Automotive Safety and Security in a Verification Continuum Context

Accelerating the Development of Automotive Electronic Systems

Jean-Marc Forey
Automotive Functional Safety Professional
Synopsys Inc.
April 2017
Agenda

Addressing the design challenges along the automotive electronic supply chain

Requirements for SoC functional safety verification
  Functional qualification
  Functional safety fault simulation

Summary
Automotive Opportunities for Semiconductor Companies

Electronics cost per car doubled in the last 10 years - Today 40% of total cost

Automotive Systems (Tier1/OEM)
- Powertrain EV/HEV (Emission)
- ADAS & Autonomous (Safety)
- Vehicle ‘Living room’ (Mobility)
- Safe (ISO 26262), Secure and Connected

Automotive Semis
- Many SoCs - vision, radar, gateways, vehicle dynamics, …
- Increasing complexity and software
- ISO 26262 Compliance
- Lead customer collaboration
Key Automotive Challenges in the Supply Chain

- **OEM Tier 1**
  - SoC/MCU w/ right functionality and performance
  - Increased complexity of ECU hardware and software content

- **Semi**
  - Deliver more software w/ high quality
  - Verify complex SoC/MCU functional, AMS, low power
  - Deliver ISO 26262 compliance
Key Automotive Challenges in the Supply Chain

... and How Market Leaders are addressing them

OEM Tier 1

- SoC/MCU w/ right functionality and performance
  - Collaborate on architecture definition

- Increased complexity of ECU hardware and software content
  - Develop and test system and ECU software in virtual environments

Semi

- Deliver more software w/ high quality
  - Start SW development earlier & validate using RTL

- Verify complex SoC/MCU functional, AMS, low power
  - Use unified verification technologies with fastest engines

- Deliver ISO 26262 compliance
  - Fault injection/report for systematic & random failures
Most Comprehensive Solution for the Supply Chain

OEM Tier 1

- Right SoC/MCU
  - Platform Architect MCO

Accelerate ECU Hardware and Software

- Saber
- Virtualizer/VDK

Collaboration Enablement

Software Avail. & Quality

- Virtualizer/VDK
- ZeBu
- HAPS

Accelerate Hardware Verification

- Planning & Coverage
- Debug
- Virtual Prototyping
- Static & Formal
- Simulation
- Emulation
- Prototyping
- VIP, Models & Databases

ISO 26262 Compliance

- Certitude
- Z01X
- Verdi

© 2017 Synopsys, Inc.
Requirements for SoC Functional Safety Verification
What is Functional Safety in ISO 26262?

- “Absence of unacceptable risk due to hazards caused by malfunctioning behavior of electrical and/or electronic systems.”
ISO 26262 Safety Principles

**Prevent / Eliminate Bugs**

- **Avoid Systematic Faults – Design Bugs** (Permanent Faults)
  - Implementation:
    - Use best practice/certified design flows
  - Verification & Validation:
    - Use best-in-class Functional Verification methodology

**Control Failures**

- **Control of Systematic Faults – Bug Escapes** (Permanent Faults)
  - Implementation:
    - Deploy comprehensive Safety Mechanisms
  - Verification & Validation:
    - Follow ISO 26262 recommendations for ASIL level

- **Control of Random Faults – H/W Failures** (Permanent or Transient Faults)

Lifecycle of Component / Automobile:

- Development & Manufacturing
- Delivery
- In Operation
Functional Safety Verification Solution

- Chip Requirements → Safety Goals
- Architecture → Safety Mechanisms
- Verification Plan → Safety Plan
- Testbench + HDL + IP/VIP + IP Safety Certification

- Fault Modeling & Injection
  - Simulation
  - Static/Formal
  - Emulation*

- Requirement Management APIs
- Prototyping
- Traceable Verification
- Automotive Protocols & Memory VIP
- Fault Injection & Simulation for Automotive Safety Verification

- Tapeout
- FMEDA Report
- Customized Safety Reports / Doc

* Future Work
Functional Verification is Essential Starting Point

Prevent / Eliminate Bugs

Avoid Systematic Faults – Design Bugs
(Permanent Faults)

Verification & Validation:
Use best-in-class Functional Verification methodology

Implementation:
Use best practice/certified design flows

• Many technologies must be used to ensure the highest functional verification quality
• Early software bring-up enables faster and more complete verification
• Verification quality analysis provides objective measure of functional verification effectiveness (fault coverage)
Functional Verification Quality Analysis with Certitude®

Certitude® Functional Qualification Solution

- Inject and qualify systematic faults at architecture, system, and RT level
- Ensure complete verification, and functional correctness of design
- Natively integrated with VCS, and works with VC Formal, and C/C++/SystemC flows
- Unified dynamic and property verification report

Measure the quality (fault coverage) of your functional verification environment

Functional Verification Environment:
- Test Cases
- Design Under Verification
- Expected Results
- Compare
- Activation
- Bug
- Propagation
- Detection
- VCS
- VC Formal
- Merge

© 2017 Synopsys, Inc.
Functional Safety Verification – Verify Control of Hardware Failures

- Hardware failures are modeled as both systematic and random faults (which may be permanent or transient)
- ISO 26262 recommends fault injection testing to verify the effectiveness of the Safety Mechanisms
- Results and reports from fault injection testing are essential for ISO 26262 work products
Functional Safety Verification

Implement and Confirm Quality of Safety Mechanisms (SM)

- Define Failure Mode and Effects Analysis (FMEA) for device
- Implement Safety Mechanisms to protect against failures
- ISO 26262 does not specify what Safety Mechanism to choose
Fault Simulation for Functional Safety

Without Safety Mechanism
- Strobe observation points
- Eliminate non-observable faults

With Safety Mechanism
- Strobe diagnostic point
- Use only faults detected w/o S.M.

Diagram:
- DUT
  - F1
  - F2
  - F3
- OBSERVATION POINTS
- STOP
- Safety Mechanism
- DIAGNOSTIC POINT
  - PASS/FAIL?
General ISO 26262 Functional Safety Verification Flow

1. Failure Mode Effects Analysis
   - Safety Plan
   - FMEA
   - Safety Verification Plan
   - Failure Mode to Safety Mechanism Mapping

2. Fault Injection Campaign
   - Fault Injection & Fault Simulation
   - Fault Injection Campaign Results

3. Calculate Metrics & Export Work Products
   - Results Analysis & FMEDA Annotation
   - Safety Verification Plan Annotated with Fault Coverage
   - FMEDA Metrics

Design

Safety Plan

FMEA

Safety Verification Plan

Failure Mode to Safety Mechanism Mapping

Fault Injection & Fault Simulation

Fault Injection Campaign Results

Results Analysis & FMEDA Annotation

Safety Verification Plan Annotated with Fault Coverage

FMEDA Metrics
ISO 26262 Functional Safety Verification Flow – Task View

- Gather and assess fundamental data related to design, safety goals and failure modes
- Decompose the design into manageable sub-blocks
- Associate sub-blocks with failure modes, safety mechanisms and other details
- Execute fault simulations to determine Diagnostic Coverage for the specified failure modes and safety mechanisms
- Calculate metrics and generate FMEA/FMEDA work products and other reports

- ASIL determination
- Design description, block diagram
- FIT rate information
- Initial list of Safety Goal Violations (device-level)
- Initial list of Failure Modes (block-level)
- List of Safety Mechanisms in place to mitigate failures
- First estimates of Diagnostic Coverage
- Based on function, structure, impact on safety
- Assign size and area information
- Assign FIT rates
- Associate blocks with Failure Modes
- Associate Failure Modes with Safety Mechanisms
- Specify Failure Mode / Safety Goal Violation relationships
- Identify fault types (permanent, transient) to be run
- Assign Failure Mode distributions (expert judgment)
- Refined estimates of Diagnostic Coverage
- Calculate preliminary metrics
- Select target Failure Mode
- Extract fault list
- Identify work load(s) to match use case
- Run fault simulation to calculate Diagnostic Coverage
- Iterate as needed
- Back-annotate Diagnostic Coverage to FMEDA
- Calculate metrics based on "real" data
- Output in standard and customers’ required formats and system inputs

© 2017 Synopsys, Inc. 17
Concurrent Fault Simulation vs. Parallel Simulation

**Parallel Simulation Technology**
One fault per simulation

- Good Machine
- Faulty Machine
- Faulty Machine
- Faulty Machine
- Faulty Machine

**Z01X Concurrent Simulation Technology**
Thousands of faults in a single simulation
Orders of magnitude faster than parallel

- Good Machine
- Differences
- Faulty Machines

**Z01X Distributed Simulation Technology**
Parallelize concurrent algorithm through LSF/SGE
Automatic dynamic fault distribution

- Good Machine
- Differences
- Faulty Machines
- Differences

© 2017 Synopsys, Inc.
Synopsys Z01X Fault Simulation Solution

Order(s) of magnitude faster than competitive solutions

Optimized concurrent fault simulator (200M+ primitives)

Verilog (1995, 2001 & 2005) and SystemVerilog (partial) support

RTL, gate and switch-level fault simulation

In use at leading automotive suppliers; over 10 years experience in Functional Safety

Z01X Is The Industry’s Leading Fault Simulation Solution for Functional Safety Verification
Summary

• Systemic complexity growth in automotive electronics is driving need for unified functional verification and functional safety verification.

• Fault injection for random failure is a key element of the verification process and needs to complement a strong functional verification approach.

• Fault solution must support concurrent and distributed simulation as well as provide traceable verification.

• Synopsys provides the fastest solution for automotive functional safety verification.