TI/TÜV Rheinland Functional Safety Seminar
China

Texas Instruments Inc.
Nov/2014
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package
• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit
• Summary
Functional Safety: Important for Many Industries

- Safety critical systems are everywhere
- Systems need to manage hazardous failures
- Many systems need to be safety-certified

Automotive and Transportation
- HEV/EV Cars
- Radar / Collision Avoidance (ADAS)
- Active suspension, ABS, electric power steering, airbag and more!
- Railway Systems
- Anti-skid control

Industrial and Medical
- Sensor & communications gateway
- Manufacturing, robotics, industrial automation, motor control
- Wind Power
- Anesthesia machines, respirators, ventilators, oxygen concentrators

Standards:
- **EN 50155** EN 50128 (railway)
- **DO-254** DO-178B (aerospace)
- **IEC 60601** (medical equipment)
- **IEC 61511** (process industry)
- **IEC 62061** ISO 13849 (machinery)
- **IEC 61508** (safety)
- **IEC 50156** (furnaces)
- **IEC 60880** (nuclear power stations)
- **ISO 26262** (automotive)
Hercules™ MCU: End Equipment

Aerospace & Railway
- Avionics / Autopilot
- Flight Control
- Anti-Skid Control
- Communications Gateway
- Motor Control
- Industrial Motor Control
- Wind Power
- Elevator
- Escalator

Industrial
- Manufacturing / Robotics
- Wind Power
- Industrial Automation / PLC
- Solar Power

Automotive
- Braking / Stability Control
- Airbag
- Hybrid & Electric Vehicles
- Electric Power Steering
- Chassis / Domain Control
- Radar / Collision Avoidance (ADAS)

Medical
- Infusion Pumps
- Oxygen Concentrators
- Respirators
- Anesthesia

Medical
- Flight Control
- Avionics / Autopilot
- Oxygen Concentrators
- Respirators
- Anesthesia

Automotive
- Hercules™ MCU
- ISO
- IEC
-Texas Instruments

Aerospace & Railway
- Hercules™ MCU
- ISO
- IEC
- Texas Instruments
TI Hercules™ MCU Platform
ARM® Cortex® Based Microcontrollers

Hercules™ MCU Platform

RM

Industrial and Medical Safety MCUs
- 80MHz to 330MHz
- 128KB to 4MB Flash
- -40 to 105°C Operation
- ENET, USB, CAN & UART
- Developed to Safety Standards
  - IEC 61508 SIL-3
  - Cortex-R – up to 550 DMIPs

TMS570

Transportation and Automotive Safety MCUs
- 80MHz to 300MHz
- 128KB to 4MB Flash
- Automotive Q100 Qualification
- -40 to 125°C Operation
- FlexRay, ENET, CAN, LIN/UART
- Developed to Safety Standards
  - ISO 26262 ASIL-D
  - IEC 61508 SIL-3
  - Cortex-R – up to 500 DMIPs

Lockstep MCUs for functional Safety
Hercules™ RM MCUs
Supporting Industrial & Medical safety

Benefits

• Lockstep ARM Cortex-R based MCU – with up to 550 peak DMIPS and 384KB to 4MB Flash Memory
• Safety Integrated in HW – provides a high level of diagnostic coverage to reduce safety software overhead
• SafeTI™ system design packages – makes it easier to achieve safety certification and get to market quickly
• Developed to safety standards – developed for use in IEC 61508 SIL-3 safety applications
• Flexible Communication and Control – Ethernet, USB, CAN. Up to 84 timer and 41 12-bit ADC channels.

Tools

Development Kit
Launchpad
ADS5060 Pro Trace
SafeTI Kit
Motor Control

Software

• Drivers & Libraries – HALCoGen peripheral driver generation tool, SafeTI™ Diagnostic Library, CMSIS DSP Library
• RTOS: SAFERTOS, CodeSys
• IDEs: Code Composer Studio, IAR
• SafeTI Compiler Qualification Kit
• SafeTI 3rd Party Ecosystem

Packages

144p QFP (20x20mm)
100p QFP (14x14mm)
337p BGA (16x16mm)
Hercules™ RM Cortex™-R Roadmap

2012

High

RM48L9x – 220MHz R4F
3MB Flash, 256kB RAM
SafeTI ISO & IEC

RM48L5x – 200MHz R4F
2MB Flash, 192kB RAM
SafeTI ISO & IEC

Mid

RM46L8x – 220MHz R4F
1.25MB Flash, 192kB RAM
SafeTI ISO & IEC

RM46L4x – 200MHz R4F
1MB Flash, 128kB RAM
SafeTI ISO & IEC

Low

RM42x – 100MHz R4
384kB Flash, 32kB RAM
SafeTI ISO & IEC

Features:

Lock Step Architecture
QEP/PWM
Ethernet
CAN CAN USB
ISO ISO 13849 IEC IEC 61508 SafeTI

2013

RM46L8x – 220MHz R4F
1.25MB Flash, 192kB RAM
SafeTI ISO & IEC

RM46L4x – 200MHz R4F
1MB Flash, 128kB RAM
SafeTI ISO & IEC

Next Gen Mid
SafeTI ISO & IEC

2014

RM57Lx – 330MHz R5F
4MB Flash, 512kB RAM

Next Gen Low
SafeTI ISO & IEC

Sampling
 Development

Production

Texas Instruments
Hercules™ TMS570 MCUs
Supporting Automotive & Transportation safety

**Benefits**

- **Lockstep ARM Cortex-R based MCU** – with up to 480 peak DMIPS and 256KB to 4MB Flash Memory
- **Safety Integrated in HW** – provides a high level of diagnostic coverage to reduce safety software overhead
- **SafeTI™ system design packages** – makes it easier to achieve safety certification and get to market quickly
- **Developed to safety standards** – developed for use in IEC 61508 SIL-3 and ISO 26262 ASIL-D safety applications
- **Flexible Communication and Control** – Ethernet, Flexray, CAN. Up to 84 timer and 41 12-bit ADC channels.

**Tools**

- Development Kit
- Launchpad
- ADS560 Pro Trace
- SafeTI Kit
- Motor Control

**Software**

- **Drivers & Libraries** – HALCoGen peripheral driver generation tool, SafeTI™ Diagnostic Library, CMSIS DSP Library,
- **RTOS** – SAFERTOS, AUTOSAR
- **IDEs**: Code Composer Studio, IAR
- **SafeTI Compiler Qualification Kit**
- **Mathworks Simulink**
- **SafeTI 3rd Party Ecosystem**

**Packages**

- 144p QFP (20x20mm)
- 100p QFP (14x14mm)
- 337p BGA (16x16mm)
Hercules™ TMS570 Cortex™-R Roadmap

2012

- TMS570LS11x – 180MHz R4F
  - 1MB Flash, 128kB RAM
  - SafeTI ISO & IEC

- TMS570LS21x – 180MHz R4F
  - 2MB Flash, 192kB RAM
  - SafeTI ISO & IEC

2013

- TMS570LS12x – 180MHz R4F
  - 1.25MB Flash, 192kB RAM
  - SafeTI ISO & IEC

- TMS570LS11x – 180MHz R4F
  - 1MB Flash, 128kB RAM
  - SafeTI ISO & IEC

Features:

- Lock Step Architecture
- ISO ISO 26262
- IEC IEC 61508

- QEP/ePWM
- Ethernet
- CAN
- FlexRay

2014

- TMS570LC – 300MHz R5F
  - 4MB Flash, 512kB RAM

- Next Gen Mid
  - SafeTI ISO & IEC

- Next Gen Low
  - SafeTI ISO & IEC

Low

- Production
- Sampling
- Development

Mid

High
# Functional Safety Standards Hardware requirements

<table>
<thead>
<tr>
<th>Standard</th>
<th>System</th>
<th>Safety Integrity</th>
<th>Architectural Metric</th>
<th>Architectural Requirement</th>
<th>Failure Rate</th>
<th>Specific MCU self-test requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>Programmable E/E systems</td>
<td>SIL – 1,2,3,4</td>
<td>SFF</td>
<td>HFT&gt;0 for SIL 4</td>
<td>PFD, PFH</td>
<td>No</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>Automotive</td>
<td>ASIL – A, B, C, D</td>
<td>SPFM / LFM</td>
<td>No</td>
<td>PMHF</td>
<td>No</td>
</tr>
<tr>
<td>EN 50129</td>
<td>Railway</td>
<td>SIL- 1,2,3,4</td>
<td>N/A</td>
<td>Follow IEC 61508</td>
<td>THR</td>
<td>CPU, Memory</td>
</tr>
<tr>
<td>ISO 22201</td>
<td>Elevator</td>
<td>SIL – 1,2,3</td>
<td>N/A</td>
<td>Dual channels for SIL3</td>
<td>N/A</td>
<td>CPU, Memory, Interrupt, Clock, I/O, Comm</td>
</tr>
<tr>
<td>IEC 61800</td>
<td>Drive</td>
<td>SIL – 1,2,3</td>
<td>SFF</td>
<td>Dependent on function</td>
<td>PFH (no PFD)</td>
<td>No</td>
</tr>
<tr>
<td>IEC 62061</td>
<td>Machinery</td>
<td>SIL – 1,2,3</td>
<td>SFF</td>
<td>Supports ISO 13849 categories</td>
<td>PFH_D</td>
<td>No</td>
</tr>
<tr>
<td>IEC 61511</td>
<td>Process Automation</td>
<td>SIL – 1,2,3</td>
<td>SFF</td>
<td>See IEC 61508</td>
<td>PFDavg</td>
<td>No</td>
</tr>
<tr>
<td>ISO 13849</td>
<td>Machinery</td>
<td>PL a,b,c,d,e</td>
<td>DC_{avg}</td>
<td>CAT B,1,2,3,4</td>
<td>MTTF_{D}</td>
<td>No</td>
</tr>
<tr>
<td>IEC 60730</td>
<td>Home Appliances</td>
<td>Class A, B, C</td>
<td>No</td>
<td>Yes (Class C)</td>
<td>No</td>
<td>CPU, Memory, Interrupt, Clock, I/O, Comm</td>
</tr>
</tbody>
</table>

**IEC** 61508 Programmable E/E systems SIL – 1,2,3,4 SFF HFT>0 for SIL 4 PFD, PFH

**ISO** 26262 Automotive ASIL – A, B, C, D SPFM / LFM No PMHF

**EN 50129** Railway SIL- 1,2,3,4 N/A Follow IEC 61508 THR CPU, Memory

**ISO** 22201 Elevator SIL – 1,2,3 N/A Dual channels for SIL3 N/A CPU, Memory, Interrupt, Clock, I/O, Comm

**IEC** 61800 Drive SIL – 1,2,3 SIL4 Apply IEC 61508 SFF Dependent on function PFH (no PFD) No

**IEC** 62061 Machinery SIL – 1,2,3 SIL4 Apply IEC 61508 SFF Supports ISO 13849 categories PFH_D No

**IEC** 61511 Process Automation SIL – 1,2,3 SIL4 Apply IEC 61508 SFF See IEC 61508 PFDavg No

**ISO** 13849 Machinery PL a,b,c,d,e DC_{avg} CAT B,1,2,3,4 MTTF_{D} No

**IEC** 60730 Home Appliances Class A, B, C No Yes (Class C) No CPU, Memory, Interrupt, Clock, I/O, Comm

**Texas Instruments**
## Typical Usage of Hercules MCU per Functional Safety Standard*

<table>
<thead>
<tr>
<th>Functional Safety Standard</th>
<th>Typical Hercules MCU Usage</th>
<th>Specific Diagnostic Requirements per Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>No</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>Single Hercules MCU ASIL A to D</td>
<td>No</td>
</tr>
<tr>
<td>EN 50129</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>Examples provided, not requirements</td>
</tr>
<tr>
<td>ISO 22201</td>
<td>Single MCU for SIL1 - SIL 2, Dual MCU for SIL 3</td>
<td>Yes</td>
</tr>
<tr>
<td>IEC 61511</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>No</td>
</tr>
<tr>
<td>IEC 61800</td>
<td>Single Hercules MCU for SIL1 - SIL 3</td>
<td>No</td>
</tr>
<tr>
<td>IEC 62061</td>
<td>Single Hercules MCU for SIL1 - SIL 3</td>
<td>No</td>
</tr>
<tr>
<td>ISO 13849</td>
<td>Single MCU for Cat B, 1, 2 from PL a to PL e, Dual MCU for Cat 3, 4 from PL a to PL e, Single MCU + TPS under evaluation for PL d CAT3</td>
<td>No</td>
</tr>
<tr>
<td>IEC 60730</td>
<td>Single MCU for Class A – C, Dual MCU for some Class C</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Items shown are typical examples. Achieved safety integrity level is the responsibility of the system developer.
Applying Functional Safety Standards

SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

**Safety Life Cycle**
- Development Process
- Safety Plan
- Documentation
- Config Management
- Change Management
- V&V
- Personnel Competence
- Certification

**Functional Safety**

**Risk reduction**

**SIL - 1/2/3/4**
- Systematic Failures
  - Software
  - Tools
- Random Failures
  - Diagnostics
  - Architectural Metric
  - Failure Rate

**Process Certification**
- Software CSP
- Compiler Qual. Kit

**Hercules™ Architecture (FMEDA)**

CSP = Compliance Support Package
Hercules™ MCU safety 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

ECC or Parity on select Peripheral, DMA and Interrupt controller RAMS

Parity or CRC in Serial and Network Communication Peripherals

GIO

Serial Interfaces

Network Interfaces

Dual ADC Cores Available

Dual High-end Timers Available

Power, Clock, & Safety

Memory

ARM® Cortex® R w/ MPU

OSC PLL

PBIST/LBIST

POR

ESM

CRC

RTI/DWWD

Memory Interface

External Memory

DMA

Enhanced System Bus and Lockstep Vectored Interrupt Module

Lockstep CPU

ARM® Cortex® R w/ MPU

Compare Module for Fault Detection

ECC for flash / RAM evaluated inside the Cortex R

Memory Protection Unit

Protective Bus and lockstep Interrupt Manager

IO Loop Back, ADC Self Test, ...

Dual ADC Cores with shared channels

On-Chip Clock and Voltage Monitoring

Error Signaling Module w/ External Error Pin

Memory BIST on all RAMS for fast memory test

ARM® Cortex® R w/ MPU

Lockstep CPU

ECC or Parity on select Peripheral, DMA and Interrupt controller RAMS

Parity or CRC in Serial and Network Communication Peripherals

ECC or Parity on select Peripheral, DMA and Interrupt controller RAMS

Parity or CRC in Serial and Network Communication Peripherals

Random

Bold items are introduced with the new Cortex®-R5 devices
2 Basis of Evaluation

The regulations and guidelines which form the basis of the type testing are listed below.

2.1 Functional Safety

<table>
<thead>
<tr>
<th>No.</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
</table>

Table 2: Functional Safety

5 Result of the concept review

5.1 Concept review based on IP-FMEAs

To evaluate the Platform Architecture according to the required failure modes defined in [N1] and [N2] for SIL 3 and ASIL D the analysis method Failure Mode and Effects Analysis (FMEA) was used. For each IP an own FMEA was created. Within these FMEAs diagnostic measures and timing aspects have been analysed. These FMEAs should be used in further development as input for the Safety requirement specification of several safety microcontroller devices.

Result:
The FMEAs provided in the documents [D1] - [D38] were made by Texas Instruments Incorporated and reviewed by TÜV SÜD. The results of the FMEAs meet the requirements according to [N1] and [N2]. These review results are recorded in [R1] - [R38]. The effectiveness of the selected diagnostic measures has to be verified on the final device.

6 Summary

For the analyzed failure modes according to [N1] - [N2] appropriate diagnostic measures to reach SIL 3 or ASIL D have been specified. A concluding re-evaluation of the IP-FMEAs has to be done in context of the final device.
SafeTI™ Hitex Safety Kit (SafeTI™- HSK)

- Cost effective entry into functional safety related to ISO26262 and IEC61508
- Evaluate the use and performance of the Hercules™ MCU safety features
- Easily apply the recommendations of the Hercules™ MCU & TP 65381 Safety Manual
- Inject System & CPU faults and Monitor and Measure the reaction via a GUI
- Includes:
  - Evaluation Board with integrated debug, USB cable and Power Supply
  - Windows-based GUI
  - Demo Application with full source code
  - Code Composer Studio™ IDE
  - HALCogen and SafeTI Diagnostic Library
  - Evaluation version of SafeRTOS
  - User Manual
Hercules™ Safety Documents

Documents provided by TI some under NDA to assist in the safety certification process:

- **Hercules™ component Safety Manual (SM)**
  Details product safety architecture and recommended usage

- **Safety Analysis Report Summary (SAR1)**
  Summary of FIT rate and FMEDA at component level for IEC 61508 and ISO 26262

- **Detailed Safety Analysis Report (SAR2)**
  - Full details of all safety analysis executed down to MODULE level for IEC 61508 and ISO 26262
  - Software tool for customizing analysis results to customer use case

- **Safety Report**
  Summary of compliance to IEC 61508 and/or ISO 26262
Safety Manual

- Summary of Development Flow
- Description of Safety Concept
- List of diagnostics
- List of assumptions
Detailed Safety Analysis Reports

- Adapt failure rate estimation model based on system usage
- Easily partition device into safety related and non-safety related functions
- Select applicable diagnostics from safety manual or apply your own diagnostics
- Automatic calculation of summarized and detailed ISO 26262 & IEC 61508 safety metrics

* FMEDA Developed with Yogitech
SafeTI™ Hardware Development Process Certification

TI’s hardware functional safety development process has been certified for:

- IEC 61508 SIL-3
- ISO 26262 ASIL-D

The certification demonstrates TI’s commitment to have a process suitable for developing hardware components that are compliant to ISO 26262 and IEC 61508.
Hercules™ and SafeTI™ Software and Tool Packages

Hercules Software and Tools
- Production quality software to easily use Hercules MCU
- Includes GUI configurator (where relevant)
- Includes User Guide and Release Notes

SafeTI Compliance Support Package
- Provide evidence to safety standards
- Includes Test Reports, Quality Metrics, Safety Manual, etc.
- Software developed to IEC 61508 & ISO 26262 requirements

SafeTI Tool Qualification Kit
- Assists in qualifying the TI ARM Compiler to functional safety standards
- Model-based tool qualification methodology
- Assessed to comply with both IEC 61508 and ISO 26262
SafeTI™ Compiler Qualification Kit

- Assists in qualifying the TI ARM C/C++ Compiler to functional safety standards
- Qualification of customer specific use case can be less restrictive than certified compilers
- Application of kit assessed by TÜV Nord to comply with both IEC 61508 and ISO 26262

Includes:
- Qualification Support Tool (model-based)
- Process specific documentation:
  - Tool Classification Report
  - Tool Qualification Plan
  - Tool Qualification Report
  - Tool Safety Manual
- ACE SuperTest™ qualification suite
- TI compiler validation test cases
- Test Automation Unit (TAU)
- 24hrs of Validas consulting services
- TÜV Nord assessment report
Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEKX kit
- Summary
SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

Workshop will address:
- How to manage MCU hardware random failures
- How to estimate failure rate vs SIL requirements
- Software support

CSP = Compliance Support Package
## Functional Safety Certification

### System

<table>
<thead>
<tr>
<th>Development Process</th>
<th>Software</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Development Process</td>
<td>MCU Software Drivers, Library Tool</td>
<td>MCU Hardware Architecture Failure rate</td>
</tr>
</tbody>
</table>

Show me evidence
IEC 61508
Hazard/Risk Analysis & SIL determination

- Hazard & Risk Analysis
- Safety Function Definition
- SIL Determination (SIL - 1/2/3/4)
- Allocation of Safety Requirements
- HW Safety Requirements (SFF, PFH)
- SW Safety Requirements
- Process Safety Requirements
Safety Function / Safe State

Hazard analysis -> Safety Function & Safe State

**Safety Function**: function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the ECU, in respect of a specific hazardous event

**Safe State**: State of the ECU when safety is achieved
**Safety Function / Safe State**

**Hazard**: High gas flow pressure

**Safety Function**: Monitor the pressure of gas flow.

**Safe State**:
1. If gas flow pressure exceeds a fixed limit, shut off the gas flow valve.
2. If a dangerous fault is detected in the system, shut off the gas flow.
Risk Analysis / Safety Integrity Level

**Risk Analysis** determines the performance requirement of the safety function, i.e. **SIL level** and how much risk reduction?

**Safety Integrity Level** (SIL 1/2/3/4) is determined by the consequence and the frequency of hazardous event. The higher the SIL level, the higher the risk reduction requirements.
Safety Integrity Level

- Safety Integrity Level is characterized by SFF and $\text{PFD}_{\text{AVG}}$ or PFH
  - Single Failure Fraction (SFF)
  - Probability of Fail on Demand Average ($\text{PFD}_{\text{AVG}}$)
  - Probability of Fail per Hour (PFH)

- $\text{SFF} = \frac{\lambda_{\text{SAFE}} + \lambda_{\text{DANGEROUS-DETECTED}}}{\lambda_{\text{SAFE}} + \lambda_{\text{DANGEROUS-DETECTED}} + \lambda_{\text{DANGEROUS-UNDETECTED}}}$

- $\text{PFH} \approx \frac{1}{\lambda_{\text{DANGEROUS-UNDETECTED}}}$

How to calculate all these?
Safety Integrity Level

Low demand functions have less stringent requirements on PFDavg to achieve a specific SIL.

High demand and continuous demand functions have more stringent requirements on PFH to achieve a specific SIL.

Type B products are complex products in which all failure modes are not known. Most semiconductors are considered Type B.

HFT = Hardware Fault Tolerance where 0=No redundancy

1 FIT = 1 failure in 1E9 hours
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, EMC
  - Failure rate data source is TI experiments in Los Alamos lab and TI lab
MCU Failure Rate Estimation

MCU failure rate ($\lambda_{MCU}$)

SRAM failure rate ($\lambda_{SRAM}$)
- Apply SRAM Diagnostics
- Failure rate analysis $\lambda_{SRAM}$, $\lambda_{SAFE}$, $\lambda_{DD}$, $\lambda_{DU}$

CPU failure rate ($\lambda_{CPU}$)
- Apply CPU Diagnostics
- Failure rate analysis $\lambda_{CPU}$, $\lambda_{SAFE}$, $\lambda_{DD}$, $\lambda_{DU}$

Flash failure rate ($\lambda_{Flash}$)
- Apply Flash Diagnostics
- Failure rate analysis $\lambda_{Flash}$, $\lambda_{SAFE}$, $\lambda_{DD}$, $\lambda_{DU}$

Apply diagnostics to detect dangerous faults until appropriate SIL metrics (SFF, PFH) are met

$\lambda_{SAFE}$ – Safe, $\lambda_{DD}$ – Dangerous Detected, $\lambda_{DU}$ – Dangerous Undetected
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
Application Example

Safety Goal: The motor shall deliver torque as commanded by the external host.

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)

Safe State (MCU)
1. Disable motor driver relay (NHET)
2. Indicate fault to system via warning lamp (GIO)
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 61508 HW metrics per SIL level.

In this example, safety critical elements are: CPU, Flash, SRAM, Interconnect, eQEP, eCAP, ePWM, System, ESM... I2C.
## Safety Function Definition

<table>
<thead>
<tr>
<th>Safety Function ID</th>
<th>Equivalent Safety Goal ID</th>
<th>Safety Function Input (MCU)</th>
<th>Safety Function Processing (MCU)</th>
<th>Safety Function Actuation (MCU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF_1</td>
<td>SG_1</td>
<td>Receive motor torque command from remote host (CAN)</td>
<td>Calculate necessary output commands to motor based on desired torque and current position</td>
<td>Drive three phase PWMs to actuate motor (ePWM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read current motor position (feedback) via quadrature decoder (eQEP)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Process safety time (PST):  
- time between occurrence of a potential dangerous failure and the hazardous event

<table>
<thead>
<tr>
<th>Equivalent Safety Goal</th>
<th>Safe State (MCU)</th>
</tr>
</thead>
</table>
| The motor shall deliver torque as commanded by the external host. | 1. Disable motor driver relay (NHET)  
2. Indicate fault to system via warning lamp (GIO) |

<table>
<thead>
<tr>
<th>SIL</th>
<th>Equivalent FTTI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10 ms</td>
</tr>
</tbody>
</table>
## MCU Safety Diagnostic Requirements per Safety Function

<table>
<thead>
<tr>
<th>Safety Requirement ID</th>
<th>Satisfies</th>
<th>Assumed Safety Diagnostic Requirement</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFR_1</td>
<td>SF_1</td>
<td>MCU safety related functional input shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_1.1</td>
<td>SFR_1</td>
<td>DCAN1 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_1.2</td>
<td>SFR_1</td>
<td>eQEP1 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_2</td>
<td>SF_1</td>
<td>MCU safety related functional output shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_2.1</td>
<td>SFR_2</td>
<td>ePWM1 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_2.2</td>
<td>SFR_2</td>
<td>ePWM2 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_2.3</td>
<td>SFR_2</td>
<td>ePWM3 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3</td>
<td>SF_1</td>
<td>MCU safety related processing shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3.1</td>
<td>SFR_3</td>
<td>Cortex R4F CPU shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3.2</td>
<td>SFR_3</td>
<td>TCM SRAM as needed to support the application shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3.3</td>
<td>SFR_3</td>
<td>TCM Flash as needed to support the application shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3.4</td>
<td>SFR_3</td>
<td>L2/L3 interconnect as needed to support the application shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_3.5</td>
<td>SFR_3</td>
<td>VIM shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4</td>
<td>SF_1</td>
<td>MCU functions necessary to support safety related input, processing, and output shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.1</td>
<td>SFR_4</td>
<td>Power supply shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.2</td>
<td>SFR_4</td>
<td>PMM shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.3</td>
<td>SFR_4</td>
<td>Clocking subsystem shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.4</td>
<td>SFR_4</td>
<td>Reset logic shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.5</td>
<td>SFR_4</td>
<td>I/O multiplexing (IOMM) shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.6</td>
<td>SFR_4</td>
<td>RTI shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.7</td>
<td>SFR_4</td>
<td>System control module shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.8</td>
<td>SFR_4</td>
<td>ESM shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.9</td>
<td>SFR_4</td>
<td>Fuse Farm shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_4.10</td>
<td>SFR_4</td>
<td>OTP configuration shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_5</td>
<td>SF_1</td>
<td>MCU functions necessary to support the safe state shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_5.1</td>
<td>SFR_5</td>
<td>NHET1 shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
<tr>
<td>SFR_5.2</td>
<td>SFR_5</td>
<td>G1O shall be considered safety critical</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>
MCU Diagnostic Tests

Start up diagnostics examples
- SRAM self test
- CPU self test
- ADC self test
- I/O loop back

Real-time diagnostics examples
- SRAM/Flash ECC
- CPU compare
- Clock monitor
- Power monitor
- MPU
What is Latent Diagnostics? Why it is important?

• Memory content OK
• No error detected by ECC
• Read to CPU OK

• Memory single bit error
• Error detected & corrected by ECC
• Read to CPU OK

• Memory single bit error
• Error NOT detected & corrected by ECC
• Read to CPU NOT OK

The bug in the ECC block will only violate the safety goal IN COMBINATION with a memory fault -> a latent fault

Need to test the diagnostic circuits such as ECC, Lock-Step Compare
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
How to implement Diagnostics?

Hercules™ Safety Manual

- 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
### IEC61508 HW Metrics Calculation
Select Safety Features - CPU

<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>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU1</td>
<td>Lockstep compare</td>
<td>1</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU2A</td>
<td>Boot time execution of LBIST STC</td>
<td>1</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU2B</td>
<td>Periodic execution of LBIST STC</td>
<td>0</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU3</td>
<td>MPU</td>
<td>0</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU4</td>
<td>Online profiling using PMU</td>
<td>0</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU5A</td>
<td>Internal watchdog -DWD</td>
<td>0</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU5B</td>
<td>Internal watchdog -DWDD</td>
<td>0</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU5C</td>
<td>External watchdog</td>
<td>1</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU6</td>
<td>Illegal operation and instruction trapping</td>
<td>1</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU7</td>
<td>SW readback of written configuration</td>
<td>1</td>
</tr>
<tr>
<td>Cortex R4F Central Processing Unit (CPU)</td>
<td>CPU8</td>
<td>Lockstep compare (CCM) self-test</td>
<td>1</td>
</tr>
</tbody>
</table>

- Safety Mechanisms associated with CPU are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
Cortex-R: Ideal for safety critical applications

Safety features
- Supports Lockstep
- Memory Protection Unit (MPU)
- Error-Correcting Code (ECC)

Higher performance
- 8-stage processor pipeline
- Dual issue – two instructions can execute in parallel
- Load store unit reduces stalling
- Pre-fetch and Branch Prediction Units
- Cached*

Real-time / Determinism
- Tightly Coupled Memory (TCM)
- Fast interrupt response
- Deterministic interrupt response

*Cortex R5 based products
CPU Self Test Controller (STC/LBIST)

- Provides High Diagnostic Coverage
- Significantly Lowers S/W and Runtime Overhead
- No SW BIST (Built In Self Test) Code overhead in Flash
- Simple to configure and start BIST via register
Memory Protection Unit (MPU)

- A Dedicated Memory Protection Unit (MPU) is implemented for select bus masters

Bus masters include the CPU, DMA, HTU and the FTU

A memory region is defined which allows read and write access for the bus master

Access outside the defined region can be any of the mode

**Read Only:** Read access allowed for the memory accesses outside the region. Write accesses are blocked

**No Access:** Read and write access is blocked.

In the event of a detected memory protection violation an error is indicated

Note: This is a simplified view. The programmer’s model differs between IP. CPU IP will have significantly more options to control access via the MPU.
Digital Windowed Watch Dog (DWWD)

- The DWWD module will reset the MCU or generate a non maskable interrupt to the CPU if the application fails to service the watchdog within the appropriate time window.
  - Safety diagnostic that can detect a runaway CPU
  - Includes a 25-bit down counter
  - Alerts the Error Signaling Module when a CPU interrupt is generated
  - Supports multiple service windows: 100%, 50%, 25%, 12.5%, 3.125%
  - Servicing requires a specific two part key sequence
  - Once enabled can only be disabled by a system or power on reset
IEC61508 HW Metrics Calculation
Select Safety Features - Flash

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Reccomendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA1</td>
<td>Flash Data ECC</td>
<td>++</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA2</td>
<td>Hard error cache and livelock</td>
<td>M</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA3</td>
<td>Flash wrapper address ECC</td>
<td>++</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA4</td>
<td>Address parity</td>
<td>++</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA5A</td>
<td>Boot time hardware CRC check of flash memory contents</td>
<td>++</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA5B</td>
<td>Periodic hardware CRC check of flash memory contents</td>
<td>+</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA6</td>
<td>Bit multiplexing in flash array</td>
<td>M</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA7</td>
<td>Flash sector protection</td>
<td>++</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA8</td>
<td>Periodic SW readback of static configuration registers</td>
<td>+</td>
</tr>
<tr>
<td>Primary Flash and Level 1 (L1) Interconnect</td>
<td>FLA9</td>
<td>SW readback of written configuration</td>
<td>++</td>
</tr>
</tbody>
</table>

- Safety Mechanisms associated with Flash are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
Flash / RAM ECC Protection

ECC evaluated in the Cortex-R CPU
- Single Bit Error Correction and Double Bit Error Detection (SECDED)
- ECC evaluated in parallel to processing data/instructions
- Minimized latency and typically no performance impact
- Protects Busses from CPU to Flash and RAM
- Address / Control parity from CPU -> Memory
- Diagnostic in Flash / SRAM wrappers
### IEC61508 HW Metrics Calculation

**Select Safety Features - SRAM**

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Recommendation</th>
<th>Diagnostic Used in Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM1</td>
<td>Data ECC</td>
<td>++</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM2</td>
<td>Hard error cache and livelock</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM3</td>
<td>Correctable ECC profiling</td>
<td>+</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM4</td>
<td>Address and control parity</td>
<td>++</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM5</td>
<td>Redundant address decode</td>
<td>++</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM6</td>
<td>Data/ECC storage in multiple physical banks</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM7A</td>
<td>Boot time PBIST check of RAM</td>
<td>++</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM7B</td>
<td>Periodic PBIST check of RAM</td>
<td>O</td>
<td>0</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM8</td>
<td>Bit multiplexing in SRAM array</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM9</td>
<td>Periodic hardware CRC check of SRAM contents</td>
<td>O</td>
<td>0</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM10</td>
<td>Periodic SW readback of static configuration registers</td>
<td>+</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM11</td>
<td>SW readback of written configuration</td>
<td>++</td>
<td>1</td>
</tr>
<tr>
<td>SRAM and Level 1 (L1) Interconnect</td>
<td>RAM12</td>
<td>SW driven RAM red.decoder and ECC test</td>
<td>++</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Safety Mechanisms associated with SRAM are selected.**
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
Programmable Memory BIST (PBIST)

- All on-chip RAMs can be tested
- Simple register setup and configuration
- Typically run at startup, but can be executed during the application
- Multiple Memory Test Algorithms
- Detects multiple failure modes

- Provides a mechanism to determine if runtime faults were caused by hard or soft error. This capability can be used to improve availability through inline recovery from soft error.
### IEC61508 HW Metrics Calculation
Select Safety Features - ESM

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Signaling Module (ESM)</td>
<td>ESM1</td>
<td>Periodic SW readback of static configuration registers</td>
<td>+</td>
</tr>
<tr>
<td>Error Signaling Module (ESM)</td>
<td>ESM2A</td>
<td>Boot time SW test of error path reporting</td>
<td>++</td>
</tr>
<tr>
<td>Error Signaling Module (ESM)</td>
<td>ESM2B</td>
<td>Periodic SW test of error path reporting</td>
<td>+</td>
</tr>
<tr>
<td>Error Signaling Module (ESM)</td>
<td>ESM3</td>
<td>Use of status shadow registers</td>
<td>++</td>
</tr>
<tr>
<td>Error Signaling Module (ESM)</td>
<td>ESM4</td>
<td>SW readback of written configuration</td>
<td>++</td>
</tr>
</tbody>
</table>

#### Safety Mechanisms associated with ESM are selected.
- ‘1’ means the safety mechanism is assumed in the HW metrics calculation
- ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
Error Signaling Module (ESM)

- Errors for Group 1
- Errors for Group 2
- Errors for Group 3

INTEN - Low Level Interrupt Handling
INTLVL - High Level Interrupt Handling
ERROR SIGNAL CONTROL
LOW TIME COUNTER PRELOAD
LOW TIME COUNTER

To Interrupt Manager
nERROR pin

Texas Instruments
Clock Monitoring

- **External clock prescaler (ECLK)**
  - Allows external monitoring of CPU clock frequency
  - Configurable pin (GIO or ECLK)

- **Oscillator monitor**
  - Detects failure if oscillator frequency exceeds defined min/max thresholds*
  - Selectable hardware response on oscillator fail
    - Reset device
    - Switch to internal ‘low power oscillator’ (LPO) clock source

- **FMPLL slip detector**
  - Indicates PLL slip if phase lock is lost
  - Selectable hardware response on PLL slip
    - Reset device
    - Switch to internal ‘low power oscillator’ (LPO) clock source
    - Switch to external oscillator clock source

* Refer to device data sheet
Dual Clock Comparator (DCC)

- The DCC module is used to measure the frequency of a clock signal using a second clock signal as a reference.
  - Allows application to ensure that a fixed frequency ratio is maintained between two clock signals
  - Supports the definition of a programmable tolerance window in terms of number of reference clock cycles
  - Supports continuous monitoring without requiring application intervention
  - Alternatively can be used in a single-sequence mode for spot measurements
  - Flexible clock source selection for Counter 0 and Counter 1 resulting in several specific use cases
### IEC61508 HW Metrics Calculation

#### Select Safety Features - CAN

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Recomendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN1A</td>
<td>Boot time SW test of function using I/O loopback</td>
<td>++</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN1B</td>
<td>Periodic SW test of function using I/O loopback</td>
<td>0</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN2</td>
<td>Information redundancy techniques including end to end safing</td>
<td>++</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN3</td>
<td>DCAN SRAM Data Parity</td>
<td>++</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN4A</td>
<td>Boot time PBIST check of DCAN RAM</td>
<td>++</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN4B</td>
<td>Periodic PBIST check of DCAN RAM</td>
<td>O</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN5</td>
<td>Bit multiplexing in DCAN RAM array</td>
<td>M</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN6</td>
<td>Periodic hardware CRC check of DCAN SRAM contents</td>
<td>O</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN7</td>
<td>Periodic SW readback of static configuration registers</td>
<td>+</td>
</tr>
<tr>
<td>Controller Area Network (DCAN)</td>
<td>CAN8</td>
<td>Software readback of written configuration</td>
<td>++</td>
</tr>
</tbody>
</table>

#### Diagnostic Used in Application?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN1A</td>
<td>1</td>
</tr>
<tr>
<td>CAN1B</td>
<td>0</td>
</tr>
<tr>
<td>CAN2</td>
<td>1</td>
</tr>
<tr>
<td>CAN3</td>
<td>1</td>
</tr>
<tr>
<td>CAN4A</td>
<td>1</td>
</tr>
<tr>
<td>CAN4B</td>
<td>0</td>
</tr>
<tr>
<td>CAN5</td>
<td>1</td>
</tr>
<tr>
<td>CAN6</td>
<td>0</td>
</tr>
<tr>
<td>CAN7</td>
<td>1</td>
</tr>
<tr>
<td>CAN8</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Safety Mechanisms associated with CAN are selected.**
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
IEC61508 HW Metrics Calculation
Select Safety Features – Power Supply

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>Feature Recommendation</th>
<th>Diagnostic Used in Application?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>PWR1</td>
<td>Voltage monitor (VMON)</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>Power Supply</td>
<td>PWR2</td>
<td>External voltage supervisor</td>
<td>++</td>
<td>1</td>
</tr>
</tbody>
</table>

- Safety Mechanisms associated with Power Supply are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet
IEC61508 HW Metrics Calculation
Select Safety Features - Package

• High diagnostic coverage is assumed for the package via
detection of failure with existing diagnostics supplemented
by application level diagnostics.
  – Examples:
    • CAN - CAN2 Information Redundancy Technique and CAN1A Boot-time I/O loop
      back SW test
    • MIBSPI - MSP2 Information Redundancy Technique and MSP1A Boot-time I/O
      loop back SW test
IEC61508 HW Metrics Calculation
Select Safety Features – IO Loop Back

• Hercules MCU I/O supports loop back for self-test. Below are examples:

Example images showing loop back configurations for CAN Core and DCAN interfaces.

Examples are extracted from TMS570LS31x/21x Technical Reference Manual SPNU499a
IEC61508 HW Metrics Calculation
Select Safety Features – IO Loop Back

Figure 25-22. I/O Paths during I/O Loopback Modes

- TX SHIFT REG
- LPBK_TYPE
- RXP_ENA
- RX SHIFT REG

---
- Checks the analog loopback path through the receive buffer
- Checks the analog loopback path through the transmit buffer
- Digital loopback path

1. This diagram is intended to illustrate loopback paths and therefore may omit some normal-mode paths.

Examples are extracted from TMS570LS31x/21x Technical Reference Manual SPNU499a
Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™I Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit

- Summary
Estimate SFF / PFH per Safety Function

Now we have a safety function and SIL requirement, → How to estimate the SFF / PFH to determine if SIL requirement can be met?
Estimate MCU SFF / PFH per Safety Function

Use Hercules MCU Detailed Safety Analysis Report & FMEDA worksheet

- Set Up Mission Profile of System
- Apply Diagnostics to Used Modules per Safety Function
- Evaluate IEC61508 Failure Rate Summary

What is the total failure rate per used conditions?

What Self-Test should be implemented?

SFF/PFH met?

N

Y

Done
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.

4.2 Summary of IEC 61508 Safety Metrics at Device Level (BGA Package)

Table 3 provides estimates of FIT rates and calculated safety metrics per IEC 61508-2:2010 using previously noted assumptions for the device in BGA package.

<table>
<thead>
<tr>
<th>Metric</th>
<th>λ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td>λ</td>
</tr>
<tr>
<td>Safety Related FIT</td>
<td>λSR</td>
</tr>
<tr>
<td>Probability of Hardware Failures</td>
<td>PFH</td>
</tr>
<tr>
<td>Safe Failure Fraction</td>
<td>SFF</td>
</tr>
<tr>
<td>Total non safety related faults</td>
<td>λns</td>
</tr>
<tr>
<td>Total safe faults</td>
<td>λs</td>
</tr>
<tr>
<td>Total dangerous faults</td>
<td>λd</td>
</tr>
<tr>
<td>Total dangerous detected faults</td>
<td>λdd</td>
</tr>
<tr>
<td>Total dangerous undetected faults</td>
<td>λdu</td>
</tr>
</tbody>
</table>
IEC61508 HW Metrics Calculation
Failure Rate

Multiple Ways for Random failure rate estimation:
- Siemens Norm SN29500:2010, "Failure Rates of Components"
- Supplier reliability data from similar products already in production and deployed under similar operating conditions

- TI has selected to use IEC/TR 62380 because it is more aligned to semiconductor physics models
- Failure rate is measured in FIT where 1 FIT is 1 fail in $10^9$ operating hours
IEC61508 HW Metrics Calculation
Failure Rate / Mission Profiles

Random Failure

Hardware Failure

Package Permanent

Die (silicon) Permanent

Die (silicon) Transient
### Table 11 – Mission profiles for automotive

<table>
<thead>
<tr>
<th>Mission profile phases</th>
<th>Temp. 1 $(t_{ac})_1$ °C</th>
<th>Temp. 2 $(t_{ac})_2$ °C</th>
<th>Temp. 3 $(t_{ac})_3$ °C</th>
<th>Ratios on/off $\tau_{on}$</th>
<th>Ratios off $\tau_{off}$</th>
<th>2 night starts $n_1$ cycles/year</th>
<th>$\Delta T_1$ °C/cycle</th>
<th>4 day light starts $n_2$ cycles/year</th>
<th>$\Delta T_2$ °C/cycle</th>
<th>Non used vehicle $n_3$ cycles/year</th>
<th>$\Delta T_3$ °C/cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motor control</td>
<td>32 0.02 6</td>
<td>60 0.01 5</td>
<td>85 0.02 3</td>
<td>0.05 8</td>
<td>0.94 2</td>
<td>670</td>
<td>$\frac{\Delta T_1}{3}$ +55</td>
<td>1340</td>
<td>$\frac{\Delta T_2}{3}$ +45</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>Passenger compartment</td>
<td>27 0.00 6</td>
<td>30 0.04 6</td>
<td>85 0.00 6</td>
<td>0.05 8</td>
<td>0.94 2</td>
<td>670</td>
<td>$\frac{\Delta T_1}{3}$ +30</td>
<td>1340</td>
<td>$\frac{\Delta T_2}{3}$ +20</td>
<td>30</td>
<td>10</td>
</tr>
</tbody>
</table>

### Table 9 – Mission profiles for Telecom

<table>
<thead>
<tr>
<th>Environment types</th>
<th>Equipment types</th>
<th>$(t_{ae})_1$ °C</th>
<th>$(t_{ae})_2$ °C</th>
<th>$\tau_1$</th>
<th>$\tau_{on}$</th>
<th>$\tau_{off}$</th>
<th>$n_1$ cycles/year</th>
<th>$\Delta T_1$ °C/cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground; benign: $(G_B)$</td>
<td>switching</td>
<td>20</td>
<td>30</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>365</td>
<td>0</td>
</tr>
<tr>
<td>Ground; benign: $(G_B)$</td>
<td>Transmitting</td>
<td>20</td>
<td>40</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>365</td>
<td>0</td>
</tr>
<tr>
<td>Ground; fixed: $(G_F)$</td>
<td>Transmitting and access</td>
<td>11</td>
<td>31</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>365</td>
<td>8</td>
</tr>
</tbody>
</table>
**IEC61508 HW Metrics Calculation**

**Automotive Motor Control Mission Profiles**

- **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

**Customer input for failure rate estimation**

<table>
<thead>
<tr>
<th>Package Used</th>
<th>TI PBGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer input for transient fault estimation</td>
<td>Application specific Flux Factor coeff. based on Jedec JESD89A</td>
</tr>
<tr>
<td>Max. power dissipation</td>
<td>Application specific power dissipation in Watts (1.04W is based on maximum datasheet value)</td>
</tr>
<tr>
<td>Assumed lifetime</td>
<td>in years</td>
</tr>
<tr>
<td>Confidence level</td>
<td>Desired confidence level of FIT rates</td>
</tr>
</tbody>
</table>

**Automotive Mission Profile:**

Total raw die permanent FIT: 9.48

Based on RM48x v1.0 FMEDA worksheet

**Operational Profile from IEC/TR 62380:2004**

<table>
<thead>
<tr>
<th>Temp1</th>
<th>Temp2</th>
<th>Temp3</th>
<th>Ratios on/off</th>
<th>2 night starts</th>
<th>4 day light starts</th>
<th>Non used vehicle</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Tac)1 °C</td>
<td>τ1</td>
<td>(Tac)2 °C</td>
<td>τ2</td>
<td>(Tac)3 °C</td>
<td>τ3</td>
<td>Fan</td>
</tr>
<tr>
<td>Profile</td>
<td>32</td>
<td>0.02</td>
<td>60</td>
<td>0.015</td>
<td>85</td>
<td>0.023</td>
</tr>
</tbody>
</table>
IEC61508 HW Metrics Calculation

Elevator Mission Profiles

• Assumed Elevator/Escalator mission profile:
  – 10 years service, 365 days per year, 18 hours on and 6 hours off per day
  – $T_{ae}$ outside ambient temp = 25c (indoor ambient temp)
  – $T_{ac}$ PCB temp = 60c
  – $T_{on} = 0.75$, $T_{off} = 0.25$
  – $N = 1 \times 365$ cycles
  – $\Delta T_j$ (chip junction temp increased vs $T_{ac}$) = 30c (assumed worst case)
  – $\Delta T = \Delta T_j / 3 + (60-25)c = 55c$

  **Customer input for failure rate estimation**

  **Package Used**
  - TI PBGA

  **Customer input for transient fault estimation**
  - Application specific Flux Factor coeff. based on Jedec JESD89A
  - 1

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

  **Assumed Lifetime**
  - in years
  - 10

  **Confidence Level**
  - Desired confidence level of FIT rates
  - 70%

  Based on RM48x v1.0 FMEDA worksheet

  **Elevator Mission Profile:**
  - Total raw permanent FIT: 103.37

  **Operational Profile from IEC/TR 62380:2004**

<table>
<thead>
<tr>
<th></th>
<th>Temp1</th>
<th>Temp2</th>
<th>Temp3</th>
<th>Ratios on/off</th>
<th>Daily on/off</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_{(bc)}$</td>
<td>32°C</td>
<td>0</td>
<td>60°C</td>
<td>0.75</td>
<td>0.75</td>
</tr>
<tr>
<td>$\tau$</td>
<td>0</td>
<td>0.75</td>
<td>85°C</td>
<td>0</td>
<td>0.25</td>
</tr>
<tr>
<td>$\Delta T_1$</td>
<td>0°C</td>
<td></td>
<td></td>
<td>365</td>
<td></td>
</tr>
</tbody>
</table>

*Texas Instruments*
IEC61508 HW Metrics Calculation

Industrial Mission Profiles

• Assumed Industrial mission profile:
  – 10 years service, 365 days per year, 24 hours per day
  – $T_{ae}$ outside ambient temp = 70°C (ambient temp)
  – $T_{ac}$ PCB temp = 90.5°C (assumption)
  – $T_{on} = 1$, $T_{off} = 0$
  – $n = 1$ cycles
  – $\Delta T_j$ (chip junction temp increased vs $T_{ac}$) = 30°C (assumed worst case)
  – $\Delta T = \Delta T_j/3 + (90.5-70)\degree C = 30.5\degree C$

Customer input for failure rate estimation

<table>
<thead>
<tr>
<th>Package Used</th>
<th>TI PBGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer input for transient fault estimation</td>
<td></td>
</tr>
<tr>
<td>Application specific Flux Factor coeff. based on Jedec JESD89A</td>
<td>1</td>
</tr>
<tr>
<td>Maximum power dissipation</td>
<td></td>
</tr>
<tr>
<td>Application specific power dissipation in Watts</td>
<td>1.04</td>
</tr>
<tr>
<td>(1.04W is based on maximum datasheet value)</td>
<td></td>
</tr>
<tr>
<td>Assumed Lifetime in years</td>
<td>10</td>
</tr>
<tr>
<td>Confidence Level Desired confidence level of FIT rates</td>
<td>70%</td>
</tr>
</tbody>
</table>

Industrial Mission Profile:
Total raw permanent FIT: 330.16

Based on RM48x v1.0 FMEDA worksheet

Operational Profile from IEC/TR 62380:2004 Echo use conditions

<table>
<thead>
<tr>
<th></th>
<th>Temp1</th>
<th>Temp2</th>
<th>Temp3</th>
<th>Ratios on/off</th>
<th>Number of On/off per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>92.5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$\tau_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$\tau_2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\tau_3$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$T_{on}$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$T_{off}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$n$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$\Delta T$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Failure Rate Definitions

- Failure rate is represented with the Greek character lambda, \( \lambda \), and can be broken into many categories.
  - \( \lambda_S \): rate of safe failures which do not affect safety function
    - \( \lambda_{SD} \): safe, detected failure rate
    - \( \lambda_{SU} \): safe, undetected failure rate
  - \( \lambda_D \): rate of dangerous failures which compromise the safety function
    - \( \lambda_{DD} \): dangerous, detected failure rate
    - \( \lambda_{DU} \): dangerous, undetected failure rate

- Note: a failure which results in the system changing mode of operation to a safe state is by definition a safe failure.

- Failure rate is often expressed in FITs. One FIT (Failure In Time) = 1 failure per billion hours of operation (1 x 10^{-9} failures/hour)
### IEC61508 HW Metrics vs Mission Profiles

**IEC61508 HW metrics with Automotive Mission Profile (70% confidence level):**

Numbers are normalized to Die Permanent Total RAW FIT

<table>
<thead>
<tr>
<th></th>
<th>Die Permanent</th>
<th>Transient</th>
<th>Package Permanent</th>
<th>Overall Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td>10.00</td>
<td>764.40</td>
<td>69.89</td>
<td>844.30</td>
</tr>
<tr>
<td>Safety related FIT</td>
<td>9.97</td>
<td>734.58</td>
<td>68.95</td>
<td>813.49</td>
</tr>
<tr>
<td>Probability of Hardware Failures - PFH (in FIT)</td>
<td>0.06</td>
<td>0.82</td>
<td>0.13</td>
<td>1.01</td>
</tr>
<tr>
<td>Safe Failure Fraction - SFF</td>
<td>99.36%</td>
<td>99.89%</td>
<td>99.82%</td>
<td>99.88%</td>
</tr>
</tbody>
</table>

**IEC61508 HW metrics with Elevator Mission Profile (70% confidence level):**

Numbers are normalized to Automotive Mission Profile Die Permanent Total RAW FIT

<table>
<thead>
<tr>
<th></th>
<th>Die Permanent</th>
<th>Transient</th>
<th>Package Permanent</th>
<th>Overall Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td>108.99</td>
<td>764.44</td>
<td>13.12</td>
<td>886.55</td>
</tr>
<tr>
<td>Safety related FIT</td>
<td>108.67</td>
<td>734.61</td>
<td>12.95</td>
<td>856.24</td>
</tr>
<tr>
<td>Probability of Hardware Failures - PFH (in FIT)</td>
<td>0.69</td>
<td>0.82</td>
<td>0.06</td>
<td>1.57</td>
</tr>
<tr>
<td>Safe Failure Fraction - SFF</td>
<td>99.36%</td>
<td>99.89%</td>
<td>99.54%</td>
<td>99.82%</td>
</tr>
</tbody>
</table>

**IEC61508 HW metrics with Industrial Mission Profile (70% confidence level):**

Numbers are normalized to Automotive Mission Profile Die Permanent Total RAW FIT

<table>
<thead>
<tr>
<th></th>
<th>Die Permanent</th>
<th>Transient</th>
<th>Package Permanent</th>
<th>Overall Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td>348.11</td>
<td>764.53</td>
<td>2.69</td>
<td>1115.33</td>
</tr>
<tr>
<td>Safety related FIT</td>
<td>347.09</td>
<td>734.71</td>
<td>2.69</td>
<td>1084.48</td>
</tr>
<tr>
<td>Probability of Hardware Failures - PFH (in FIT)</td>
<td>2.20</td>
<td>0.84</td>
<td>0.12</td>
<td>3.16</td>
</tr>
<tr>
<td>Safe Failure Fraction - SFF</td>
<td>99.36%</td>
<td>99.89%</td>
<td>95.45%</td>
<td>99.71%</td>
</tr>
</tbody>
</table>

- Higher raw permanent FIT rate because of much longer ‘on’ time
- No significant difference of Safe Failure Fraction (SFF)
- Probability of Hardware Failure (PFH) increases in proportion to raw rate rate increase.

Based on RM48x v1.0 FMEDA worksheet
# IEC61508 HW Metrics Calculation

## Impact of Confidence Level

### Confidence level 70%

<table>
<thead>
<tr>
<th></th>
<th>Permanent FIT</th>
<th>Transient FIT</th>
<th>Package FIT</th>
<th>Overall FIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent FIT</td>
<td>6.20E-10</td>
<td>6.80E-10</td>
<td>6.00E-11</td>
<td>1.36E-09</td>
</tr>
<tr>
<td>Elevator mission profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Number of units in field**: 1000000
- **Number of device hours per day**: 18

<table>
<thead>
<tr>
<th>Device operating year</th>
<th>1</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of device operating year</td>
<td>1.00E+06</td>
<td>5.00E+06</td>
<td>1.00E+07</td>
<td>1.50E+07</td>
<td>2.00E+07</td>
</tr>
<tr>
<td>Total number of device operating hours</td>
<td>6.57E+09</td>
<td>3.29E+10</td>
<td>6.57E+10</td>
<td>9.86E+10</td>
<td>1.31E+11</td>
</tr>
<tr>
<td>Estimated number of failures due to Permanent fault</td>
<td>4.1</td>
<td>20.4</td>
<td>40.7</td>
<td>61.1</td>
<td>81.5</td>
</tr>
<tr>
<td>Estimated number of failures due to Transient fault</td>
<td>4.5</td>
<td>22.3</td>
<td>44.7</td>
<td>67.0</td>
<td>89.4</td>
</tr>
<tr>
<td>Estimated number of failures due to Package fault</td>
<td>0.4</td>
<td>2.0</td>
<td>3.9</td>
<td>5.9</td>
<td>7.9</td>
</tr>
<tr>
<td>Estimated number of failures due to Overall fault</td>
<td>8.9</td>
<td>44.7</td>
<td>89.4</td>
<td>134.0</td>
<td>178.7</td>
</tr>
</tbody>
</table>

### Confidence level 99%

<table>
<thead>
<tr>
<th></th>
<th>Permanent FIT</th>
<th>Transient FIT</th>
<th>Package FIT</th>
<th>Overall FIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent FIT</td>
<td>2.39E-09</td>
<td>2.61E-09</td>
<td>2.20E-10</td>
<td>5.22E-09</td>
</tr>
<tr>
<td>Elevator mission profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Number of units in field**: 1000000
- **Number of device hours per day**: 18

<table>
<thead>
<tr>
<th>Device operating year</th>
<th>1</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of device operating year</td>
<td>1.00E+06</td>
<td>5.00E+06</td>
<td>1.00E+07</td>
<td>1.50E+07</td>
<td>2.00E+07</td>
</tr>
<tr>
<td>Total number of device operating hours</td>
<td>6.57E+09</td>
<td>3.29E+10</td>
<td>6.57E+10</td>
<td>9.86E+10</td>
<td>1.31E+11</td>
</tr>
<tr>
<td>Estimated number of failures due to Permanent fault</td>
<td>15.7</td>
<td>78.5</td>
<td>157.0</td>
<td>235.5</td>
<td>314.0</td>
</tr>
<tr>
<td>Estimated number of failures due to Transient fault</td>
<td>17.1</td>
<td>85.7</td>
<td>171.5</td>
<td>257.2</td>
<td>343.0</td>
</tr>
<tr>
<td>Estimated number of failures due to Package fault</td>
<td>1.4</td>
<td>7.2</td>
<td>14.5</td>
<td>21.7</td>
<td>28.9</td>
</tr>
<tr>
<td>Estimated number of failures due to Overall fault</td>
<td>34.3</td>
<td>171.5</td>
<td>343.0</td>
<td>514.4</td>
<td>685.9</td>
</tr>
</tbody>
</table>

### Pessimistic estimation

Field data are orders of magnitude better

Based on RM48x v1.0 FMEDA worksheet
FMEDA worksheet – Product Function Tailoring

Inputs for application specific tailoring of failure rates

<table>
<thead>
<tr>
<th>Memory size</th>
<th>Total Size</th>
<th>User Size</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRAM</td>
<td>256</td>
<td>256</td>
<td>Kbytes</td>
</tr>
<tr>
<td>FLASH</td>
<td>3</td>
<td>3</td>
<td>Mbytes</td>
</tr>
<tr>
<td>FLASH-FEE</td>
<td>64</td>
<td>64</td>
<td>Kbytes</td>
</tr>
</tbody>
</table>

### Modules used for Safety Function / Safety Goal

- **CPU SubSystem**
  - Cortex R4F Central Processing Unit (CPU)
  - Vectorized Interrupt Module (VIM)
  - CPU SubSystem
  - LBIST
  - Joint Technical Action Group (JTAG) Debug/Trace/Callibration Access
  - Cortex R4F Central Processing Unit (CPU) debug and trace
  - Data Modification Module
  - Parameter Overlay Module
  - RAM Trace Port

- **RAM System**
  - SRAM and Level 1 (L1) Interconnect

- **Flash System**
  - One Time Programmable (OTP) Flash Static
  - Primary Flash and Level 1 (L1) Interconnect
  - Flash emulated EEPROM (FEE)
  - Level 2/Level 3 (L2/L3) Interconnect

- **SYSTEM**
  - Error Signaling Module (ESM)
  - Power Management Module (PMM)
  - Reset
  - System Control
  - Clock
  - EFuse Static Configuration
  - Direct Memory Access (DMA)
  - Input/Output (I/O) Multiplexing (IGMM)

- **Peripheral**
  - FlexRay Including FlexRay Transfer Unit (FTU)
  - Controller Area Network (DCAN1)
  - Controller Area Network (DCAN2)
  - Controller Area Network (DCAN3)
  - General Purpose Input/Output (GPIO)
  - Local Interconnect Network (LIN)
  - Serial Communications
  - Multi-Buffered Analog to Digital Converter (MibADC1)
  - Multi-Buffered Analog to Digital Converter (MibADC2)
  - Multi-Buffered Serial Peripheral Interface (MibSPI1)
  - Multi-Buffered Serial Peripheral Interface (MibSPI2)
  - Multi-Buffered Serial Peripheral Interface (MibSPI3)
  - Next Generation High End Time (N2HET1) Including HET Transfer Unit (HTU1)
  - Next Generation High End Time (N2HET2) Including HET Transfer Unit (HTU2)
  - Serial Peripheral Interface (SPI2)
  - Serial Peripheral Interface (SPI4)
  - Real Time Interrupt (RTI) Operating System Timer
  - Ethernet
  - External Memory Interface (EMIF)
  - Universal Serial Bus (USB)
  - Inter-Integrated Circuit (I2C)
  - Power Supply

- **Package**

- **Allow customization of failure rate estimation**
- **Include only MCU modules used by application**
- **Include actual Flash and SRAM memory size used**
Safety mechanisms considered in the FMEDA worksheet – Safety Mechanisms Tailoring

- Allow customization of diagnostics selection.
- For example, CPU lock-step compare and boot time LBIST are used, while periodic LBIST is not used.
**FMEDA worksheet – Package/Pin Tailoring**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Number of pins (PBGA)</th>
<th>Number of pins (QFP)</th>
<th>Safety related 1=YES, 0=NO</th>
<th>Related Part</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADREFHI</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>ADREFLO</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>VCCAD</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>VSSAD</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>AD1EVT</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>AD2EVT</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>AD1IN</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>AD1IN/AD2IN</td>
<td>16</td>
<td>16</td>
<td>1</td>
<td>Multi-Buffered Analog to Digital Converter</td>
</tr>
<tr>
<td>NHET1</td>
<td>31</td>
<td>31</td>
<td>1</td>
<td>Enhanced High-End Timer Modules (NHET)</td>
</tr>
<tr>
<td>NHET2</td>
<td>18</td>
<td>9</td>
<td>1</td>
<td>Enhanced High-End Timer Modules (NHET)</td>
</tr>
</tbody>
</table>

**Allow customer to adjust the number of pins used by module in its application**

- Example: 31 NHET1 pins are available, if only 20 pins are used, change to 20

**Allow customer to input pin-level application diagnostic with its own diagnostic coverage number**
### Summary of IEC 61508 Metrics Examples – Permanent/Transient & Die/Package:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Die</th>
<th>Package</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total FIT (Raw FIT)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permanent</td>
<td>10.00</td>
<td>69.89</td>
<td>844.30</td>
</tr>
<tr>
<td>Transient</td>
<td>764.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety related FIT</td>
<td>9.97</td>
<td>68.95</td>
<td>813.49</td>
</tr>
<tr>
<td>Probability of Hardware Failures - PFH (in FIT)</td>
<td>0.06</td>
<td>0.13</td>
<td>1.01</td>
</tr>
<tr>
<td>Safe Failure Fraction - SFF</td>
<td>99.36%</td>
<td>99.82%</td>
<td>99.88%</td>
</tr>
</tbody>
</table>

Numbers are normalized to Die Permanent Total RAW FIT

IEC 61508 categorization

<table>
<thead>
<tr>
<th>Metric</th>
<th>Die</th>
<th>Package</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total faults</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permanent</td>
<td>10.00</td>
<td>69.89</td>
<td>844.30</td>
</tr>
<tr>
<td>Transient</td>
<td>764.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety related faults</td>
<td>9.97</td>
<td>68.95</td>
<td>813.49</td>
</tr>
<tr>
<td>Total non safety related faults</td>
<td>0.03</td>
<td>0.94</td>
<td>30.80</td>
</tr>
<tr>
<td>Total Safe faults</td>
<td>5.24</td>
<td>34.47</td>
<td>412.50</td>
</tr>
<tr>
<td>Total dangerous faults</td>
<td>4.73</td>
<td>34.47</td>
<td>401.00</td>
</tr>
<tr>
<td>Total dangerous Detected faults</td>
<td>4.67</td>
<td>34.35</td>
<td>399.99</td>
</tr>
<tr>
<td>Total dangerous Undetected faults</td>
<td>0.06</td>
<td>0.13</td>
<td>1.01</td>
</tr>
</tbody>
</table>

Details of IEC 61508 Metrics:

- For Permanent and Transient faults
- By modules (CPU, Flash, SRAM, DCAN, ADC…)

Based on RM48x v1.0 FMEDA worksheet
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
Hercules™ SafeTI™ Diagnostic library

- SafeTI™ Diagnostic Library = **Executable version of Safety Manual**.

- **Highlights**
  - Optimized API mapping to the MCU’s Safety features as documented in the device Safety Manual.
  - Software abstraction for MCU’s Safety features to an application developer.
  - Uniform API across various members of the Hercules family.
  - Developed compliant to an ISO26262 and IEC61508 development process.
Hercules™ SafeTI™ Diagnostic Library features

- **Initialization** functions for the device
  - Common functionality (Core registers, stack)
  - Safety measures (RAM init, enable ECC, ESM init)

- API to *invoke PBIST* on memories.

- API to *invoke LBIST* self tests.

- **Boot time/Run time verification** of integrated HW safety diagnostics to prevent latent faults.

- Create artificial faults (**Fault injection**) to allow testing of application fault handling.

- Provide an **Error Signaling Module (ESM) handler** which can capture and report faults to the application through a **callback** routine.

- **Profiling** for measuring time spent in diagnostic tests/fault handling, for enabling optimization of Run time safety measures by application developer.

- **Comprehensive documentation** which explains mapping from Safety manual to SafeTI™ Diagnostic Library API.

- Released in a **SafeTI™ Software Compliance Support Package (SCSP)** which aids in ISO26262 or IEC61508 certification of customer product.

- Current implementation is limited to “safe island” set of peripherals.
# Safety Manual to API mapping

## SafeTI™ Diagnostic Library 1.0.0

**SafeTI™ Diagnostic Library for the Hercules processors**

### Device Partition

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique Identifier</th>
<th>Safety Feature or Diagnostic</th>
<th>API Name</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Supply</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PWR1</td>
<td>Voltage monitor (VMON)</td>
<td></td>
<td>Not applicable</td>
<td>No software control, always enabled in hardware</td>
</tr>
<tr>
<td>PWR2</td>
<td>External voltage supervisor</td>
<td></td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td><strong>Power Management Module (PMM)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PMM1</td>
<td>Lockstep PSCON</td>
<td></td>
<td>$SL_{SelfTest_PSCON}$</td>
<td></td>
</tr>
<tr>
<td>PMM2</td>
<td>Privileged mode access and multi-bit keys for control registers</td>
<td></td>
<td>$SL_{SelfTest_PSCON}$</td>
<td></td>
</tr>
<tr>
<td>PMM3</td>
<td>Periodic software readback of static configuration registers</td>
<td></td>
<td>$SL_{ReadCompare}$</td>
<td></td>
</tr>
<tr>
<td>PMM4</td>
<td>Software readback of written configuration</td>
<td></td>
<td>$SL_{ReadCompare}$</td>
<td></td>
</tr>
<tr>
<td><strong>Clock</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLK1</td>
<td>LPOCLKDET</td>
<td></td>
<td>Not applicable</td>
<td>External source for fault</td>
</tr>
<tr>
<td>CLK2</td>
<td>PLL slip detector</td>
<td></td>
<td>$ESM_{Application_Callback}$</td>
<td></td>
</tr>
<tr>
<td>CLK3</td>
<td>Dual Clock Comparator (DCC)</td>
<td></td>
<td>$ESM_{Application_Callback}$</td>
<td></td>
</tr>
<tr>
<td>CLK4</td>
<td>External monitoring via ECLK</td>
<td></td>
<td>Not applicable</td>
<td>External monitoring</td>
</tr>
<tr>
<td>CLK5A</td>
<td>Internal watchdog - DWD</td>
<td></td>
<td>Not applicable</td>
<td>External source for fault</td>
</tr>
<tr>
<td>CLK5B</td>
<td>Internal watchdog - DWWD</td>
<td></td>
<td>Not applicable</td>
<td>External source for fault</td>
</tr>
<tr>
<td>CLK5C</td>
<td>External watchdog</td>
<td></td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>CLK6</td>
<td>Periodic software readback of static clock configuration registers</td>
<td></td>
<td>$SL_{ReadCompare}$</td>
<td></td>
</tr>
<tr>
<td>CLK7</td>
<td>Software readback of written configuration</td>
<td></td>
<td>$SL_{ReadCompare}$</td>
<td></td>
</tr>
<tr>
<td><strong>Reset</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RST1</td>
<td>External monitoring of warm reset</td>
<td></td>
<td>Not applicable</td>
<td>External monitoring</td>
</tr>
<tr>
<td>RST2</td>
<td>Software check of last reset</td>
<td></td>
<td>$SL_{Init_ResetReason}$</td>
<td></td>
</tr>
<tr>
<td>RST3</td>
<td>Software warm reset generation</td>
<td></td>
<td>$SL_{SW_Reset}$</td>
<td></td>
</tr>
<tr>
<td>RST4</td>
<td>Glitch filtering on reset pins</td>
<td></td>
<td>Not applicable</td>
<td>No software control, always enabled in hardware</td>
</tr>
<tr>
<td>RST5</td>
<td>Use of status shadow registers</td>
<td></td>
<td>$SL_{Init_ResetReason_XInfo}$</td>
<td></td>
</tr>
</tbody>
</table>
Hercules MCU safety features and SafeTI™ Diagnostic Library

- API for running LBIST on the CPU by the STC.
- API also supports selfcheck feature of STC, which tests the signature compare logic.
- Logical / physical design optimized to reduce probability of common cause failure.

- API to perform test on the ECC diagnostic feature.
- API to run the diagnostic modes on Flash memories.
- API to perform CRC calculation on memory ranges.
- API to run PBIST algorithms on all memories.
- Includes ESM handler and provides an example application with an abort handler.
- Allows application to register a callback for the fault handling.
- On-Chip Clock and Voltage Monitoring
  - API for testing the safety diagnostics on PSCON.
  - API for testing the safety diagnostics on EFUSE.

- IO Loop Back, ADC Self Test, ...
- Dual ADC Cores with shared channels

**Hardware Diagnostics**
- Safe Island Hardware diagnostics (RED)
- Blended HW diagnostics (BLUE)
- Non Safety Critical Functions (BLACK)

**Memory**
- Flash w/ ECC
- RAM w/ ECC
- Flash EEPROM w/ ECC

**Power, Clock, & Safety**
- OSC PLL
- PBIST/LBIST
- POR
- ESM
- CRC
- RTI/DWWD

**Memory Interface**
- Calibration
- JTAG Debug
- Embedded Trace
- External Memory

**DMA**

**Enhanced System Bus and Vectored Interrupt Module**

**Serial Interfaces**

**Network Interfaces**

**Dual ADC Cores**

**Multiple Timers**

**GIO**
User examples

- SafeTI™ Diagnostic Library is integrated into the Hitex Safety Kit.
Hitex Kit

Example User Application
- SAFERTOS
- TI Safety Library
- HW Abstraction Layer

SafeTI-HSK Board

Hercules™ MCU
- Safety MCU

Power Supply
- Vcc, SPI, Reset
- Fault Injection and Monitoring

Hercules™ MCU
- Control MCU
- SPI (Fault Injection and Monitoring)

Host Control GUI

Host/Board Communication
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
Hercules™ and SafeTI™ Software and Tool Packages

Hercules Software and Tools

Hercules standard software and tools packages
- Assists in software development on Hercules Safety MCUs
- Provides the actual software/tool with source code, GUI, …
- User guides, datasheets, release notes, …
- Regular updates for enhancements, fixes, …

Free / click wrap license agreement

SafeTI Compliance Support Package

SafeTI software documentation and testing
- Assists customer to comply to functional safety standards
- Safety Requirements Document, Code Review and Coverage Reports, Unit Test Results, Software Safety Manual, ….
- Unit Test capability using LDRAunit (if applicable)

See Pricing / signed license agreement

SafeTI Tool Qualification Kit

SafeTI tool documentation and qualification
- Assists customer to qualify tool to functional safety standards
- TI Test Automation Unit or LDRAunit (if applicable)

See pricing / signed license agreement
# Hercules Software and Tool Packages

<table>
<thead>
<tr>
<th>Standard Package</th>
<th>Compliance Support Package</th>
<th>Tool Qualification Kit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code in source form (see note)</td>
<td>Software Safety Requirements Document</td>
<td>Tool Safety Requirements Document</td>
</tr>
<tr>
<td>GUI for user configuration (if applicable)</td>
<td>Software Safety Architecture Document</td>
<td>Tool Safety Architecture Document</td>
</tr>
<tr>
<td>Data sheet</td>
<td>Quality Review Report</td>
<td>Quality Review Report</td>
</tr>
<tr>
<td></td>
<td>Unit Test Regression Report</td>
<td>Unit Test Regression Report</td>
</tr>
<tr>
<td></td>
<td>Traceability report</td>
<td>Traceability report</td>
</tr>
<tr>
<td></td>
<td>Test Results Report</td>
<td>Test Results Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compliance Level Tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Templates for Compliance Documentation</td>
</tr>
<tr>
<td></td>
<td><strong>Executable Test Cases</strong>*</td>
<td><strong>Executable Test Cases</strong>*</td>
</tr>
<tr>
<td>Click Wrap License</td>
<td>Signed License Agreement</td>
<td>Signed License Agreement</td>
</tr>
<tr>
<td>Free</td>
<td>See Pricing Table</td>
<td>See Pricing Table</td>
</tr>
</tbody>
</table>

* - these are provided for software that is configurable by user (ie; HALCoGen and CCS Compiler)
SafeTI™ Compliance Support Packages

Following artifacts are provided as part of a SafeTI™ Compliance Support Package:

1. **Software/Tool Safety Requirements document**
   - Defines both functional and safety requirements of the software/tool

2. **Software/Tool Safety Architecture Document**
   - Defines the architecture of the software/tool including safety provisions

3. **Code Review Report**
   - Provides the MISRA-C:2004 violations for the file

4. **Quality Review Report**
   - Provides the HIS Quality metrics for the file.

5. **Dynamic Coverage Analysis Report**
   - Provides the Statement, Branch, and MC/DC Coverage information

6. **Unit Test Regression Report**
   - Shows the unit tests performed and the result of each unit test.

7. **Test Manager report**
   - Summary of the Code Review, Quality Review and Unit Test Reports.
8. Test Results Report
   - unit tests
   - safety functional tests
   - performance tests/resource usage tests
   - interface tests
   - fault injection tests

9. Traceability report
   - requirements to design
   - requirements to source code
   - requirements to test case
   - backwards traceability

10. Software Safety Manual
    - describes how to integrate safely into end user application software

11. ISO 26262 / IEC 61508 assessment report
    - shows review of entire development process (internal assessment)

12. Executable test cases (HALCoGen only)
    - setup for user defined configuration

13. Test Automation Unit (HALCoGen only)
    - for executing unit tests with user defined configuration
## Software Compliance Support Package Deliverables

<table>
<thead>
<tr>
<th>ISO 26262 and IEC61508 Standards</th>
<th>TI Work Products</th>
<th>TI SW Product Lifecycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262 Clause</td>
<td>IEC 61508 Clause</td>
<td>ISO 26262 Work products</td>
</tr>
<tr>
<td>6 Specification of software safety requirements</td>
<td>7.2.2 Software safety requirements specification</td>
<td>6.5.1 Software safety requirements specification</td>
</tr>
<tr>
<td>Bi-Directional Traceability</td>
<td>Forward and Backward Traceability at all stages</td>
<td>Verification Reports</td>
</tr>
<tr>
<td>7 Software architectural design</td>
<td>7.4.3 Requirements for SW Architecture Design development</td>
<td>7.5.1 Software architectural design specification</td>
</tr>
<tr>
<td>9 Software unit testing</td>
<td>7.4.5 Detailed design and development (individual software module design);</td>
<td>9.5.3 Software verification report (refined)</td>
</tr>
<tr>
<td>10 Software integration and testing</td>
<td>7.4.8 Software integration testing;</td>
<td>10.5.3 Embedded software verified and tested integrated programmable electronics</td>
</tr>
<tr>
<td>11 Verification of software safety requirements</td>
<td>7.7.2 Software aspects of system safety validation</td>
<td>11.5.3 Software verification results; validated software</td>
</tr>
</tbody>
</table>

---

**Texas Instruments**

90
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package
• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit
• Summary
The SafeTI™ - HSK Hardware

HSK hardware platform:

• **Safety application unit** on which the Demo application is run. This includes The Safety MCU or Safety Device Under Test (SDUT) -- TMS570 or RM48, Power supply/WD companion chip (TPS65381), Accelerometer, Temperature Sensor, HMI (4XLED, potentiometer, Pixel display..), CAN (transceiver & connector) and motor control interface (DIMM connector)

• **Control and Monitoring unit** (CMU): This includes the control and monitor device (RM48x) to inject faults and monitor fault reaction, Fault injection logic, Error indication and power supply to the control monitor unit

• **Host/Debug interface**: This includes a USB HUB controller (to manage USB communication between the Host workstation and onboard MCU’s) and Serial communication port converters (FTDI ) from the USB HUB to the Safety DUT (JTAG) and CMU device (JTAG and UART(for the GUI))

• The board utilizes an industry standard **DIMM** form factor. Uses the standard 100-pin connector foot print to plug into selected TI’s motor control kits

• Standard 20 pin external JTAG header to facilitate expandability Non-CCS IDE’s like IAR and Keil
The SafeTI™- HSK GUI

- Communicates permanently with the kit to request status information
- Monitors different voltages of power supply ranges
- Possibility to inject faults (disturb power supply or simulate errors in the application)
  The system reaction is monitored with timestamps (fault injection, fault indication, enter safe-state)
- Measure runtime execution of safety tests. This gives the user a clear picture how to configure or calibrate his application
- Ability to configure settings for Error Signalling Module and TPS6538x
- Application information is visualized e.g. acceleration, temperature and some task state information
The SafeTI™- HSK GUI Overview

• GUI overview
The SafeTI™- HSK GUI Validation and Calibration
The SafeTI™- HSK CPU Lock-Step Compare Fault Injection

- CCM-R4F compares the outputs of two CPUs running in a 1oo1D lockstep configuration
- The ESM error flag “CCM-R4F - compare” is asserted whenever the CPU compare error is detected.
- For diagnostic purposes, the CCM-R4F also incorporates a self-test capability and error forcing capability.
- FMEDA requires gate-level fault injection (simulation) work to prove effectiveness of on chip diagnostics
The SafeTI™- HSK SRAM DATA ECC Fault Injection

- ECC controllers are located inside the CPU
  - Interconnect between CPU and the memory is covered by the diagnostic
  - ECC logic itself is checked on a cycle by cycle basis
  - Single Error Correction Double Error Detection (SECDED) logic

- 8 bits of ECC for every 64 bits of data access from the CPU
The SafeTI™- HSK GUI settings/application
Agenda

• Overview of Hercules™ MCU and SafeTI™ Design package

• Hercules™ MCU Functional Safety How-To Workshop
  – Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  – Safety Critical Elements identification and Diagnostic Requirements
  – Safety Manual and Diagnostics Selection
  – Mission Profile and Failure Rate Estimation
  – SafeTI™ Diagnostic Library
  – SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  – Fault Injection with HITEX kit

• Summary
Hercules MCUs: Accelerating Safety Products to Market

**Hercules Safety MCU**

- **Certified Safety Hardware Architecture**
  - Pre-approved for ISO 26262, IEC 61508
  - Proven in use
  - Device FMEDA, FIT reports

- **Only Lockstep ARM supplier**
  - Non-proprietary
  - Market accepted
  - Respected heritage

- **Production Quality Safety Software**
  - Pin & SW Compatible
  - Safety Chipset
  - SafeTI Program

- **Comprehensive Portfolio Complementary Analog**

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

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

- **Complementary Analog**

- **Usable by customer**
  - Certification Ready
  - ISO 26262, IEC 61508 compliant

**• Software**
**• Development Tools**
**• Consulting & Training**

**• Ease development**
**• Aid certification**

**• Usable by customer**
**• Certification Ready**
**• ISO 26262, IEC 61508 compliant**

**• Pre-approved for ISO 26262, IEC 61508**
**• Proven in use**
**• Device FMEDA, FIT reports**

**• Non-proprietary**
**• Market accepted**
**• Respected heritage**

**• Pin & SW Compatible**
**• Safety Chipset**
**• SafeTI Program**

**• Software**
**• Development Tools**
**• Consulting & Training**

**• Ease development**
**• Aid certification**

**• Usable by customer**
**• Certification Ready**
**• ISO 26262, IEC 61508 compliant**
Hercules™ Training  www.ti.com/herculestraining

1 Day Training Class: Hercules 1 Day Safety Seminar

- Introduction
- What is Functional Safety?
- Safety Standards Overview
- IEC 61508 Safety Standard
- ISO 26262 Safety Standard
- Random Fault Management
- Safety System Architectures
- Hercules Safety Concept

- Lab 1: Hercules MCU Demos
- Hercules Architecture
- Development Tools: HW kits, SW tools
- Embedded Flash Memory tools
- Real Time Interrupt (RTI)
- Vectored Interrupt Manager (VIM)
- Direct Memory Access (DMA)
- General-purpose I/O (GIO) & NHET

- Lab 2: Using NHET as GIO
- Communication Interfaces: UART, LIN, CAN, FlexRay, Multi-Buffered Serial Peripheral Interface (MibSPI)
- Lab 3: PC to SCI Communication
- External Memory Interface (EMIF) / Parameter Overlay
- Multi-buffered Analog-to-Digital Converter (MibADC)
- Support Structure: Web, Forum, WIKI

Who should attend:
- Hardware and Software Developers
- Project Managers
- Safety Specialists
- Anyone interested in Hercules MCUs and functional safety

3 Day Training Class: Safety Critical Design and Programming with ARM® Cortex®-R4F based Hercules MCUs

Day 1
- Welcome and Intro
- Hercules Product Overview / MCU Roadmap
- Safety Standards and Hercules Safety Features
- HALCoGen / Exercise
- Code Composer Studio / Demonstration / Exercise
- Compiler / Exercise
- Flash Overview
- Flash Tools: nowFlash™, nowECC™, nowProfile™

Day 2
- Summary / Questions
- ARM® Cortex®-R4F CPU Architecture Overview
- System Module Overview
- Device setup/startup, Real Time Interrupt Module, Vectored Interrupt Manager
- CRC Controller, CPU Compare Module, Error Signaling Module
- General Purpose I/Os / Supply
- Direct Memory Access Controller (DMA)
- Serial Communication Interface (SCI/UART/LIN)

Day 3
- Summary / Questions
- Multi-Buffer Serial Peripheral Interface (SPI / MIBSPI-P)
- DCAN
- FlexRay / Transfer Unit
- Multi-Buffer ADC (MIBADC)
- External Memory Interface (EMIF) / Parameter Overlay Module (POM)
- NHET (High End Timer) IDE
- NHET
- NHET Transfer Unit
- Summary & Questions
Thank You

Contact Information:
Hoiman Low: hm-low@ti.com
重要声明

德州仪器(TI)及其下属公司有权根据JESD48最新标准，对所提供的产品和服务进行更正、修改、增强、改进或其它更改，并有权根据JESD48最新标准中止提供任何产品和服务。客户在下订单前应获取最新的相关信息，并验证这些信息是否完整且是最新的。所有产品的销售都遵循在订单确认时所提供的TI销售条款与条件。

TI保证其所销售的组件的性能符合产品销售时TI半导体产品销售条件与条款的适用规范。仅在TI保证的范围内，且TI认为有必要时才会使用测试或其它质量控制技术。除非适用法律做出了硬性规定，否则没有必要对每种组件的所有参数进行测试。

TI对应用帮助或客户产品设计不承担任何义务。客户应对其使用TI组件的产品和应用自行负责。为尽量减小与客户产品和应用相关的风险，客户应提供充分的设计与操作安全措施。

TI不对任何TI专利权、版权、屏蔽作品权或其它与使用了TI组件或服务的组合设备、机器或流程相关的TI知识产权中授予的直接或隐含权利作出任何保证或解释。TI所发布的与第三方产品或服务有关的信息，不能构成从TI获得使用这些产品或服务的许可、授权、或认可使用此类信息可能需要获得第三方的专利权或其它知识产权方面的许可，或是TI的专利权或其它知识产权方面的许可。

对于TI的产品手册或数据表中TI信息的重要部分，仅在没有对内容进行任何篡改且带有相关授权、条件、限制和声明的情况下才允许进行复制。TI对此类篡改过的文件不承担任何责任或义务。复制第三方的信息可能需要服从额外的限制条件。

在转售TI组件或服务时，如果对该组件或服务参数的陈述与TI标明的参数相比存在差异或虚假成分，则会失去相关TI组件或服务的所有明示或暗示授权，且这是不正当的、欺诈性的商业行为。TI对任何此类虚假陈述均不承担任何责任或义务。

在某些场合中，为了推进安全相关应用有可能对TI组件进行特别的促销。TI的目标是利用此类组件帮助客户设计和创立其特有的可满足适用功能安全标准和要求的终端产品解决方案。尽管如此，此类组件仍然服从这些条款。

TI组件未获得用于FDA Class III（或类似的生命攸关医疗设备）的授权许可，除非各方授权官员已经达成了专门管控此类使用的特别协议。

只有那些TI特别注明属于军用等级或"增强型塑料"的TI组件才是设计或专门用于军事/航空应用或环境的。购买者认可并同意，对并非指定面向军事或航空航天用途的TI组件进行军事或航空航天方面的应用，其风险由客户单独承担，并且由客户负责满足与此类使用相关的所有法律法规要求。TI已明确规定符合ISO/TS16949要求的产品，这些产品主要用于汽车。在任何情况下，因使用非指定产品而无法达到ISO/TS16949要求，TI不承担责任。

<table>
<thead>
<tr>
<th>产品</th>
<th>应用</th>
<th>网址</th>
</tr>
</thead>
<tbody>
<tr>
<td>数字音频</td>
<td>通信与电信</td>
<td><a href="http://www.ti.com/audio">www.ti.com/audio</a></td>
</tr>
<tr>
<td>放大器和线性器件</td>
<td>计算机及周边</td>
<td><a href="http://www.ti.com/amplifiers">www.ti.com/amplifiers</a></td>
</tr>
<tr>
<td>数据转换器</td>
<td>消费电子</td>
<td><a href="http://www.ti.com/dataconverters">www.ti.com/dataconverters</a></td>
</tr>
<tr>
<td>DLP®产品</td>
<td>能源</td>
<td><a href="http://www.dlp.com">www.dlp.com</a></td>
</tr>
<tr>
<td>DSP - 数字信号处理器</td>
<td>工业应用</td>
<td><a href="http://www.ti.com/dsp">www.ti.com/dsp</a></td>
</tr>
<tr>
<td>时钟和计时器</td>
<td>医疗电子</td>
<td><a href="http://www.ti.com/clockandtimers">www.ti.com/clockandtimers</a></td>
</tr>
<tr>
<td>接口</td>
<td>安防应用</td>
<td><a href="http://www.ti.com/interface">www.ti.com/interface</a></td>
</tr>
<tr>
<td>逻辑</td>
<td>汽车电子</td>
<td><a href="http://www.ti.com/logic">www.ti.com/logic</a></td>
</tr>
<tr>
<td>电源管理</td>
<td>视频和影像</td>
<td><a href="http://www.ti.com/power">www.ti.com/power</a></td>
</tr>
<tr>
<td>微控制器(MCU)</td>
<td>德州仪器在线技术支持社区</td>
<td><a href="http://www.ti.com/microcontrollers">www.ti.com/microcontrollers</a></td>
</tr>
<tr>
<td>RFID系统</td>
<td></td>
<td><a href="http://www.ti.com/rfidsys">www.ti.com/rfidsys</a></td>
</tr>
<tr>
<td>OMAP®应用处理器</td>
<td></td>
<td><a href="http://www.ti.com/omap">www.ti.com/omap</a></td>
</tr>
<tr>
<td>无线连通性</td>
<td></td>
<td><a href="http://www.ti.com/wirelessconnectivity">www.ti.com/wirelessconnectivity</a></td>
</tr>
</tbody>
</table>

邮寄地址：上海市浦东新区世纪大道1568号，中建大厦32楼邮政编码：200122
Copyright © 2014，德州仪器半导体技术（上海）有限公司