Emerging Challenges and Solutions in Functional Safety and Security for Automotive, AI, Data Center, and Space Chips

SemIsrael Expo, 11 November 2025

Video recording of this presentation is at: https://youtu.be/JLj0wRr1pRQ

Optima Design Automation

Jamil Mazzawi, CEO ,
info@optima-da.com

www.optima-da.com

OPTIMA

This presentation is high level overview of:

- Safety and Security challenges of modern chips
  - Automotive, AI, Data Center and Space segments
- Relevant standards
- Required fault-modeling
- Common Safety Mechanism and Security protections
- EDA challenges in verifying these
- How Optima solutions solves these challenges

Optima provides power full EDA solutions (and services)
for both Functional Safety Security Verification (pre-silicon)
These slides gives VERY high level-intro on these 2 topics,
more on the challenges and less on the details of Optima's solutions (to fit in 20 min talk)
We will be happy to schedule meeting to discuss our solutions in more details!

Optima's vision:

Provide maximum automation and integration for all Functional Safety and IC-Security EDA challenges, to allow our customer to achieve faster convergence on their FuSa and IC-Security targets, and to create Safe and Secure chips and IPs at fraction of the cost and effort

OPTIMA

Enabling the highest Functional Safety and IC-Security levels at fraction of effort

Founded in 2014, in Nazareth, Israel

TÜV NORD Trusted Tool
OPTIMA-SA™
OPTIMA-HE™
OPTIMA-SE™
Qualified up to
ISO 26262:2018 ASIL D

SGS TÜV SAAR
ASIL D READY
Functional Safety
www.sgs-tuev-saar.com

Functional Safety and ISO-26262 Optima Safety Platform: OSP

Optima-SA™
Static Analysis Solution

Accurate failure-mode-sizing for FMEDA, early identification of Safety issues

Optima-CA™
Constant Analysis

Measure impact of low-toggle on Safety

Identify unused logic, classify as Safe

Optima-HE™
Hard-Error Coverage: Measure & Boost

Rapid fault coverage measurement with automated coverage boosting

Optima-SE™
Soft-Error/ Transient Fault Mitigation

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

IC-Security Verification

Optima-FAS™ Optima-SIFA™

Fault Attack & Side Ch. Simulation

Security Information Flow Analysis

Safety Services

Sample of possible service packages:

Safety Concept

Safety implementation

Safety Verification

STL Convergence

STL Development from scratch

Test Pattern convergence

Kick starter package

Technologies

- **Built in Fault-simulator:** Orders of magnitude faster than competitors, multi-threaded
- **Semi-formal analysis engines:** Static Analysis, Constant Analysis
- **Debug and recommendation Engines:** SCM, DCM, Test Optimization

Multiple chip segments has Safety and Security requirements

Safety

- Automotive – ISO 26262
- Data Center
  - Soft-error detection & mitigation
  - In-system monitoring
  - FIT rate compliance
- Space chips
  - Soft-error detection & mitigation
- Industrial – ICE 61508

Security

- Automotive – ISO 21434
- Other Segments:
  - Smart-Card chips
  - Gaming chips
  - Space chips
- Needs
  - Securing the Secret assets in the chip
  - Protection against Fault-injection and side-channel attacks






Functional Safety (FuSa) in 1 slide:

- Faults can happen in the chips, while they are working!
- FuSa is about: Preventing faults, Detecting them or Correcting them fast-enough to allow the system to take the right action
- What are faults?

Hard Errors – Permeant faults	Soft Errors – Transient faults
• Permanent damage to the chip • Due to wear and tear • Happens while the chip is working • Mostly modeled as: stuck-at-1 and stuck-at-0	• No permanent damage to the chip • Bit-flip on flip-flop (change from 0 -> 1 or 1 -> 0) • Happens while the chip is working

Safety Mechanisms are used: to Prevent, Detect or Correct faults

Chip designer needs to add Safety Mechanisms (SM) to their chips to Prevent, Correct or Detect faults. Examples:

- Parity, CRC and ECC: can detect and correct
- DCSL (Dual Core Lock Step): a module is duplicated twice, all the outputs are compared every cycle => allows detection of faults
- TMR (Triple Module Level Redundancy): detection & correction
- TMR at the flip-flip level: detection & correction => Prevention
- STL – Software test Library – software that perform “self-test” to test the CPU
- SLT - System-Level Test – similar to STL but for data-center chips
- Test Pattern – used mostly for data-transformers designs
- And more ….

Illustrating FuSa challenges using 3 Safey mechanisms examples

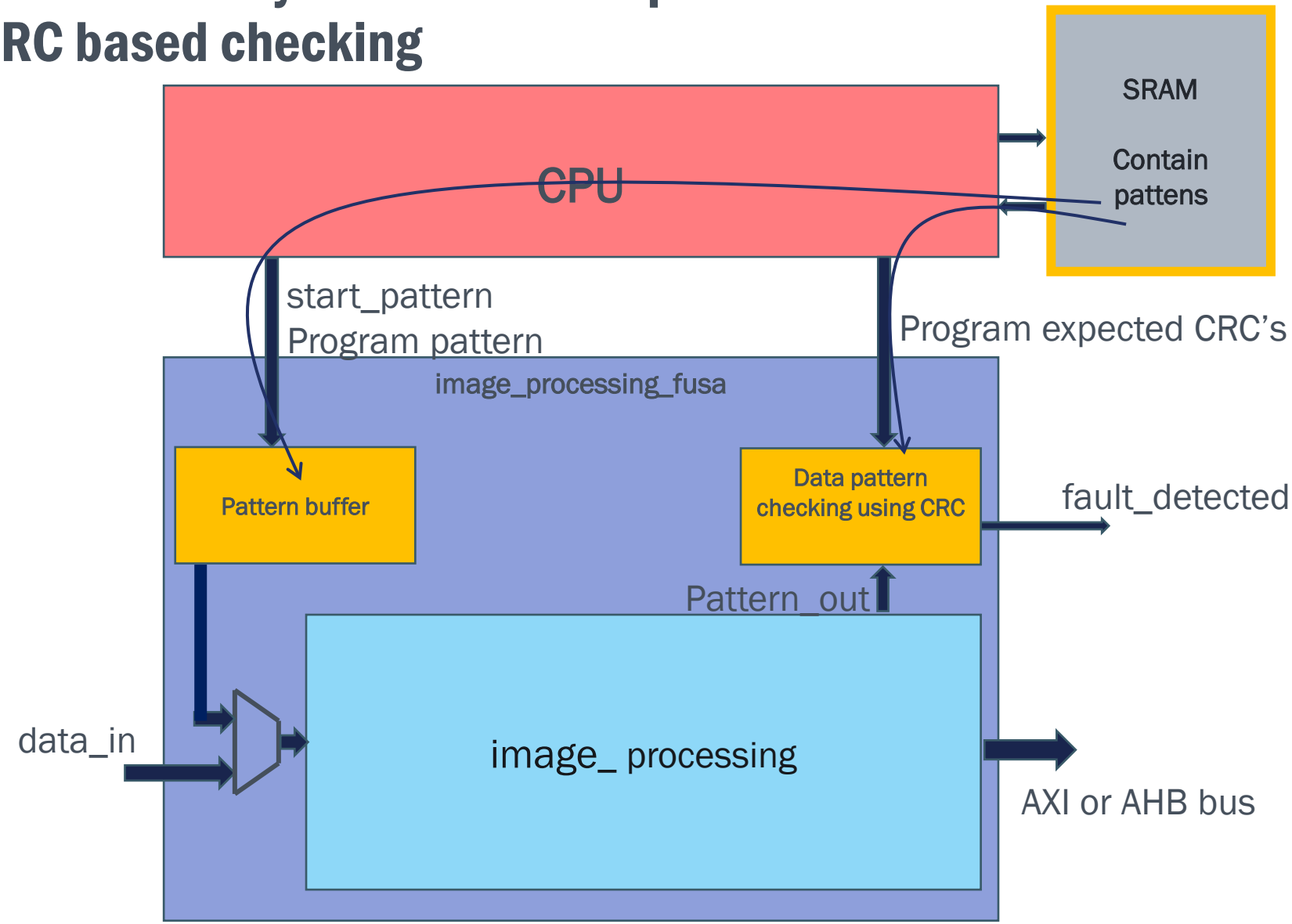
- Data-Pattern
  - For Hard Error Detection
  - In Image Processing unit
  - ASIL-B to ASIL-D
- STL
  - Hard Error Detection
  - In ASIL-B CPU
- Flip-flop level selective-hardening
  - For soft-error prevention
  - Any design
  - Any ASIL

Ex1: Data-Pattern for Hard Error Detection in Image Processing unit

- Used mostly on designs that performs calculations or data transformation, designs that take “frame_in” as input, transform it, and send it out as “frame_out”
- Examples:
  - Image processing
  - AI
- The Data-Pattern Safety Mechanism sends N fixed and known frame_in’s, then compares the output frames to match expected frame_out
- If frame_out do not match the expected, a fault was detected

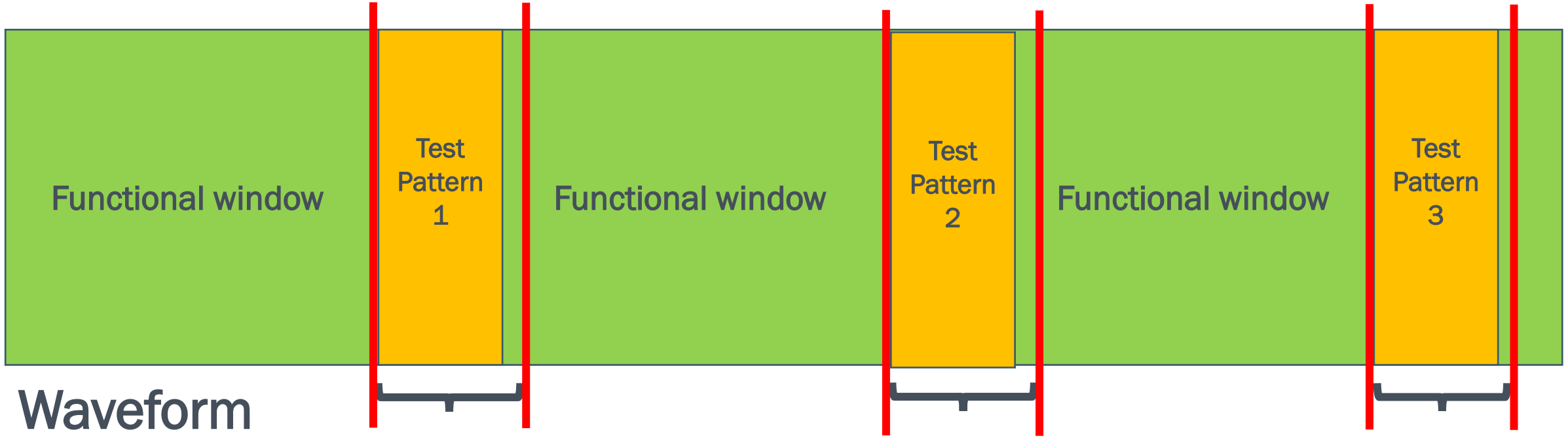
SM: Data pattern

Patterns saved in memory CPU moves the pattern to a buffer CRC based checking



SM: Test Pattern:

Test Patterns are sent in dedicated time-windows during chip operation



The goal from Functional Safety verification for data-pattern:

- How many of the possible faults can my N=3 frames detect?
  - I need to reach Diagnostic Coverage rate of DC=90%
- If my 3 frames don't detect enough, how do I create "smarter frames" that detects more faults?
- How can I reach my Detection rate with the least number of frames?

- EDA challenges:
  - Fault-simulation time can be very long
  - How do I automate the process?
  - How do I know how to improve my "frames" given coverage results?
  - How do I deal with unused parts of the RTL?
  - How do I shorten my STL run time?

Ex2: STL Software Test Library

- Relevant mostly for CPU's
- A self-test software that needs to test all the logic of the CPU
- Benefit: Zero Hardware cost
- Drawback: very hard to reach required coverage
  - Usually used for ASIL-B CPUs
  - So, DC requirement is 90%

```
li t0, 5              # t0 <= 5
li t1, 7              # t1 <= 7
add t2, t0, t1        # t2 <= t0+t1
li t3, 12             # t3 <= 12
bne t3, t2, fault_detected # Branch
…
#fault_detected:
 … Report error was detected
```

The goal from Functional Safety verification for STL:

- I need to reach certain DC
  - DC=90% means 90% of the possible faults need to be detected by some STL code!
- Reduce the length of the STL
  - Running STL means stopping the CPU from performing its functional operation
  - So, reducing this “interrupt” time is very important
- Process:
  - Write version 1 of the STL
  - Perform fault-simulation
  - Examine results
  - Improve STL to detect more faults
  - Repeat until reaching the goal
- EDA challenges:
  - Fault-simulation time can be very long
  - How do I automate the process?
  - How do I know how to improve my STL given coverage results?
  - How do I deal with unused parts of the RTL?
  - How do I shorten my STL run time?

Ex3: Flip-flop level selective-hardening for soft-error

- Soft-error can happen at any flop-flop while operating and its value is flipped
- According to multiple researches and industry experience:
  - Not all flops are critical to the operation of the system
  - Many soft-error will be corrected “naturally” by the HW
- So, if we know which flip-flops are critical, we can harden only these flip-flops
  - Hence, solve the problem, with low silicon and power cost
- In many cases, and in combination with other SM’s, only 5-10% of the flip flops need to be harden to reach the required standard goals

Relevant Segments: Automotive ISO-26262, Space, Data Center

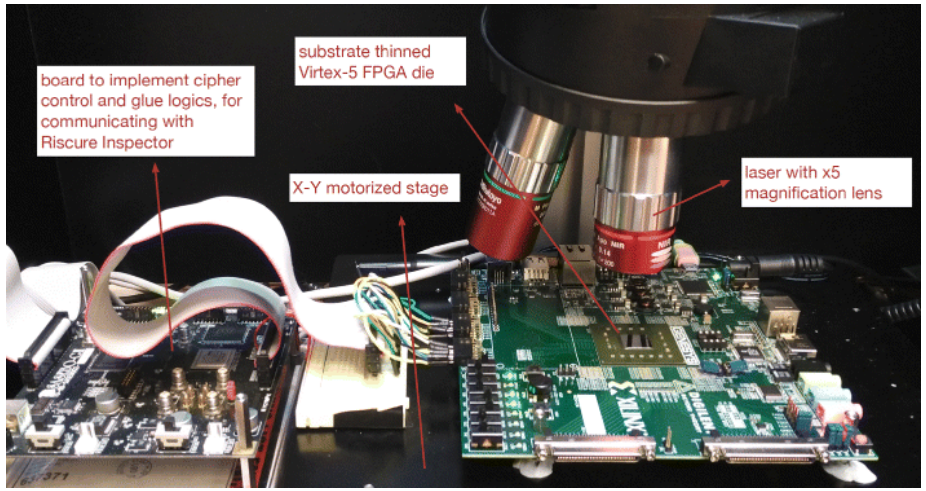
Goals and challenges faced in Soft-error mitigation

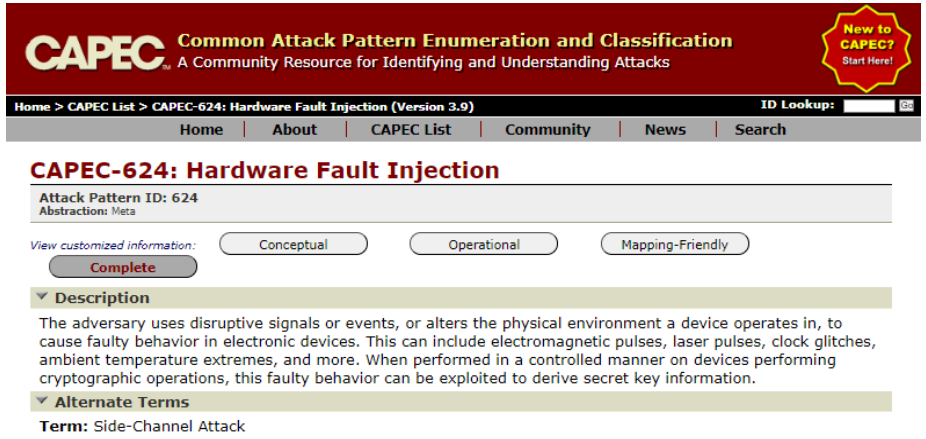
- Goals:
  - How can I identify the flip-flops to protect?
  - Once protection is added, how can I measure its effectiveness
  - What if I mix and match different Safety Mechanisms?

- EDA challenges:
  - If “normal” fault-simulators are is used, this can very long fault-simulation campaign (weeks to months for each run)
  - How do I collect and manage results for millions for flip-flops in modern chips?
  - What methodology should I use?

Security: Fault-injection and side channel Attack

- Modern chips includes “secret assets”
  - Like encryption keys
- These assets are hard-coded inside the chip
- Attackers can and do:
  - Buy a device with the chip from the open market
  - Attack the chip in very sophisticated labs
  - Using attacks like: Laser or EM based fault-injection
  - And use Side channel to extract the secret assets from the chip
- Once the secrete assets are extracted
  - Any device with the same chip can be attacked
- Fault Injection Attack is one of the key attacks defined in CAPEC as #624





Implementing and verifying counter-measure against this attack

- Chips designer needs to implement counter measure to protect against these attacks
- Once implemented, “verification” of its effectiveness is required.
- Today, most chip companies rely on either:
  - FPGA based lab-based testing => expensive, less visibility
  - Post-silicon, lab-based testing => Very expensive, less visibility, late in the cycle to correct

Mitigations

Implement robust physical security countermeasures and monitoring.

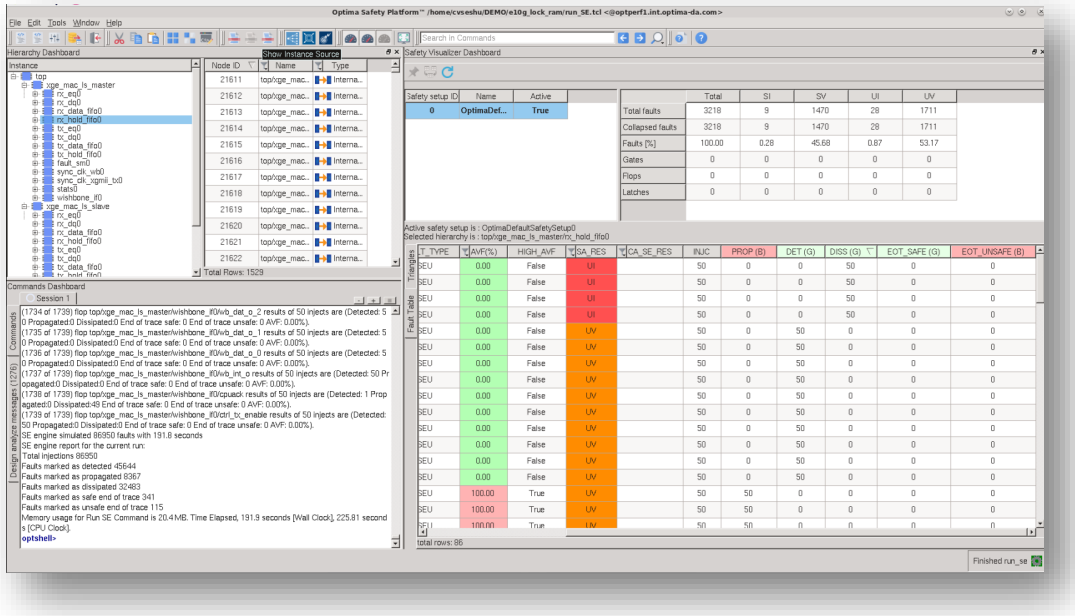
Related Weaknesses

CWE-ID	Weakness Name
1247	Improper Protection Against Voltage and Clock Glitches
1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications
1256	Improper Restriction of Software Interfaces to Hardware Features
1319	Improper Protection against Electromagnetic Fault Injection (EM-FI)
1332	Improper Handling of Faults that Lead to Instruction Skips
1334	Unauthorized Error Injection Can Degrade Hardware Redundancy
1338	Improper Protections Against Hardware Overheating
1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments

Optima is offering pre-silicon-based solution

Introducing: the Optima Safety and Security Platform

- Single software platform for all your FuSa and Security challenges.
- Dedicated flows and methodology for:
  - STL development
  - Data-Pattern
  - Soft-errors
  - Security and Fault Attack simulation
- Automated FMEDA reporting
- Automated fault-debug flow



Ultra-fast faut-analysis and fault-simulation engines

Used by multiple customers in 8 countries

OSP is ISO-26262 certified by TÜV Nord and SGS-TUV

❑What is certified:

- Optima Safety Platform with all its configurations: SA, CA, SE and HE

❑Certification type:

- Trusted Tool

❑Certification level:

- Up to ASIL D
- OSP can be used during the development of Safety related system up to ASIL D according to ISO 26262

❑**FSCSE:** 3 team members have personal ISO 26262 certification

SGS TÜV SAAR

CERTIFICATE NO FS/71/220/23/1030 PAGE 1/1

ZERTIFIKAT NR.:

LICENCE HOLDER & MANUFACTURER

GENEHMIGUNGSINHABER & HERSTELLER

Optima Design Automation Ltd.
Gallery building, 2004 Street #1
P.O. Box 266
Nazareth, 1610102
Israel

PROJECT NO/-ID	LICENSED TEST MARK	CERT. REPORT NO.
T4ZF-AU01	SGS TÜV SAAR ASIL D READY Functional Safety	T4ZF0001 is an integral part of this certificate.

Certified product(s) Tool Classification Report for Optima Safety Platform

Revision 2.0

Tested according to ISO 26262-8:2018; clause 11.5

Technical Data and Parameter The "Tool Classification Report for Optima Safety Platform" and the "Optima Safety Platform™ (OSP) User Guide" provides a description and best practices information in the use of Optima Safety Platform.
The argumentation of the "Tool Classification Report for Optima Safety Platform" shows an increased level of confidence due to the classification process to meet a TCL1.
Therefore, Optima Safety Platform can be used during developing of safety related systems up to ASIL D according to ISO 26262.

TÜV NORD

DAkkS Deutsche Akkreditierungsstelle D-ZE-11074-01-00

Certificate

No. 1435.IM.115125/20, V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies to

Optima Design Automation
Nazareth, 16102,
ISRAEL

that the application suite

Optima Safety Platform
OPTIMA-SA™, OPTIMA-HE™, OPTIMA-SE™

meets the tool requirements listed in the below mentioned standards

- ISO 26262:2018; Part 8; Section 11; Qualified up to ASIL D

Certification Program Leittechnik (SEB-ZE-SEECERT-VA-320-20, Rev. 5.1/4.19)

Base of certification is the report 1435.IM.115125/20TB and the tracking list in the valid version. This certificate entitles the holder to use the pictured Trusted Tool mark

Valid until: 2026-06-29
File reference: 8117498213

Hamburg, 2021-06-29

B. Pfuff
Bianca Pfuff

TÜV NORD Trusted Tool
OPTIMA-SA™
OPTIMA-HE™
OPTIMA-SE™
Qualified up to
ISO 26262:2018 ASIL D

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany

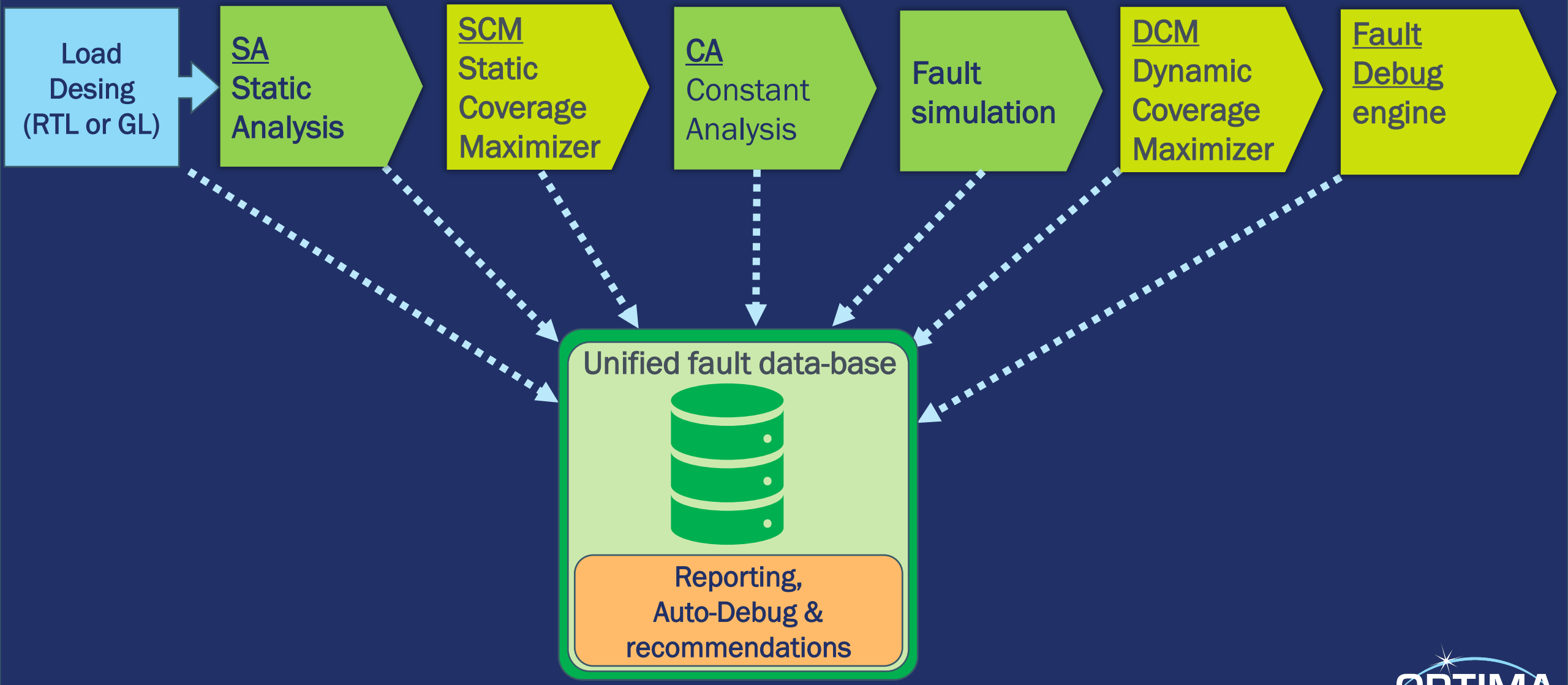
Fault Analysis != Fault Simulation

- Fault Analysis includes multiple engines

  Fault-simulation is one of these engines

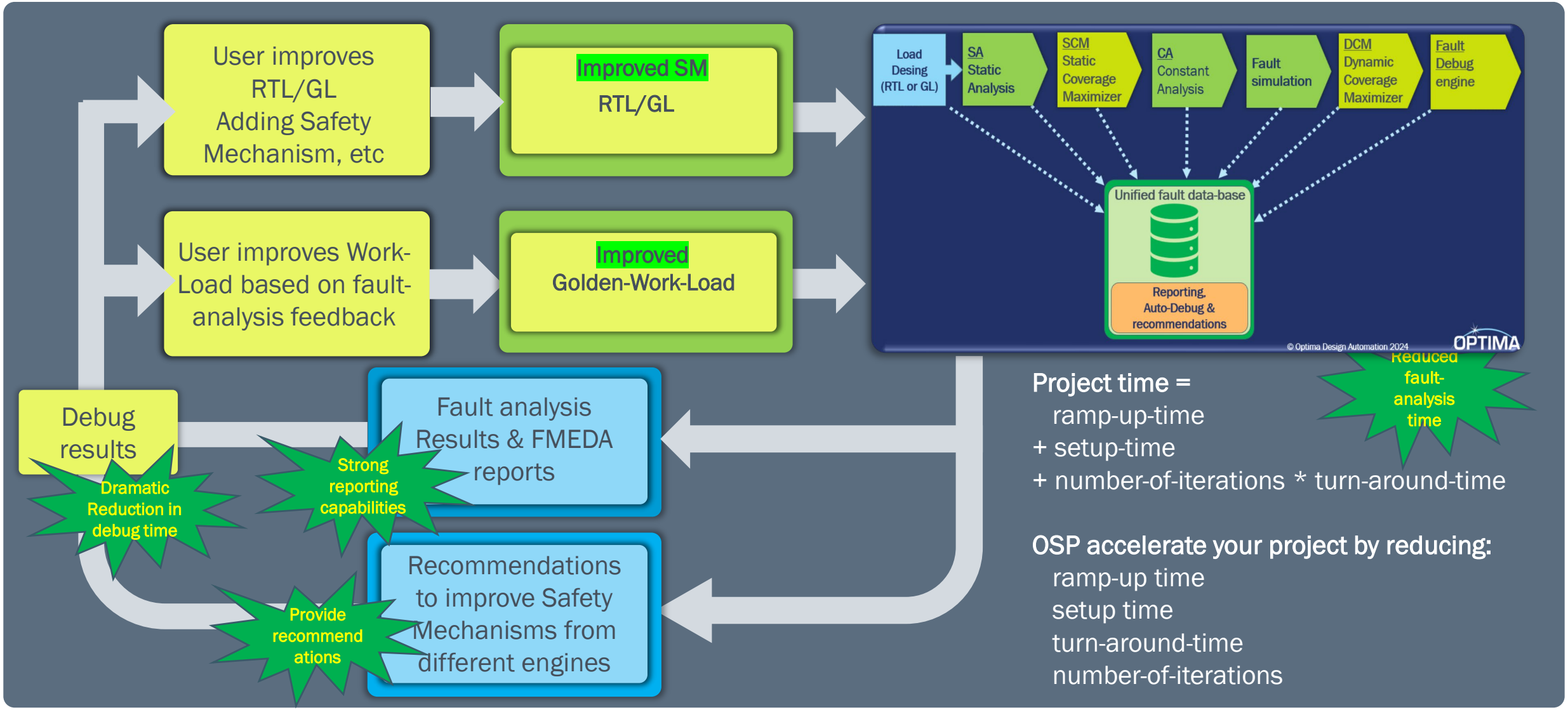
- Each engine specializes in identifying or resolving certain type of faults
- Multiple engines allow user much deeper understanding of the fault-analysis results & make debug much easier

OSP's Automated and integrated Fault-analysis flow



OPTIMA

Fault analysis cycle and it's challenges



Functional Safety and IC Security Solutions

For more information and to schedule a demo meeting, please drop us an e-mail

www.optima-da.com

info@optima-da.com