THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY: CEDA IEEE Council on Electronic Design Automation, SIGDA ACM

Improving Software Libraries used as Safety Diagnostics for DSPs with DCLS, in Next-Gen Battery Management Systems, to achieve ASIL-D

DUKOSI Ltd
Jon Goldfinch jgoldfinch@dukosi.com
Anders Convery aconvery@dukosi.com
Madhu Babu mbabu@dukosi.com
Ross Ballany rballany@dukosi.com

Optima Design Automation Ltd:
Sesha Sai Kumar C V cvseshu@optima-da.com
Jamil R Mazzawi jamil@optima-da.com

This paper was presented at DAC 2026

Abstract of the paper:

This presentation details a methodology to achieve ISO-26262 ASIL-D compliance for Digital Signal Processors (DSPs) used in automotive Battery Management Systems (BMS).

ASIL-D is the most stringent automotive safety level, requiring 99% Single Point Fault Metric (SPFM). The primary safety mechanism employed in the given design is Dual Core Lock Step (DCLS).

To validate and improve diagnostic coverage, the Dukosi team utilized the Optima Safety Platform (OSP), an ISO 26262 certified tool, which can be used for FuSa design verification up to ASIL-D, to **perform exhaustive gate-level fault injection analysis**.

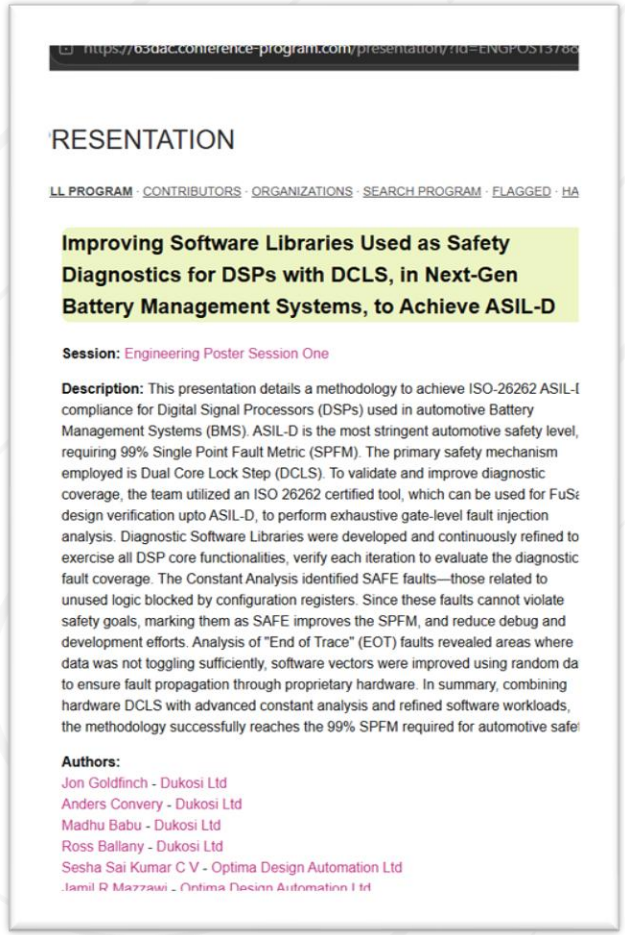
Diagnostic Software Libraries were developed and continuously refined to exercise all DSP core functionalities, verify each iteration to evaluate the diagnostic fault coverage, and prove the correctness of DCLS.

The OSP Constant Analysis (CA) engine identified SAFE faults - those related to unused logic, blocked by constant configuration registers in the given Assumptions of Use (AoU). Since these faults cannot violate safety goals, marking them as SAFE improves the SPFM, and reduce debug and development efforts.

Analysis of "End of Trace" (EOT) faults revealed areas where data was not toggling sufficiently, software vectors were improved using random data to ensure fault propagation through proprietary hardware.

In summary, combining hardware DCLS with advanced constant analysis and refined software workloads, the methodology successfully reaches the 99% SPFM required for ASIL-D.

Link to DAC page:
https://63dac.conference-program.com/presentation/?id=ENGPOST378&sess=sess264



RESENTATION

LL PROGRAM · CONTRIBUTORS · ORGANIZATIONS · SEARCH PROGRAM · FLAGGED · HA

Improving Software Libraries Used as Safety Diagnostics for DSPs with DCLS, in Next-Gen Battery Management Systems, to Achieve ASIL-D

Session: Engineering Poster Session One

Description: This presentation details a methodology to achieve ISO-26262 ASIL-I compliance for Digital Signal Processors (DSPs) used in automotive Battery Management Systems (BMS). ASIL-D is the most stringent automotive safety level, requiring 99% Single Point Fault Metric (SPFM). The primary safety mechanism employed is Dual Core Lock Step (DCLS). To validate and improve diagnostic coverage, the team utilized an ISO 26262 certified tool, which can be used for FuSa design verification upto ASIL-D, to perform exhaustive gate-level fault injection analysis. Diagnostic Software Libraries were developed and continuously refined to exercise all DSP core functionalities, verify each iteration to evaluate the diagnostic fault coverage. The Constant Analysis identified SAFE faults—those related to unused logic blocked by configuration registers. Since these faults cannot violate safety goals, marking them as SAFE improves the SPFM, and reduce debug and development efforts. Analysis of "End of Trace" (EOT) faults revealed areas where data was not toggling sufficiently, software vectors were improved using random da to ensure fault propagation through proprietary hardware. In summary, combining hardware DCLS with advanced constant analysis and refined software workloads, the methodology successfully reaches the 99% SPFM required for automotive safe

Authors:
Jon Goldfinch - Dukosi Ltd
Anders Convery - Dukosi Ltd
Madhu Babu - Dukosi Ltd
Ross Ballany - Dukosi Ltd
Sesha Sai Kumar C V - Optima Design Automation Ltd
Jamil R Mazzawi - Optima Design Automation Ltd

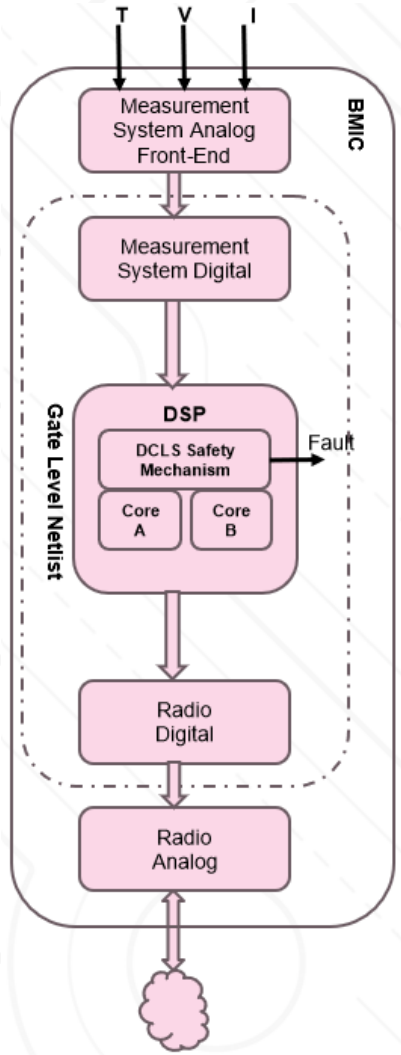
Motivation

- A BMS (Battery Management System) consists of a network of BMICs
  - BMICs (Battery Monitoring ICs) implements battery measurement functions for each cell measuring Current, Voltage and Temperature
  - BMICs are Connected wirelessly to a hub and System controller
  - BMICs need to be reliable and are designed as SEooC (Safety Element out of Context)
- This BMIC, designed as SEooC, required to be up to ASIL-D, which is used in an automotive ASIL-D system defined as per ISO26262
  - ASIL-D is the most stringent level of safety, where a malfunction could be life threatening
  - SPFM (Single Point Fault Metric) for ASIL-D is 99%
- BMIC key element is a DSP (Digital Signal Processor) in critical path
  - Analyzes measured data
- Safety Mechanism to achieve the ASIL-D for DSP IP is DCLS (Dual Core Lock Step)
- Fault Injection analysis to be used to assess the safety mechanism and compute SPFM on the gate level netlist
- This paper discusses methodology to achieve ASIL-D coverage for DSP in BMIC

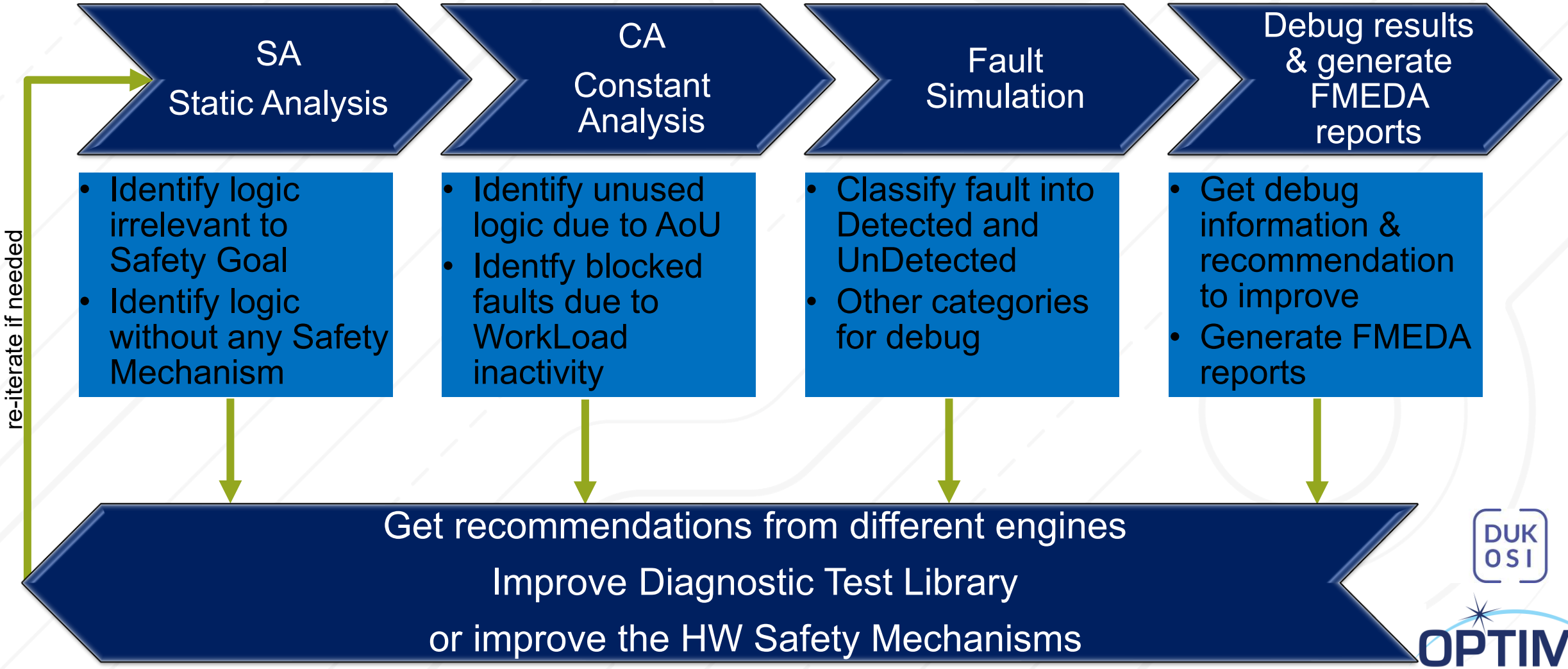
Summary:
BMIC chips are used inside the battery cell in BMS
BMIC has DSP inside it and has SEooC ASIL-D requirements
In this project, DCLS was used, with fault-analysis and fault-simulation with the Optima Safety Platform

99% Fault coverage for DSP path in BMIC (main Idea)

- Software Library is loaded and executed to find DSP core behavior
- Dual Core Lock Step (DCLS) mechanism used for Functional Safety requirements of DSP cores
- While DCLS is commonly considered to be able to detect all faults, this detection will not happen without the right exercising of the DSLC
- Decided to improve DCLS with Software Library (SL) that exercise the design to allow fault-detection by DCLS
- Methodology used to improve Software Library to cover faults achieving ASIL-D level of 99%
  - Methodology is: Static Analysis, Constant Analysis, Fault Simulation then fault-debug for undetected faults
- Used the Optima Safety Platform, an ISO26262 Certified tool for Fault Analysis and Fault Simulation
  - OSP has: Evaluated Tool Confidence level for up to ASIL-D as per ISO26262-8:11
- Challenges
  - Gate Level Netlist design for Fault analysis
  - DC to be computed only with Outputs of DSP cores are faulty
  - DC to be computed with exhaustive fault injection



High level diagram of the Methodology



Iterative Methodology to improve Software Library for DSP

- Software Library for DSP safety diagnostics is developed
  - Code that exercises all functionality of DSP cores
- Detection and Failure Strobes are identified in the design
  - Fault_dcls pin as Detection, DSP outputs as failure
- Static Analysis classified faults into various categories
  - Its important to look at **UI**: **Unsafe Invisible** faults to incorporate new safety hardware
- Choose Golden Workload for fault simulation representing the final Software
- Increase faults covered by SMs:
  - Focus on reducing **UI** by introducing new SM or rectifying the existing
  - Find residual faults in **UV(Unsafe Visible)** by fault injection simulation
  - Change Software Library to exercise more functionality of DSP cores
- Find safe faults which are blocked by design and workload constants
  - Constants analysis can help identify faults that are blocked and not violating the safety goal
- Iterate to improve Diagnostic Software to cover 99% faults achieving ASIL-D

Improving Diagnostic Coverage

- Identifying more SAFE faults using Constant Analysis
  - Design Constants: Registers that are initialized will block some logic/faults
  - General Purpose registers are loaded with constants in Software Library
    - These constants Block more faults
- Constants Analysis is run with both Design Constants and Workload Constants
  - All Blocked and Masked faults are marked as SAFE
- SAFE faults by Constant Analysis will never Violate Safety Goal. This improves the SPFM
- Hard Error Simulation is run on Unsafe Visible (UV) faults, which shows some faults in the proprietary hardware implementations not covered
- Fault Debug Flow
  - Some of the End Of Trace (EOT) faults show that fault injected not propagating in the design
  - The faults which are simply at the injected place itself means, data is not toggling enough to allow them to propagate and get detected.
  - Improve the software with random data for the proprietary hardware
- Improved the Vectors (Software Library) and iterated to close the Diagnostics to achieve 99% SPFM of ASIL-D

Summary

- DCLS implementation sometimes thought of giving full coverage of faults
- If not implemented correctly or no exhaustive vectors for DSP core, in Safety Diagnostic Software Library may not give the required fault coverage
- It is required to Do fault injection analysis as prescribed in ISO26262-11:4.8.1
- By combining **DCLS hardware**, **Constant Analysis**, and **refined vectors in Software Library**, the methodology improves diagnostic coverage to the required **99% SPFM** for ASIL-D
- This paper highlights the iterative nature of the Fault Coverage Closure, specific needs for debug of undetected faults and the need for high performance Fault Analysis tool certified for ISO26262 process.

For more details about this and other success stories,

please contact Optima for more details: sales@optima-da.com