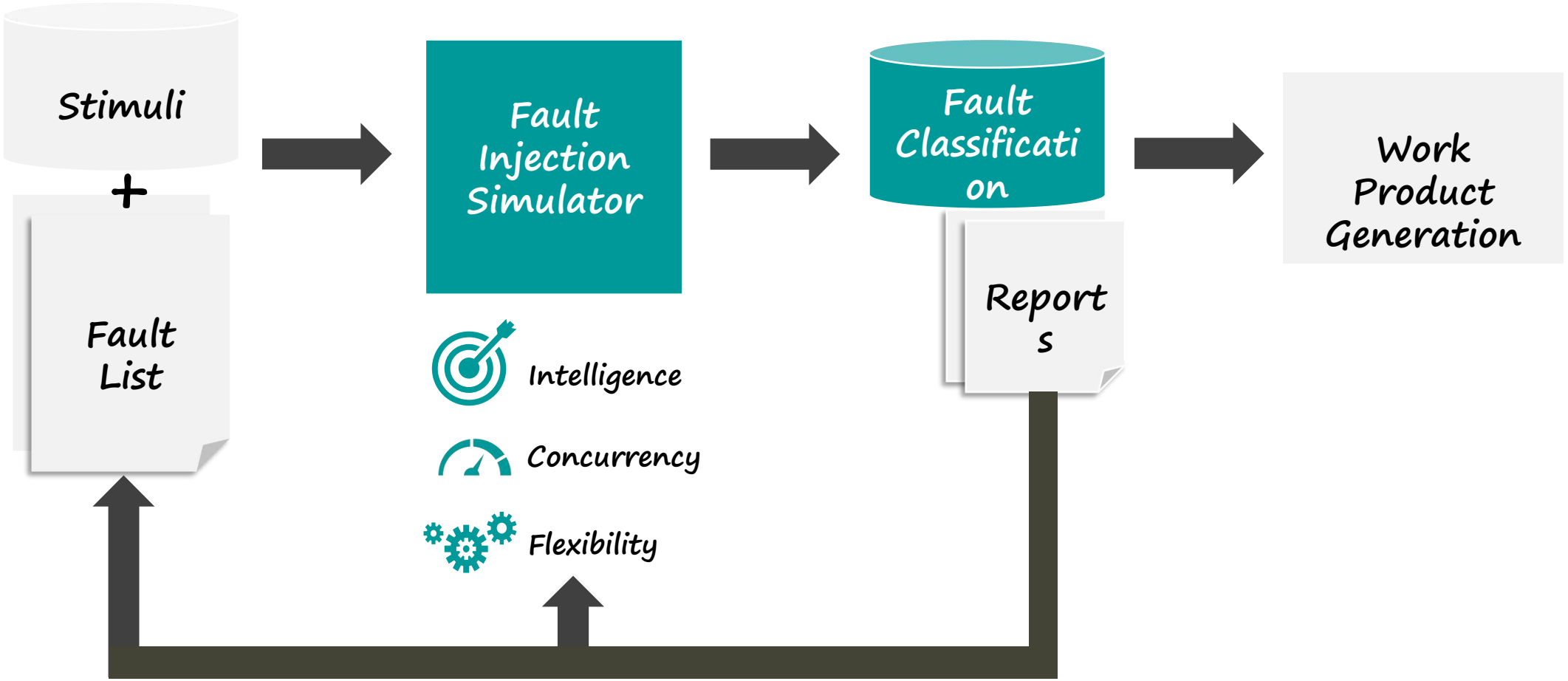


Handle unresolved faults

Alternatives were employed but face uncertainty with various impacts and limitations

SIEMENS

The Demand for Dedicated Fault Injection Simulator



KaleidoScope Fault Injection Basics

Austemper KaleidoScope for managed, high performance safety verification

Design for Safety

IC Development

Safety Analysis

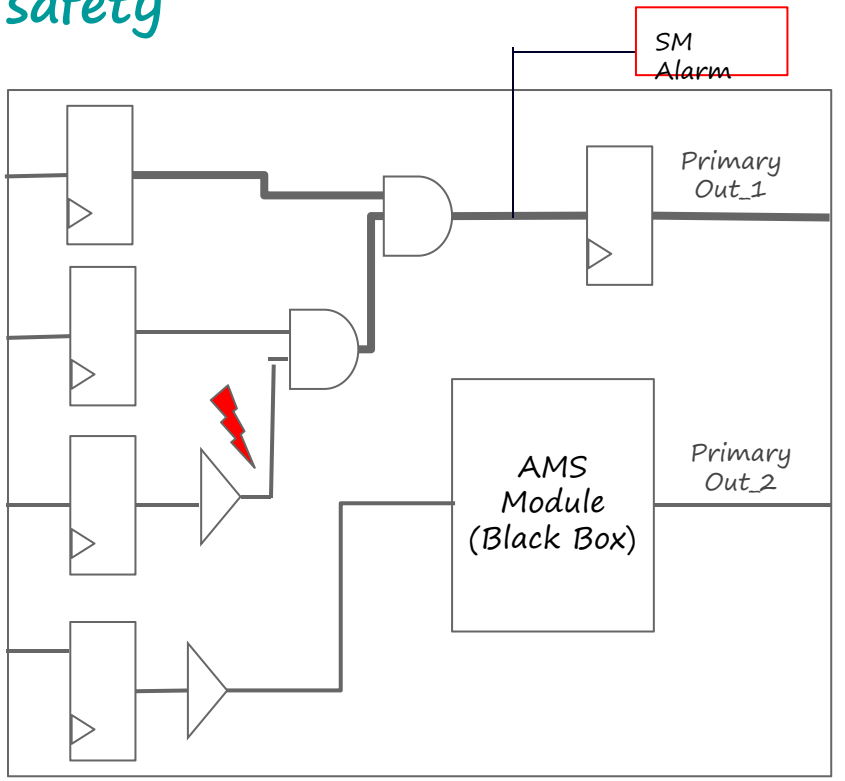
Safety Analysis

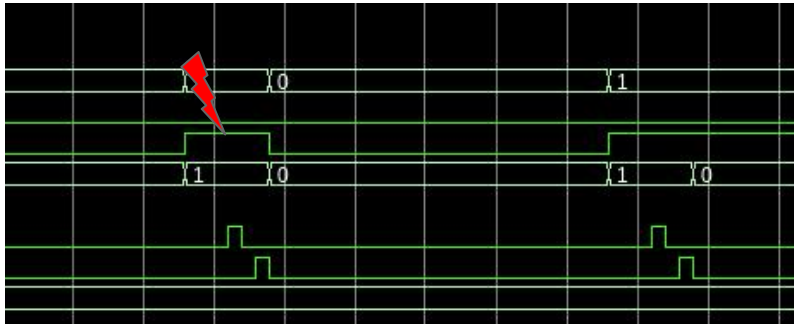
Safe Design

RTL Sims

Safety Alarms

Fault List

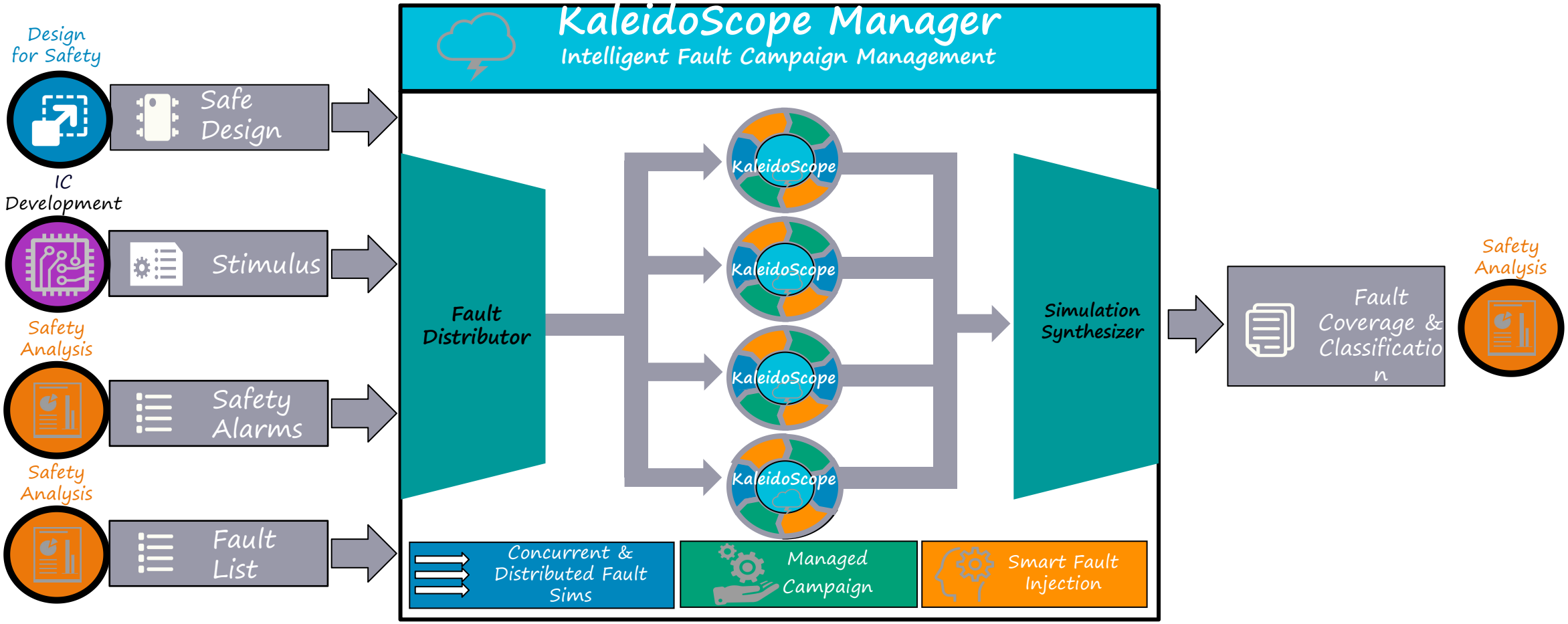




SIEMENS

KaleidoScope Manager

Intelligent fault campaign management optimizing efficiency across platforms



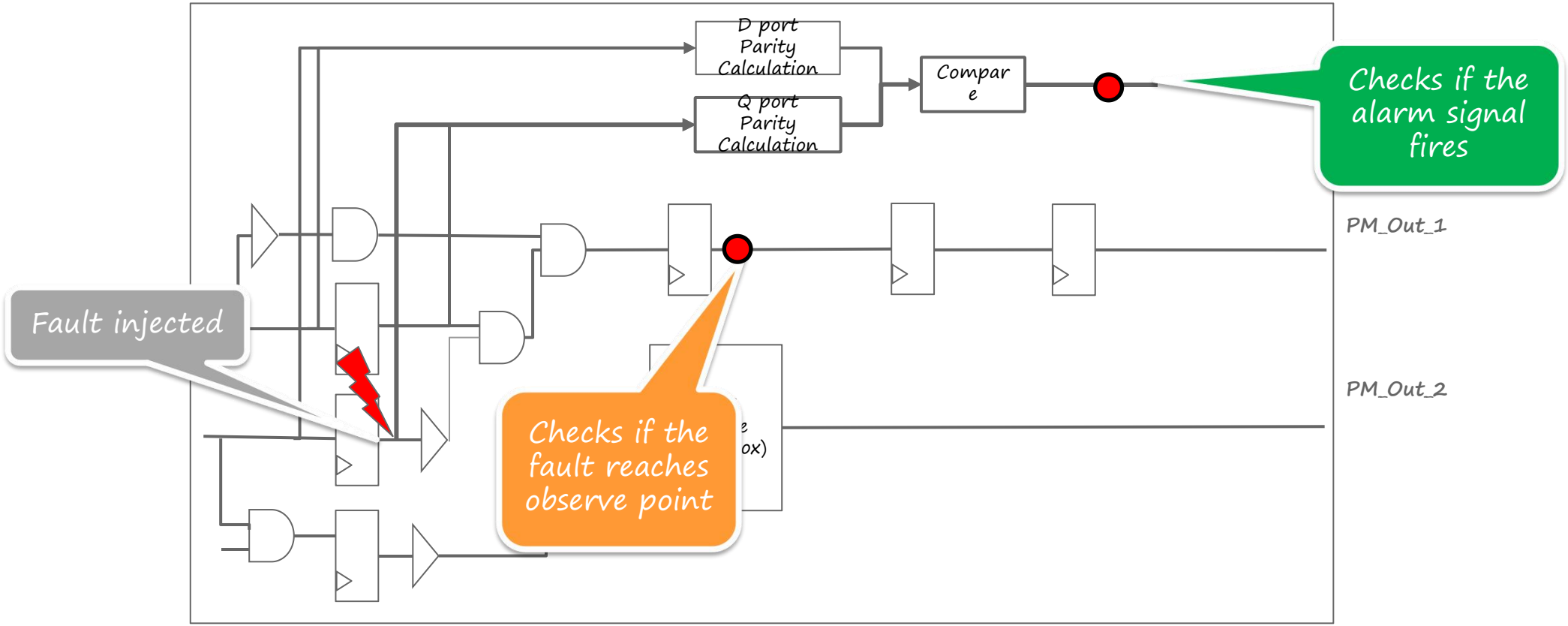
SIEMENS

KaleidoScope Results Classification

SIEMENS

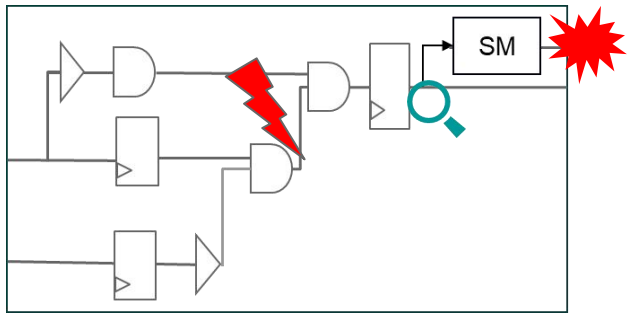
Monitoring Alarm Signals and Observe Points

KaleidoScope monitors observe points and alarm signals to determine the classification of an injected fault:

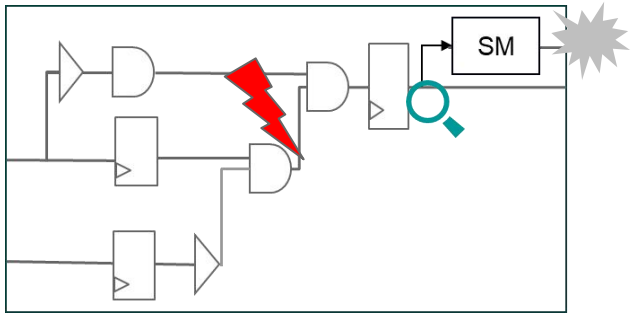


SIEMENS

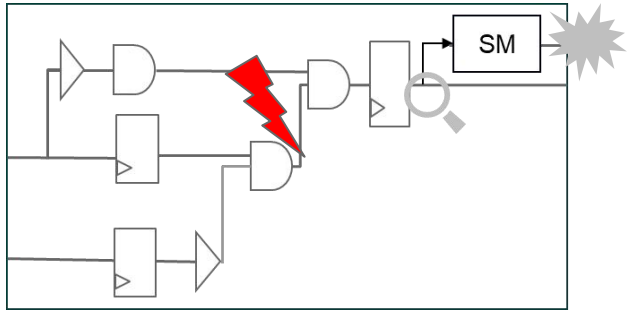
Fault Classification in KaleidoScope



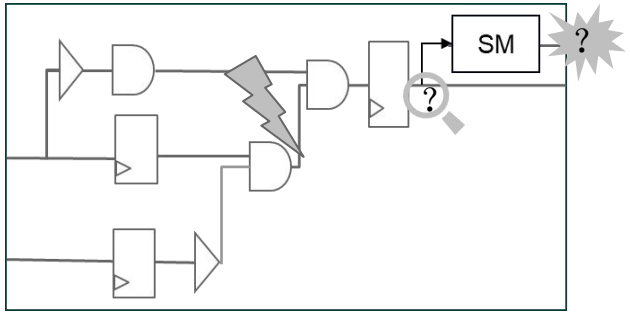
Detected_Observed



Undetected_Observed



Undetected_Unobserved



Unclassified

SIEMENS

Determine next steps for unresolved faults
Reports providing the first line of fault classification

```
% head Kman.ErrorHSE.rpt
#ErrorNet                        ErrorVal  TriggerTime  FailTime  AlarmTime  FaultResolution  Rational                 VCDFileName
<path>.mem_rd_en_dly             1         155          155       0          Reached_BBox     <path>.i_sram.WrEn       qwave.vcd
<path>.w_b_counter.countval[3]   1         155          155       0          Reached_BBox     <path>.i_sram.WrAddr[3]  qwave.vcd
<path>.w_b_counter.n1            1         155          160       0          Reached_BBox     <path>.i_sram.WrAddr[3]  qwave.vcd
<path>.w_b_counter.n6            1         155          480       0          Reached_Async    reset                          qwave.vcd
```

```
% head Kman.NotInjected.rpt
#ErrorNet                        ErrorVal
axi_cross_wrapper_ATD_wrapper_ATD.u_axi_cross_wrapper_ATD.u_axi_cross.u_axi_cross_wr_ch.state[2] SA0
axi_cross_wrapper_ATD_wrapper_ATD.u_axi_cross_wrapper_ATD.u_axi_cross.u_axi_cross_rd_ch.state[2] SA0
axi_cross_wrapper_ATD_wrapper_ATD.u_axi_cross_wrapper_ATD.u_axi_cross.u_axi_cross_rd_ch.state[1] SA0
```

Fault Campaign Acceleration

Strategies Introduced by KaleidoScope Users

SIEMENS

Rambus – RT-640

"RT-640 是一种具有近300 万个故障的复杂设计，其目标是达到 ISO 26262 ASIL-B 认证级别。

"...该评估利用了 IBM LSF 高性能计算环境，并行执行了多达 90 项故障仿真，大约用时 12 天完成。

"...对于永久和瞬时 故障，我们获得了 91.9% 的总 SPFM 和 75% 的总 LFM，完全符合达到 ASIL-B 级别的要求。"

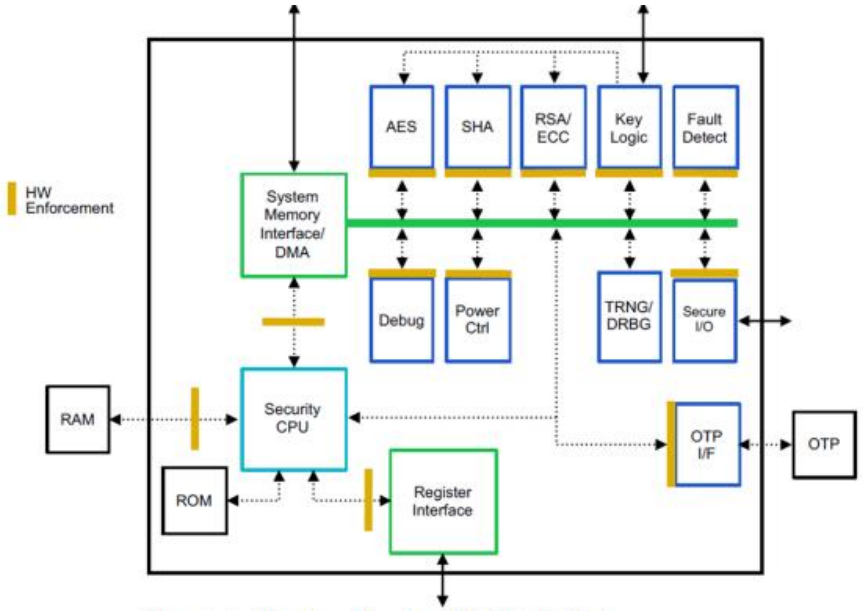


Figure 1: Architecture of Rambus RT-640 Root of Trust.

数字工业软件

Rambus RT-640 的 ISO 26262 认证之路

执行摘要

现代汽车中集成的 IC 数量与日俱增，与此同时，随着技术的进步，这些 IC 也变得越来越复杂。在这类应用场景中，故障可能导致危及生命，因此，采用可靠且安全的 IC 变得至关重要。Rambus RT-640 提出了一种符合汽车功能安全标准 ISO 26262 的硬件信任根，利用先进的防篡改信息安全技术，针对各种故障（包括永久、瞬时和潜在故障）以及硬件和软件攻击提供保护。在本文中，我们将介绍 RT-640 为达到 ASIL-B 认证级别而进行的功能安全评估。我们将展示为成功评估这款完整的工业规模 SoC 而实现的方法，利用近 300 万个故障，达到 91.9% 的总 SPFM 和 75% 的总 LFM，完全符合 ASIL-B 级别的要求。

Victor Arribas，Rambus Inc.；Pierre Bayon，Rambus Inc.；Vedant Garg，Siemens EDA

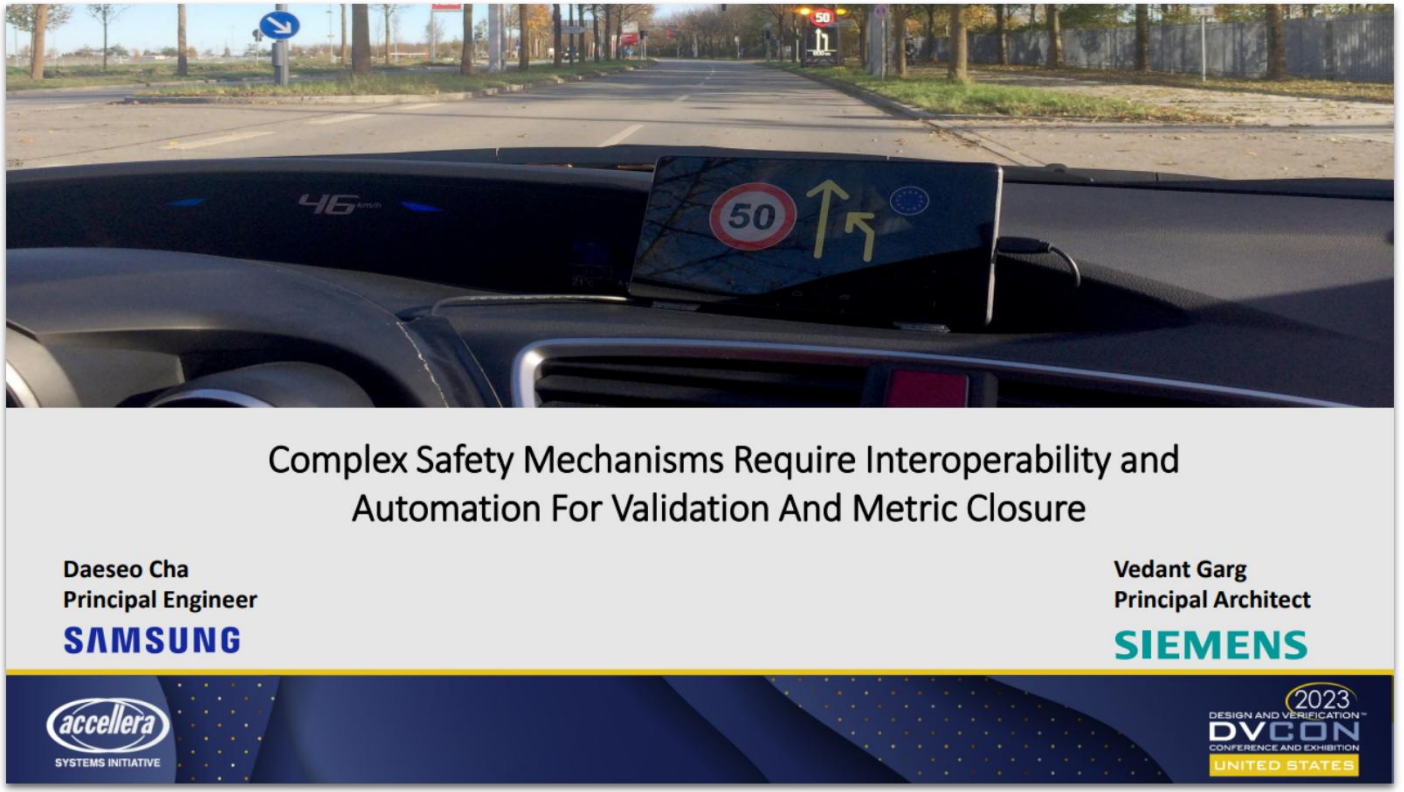
SIEMENS

Samsung – Experiment on Automotive SoC

"Advanced methodologies such as safety analysis for optimization and fault pruning, concurrent fault simulation, fault emulation, and formal based analysis are deployed in this project to validate the safety requirements for the Automotive SoC"

Final Result	Faults (SA0 + SA1)	Fault Distribution(%)
Detected Observed	3125	77.18
Detected Unobserved	0	0.00
Undetected Observed (Residual) 10 fault moved to SAFE Fault	69	1.70
Undetected Unobserved (conservatively Residual)	280	6.92
Safe Fault - Dead Logic	234	5.78
Safe Fault Formal COI analysis Signal Back Propagation Safe Fault Configuration (Engineer's justification)	341	8.42
Sub Total 4782 – 733 (Not Injected)	4049	100.00

CPU + Cache mem	Final SPFM (%)
DCPerm	91.3805878
MOE	±1.293%



SIEMENS

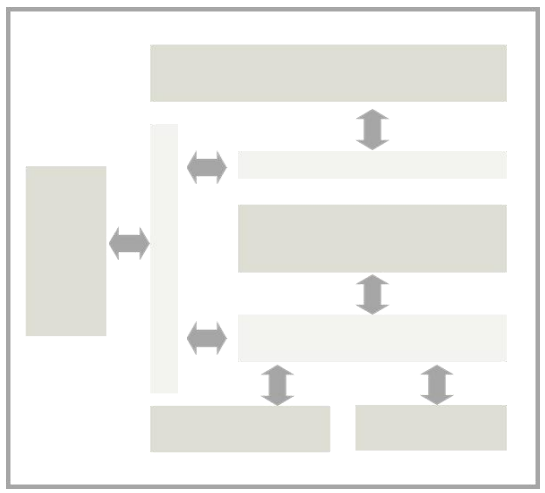
Fault List Optimization

An exhaustive fault campaign involves injecting and propagating millions of faults, which is a challenging task.
Fault list optimization techniques determine which faults could be excluded from the fault list for the current fault campaign.

General Optimization

- Faults that won't propagate
- Non-safety related faults
- Equivalent faults
- Failure Mode related faults

Fault List Optimization – Identify Non-Safety Related Nodes



Design with Safety Mechanisms

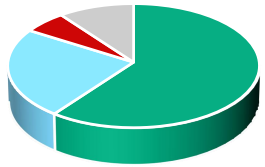
Non-Safety related faults

Safety related faults

Fault Campaign Target

Fault Campaign

Fault Classifications



Detected
Non-safety related
Undetected
Unclassifiifed

SIEMENS

Fault List Optimization using Austemper – Safety Mechanism Aware Faults

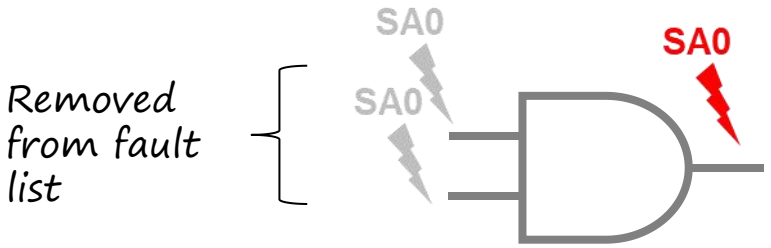
Austemper SafetyScope generates fault lists based on design files and the Safety Mechanism mapping files provided by user

- Permanent & Transient faults
- Only includes faults related to the specified Safety Mechanisms
- Faults defined as safe are excluded
- Read by KaleidoScope

SIEMENS

Fault List Optimization using Austemper – Collapsed Fault List Generation

Redundant faults are identified and fault list reduction is performed.

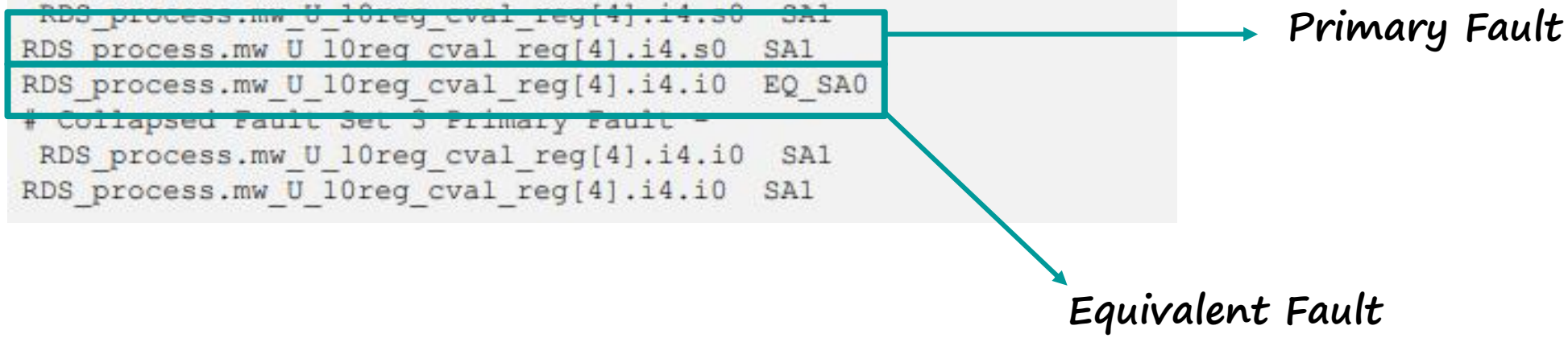


*SA0 on any one of the inputs results in a SA0 on the output. The three inject sites for the AND gate can be reduced to a single inject site (output)

SIEMENS

Collapsed Fault List Samples

```
# Port  Fault_Type
# Collapsed Fault Set 1 Primary Fault -
 RDS_process.mw_U_10reg_cval_reg[4].i4.s0  SA0
RDS_process.mw_U_10reg_cval_reg[4].i4.s0  SA0
# Collapsed Fault Set 2 Primary Fault -
 RDS_process.mw_U_10reg_cval_reg[4].i4.s0  SA1
RDS_process.mw_U_10reg_cval_reg[4].i4.s0  SA1
RDS_process.mw_U_10reg_cval_reg[4].i4.i0  EQ_SA0
# Collapsed Fault Set 3 Primary Fault -
 RDS_process.mw_U_10reg_cval_reg[4].i4.i0  SA1
RDS_process.mw_U_10reg_cval_reg[4].i4.i0  SA1
```

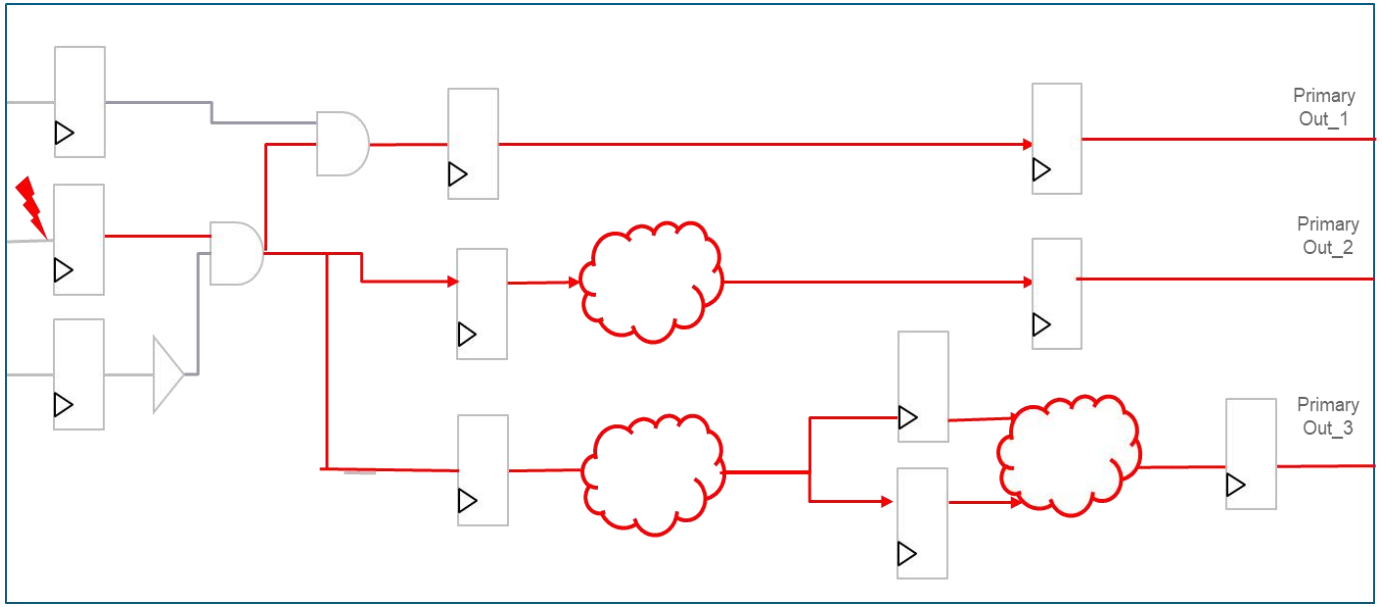


SIEMENS

The Limiting Factor

The amount of concurrent **faulty signals active** influences most the performance of a fault campaign

- Active Fan-outs ↑↑
- Active Faulty Signals ↑↑
- Signals Tracked ↑↑
- Computation Time ↑↑

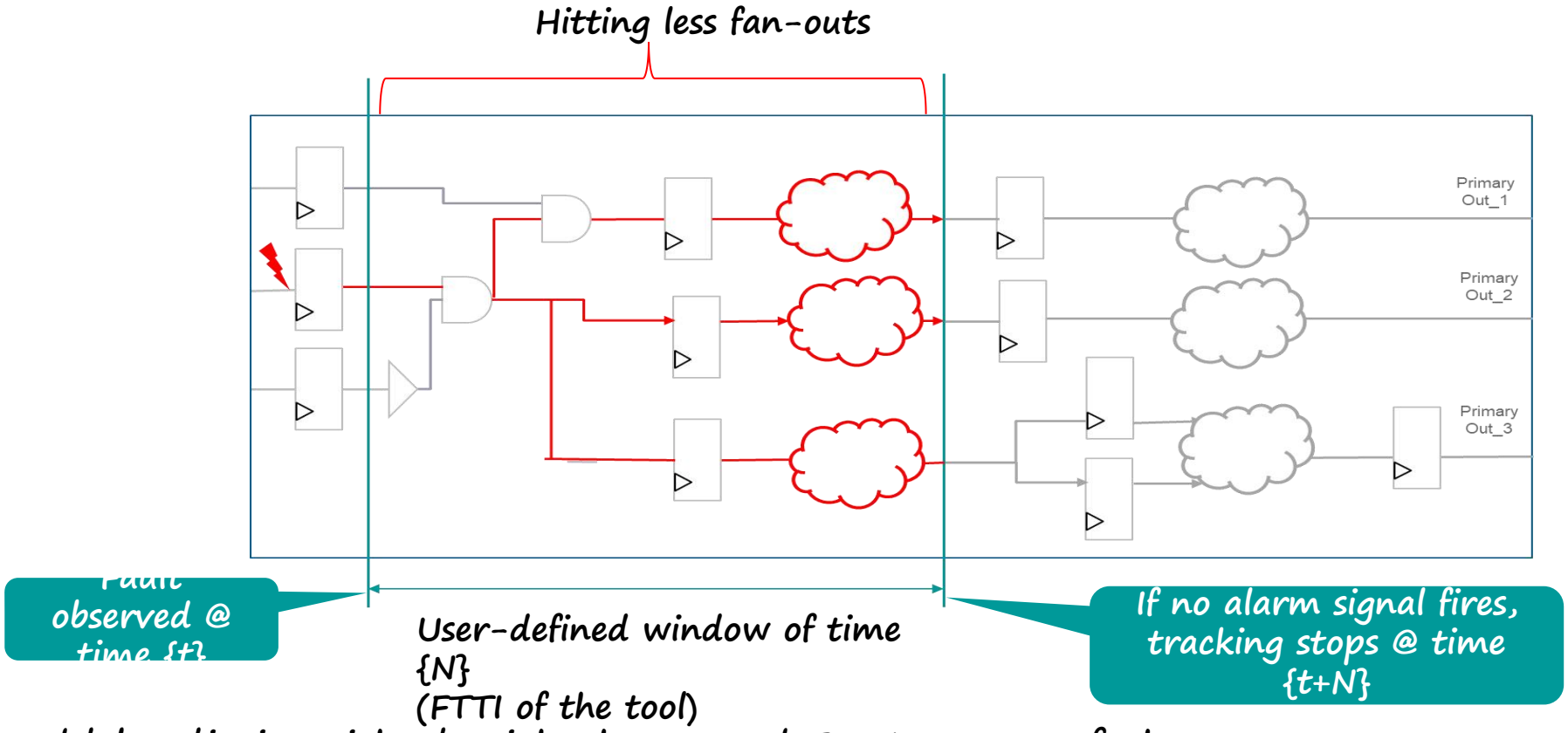


- A fault keeps propagating util the tool sees alarm signal fires.

SIEMENS

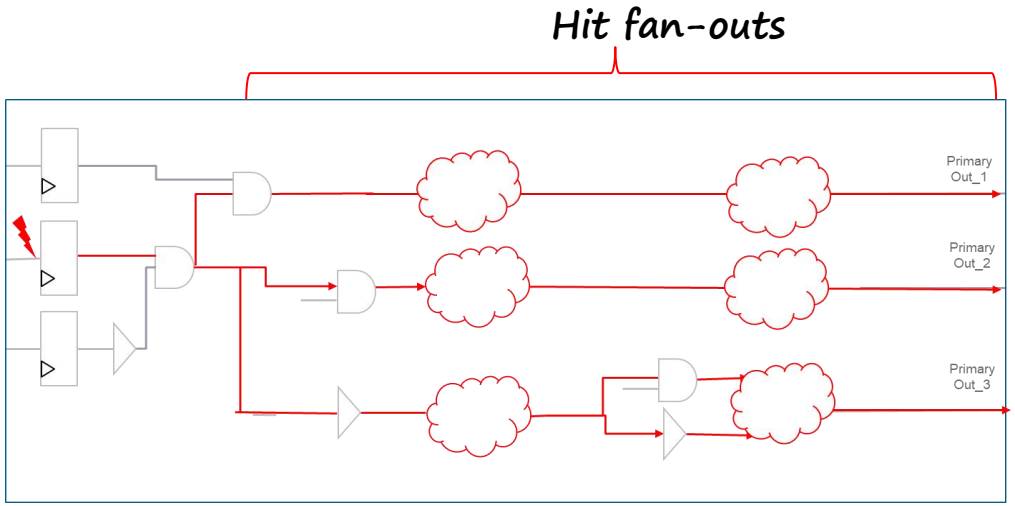
Avoid the Fan-out Expansion

In KaleidoScope, user can define the max time an observed fault is allowed in the system before an alarm fires, otherwise the faults are deemed as not detected

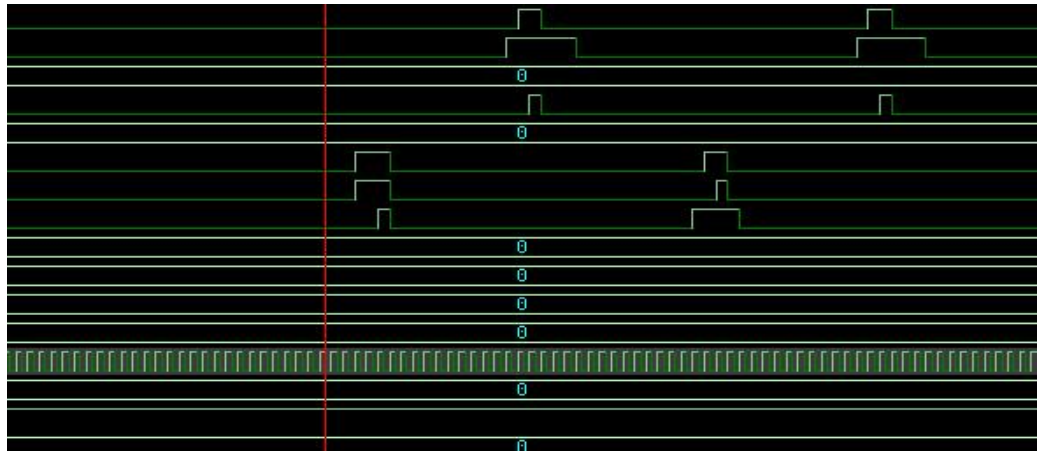


- Should be distinguished with the actual FTTI target of the core
- Find a balance to avoid missing alarm signals

Avoid the Fan-out Expansion



A fault hasn't reached an observe point and keeps propagating



Tool goes through the entire waveform until it finds the 1st injectable time point

Narrow down the search space by controlling the start and end simulation times

```
# qwave FILE     SIM_START_TIME     MAX_INJECT     SIM_END_TIME       FTTI
 DROP_NO_DEVIATION
one.db           100                500            10000              200
 700
two.db           150                -1             10000              -1
  600
```

Controlling sim_start_time and sim_end_time in KaleidoScope

SIEMENS

Avoid the Fan-out Expansion

KaleidoScope automatically divides fault campaigns into smaller parallel fault campaigns

- Specify the maximum number of concurrent faults in each parallel run
- Prevent having too many Undetected faults active and propagating

```
KaleidoScope \
        --mode                  kmanager_distributed          \
        --filelist              ./Inputs_KS/axi_cross_safety.f \
        --clkdef                ./Inputs_KS/axi_cross.clk     \
        --black_box_inst        ./Inputs_KS/inst_bbox.bbox    \
        --ini                   bbox_wildcard=true            \
        --ini                   print_blackbox_rpt=true       \
        --error_inject_inst     tb_top.u_dut.u_axi_cross      \
        --sim_vcd               ./Inputs_KS/vcd_filter.f      \
        --top axi_cross_wrapper_ATD_wrapper_ATD_wrapper_ATD   \
        --alarm                 ./Inputs_KS/AlarmList.txt     \
        --sim_start_time        150                           \
        --max_concurrent_fault  500                           \
        --fault_list            ./Inputs_KS/Fault_KMan.list   \
        --log_file Kman_run.log
```

- From Rambus's experiments, 600 to 1000 faults were their preferred numbers

SIEMENS

Speed up the Fault Campaign

Optimized Fault List

Accurate Tool FTTI

Max Concurrent Faults

High-toggling Waveform

Austemper SafetyScope

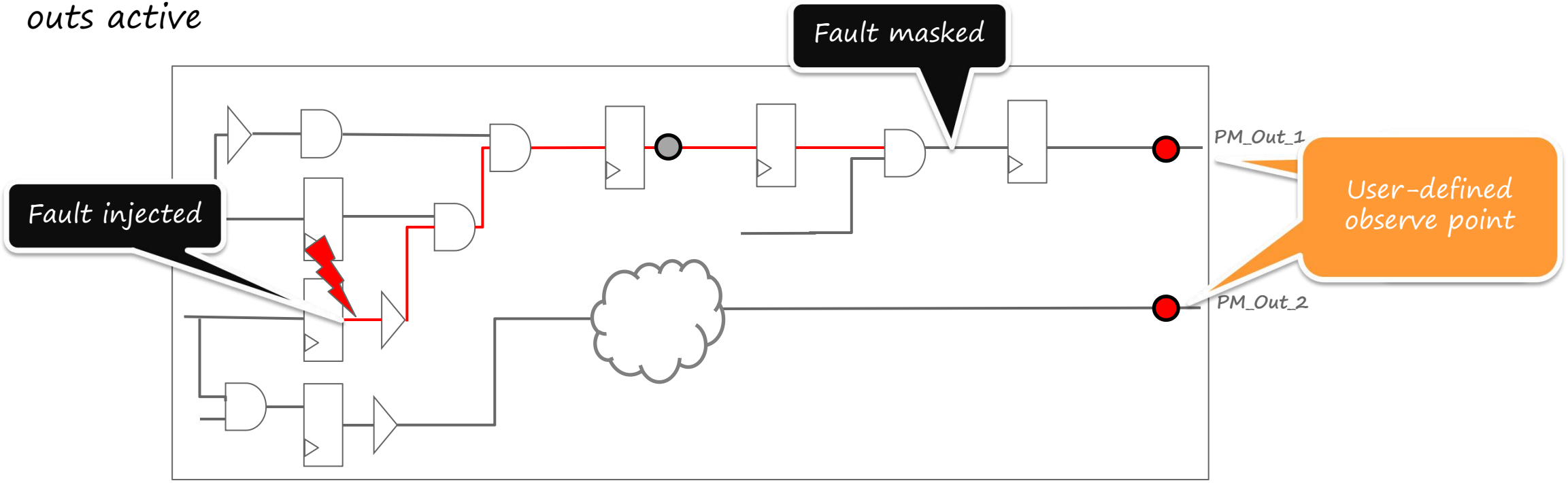
Austemper KaleidoScope

SIEMENS

Enable an Accurate Classification

The faults that will pose a risk for the core are faults that propagate to the primary outputs of RT-640

- By changing the default observe points to the core's primary outputs, the faults which are masked later in the circuit will be classified as Undetected_Unobserved as expected
- The problem is that these faults propagate much further, increasing the number of fan-outs active



SIEMENS

Two-step Fault Campaign
Reach a Great Compromise Between Efficiency and Thoroughness

Step 1

Run a first fault campaign with smaller FTTI and default observe points

- Rapidly process faults that can be detected within a smaller FTTI
- Other undetectable but observed faults are dropped after the FTTI which **avoids a blowup of active signals due to fan-outs**
- Determine faults not injectable

Step 2

Run a second fault campaign with selected faults from Step 1 and primary outputs defined as observe points

- A smaller fault list with only the *Undetected_Observed faults*
- Can find the **truly dangerous** ones that are reaching the primary outputs without setting the alarm signals

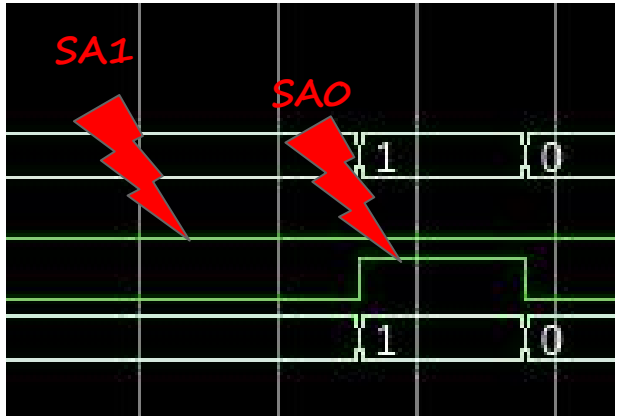
✓ **Efficient default observe point** ✓

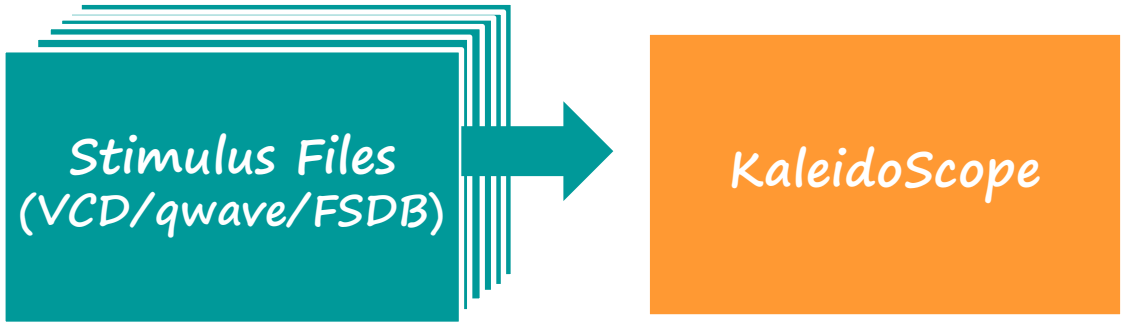
Complying with the classification model

Handling the Unclassified Faults – Not Injected

The downside of fault injection is its high dependence on the input stimuli

- Around 1/3 of the total faults are not classified
- Part of them are not injected
- Need higher-quality input stimuli to exercise the full core and have every signal toggling

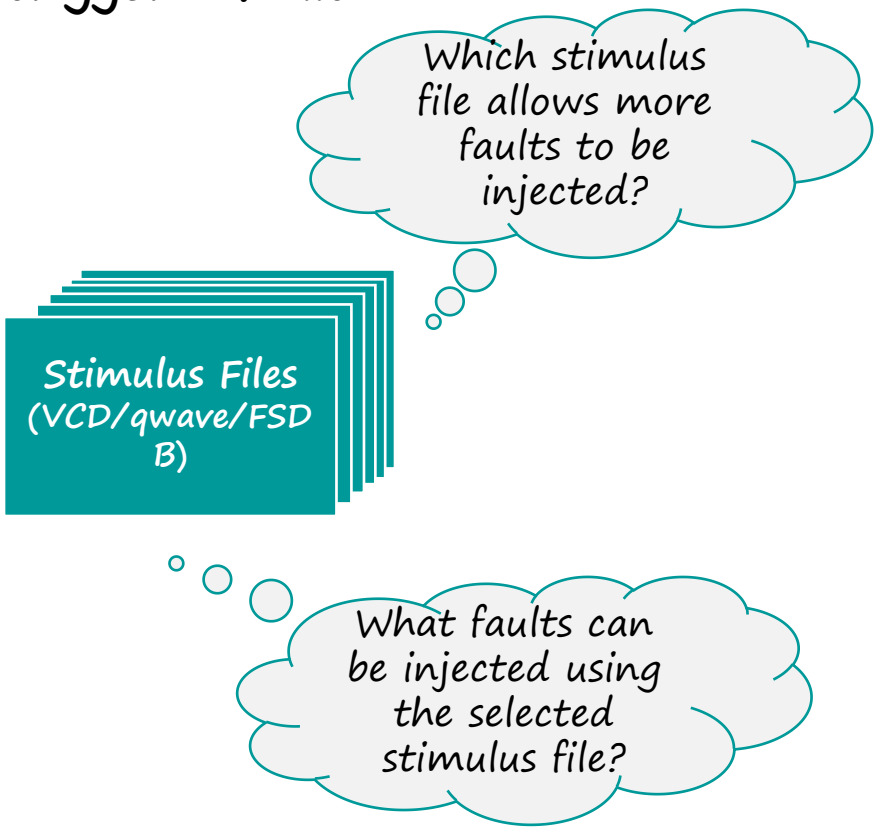




SIEMENS

Stimulus Grading
Rank stimulus for fault campaign efficiency

Ranks VCD/FSDB stimulus files by their ability to trigger a fault



#VCD_Name		SA1_count	SA0_count
<path>/vcds/qwave_rxtx_123.vcd	3624	3504	
<path>/vcds/qwave_rxtx_456.vcd	3624	3504	
<path>/vcds/qwave_tx_pkt_890459872.vcd	2967	2873	
<path>/vcds/qwave_tx_pkt_822784415.vcd	2967	2872	
<path>/vcds/qwave_reg_reset_28925691.vcd	1657	1608	

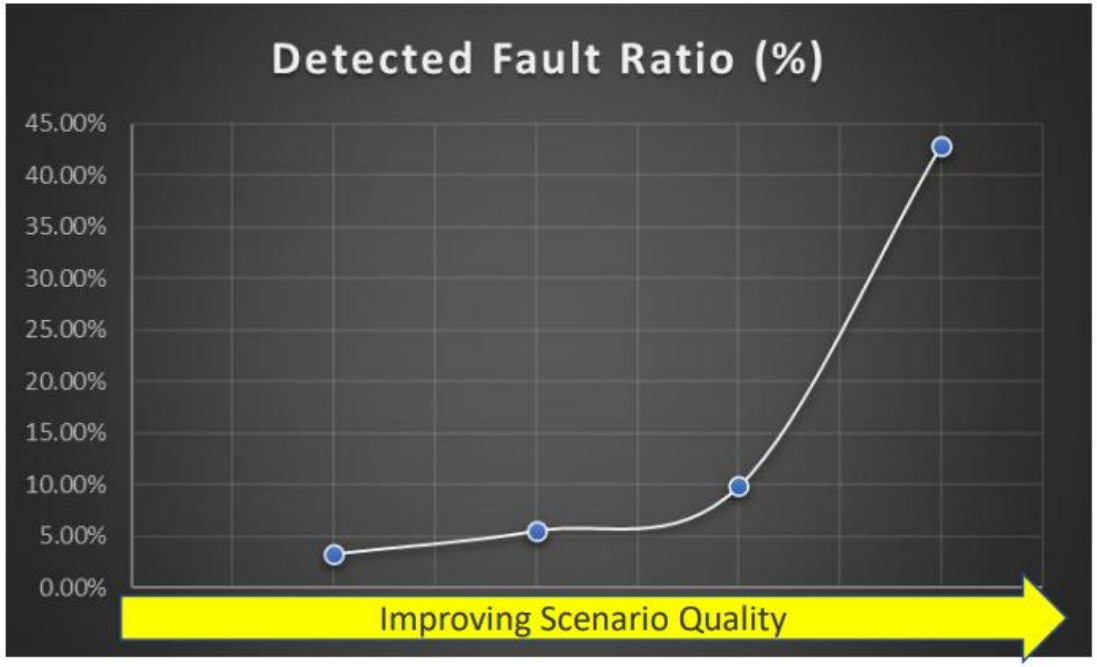
#VCD_File_Name	Total_Faults_count(SA1+SA0)
<path>/vcds/qwave_rxtx_123.vcd	7128
<path>/vcds/qwave_rxtx_456.vcd	7128
<path>/vcds/qwave_tx_pkt_890459872.vcd	5840
<path>/vcds/qwave_tx_pkt_822784415.vcd	5839
<path>/vcds/qwave_reg_reset_28925691.vcd	3265

SIEMENS

Experiment on Automotive SoC – Bus

The bus interface requires end-to-end protection where fault injection with simulation was determined to be efficient

- The initial set of stimuli didn't provide enough coverage
- More tests which have high traffic on the BUS to mimic the runtime operation state of the SoC



BUS Related Logic	Total Faults (SA0 + SA1)	Scenario 1: Detected	Scenario 2: Detected	Scenario 3: Detected	Scenario 4: Detected	Scenario 5: Detected
Fault (%)	100%	3.27%	5.50%	9.80%	42.81%	(TBD)

SIEMENS

Non-injected Faults Reduction

However, it is not always possible to provide enough stimuli of the right quality…

- Some blocks were tested with different testbench
- Not all the modes are used in the current configuration
- Take time to create new stimuli for EVERY non-classified fault

SIEMENS

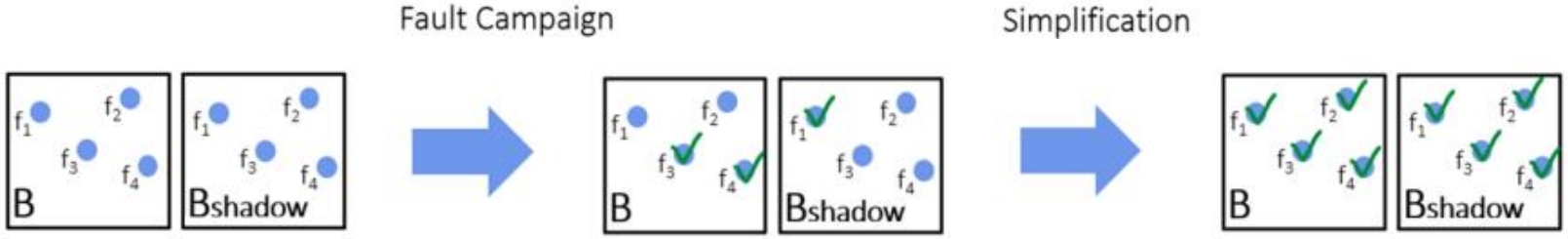
Non-injected Faults Reduction

Bus-simplification

- One or more bits detected for a particular fault
- No fault from the bus classified as not-detected

- Deem the other bits of this bus as detected

Duplication-simplification



- Multiple faults within a duplicated module detected
- No faults from this module classified as not-detected

- Deem the other faults in this duplicate module as detected

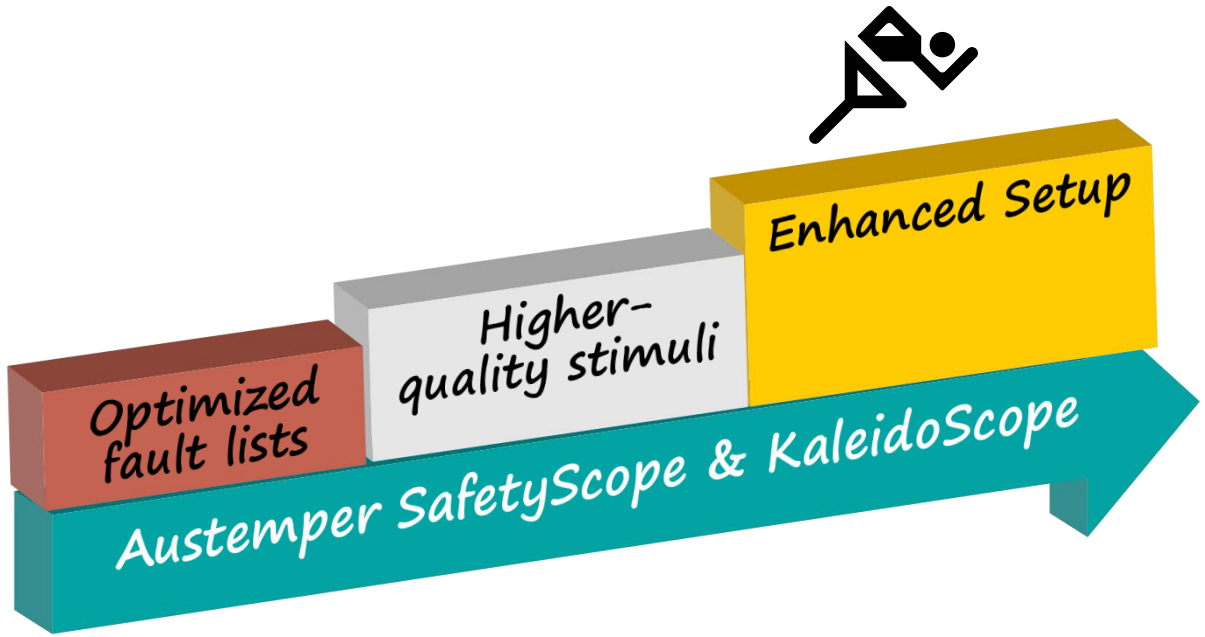
SIEMENS

Summary

Optimize fault lists
- Safety Mechanism Aware Fault list
- Collapsed faults list
- Safety-related faults

Improve stimuli quality
- Stimulus grading

Enhance setup
- Avoid activating too many fan-outs in a single simulation run



Perform analysis to reduce unclassified faults
- Engineering judgement
- Simplification strategies

Exploit the advanced tool that supports managed, high-performance safety verification
- Distributed fault campaign
- Clear fault classification

SIEMENS

References

Complex Safety Mechanisms Require Interoperability and Automation For Validation And Metric Closure, DVCON US 2023
Rambus RT-640 road to ISO26262 certification, Rambus white paper
Constructing an Efficient Fault Campaign, Verification Academy Course
Orchestrating an Efficient ISO 26262 Fault Campaign, Siemens EDA white paper
Austemper Tools: https://resources.sw.siemens.com/en-US/fact-sheet-austemper-analysis-and-fault-simulation
Mentor + Siemens Provides Solutions and Expertise to Achieve Rapid, Verification Academy Course
ISO 26262 Part 5: Product development at the hardware level, Second edition 2018-12

SIEMENS

Thank you!

Kara Liu
DVT Application Engineer
kara.liu@siemens.com

SIEMENS