A tool based estimation computation method of MCU random failure rate & functional safety metrics

Yogitech / Texas Instruments

Riccardo Mariani – YOGITECH, CTO
Hoiman Low – TI Safety MCU, FSCAE
July / 2015
Topics

• YOGITECH
  – IEC 61508 and ISO 26262 hardware random fault management requirements
    – problems/challenges
  – YOGITECH fRTools: Safety Designer and Safety Verifier Tool Suites
  – How the YOGITECH flow was used for TI
  – YOGITECH solutions for system integrators

• Texas Instruments
  – Apply functional safety standard to manage HW random failures
  – Hercules MCU safety manual and safety analysis report
  – Hercules MCU FMEDA for usage environment and safety function tailoring

• Q&A (10 minutes)
Topics

• YOGITECH
  – IEC 61508 and ISO 26262 hardware random fault management requirements
    – problems/challenges
  – YOGITECH fRTools: Safety Designer and Safety Verifier Tool Suites
  – How the YOGITECH flow was used for TI
  – YOGITECH solutions for system integrators

• Texas Instruments
  – Apply functional safety standard to manage HW random failures
  – Hercules MCU safety manual and safety analysis report
  – Hercules MCU FMEDA for usage environment and safety function tailoring

• Q&A (10 minutes)
About YOGITECH

• Founded in 2000

• **Mission:** be the lead provider of services and solutions to silicon vendors and system integrators to help them meet their functional safety challenges

• Currently 46 people - headquarter in Pisa (Italy), office in Milan (Italy), branch in Japan (YOGITECH KK)

• **Main markets:**
  – automotive, industrial, medical, railway

• **Customers:**
  – most of IP and IC providers
  – major Tier2, Tier1 and OEM worldwide
Requirements on HW random fault

- Both IEC 61508 and ISO 26262 requires to carefully evaluate the impact of HW random fault.

- In essence, using ISO 26262 as example:

\[
\lambda_{RF} = \lambda \times \sum_{FM} \Lambda_{FM} \times (1 - F_{safe FM}) \times (1 - K_{FMC,RF_{FM}})
\]

- Failure rate of the safety related faults
- Failure modes distribution
- Fraction of faults leading to safe failures
- Fraction of not safe faults prevented by safety mechanisms from violating the safety goal
Challenges on HW random fault

• $\lambda =$ base failure rate is strongly dependent from the selected reliability handbook, operational profile, integrated circuit characteristics etc…

• $\Lambda =$ failure mode distribution strictly depends on the inner architecture of the integrated circuit.

• $F_{\text{safe}} =$ fraction of safe failures depends on architectural safeness but the most contribution is given by the specific use case of the end customer.

• $K_{\text{RF}} =$ diagnostic coverage strictly depends on the inner architecture of the integrated circuit and the selected safety mechanism (that can be either HW or SW based or an assumption of use)
The black-box approach

- A typical black-box functional safety analysis is based on:
  - collecting data from block diagrams and component user manuals
  - assuming an equal failure mode distribution
  - assuming an equal split between dangerous and safe failures
  - claiming a diagnostic coverage without a detailed quantitative analysis and accurate safety verification

- The complexity of modern integrated circuits in terms of number of transistors, CPU features, bus architecture, memory size and the complexity of the safety application are such that the adoption of a black-box approach is no longer realistic.

- The black-box approach is leading to an unacceptable gap between estimated and measured safety integrity level.
YOGITECH enabled

- YOGITECH enables the highest safety integrity levels for integrated circuits to be achieved by means of fRMethodology, a patented white-box approach to perform functional safety analyses and safety-oriented design exploration of integrated circuits, according to functional safety standards.

- fRMethodology mainly consists of:
  - **dividing** the component into elementary parts by using automatic tools to guarantee the completeness of the analysis;
  - **computing** the safety metrics by looking to the fault models of each elementary part, attributing the failure rate, the safeness ($F_{safe}$) and estimating the diagnostic coverage of the planned HW or SW safety mechanisms;
  - **verifying** the safety metrics by an extensive fault injection campaign simulating permanent, transient and common cause faults.
**fRMethodology flow**

---

**Key ISO 26262 requirements covered by fRMethodology**

- Review of Functional Safety Management / Process Safety Audit (ISO 26262-2 and -10)
- Definition of assumed safety requirements with respect to Functional (ISO 26262-3) and Technical (ISO 26262-4) safety concepts
- Specification / review of HW safety requirements, HW design and HW-SW interface (ISO 26262-5)
- Computation of the failure rates, preparation / review of FMEA, DFMEA, FMEDA, FTA (ISO 26262-5, -10)
- Evaluation of HW architectural metrics and safety goal violations due to random HW failures, including providing suggestions & solutions about how to cover the gaps, if any (ISO 26262-5, -10)
- Preparation / review of Verification and Validation plan (ISO 26262-4, -5, -8)
- Verification and validation of effectiveness of safety mechanisms, including fault injection (ISO 26262-4 and ISO 26262-5)
- Specification / review of SW safety requirements with respect to FW and SW units (ISO 26262-6)
- Review of SW tools confidence in use (ISO 26262-8)
- Review of ASIL decomposition, FFI and DFA analyses (ISO 26262-9)
- Review of degree of fulfilment of IC specific recommendations, IC Safety Manual (ISO 26262-10)
The \textbf{fRTools} are a collection of licensable tool suites that allows the user to independently perform FMEDA and safety verification of integrated circuits according to the requirements of IEC 61508 and ISO 26262.

With the fRTools YOGITECH’s customers can run the safety analysis and verification of their designs, in their own design environment, maintaining the full control of their intellectual property, while still being sure to have gone through all the steps included in the fRMetholodogy coherently to the target safety standards.

\textbf{fRTools portfolio includes:}

- \textbf{SAFETY DESIGNER TOOL SUITE}
- \textbf{SAFETY VERIFIER TOOL SUITE}
- \textbf{SAFETY ARCHITECTURE ANALYZER}
fRTool Suites

END USER

IC safety databases

Safety Architecture Analyser (H2 2015)

Safety Designer tool suite

EP Extractor

Safety Designer

SILICON/ IP PROVIDER

Safety Concept

Safety Designer Tool Suite

EP Extractor

Vector Manager

Operational Profile

Safety Verifier (permanent faults)

Safety Verifier (transient faults)

Safety Verifier (special faults)

IC database

Simulators (Third Party)

EP = elementary part

- Adjusting proportion of safe failures
- Adding (or disabling) safety mechanisms
- Changing operational profiles
- Computing system level metrics

- Computing failure rates
- Determining failure modes and failure modes distribution
- Doing safety analyses like FMEA, FTA and DFA
- Comparing estimations with fault injection results
- Preparing Safety Verific. Plan

- Importing Safety Verific. Plan
- Preparing the fault injection setup including generating the fault lists from IC database, generating vectors for black-box macros etc...
- Injecting permanent, transient and special (e.g. shorts, clock, reset) faults
Safety Designer Tool Suite

- It automates the safety analysis of integrated circuits according to safety standards like ISO 26262 and IEC 61508.

- It allows the user to analyze the integrated circuit at different levels of abstraction, to partition it into its elementary parts, to associate the failure modes to functional blocks and elementary parts, to compute the safety metrics and to estimate the safeness and diagnostic coverage.

- **Main features**
  - Computing failure rates
  - Determining failure modes and associating them with the IC database to compute failure modes distribution
  - Doing safety analyses like FMEDA, FTA and DFA
  - Preparing Safety Verification Plan
  - Comparing estimations with fault injection results
Safety Verifier Tool Suite

- It automates the verification of safety metrics (safeness and diagnostic coverage of HW and SW mechanisms) by managing fault injection campaigns on integrated circuits.
- It allows the user to partition the campaign according to the Safety Verification Plan defined in Safety Designer.
- It manages all the necessary simulations (run by an external fault or functional simulator, depending on the fault model) and integrates the results into a comprehensive view.

**Main features**
- Importing Safety Verification Plan from SD
- Preparing the fault injection setup including generating the fault lists from IC database, generating vectors for black-box macros etc...
- Injecting permanent, transient and special (e.g. shorts, clock, reset) faults
- Categorizing faults according to safety standards
How this flow was used in TI context

- Processing the TI MCU database to partition it in elementary parts (EP)
- Quantitative FMEDA with Safety Designer in order to:
  - automatically compute EP failure mode distribution
  - estimate the safeness $F_{safe}$ of each EP
  - define MCU safety requirements, i.e. the target DC and the balance with AoU
- MCU implementation by TI
- Execution of the safety verification by means of an exhaustive fault injection campaign aimed to verify:
  - the estimated safeness $F_{safe}$
  - the diagnostic coverage achieved by the safety mechanisms embedded in TI MCU and the AoU listed in TI MCU Safety Manual
How this flow was used in TI context /2

• Very detailed computation of the MCU TI failure modes distribution based on the actual post-layout database
  – Hundred of thousands of elementary parts

• Estimation of safeness and diagnostic coverage has been done at a very detailed level to decrease as much as possible the loops between safety analysis and safety verification

• Careful selections of the workload using during fault injection in order to guarantee the highest accuracy of safeness and diagnostic coverage verification

• Each safety mechanism has been verified separately, to allow flexibility for the end user to switch on/off a safety mechanism and easily re-compute the safety metrics
Solutions for system integrators

- To support system integrators, YOGITECH offers also a wide set of SW Test Libraries (faultRobust SW Test Library, fRSTL)

- YOGITECH is available to implement custom SW Test libraries e.g. to implement Assumptions of Use

- Main features of fRSTL:
  - **Accuracy**
    - Coverage is guaranteed by YOGITECH fRTools (IC database analysis + fault injection)
  - **Modularity**
    - ensured by the structure consisting of a Test Interface and Test Segments (TS)
  - **Flexibility**
    - allowing the user to either run the full test suite or a subset, or to extend the test suite addressing specific requirements
  - **Easy integration**
    - STL mostly written in C and optimized assembler coding
  - **Low impact**
    - for the application SW thanks to the optimization in size and run time allowed by the fRMethodology flow

Each TS:
- targets a specific function or a group of functions of the component
- provides pass/fail information and self-checking signatures (CRC)
- may be interrupted at any time by the application SW
YOGITECH faultRobust technology

The one stop shop for Functional Safety

- **fRTools**: EDA tools enabling customers to independently perform safety analysis and verification
- **fRMethdology**: Functional safety analysis and verification
- **fRSTL**: Software Test Libraries implementing safety mechanisms
- **fRIPs**: Hardware IPs implementing safety mechanisms
Topics

• Yogitech
  – IEC 61508 and ISO 26262 hardware random fault management requirements – problems/challenges
  – Yogitech fRTools: Safety Designer and Safety Verifier tool suites
  – MCU random fault estimation, diagnostics effectiveness, calculation of safety metrics

• Texas Instruments
  – Apply functional safety standard to manage HW random failures
  – Hercules MCU safety manual and safety analysis report
  – Hercules MCU FMEDA for usage environment and safety function tailoring

• Q&A (10 minutes)
SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

- How to manage MCU hardware random failures
- How to estimate failure rate vs ASIL requirements
ISO 26262 / IEC 61508 Risk reduction

**Functional Safety**
- Item Definition
- Hazard & Risk Analysis
- SIL / ASIL Determination
- Safety goal Safety Function
- Allocation of Safety Requirements
- HW Safety Metrics

**Example**
- EV traction motor control
- Too high motor positive torque -> Causing collision
- ASIL-C
- Avoid too high positive torque
- Implement MCU diagnostics to monitor PWM
- Computation of SPF / PMHF

**Safety goal**
- Safety Function

**Safety Function**
- SIL / ASIL Determination

**SIL / ASIL Determination**
- Hazard & Risk Analysis

**Hazard & Risk Analysis**
- Safety goal Safety Function

**Safety goal Safety Function**
- Allocation of Safety Requirements

**Allocation of Safety Requirements**
- HW Safety Metrics

**HW Safety Metrics**
- ISO 26262 / IEC 61508 Risk reduction

**What is the function?**
- Identify hazard
- Categorize risk

**Identify hazard Categorize risk**
- What is tolerable risk?

**What is tolerable risk?**
- Safety requirements & Failure mode/rate & Diagnostics

**Safety requirements & Failure mode/rate & Diagnostics**
- Sufficient risk reduction?

**Sufficient risk reduction?**
Application Example

Function: The traction motor shall deliver torque as commanded by the external host.

- **Motor Torque Command from Remote Host**
- **Transceiver**
- **Motor Position Feedback**
- **Safety Function Input (MCU)**
  - Receive motor torque command from remote host (CAN)
  - Read current motor position (feedback) via quadrature decoder (eQEP)
- **Quadrature Encoder**
- **DCAN1**
  - 1.2v 5v 3.3v
  - Oscin Oscout
- **System Reset**
- **Voltage Regulator**
- **5-16MHz Clock Crystal**
- **Hercules MCU**
- **Safety Function Processing (MCU)**
  - Calculate necessary output commands to motor based on desired torque and current position
- **ePWM1**
- **ePWM2**
- **ePWM3**
- **NHET1**
- **Pre Drivers**
- **H Bridge Drivers**
- **BLDC Motor**
- **Motor Position Feedback**
- **Warning Lamp**
- **GIO**
- **Safe State (MCU)**
  - 1. Disable motor driver relay (NHET)
  - 2. Indicate fault to system via warning lamp (GIO)
- **Safety Function Actuation (MCU)**
  - Drive three phase PWMS to actuate motor (ePWM)
**Application Example**

Hazard: Too high positive torque -> Risk: Collision -> ASIL-C
Safety Goal: Avoid too high positive torque

**Hercules MCU**

- DCAN1
- Voltage Regulator
- 5-16MHz Clock Crystal
- OSCIN OSCOUT
- nPORRST
- 1.2v 5v 3.3v

**Safety Function Input (MCU)**
- Receive motor torque command from remote host (CAN)
- Read current motor position (feedback) via quadrature decoder (eQEP)

**Safety Function Processing (MCU)**
- Calculate necessary output commands to motor based on desired torque and current position

**Safety Function Actuation (MCU)**
- Drive three phase PWMs to actuate motor (ePWM)

**Safety Function Actuation (MCU)**
- Pre Drivers
- H Bridge Drivers
- BLD C Motor

**Safe State (MCU)**
1. Disable motor driver relay (NHET)
2. Indicate fault to system via warning lamp (GIO)

**Safety function:**
PWM signals shall be monitored

**Hazard:**
Too high positive torque

**Risk:**
Collision

**ASIL-C**

**Safety Goal:**
Avoid too high positive torque
MCU Safety Critical Elements **per Safety Function**

- Safety Critical Elements are elements within MCU that implement the safety function.
- Diagnostics are necessary to detect safety related failures.
- Sufficient diagnostics coverage (DC) is needed to meet required IEC 26262 HW metrics per ASIL level.
- In this example, safety critical elements are: CPU, Flash, SRAM, Interconnect, eQEP, eCAP, ePWM, NHET1 System, ESM...
Managing Hardware Random Failures

- Millions of transistors, metal lines, resistors, capacitors..
- Each component could fail (permanent and/or transient)
- A component failure could lead to a system failure

ECU

MCU

- Failure rate is measured in Failure In Time (FIT)
- 1 FIT is 1 fail in $10^9$ operating hours
- Assuming 1 million cars on the road with 4 driving hours per day per car on average:
  - 100 FIT => ~150 failures per year

<table>
<thead>
<tr>
<th>ASIL</th>
<th>SPFM</th>
<th>PMHF (FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIL B</td>
<td>&gt;90%</td>
<td>&lt;100</td>
</tr>
<tr>
<td>ASIL C</td>
<td>&gt;97%</td>
<td>&lt;100</td>
</tr>
<tr>
<td>ASIL D</td>
<td>&gt;99%</td>
<td>&lt;10</td>
</tr>
</tbody>
</table>

- What is the total system failure rate?
- Apply diagnostic until total system failure rate is below functional safety requirement

Unacceptable risk

Tolerable risk
MCU Failure Mode and Failure Rate

- **Permanent random failures:**
  - Tox integrity, Short, Open, Stuck At, Drift ....

- **Source of permanent component failure rate data:**
  - MILHDBK 217F
  - SN29500
  - IEC/TR 62380
  - Supplier reliability data
  - ...

- TI uses IEC/TR 62380 where # of transistors, # of memory bits, temperature and package effect can be modeled.

- Failure rate is commonly expressed in FIT (Failure In Time)
  - 1 FIT = 1 failure in 1E9 hours.

- **Transient random failures:**
  - Cosmic Rays

- Failure rate data source is TI experiments in Los Alamos lab and TI lab
Hercules™ MCU safety diagnostic features

- CPU Self Test Controller requires little S/W overhead
- Physical design optimized to reduce probability of common cause failure
- Lockstep CPU & Lockstep Interrupt Fault Detection
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R
- Controller requires little S/W overhead
- Physical design optimized to reduce probability of common cause failure
- Lockstep CPU & Lockstep Interrupt Fault Detection
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R

- Lockstep CPU & Lockstep Interrupt Fault Detection
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R

- ECC or Parity on select Peripheral, DMA and Interrupt controller RAMS
- Parity or CRC in Serial and Network Communication Peripherals

- DMA
- Enhanced System Bus and lockstep Vectored Interrupt Module

- Memory Interface
- External Memory

- Power, Clock, & Safety
- OSC PLL
- PBIST/LBIST
- POR
- CRC
- ESM
- RTI/DWWD
- Memory BIST on all RAMS for fast memory test
- Error Signaling Module w/ External Error Pin
- On-Chip Clock and Voltage Monitoring
- Protected Bus and lockstep Interrupt Manager
- IO Loop Back, ADC Self Test, …
- Dual ADC Cores with shared channels

- Serial Interfaces
- Network Interfaces
- Dual ADC Cores Available
- Dual High-end Timers Available
- GIO

Bold items are introduced with the new Cortex®-R5 devices
How to implement Applicable Diagnostics?

Hercules™ Safety Manual

Safety Manual for TMS570LS12x and 11x Hercules™ ARM®-Based Safety Critical Microcontrollers

User’s Guide

Texas Instruments

Table 2. Summary of Safety Features and Diagnostics

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique Identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Recommendation</th>
<th>Possible ISO 61508:2010 Fault Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>PWR1</td>
<td>Voltage monitor (VMON)</td>
<td>M</td>
<td>External Voltage Supervisor</td>
</tr>
<tr>
<td></td>
<td>PWR2</td>
<td>External voltage supervisor</td>
<td>++</td>
<td>Voltage monitor (VMON)</td>
</tr>
<tr>
<td></td>
<td>PWR4</td>
<td>Lockstep PSCON</td>
<td>M</td>
<td>Lockstep TEST</td>
</tr>
<tr>
<td></td>
<td>PWR5</td>
<td>Privileged mode access and multi-bit keys for control registers</td>
<td>M</td>
<td>Software test of register configuration and error response</td>
</tr>
<tr>
<td></td>
<td>PWR6</td>
<td>Periodic software readback of static configuration registers</td>
<td>++</td>
<td>CPU lockstep</td>
</tr>
<tr>
<td></td>
<td>PWR7</td>
<td>Software readback of written configuration</td>
<td>++</td>
<td>PSCAN lockstep self-test</td>
</tr>
<tr>
<td></td>
<td>PWR8</td>
<td>PSCAN lockstep comparator self-test</td>
<td>++</td>
<td>SelfTest autovoltage</td>
</tr>
</tbody>
</table>

• An overview of the safety architecture for management of random failures
• The details of architecture partitions, implemented safety mechanisms, and recommended usage
• Failure modes and failure rates
• Use Chapter 6 to determine applicable safety mechanisms by MCU module such as CPU, SRAM, PWR…
Detailed Safety Analysis Report & FMEDA worksheet

**Detailed Safety Analysis Report**
- Assumptions of use applied in calculation of safety metrics
- Summary of IEC 61508 or ISO 26262 standard safety metrics at the MCU component level
- A fault model used to estimate device failure rates and an example of customizing this model for use with the example application.
- FMEDA with details to the sub-module level of the MCU, that enables calculation of safety metrics based on customized application of diagnostics

**Use of FMEDA worksheet**
- **FIT Estimation sheet** to tailor use conditions
- **Product Function Tailoring sheet** to select MCU modules used in safety function
- **Pin Level Tailoring sheet** to select MCU pins used in safety function
- **Safety Mechanism Tailoring sheet** to select applied Safety mechanisms
- **Summary and Details-ISO26262 or IEC61508 sheets** to determine if MCU and modules safety metrics are met.

Available under NDA

TMS570LS12x Detailed Analysis Report spnu531a

Failure mode distribution calculated with TI MCU database using YOGITECH Safety Designer tool
Failure mode coverage verified by fault injection in the TI MCU database using YOGITECH Safety Verifier tool
ISO 26262 / IEC61508 HW Metrics Calculation
Failure Rate / Mission Profiles

Random Hardware Failure

- Package Permanent
- Die (silicon) Permanent
- Die (silicon) Transient
ISO 26262/IEC61508 HW Metrics Calculation
Mission Profiles

Customer input for failure rate estimation

Package Used
Customer input for transient fault estimation
Application specific Flux Factor coeff. based on Jedece JESD89A

Maximum power dissipation
Application specific power dissipation in Watts
(1.04W is based on maximum datasheet value)

Safe / Dangerous Ratio
Derating to be applied to FIT rates

Confidence Level
Desired confidence level of FIT rates

Operational Profile from IEC/TR 62380:2004

<table>
<thead>
<tr>
<th>Temp1</th>
<th>Temp2</th>
<th>Temp3</th>
<th>( \tau_1 )</th>
<th>( \tau_2 )</th>
<th>( \tau_3 )</th>
<th>( T_{on} )</th>
<th>( T_{off} )</th>
<th>( n_1 )</th>
<th>( \Delta T_{1-c} )</th>
<th>( n_2 )</th>
<th>( \Delta T_2 )</th>
<th>( n_3 )</th>
<th>( \Delta T_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>0.02</td>
<td>60</td>
<td>0.015</td>
<td>85</td>
<td>0.023</td>
<td>0.058</td>
<td>0.942</td>
<td>670</td>
<td>( \Delta T/3+55 )</td>
<td>1340</td>
<td>( \Delta T/3+45 )</td>
<td>30</td>
<td>10</td>
</tr>
</tbody>
</table>

- **Automotive Mission Profile in IEC/TR 62380 (FMEDA worksheet default):**
  - 10 years service with 3 phases per day – night, day, not used
    - 2 night trips per day, 4 day trips per day, 30 days shut down
  - 3 temperature phases
    - Engine cold, Engine warm, Engine hot
  - On/Off ratio: 0.058 / 0.942

Based on TMS570LS12x v1.0 FMEDA worksheet
FMEDA worksheet – Product Function Tailoring

### Modules used for Safety Function / Safety Goal

<table>
<thead>
<tr>
<th>CPU Subsystem</th>
<th>CPU</th>
<th>Cortex R4F Central Processing Unit (CPU)</th>
<th>YES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Subsystem</td>
<td>VIM</td>
<td>Vectorized Interrupt Module (VIM)</td>
<td>YES</td>
</tr>
<tr>
<td>CPU Subsystem</td>
<td>NA</td>
<td>LEBST</td>
<td>NO</td>
</tr>
<tr>
<td>CPU Subsystem</td>
<td>PBIST</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>DEBUG</td>
<td>JTAG</td>
<td>Joint Test Action Group (JTAG)</td>
<td>NO</td>
</tr>
<tr>
<td>DEBUG</td>
<td>DASS</td>
<td>Cortex R4F Central Memory Access Unit (DMAC)</td>
<td>NO</td>
</tr>
<tr>
<td>DEBUG</td>
<td>POM</td>
<td>Parameter Overlay Module</td>
<td>NO</td>
</tr>
<tr>
<td>RAM System</td>
<td>RAM</td>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>YES</td>
</tr>
<tr>
<td>Flash System</td>
<td>CIP</td>
<td>On-Chip Programmable (OTP) Flash Static</td>
<td>YES</td>
</tr>
<tr>
<td>Flash System</td>
<td>FLA</td>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>YES</td>
</tr>
<tr>
<td>Flash System</td>
<td>EEP</td>
<td>Flash-emulated EEPROM (EEP)</td>
<td>YES</td>
</tr>
<tr>
<td>INTERCONNECT</td>
<td>INC</td>
<td>Level 3 and Level 3 (L3-L3) Interconnect</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>ESM</td>
<td>Error Reporting Module (ESR)</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>PMM</td>
<td>Power Management Module (PMM)</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>SRT</td>
<td>Reset</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>SYS</td>
<td>System Control</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>CLK</td>
<td>Clock</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>MPU</td>
<td>MPU Static Configuration</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>DMA</td>
<td>Direct Memory Access (DMA)</td>
<td>YES</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>IOM</td>
<td>Input/Output (IO) Multiplexing (IOMUX)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>FIPO</td>
<td>Flexibility Interconnect Point Out (FIPO)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAN</td>
<td>Controller Area Network (CAN)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAN</td>
<td>Controller Area Network (CAN)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAN</td>
<td>Controller Area Network (CAN)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>I/O</td>
<td>General Purpose Input/Output (GPIO)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>ULI</td>
<td>Local Interconnect Network (LIN)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SCI</td>
<td>Serial Communications</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>ADC</td>
<td>Multi-Buffer Analog to Digital Converter (MADC1)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>ADC</td>
<td>Multi-Buffer Analog to Digital Converter (MADC2)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>MSP</td>
<td>Multi-Buffer Serial Peripheral Interface (MSP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>MSP</td>
<td>Multi-Buffer Serial Peripheral Interface (MSP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SER</td>
<td>Nested Generation High-End (SER) (SER)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SER</td>
<td>Nested Generation High-End (SER) (SER)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SPI</td>
<td>Serial Peripheral Interface (SPI)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SPI</td>
<td>Serial Peripheral Interface (SPI)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>RTI</td>
<td>Real Time Interrupt (RTI) Operating System Timer</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>ETH</td>
<td>Ethernet</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>SPIF</td>
<td>External Memory Interface (SPIF)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>USB</td>
<td>Universal Serial Bus (USB)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>I2C</td>
<td>I2C Inter-Integrated Circuit (I2C)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAP</td>
<td>Enhanced Capture (eCAP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAP</td>
<td>Enhanced Capture (eCAP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAP</td>
<td>Enhanced Capture (eCAP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAP</td>
<td>Enhanced Capture (eCAP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>CAP</td>
<td>Enhanced Capture (eCAP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>QEP</td>
<td>Enhanced Quadrature Encoder Pulse (eQEP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>QEP</td>
<td>Enhanced Quadrature Encoder Pulse (eQEP)</td>
<td>NO</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM1)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM2)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM3)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM4)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM5)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM6)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>PWM</td>
<td>Enhanced Pulse Width Modulators (ePWM7)</td>
<td>YES</td>
</tr>
<tr>
<td>Peripheral</td>
<td>MUS</td>
<td>Power Supply</td>
<td>YES</td>
</tr>
<tr>
<td>Package</td>
<td>NA</td>
<td>Package</td>
<td>YES</td>
</tr>
</tbody>
</table>

- **Module is not used in the function being analyzed**

- Allow customization of failure rate estimation
- Include only MCU modules used by application
- Include actual Flash and SRAM memory size used

Based on TMS570LS12x v1.0 FMEDA worksheet
### Safety mechanisms considered in the FMEDA

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Diagnostic Used in Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>PWR1</td>
<td>Voltage monitor (VMON)</td>
<td>1</td>
</tr>
<tr>
<td>Power Supply</td>
<td>PWR2</td>
<td>External voltage supervisor</td>
<td>1</td>
</tr>
<tr>
<td>Power Management Module (PMM)</td>
<td>PMM1</td>
<td>Lockstep PSCON</td>
<td>1</td>
</tr>
<tr>
<td>Power Management Module (PMM)</td>
<td>PMM2</td>
<td>Privileged Mode Access and Program Sequence Control Registers</td>
<td>1</td>
</tr>
<tr>
<td>Power Management Module (PMM)</td>
<td>PMM3</td>
<td>Periodic SW readback of static configuration registers</td>
<td>1</td>
</tr>
<tr>
<td>Power Management Module (PMM)</td>
<td>PMM4</td>
<td>SW readback of written configuration</td>
<td>1</td>
</tr>
<tr>
<td>Power Management Module (PMM)</td>
<td>PMM5</td>
<td>PSCON lockstep compare self-test</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK1</td>
<td>LPOCLKDET</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK2</td>
<td>PLL slip detector</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK3</td>
<td>Dual Clock Comparator (DCC)</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK4</td>
<td>External monitoring via ECLK</td>
<td>0</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK5A</td>
<td>Internal watchdog -DWD</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK5B</td>
<td>Internal watchdog -DWWD</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK6</td>
<td>Periodic SW readback of static clock configuration registers</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK7</td>
<td>SW readback of written configuration</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK8</td>
<td>Software test of DCC operation</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK9</td>
<td>Software test of DWD operation</td>
<td>1</td>
</tr>
<tr>
<td>Clock</td>
<td>CLK10</td>
<td>Software test of DWWD operation</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST1</td>
<td>External monitoring of warm reset</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST2</td>
<td>SW check of last reset</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST3</td>
<td>SW warm reset generation</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST4</td>
<td>Glitch filtering on reset pins</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST5</td>
<td>Use of status shadow registers</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST6</td>
<td>External watchdog</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST7</td>
<td>Periodic SW readback of static configuration registers</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST8</td>
<td>SW readback of written configuration</td>
<td>1</td>
</tr>
<tr>
<td>Reset</td>
<td>RST9</td>
<td>Software test of basic reset functionity</td>
<td>1</td>
</tr>
</tbody>
</table>

- Allow customization of diagnostics selection – ‘1’ diagnostic used, ‘0’ diagnostic not used
- Consult Safety Manual Chapter 6

Based on TMS570LS12x v1.0 FMEDA worksheet
### FMEDA worksheet – Metrics Summary / Details

**Summary of ISO 26262 Metrics Examples – Permanent/Transient & Die/Package:**

<table>
<thead>
<tr>
<th>Metric Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td></td>
</tr>
<tr>
<td>Safety related FIT</td>
<td></td>
</tr>
<tr>
<td>Probabilistic Metrics for random Hardware Failures - PMHF (in FIT)</td>
<td></td>
</tr>
<tr>
<td>Single Point Fault Metric - SPFM</td>
<td>99.58% 99.93%</td>
</tr>
<tr>
<td>Latent Fault Metric - LFM</td>
<td>99.98% NA</td>
</tr>
</tbody>
</table>

ISO 26262 categorization as in ISO 26262:2011-10, 8.1.8

<table>
<thead>
<tr>
<th>Metric Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total faults</td>
<td>$\lambda$</td>
</tr>
<tr>
<td>Total Safety Related faults</td>
<td>$\lambda_{SR}$</td>
</tr>
<tr>
<td>Total Not Safety Related faults</td>
<td>$\lambda_{NSR}$</td>
</tr>
<tr>
<td>Total Safe faults</td>
<td>$\lambda_{S}$</td>
</tr>
<tr>
<td>Total not Safe faults</td>
<td>$\lambda_{NS}$</td>
</tr>
<tr>
<td>Total faults with prob. of violate the SG</td>
<td>$\lambda_{PVSG}$</td>
</tr>
<tr>
<td>Total single point faults</td>
<td>$\lambda_{SPF}$</td>
</tr>
<tr>
<td>Total residual faults</td>
<td>$\lambda_{RF}$</td>
</tr>
<tr>
<td>Total Multi Point $^{(ad)}$</td>
<td>$\lambda_{MPF}{}^{(ad)}$</td>
</tr>
<tr>
<td>Total Multi Point $^{(l)}$</td>
<td>$\lambda_{MPF}{}^{(l)}$</td>
</tr>
<tr>
<td>Total Multi Point detected faults</td>
<td>$\lambda_{MPF_{det}}$</td>
</tr>
<tr>
<td>Total Multi Point latent faults</td>
<td>$\lambda_{MPF_{lat}}$</td>
</tr>
</tbody>
</table>

**Data available under NDA**

FMEDA worksheet is available under NDA

Based on TMS570LS12x v1.0 FMEDA worksheet
# FMEDA worksheet – Metrics Summary / Details

## Details of ISO 26262 Metrics Examples – Permanent/Transient & Die/Package:

### Permanent faults

<table>
<thead>
<tr>
<th>Component level</th>
<th>Device Partition (according to TI SM)</th>
<th>Raw Permanent faults FIT</th>
<th>Total Safety Related faults</th>
<th>Fail rate Safe Fault not to be considered in the analysis Lambda nBR [i, j]</th>
<th>Fail rate Safe Fault Lambda S [i]</th>
<th>Fail rate non-Safe Fault Lambda nS [i]</th>
<th>Residual Fault failure rate Lambda RF [i, j]</th>
<th>Lambda MPF [ad]</th>
<th>Lambda MPF [t]</th>
<th>Multipoint fault detected Lambda MPF det [v, w]</th>
<th>Single Point Fault Metric $M_{SPFM}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU SubSystem</td>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.96%</td>
</tr>
<tr>
<td>CPU SubSystem</td>
<td>Vectorized Interrupt Module (VIM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.76%</td>
</tr>
<tr>
<td>CPU SubSystem</td>
<td>LBIST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>CPU SubSystem</td>
<td>PBIST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>JTAG SubSystem</td>
<td>JTAG Technical Access Group (TJTAG), Debug/Trace/Calibration Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>JTAG SubSystem</td>
<td>Cortex R4F Central Processing Unit (CPU), debug and trace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>JTAG SubSystem</td>
<td>Panoram Overlay Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>RAM System</td>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.92%</td>
</tr>
<tr>
<td>Flash System</td>
<td>One Time Programmable (OTP) Flash Static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.65%</td>
</tr>
<tr>
<td>Flash System</td>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.61%</td>
</tr>
<tr>
<td>Flash System</td>
<td>Flash controlled EEPROM (FEE)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99.95%</td>
</tr>
</tbody>
</table>

### Transient faults

| Component level | Device Partition (according to TI SM) | Raw Transient faults FIT | Total Safety Related faults | Fail rate Safe Fault not to be considered in the analysis Lambda nBR [i, j] | Fail rate Safe Fault Lambda S [i] | Fail rate non-Safe Fault Lambda nS [i] | Residual Fault failure rate Lambda RF [i, j] | Lambda MPF,ad | Lambda MPF,t | Single Point Fault Metric $M_{SPFM}$ |
|-----------------|--------------------------------------|--------------------------|-----------------------------|----------------------------------------------------------------|----------------------------------|------------------------------------------|---------------------------------------------|----------------|----------------|-------------------------------|-------------------------------|
| CPU SubSystem   | Cortex R4F Central Processing Unit (CPU) |                          |                             |                                                                      |                                  |                                          |                                             |                |                |                                               | 99.95%                        |
| CPU SubSystem   | Vectorized Interrupt Module (VIM)     |                          |                             |                                                                      |                                  |                                          |                                             |                |                |                                               | 99.65%                        |
| CPU SubSystem   | LBIST                                |                          |                             |                                                                      |                                  |                                          |                                             |                |                |                                               | NA                            |
| CPU SubSystem   | PBIST                                |                          |                             |                                                                      |                                  |                                          |                                             |                |                |                                               | NA                            |

Data available under NDA

FMEDA worksheet is available under NDA

Details of ISO 26262 Metrics:
- For Permanent and Transient faults
- By modules (CPU, Flash, SRAM, DCAN, ADC…)

Based on TMS570LS12x v1.0 FMEDA worksheet
ISO 26262 / IEC 61508 Risk reduction

### Functional Safety

- **Item Definition**
- **Hazard & Risk Analysis**
- **SIL / ASIL Determination**
- **Safety Goal Safety Function**
- **Allocation of Safety Requirements**
- **HW Safety Metrics**

### Example

**What is the function?**
- EV traction motor control

**What is tolerable risk?**
- ASIL-C

**Safety requirements & Failure mode/rate & Diagnostics**
- Avoid too high positive torque

**Sufficient risk reduction?**
- Implement MCU diagnostics to monitor PWM

**Computation of SPFM / PMHF**
- Too high motor positive torque -> Causing collision

- **Use Safety Manual Chapter 6 to determine applicable safety mechanisms by MCU module such as CPU, SRAM, PWR...**

- **Use FMEDA worksheet**
  - **FIT Estimation sheet** to tailor use conditions
  - **Product Function Tailoring sheet** to select MCU modules used in safety function
  - **Pin Level Tailoring sheet** to select MCU pins used in safety function
  - **Safety Mechanism Tailoring sheet** to select applied Safety mechanisms
  - **Summary and Details-ISO26262 or IEC61508 sheets** to determine if MCU and modules safety metrics are met.
## Hercules and SafeTI Process Certifications

<table>
<thead>
<tr>
<th>Product</th>
<th>Standard</th>
<th>Assessor</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM48x (20 Devices)</td>
<td>IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3</td>
<td><img src="image1.png" alt="TUV SUD logo" /></td>
<td><img src="image2.png" alt="" /></td>
</tr>
<tr>
<td>RM46x (12 Devices)</td>
<td>IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3</td>
<td><img src="image1.png" alt="TUV SUD logo" /></td>
<td><img src="image2.png" alt="" /></td>
</tr>
</tbody>
</table>

56 Hercules products certified and counting!!

RM48x and RM46x certified to IEC 61508 SIL 3 for Industrial functional safety applications.

TMS570LS31x/21x and TMS570LS12x/11x certified to ISO 26262 ASIL D for Automotive functional safety applications.

SafeTI Hardware and Software development processes also certified.

Reduce time and effort to certify your end system!!
Hercules™ RM Cortex-R® MCU platform
For Industrial and Medical

ISO 13849 / IEC 61508 / IEC 60601

Sensors
Relays
Pumps
Drives
Plc
Pumps
CPAP

-40 to 105°C
100K POH
High MTBF
Long life supply
High volume

• RM46L8
220 MHz
1.2MB Flash
192kB RAM
144p QFP
337p BGA

• RM44L9
220 MHz
1MB Flash
128kB RAM
144p QFP
337p BGA

• RM44L2
80MHz
128kB Flash
32kB RAM
100p QFP
337p BGA

• RM41L2
80MHz
128kB Flash
32kB RAM
100p QFP

• RM42L4
100 MHz
384kB Flash
32kB RAM
100p QFP
144p QFP
337p BGA

• RM44L5
200 MHz
768kB Flash
128kB RAM
100p QFP
144p QFP
337p BGA

• RM46L8
220 MHz
2MB Flash
256kB RAM
144p QFP
337p BGA

• RM48L9
220 MHz
3MB Flash
512kB RAM
144p QFP
337p BGA

• RM57L
330 MHz
4MB Flash
512kB RAM
337p BGA

Temperature
Reliability
Supply
Safety

- RM46L Certified to IEC61508 SIL 3
- 100K POH
- High MTBF
- Long life supply
- High volume

High Next

Compatible 337-pin BGA, 144-pin QFP package
Compatible 100-pin QFP package

38
Hercules™ MCUs: Accelerating Safety Products to Market

- **Broad Eco-system**
  - Software
  - Development Tools
  - Consulting & Training

- **Certified Safety Hardware Architecture**
  - Pre-approved for ISO 26262, IEC 61508
  - Safety Analysis Report with FMEDA, FIT

- **Unique Tools for Safety Development**
  - Ease development
  - Aid certification

- **Production Quality Safety Software**
  - Usable by customer
  - Certification Ready
  - ISO 26262, IEC 61508 compliant

- **Comprehensive Portfolio Complementary Analog**
  - Pin & SW Compatible
  - Safety Chipset
  - SafeTI Program

- **ARM based Lockstep MCU supplier**
  - Non-proprietary
  - Market accepted
  - Respected heritage
Thank You

Contact Information:
Riccardo Mariani@yogitech.com
Hoiman Low: hm-low@ti.com