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
*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**
- Dedicate STL process that reads and writes to CPU register to check its 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
- Lack of visibility to improve coverage: very manual process
- Lack of automation

General challenge:
- Lack of automation

Flowchart:
- Write SW Test
- Measure Coverage
  - Enough?
    - Yes: Done
    - No: Measure Coverage
Challenges:

A. Write SM
B. Run w/ competing tool
C. Examine Coverage
   Results: Meeting req?
   - No: Come up with ways to improve coverage
   - Yes: Fine-tune SM

#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

1. IP Design w/ Resource Data
2. Safety Setup
3. IP Design w/ Resource Data and structural analysis results
4. Fault Injection Campaign commands
5. Fault Injection Results

User loads design in Optima
Optima performs structural analysis
Optima performs fault-injections campaigns

User decide on Safety Setup
User decides on fault-injection needed FME(D)A, FTA, DFA
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
High-level Safety Flow

- Pre-RTL analysis
  - FMEA/FMEDA
  - Estimate

- RTL based analysis
  - Structural analysis
  - Fault-simulation

- Netlist based analysis
  - Structural analysis
  - Fault-simulation

- 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
- 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

E10GMAC (master)

Unit inputs

Internal memory

Compare outputs

Unit outputs

Failure-strobes

Detection-strobes

E10GMAC (shadow)

Internal memory

set_output_criticality ALL_OUTPUTS
set_detection_nodes {fault_detected}
Optima’s Structural analysis

Failure Strobes (Critical COI)

SI
Safe Invisible

UI
Unsafe Invisible
Structural analysis

Detection Strobes (Detection COI)

SI
Safe Invisible

SV
Safe Visible
Structural analysis

- **Safe Visible (SV)**
- **Unsafe Visible (UV)**
- **Unsafe Invisible (UI)**
- **Safe Invisible (SI)**

- **Detection Strobes (Detection COI)**
- **Failure Strobes (Critical COI)**

**Failure Strobes**
- **Critical COI**

**Detection Strobes**
- **Detection COI**

**Unsafe Visible (potentially detectable)**
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"

Diagram Courtesy International Standards Organization (ISO)
Mapping Optima’s Structural analysis to FMEDA terms

- **SF** Safe Faults
- **SI** Safe Invisible
- **SV** Safe Visible
- **UI** Unsafe Invisible
- **UV** Unsafe Visible (potentially detectable)
- **Residual Faults & Multi point Faults: Detected & Intermixed**
- **SPF** Single Point faults
Optima-SA™ demo
### 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….

- **SF** Safe Faults
- **SI** Safe Invisible
- **SV** Safe Visible
- **UV** Unsafe Visible (potentially detectable)
- **UI** Unsafe Invisible
- **Residual Faults & Multi point Faults: Detected & Intermixed**
- **SPF** Single Point faults
Optima-HE results:

- SI: Safe Invisible
- SV: Safe Visible
- UI: Unsafe Invisible
- UVD: Unsafe Visible Detected
- UVR: Unsafe Visible Residual
- UVR: Unsafe Visible Residual
- UV - Unsafe Visible
Optima-HE results:

- **SF** – Safe Faults
- **Multi point faults: Detected**
- **Residual Faults**

**UI**
- Unsafe Invisible
- Unsafe Visible
- Unsafe Visible Residual

**SV**
- Safe Visible

**UI**
- Unsafe Invisible

**UVD**
- Unsafe Visible Detected

**UVR**
- Unsafe Visible Residual

**U - Unsafe Visible**

**SPF** – Single Point faults

**SPFM**

\[SPFM = \frac{UVD}{UI + UV} = \frac{UVD}{UI + UVR + UVD} = 1 - \frac{UI + UVR}{UI + UV}\]
Optima-HE™: Complete Hard-errors solution

- RTL/Gate-level
- Safety Setup
- Coverage goal

Optima HE™: Complete Hard-errors solution

- Coverage results
- CoverageMaximizer™ recommendations
- FMEDA Parameters for ASIL calculations
- FMEDA data for Medini

Optima FAULT INJECTION ENGINE (FIE™)
Over 1,000X faster than competing solutions
Application Example: Tuning STL – Software Test Library

A: Write STL

B: Run Optima-HE

C: Examine Coverage Results: Meeting req?
   Yes: Done
   No: Examine Coverage Maximizer™ outputs

D: Examine Coverage Maximizer™ outputs
   No: Fine-tune STL based on CB
   Yes: 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

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Exhaustive fault simulation</td>
<td>• Faster fault simulation</td>
</tr>
<tr>
<td>• Safety-Mechanism coverage</td>
<td>• High accuracy</td>
</tr>
<tr>
<td>• CoverageMaximizer™:</td>
<td>• Low effort coverage boosting</td>
</tr>
<tr>
<td>• guidance for raising coverage</td>
<td>• Reduce Time-to-Market</td>
</tr>
<tr>
<td>• For both gate-level and RTL</td>
<td>• Reduce design costs</td>
</tr>
<tr>
<td></td>
<td>• Reduce needed compute resources</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Method</th>
<th>Cost Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit-level Lockstep mechanism</td>
<td>70% more silicon</td>
</tr>
<tr>
<td>Hardening all flops</td>
<td>30% more silicon</td>
</tr>
<tr>
<td>Selective flip-flop hardening</td>
<td>1-5% more silicon</td>
</tr>
<tr>
<td>Using older silicon nodes (like 180nm)</td>
<td></td>
</tr>
<tr>
<td>Using special Rad-Hard silicon technology</td>
<td></td>
</tr>
</tbody>
</table>
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 projects 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.

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.

Does your derated-FIT rate meet your requirements?
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

- **AVF report** (for selective hardening)
- **FMEDA Parameters for ASIL calculations**
- **Audit trail** (for certification)

**Optima FAULT INJECTION ENGINE (FIE™)**
Over 1,000 faster than competing solutions
Another way to look at it: FIT rate calculation

**Without knowing** the “personal” AVF of each flip-flop

\[ \text{FIT}_{\text{chip}} = n \times \text{fit}_{\text{unhard}} \]

**With knowing** the “personal” AVF of each flop

(Using Optima-SE or other methods)

\[ \text{FIT}_{\text{chip}} = \sum_{k=0}^{n} (\text{AVF}(k) \times \text{fit}_{\text{unhard}}) \]

**Without hardening**

**With knowing** the “personal” AVF of each flop

(Using Optima-SE or other methods)

**With selective hardening of m flops**

\[ \text{FIT}_{\text{chip}} = \sum_{k=0}^{m-1} (\text{AVF}(k) \times \text{fit}_{\text{hard}}) + \sum_{i=m}^{n} (\text{AVF}(i) \times \text{fit}_{\text{unhard}}) \]

\[ n = \text{Number of flops in the chip/IP/unit} \]
\[ \text{AVF}(k) = \text{The “personal” AVF of specific flop } k \]
\[ m = \text{number of hardened flops} \]

\[ \text{FIT}_{\text{chip}} = \text{FIT Rate for the chip/IP/unit from flop from soft-error} \]
\[ \text{fit}_{\text{unh}} = \text{FIT Rate of a single flop, unhardened regular flop} \]
\[ \text{fit}_{\text{hard}} = \text{FIT Rate of a single flop, for hardened flop} \]
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

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculate derated FIT rate</td>
<td>• High accuracy</td>
</tr>
<tr>
<td>Selective-hardening</td>
<td>• Improve ASIL</td>
</tr>
<tr>
<td>Lower FIT rate to close to 0</td>
<td>• Reduce:</td>
</tr>
<tr>
<td>Measure SM effectiveness</td>
<td>• Time-To-Market</td>
</tr>
<tr>
<td>1,000x faster than competing solutions</td>
<td>• Silicon and power</td>
</tr>
<tr>
<td></td>
<td>• Compute-resources needs</td>
</tr>
</tbody>
</table>
Terminology
<table>
<thead>
<tr>
<th>“Old” Scientific term</th>
<th>ISO-26262 term</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| SEU                    | TF Transient-fault | Bit-flip at a storage element:  
| Single Event Upset     |                | • memory bit  
|                        |                | • latch  
|                        |                | • flop  
|                        |                | Soft: No hardware damage happened |
| SE                     | TF Transient-fault | Particle hitting a gate, causing a glitch that travels through the combinatorial logic |
| Soft-Error             |                | It may be latched at flip-flop ➔ become SEU  
|                        |                | Mostly, it will not be latched and dissipate |
| SET                    | TF Transient-fault | Physical damage in the chip.  
| Single Event Transient |                | 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