Subset of material used at this year's DVCon Europe

ISO26262 – This Changes Everything!

John Brennan, Viktor Preis
Cadence Design Systems, Inc.

accellera SYSTEMS INITIATIVE

cadence™

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

Four disruptive trends in Automotive

Main Semiconductor innovation drivers

Safety: ADAS/Autonomous Driving

Connectivity: Car-2-X, Always on

E-Mobility: Electrical Vehicle

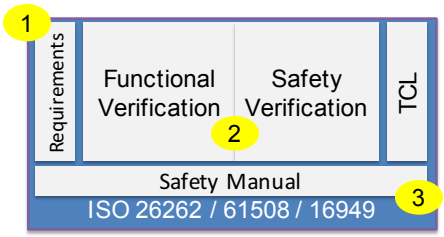
Efficiency: Emission Reduction

accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

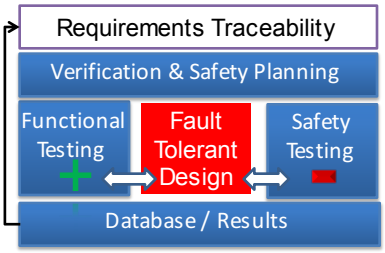
ISO 26262 standard documents functional safety

1. Safety culture
   - Requirements tracing from system to component
   - Prevents problems from arising
2. Quality measurement
   - Functional verification at all levels of abstraction and for all system elements
   - Safety verification measures response of systems to undesired/unplanned events



3. Documentation
   - Document tool confidence level (TCL) to show that tools did not inject or fail to detect safety violations
   - Document complete compliance (safety manual) per product (semi or ECU)

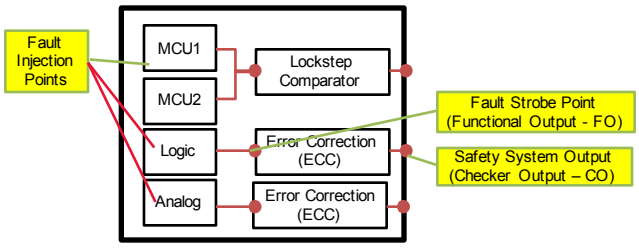
Implications for D&V Tools



- Fault tolerant designs are necessary to reduce the FIT
- Positive testing (functional testing) on the design is the needed prior to safety testing
- Negative testing (functional safety) on the design is comprised of two areas;
  - Specific tests based on failure modes
  - Statistical tests ensure design integrity
- Testing all nodes is not required
- Testing transient faults is required to prove design integrity

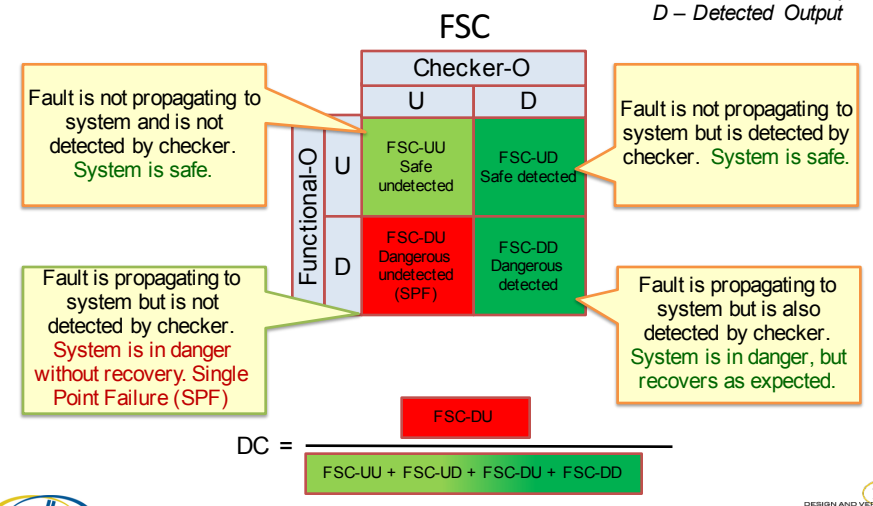
Example: Design

- Verify correct system behavior (functional verification)
  - Use metrics to trace completeness of digital and analog verification
  - Include both positive and negative testing
- Verify correct system response (functional safety)
  - Use metrics to trace fault injection to safety system output
  - Tests enough fault injection to achieve confidence in safety systems
  - Safe faults are detected at FO and CO within time constraints
  - Design blocks and checkers are in isolated sections of the LSI
  - Unlike DFT: 2 strobe points, transient faults, only run on safety critical sections



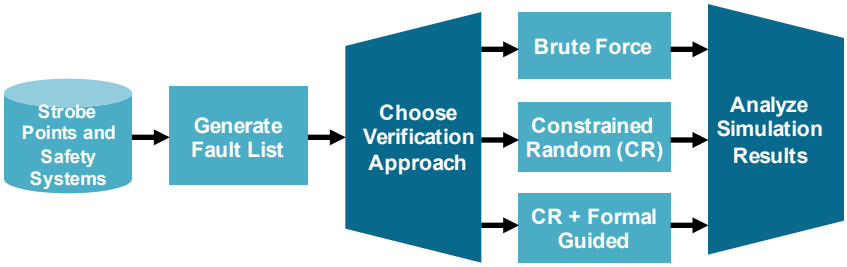
Fault Safety Classification (FSC)

U – Undetected Output
D – Detected Output



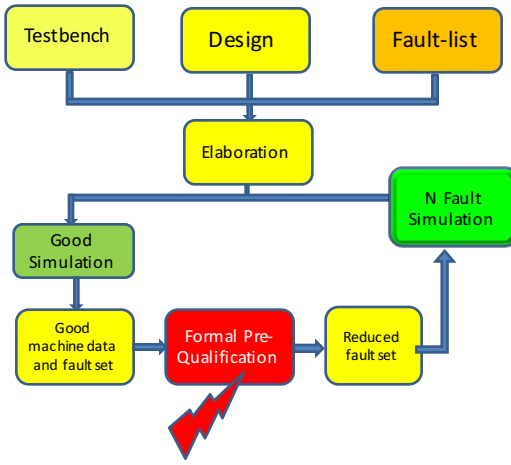
$$DC = \frac{FSC\text{-}DU}{FSC\text{-}UU + FSC\text{-}UD + FSC\text{-}DU + FSC\text{-}DD}$$

Safety: Brute force wont scale!



- Brute force – all fault types on all faults' insertion points
  - Becomes computationally impossible after 10^6 gates
- Constrained random – sampling within safety-critical area
  - Combines randomized fault injection with coverage analysis
- CR + Formal guided – optimize fault list with CR
  - Most optimized solution

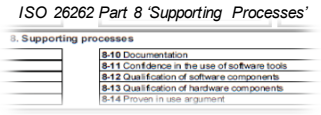
Fault Injection Campaign Execution



- Formal fault list reduction
- Formal fault detectability

Tool Confidence Level (TCL)

- TCL is a mandatory part of the ISO26262
  - Customers need to supply a **Software Tool Criteria Evaluation Report** for each design



- Tool confidence and functional confidence are not the same
- TCL is exclusively a measure of the ability to detect tool errors
  - Use cases where good input is provided but an unexpected output is created
- Cadence provides TCL compliance documents that will save customers time and resources
  - Cadence safety manuals and tool classification documents provide use case foundation layer
  - Customers can add use cases on the foundation layer as needed

accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

Summary

- Highlights
  - Functional Safety requires a **new generation** of Fault Injection technology
  - Fault Injection is **much more exhaustive** than Functional Verification
  - Cadence provides a technology to **reduce** the effort to instrument and execute the Fault Injection Campaigns
- **Fault Injection** technology is now mature and fully available
  - Incisive® Functional Safety Simulator
  - JasperGold® Formal FSV app
- **Fault Injection Campaign Executor** simplifies the job
  - **Automated** and **Optimized** Fault Injection Campaign execution
  - Based on existing technology: Incisive® (IFSS, vManager)
  - Links to Functional Safety Analysis

accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

Questions

Thank You.

accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE