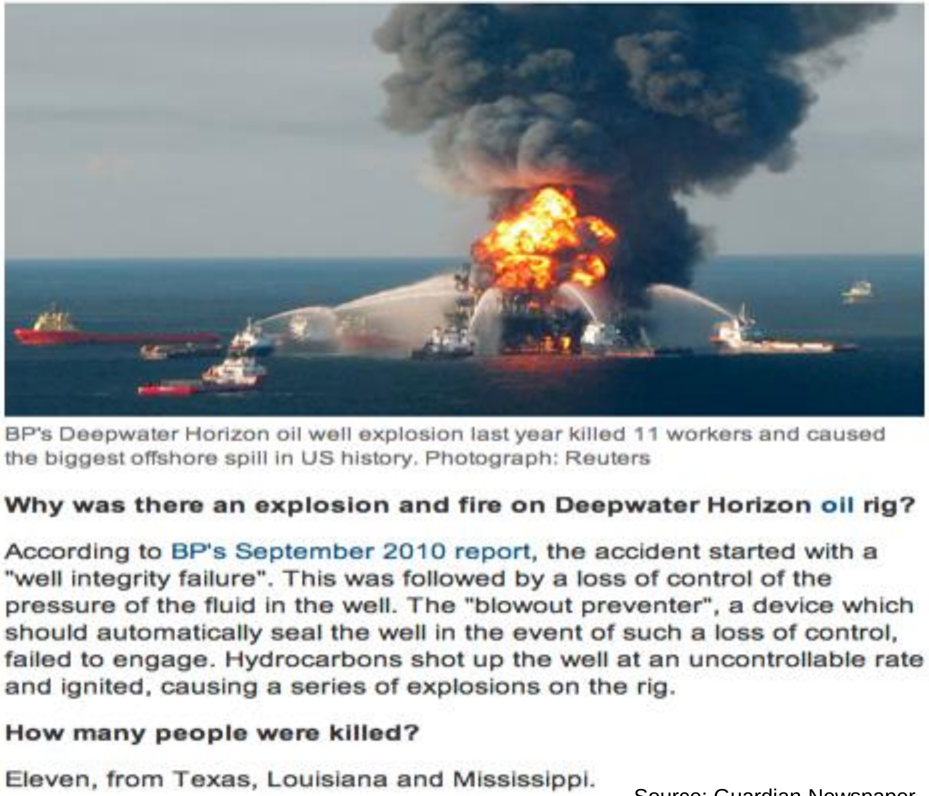
Hercules™ Microcontrollers

Automotive Functional Safety

Battery Management Systems,EPS,Braking Systems,VCU in EV/HEV Application

Why Functional Safety?



BP's Deepwater Horizon oil well explosion last year killed 11 workers and caused the biggest offshore spill in US history. Photograph: Reuters

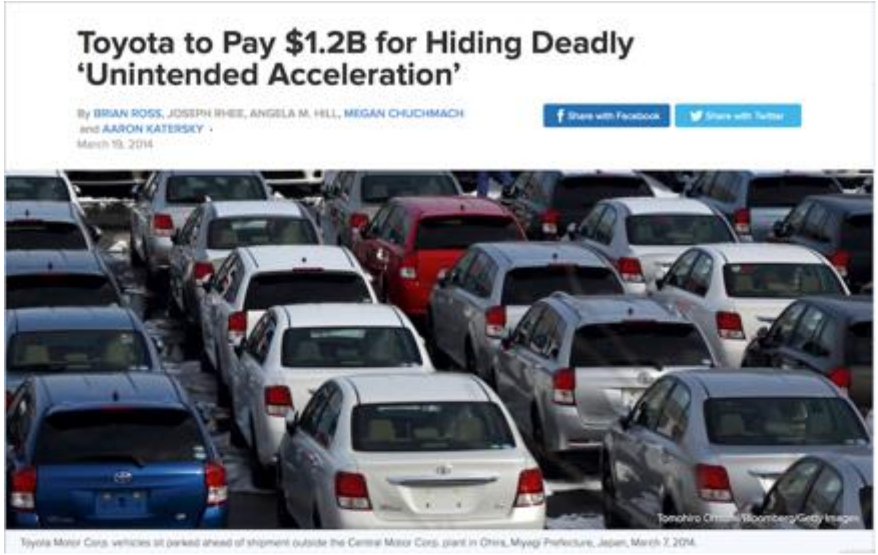
Why was there an explosion and fire on Deepwater Horizon oil rig?

According to BP's September 2010 report, the accident started with a "well integrity failure". This was followed by a loss of control of the pressure of the fluid in the well. The "blowout preventer", a device which should automatically seal the well in the event of such a loss of control, failed to engage. Hydrocarbons shot up the well at an uncontrollable rate and ignited, causing a series of explosions on the rig.

How many people were killed?

Eleven, from Texas, Louisiana and Mississippi.

Source: Guardian Newspaper



Toyota to Pay $1.2B for Hiding Deadly 'Unintended Acceleration'

By BRIAN ROSS, JOSEPH RHEE, ANGELA M. HILL, MEGAN CHUCHMACH and AARON KATERSKY ·
March 19, 2014

Tomohiro Ohsumi/Bloomberg/Getty Images

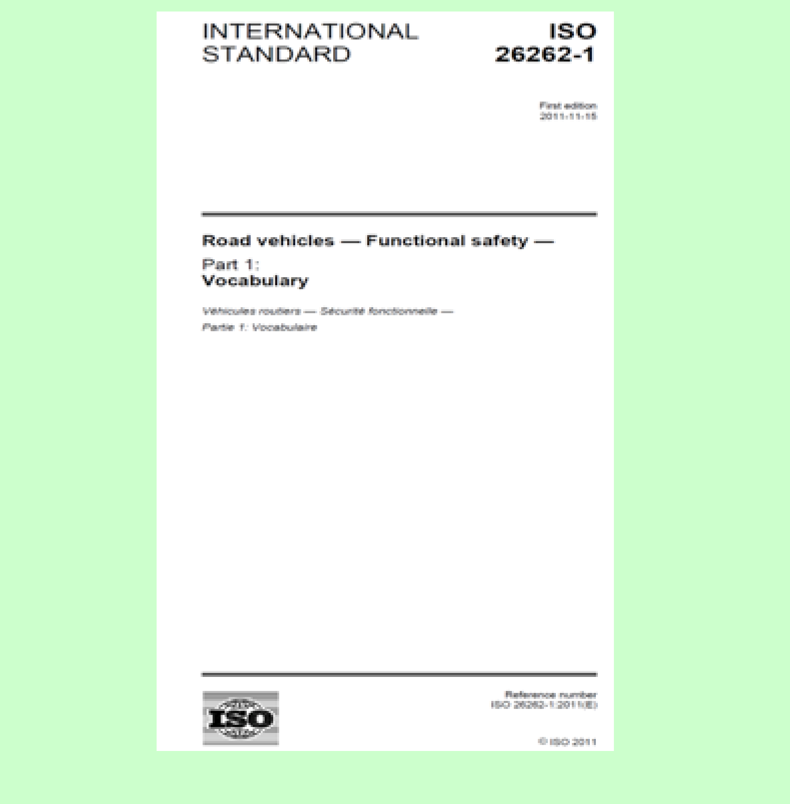
Toyota Motor Corp. vehicles sit parked ahead of shipment outside the Central Motor Corp. plant in Ohira, Miyagi Prefecture, Japan, March 7, 2014.

Source: ABC News

Functional Safety goals:

- Perform intended functions
- When fail, fail predictably

ISO 26262 – Functional Safety of Road Vehicles



INTERNATIONAL STANDARD

ISO 26262-1

First edition
2011-11-15

Road vehicles — Functional safety —

Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2011(E)

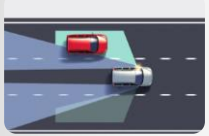
© ISO 2011

- Automotive specific interpretation of IEC 61508 but replaces it rather than extending it.
- Aligns automotive life cycle and supply hierarchy.
- Separates component design from system design. **Most complex components must comply to standard**.
- TI participates in US and international working group as well as leading Semiconductor subgroup:
  - ISO/TC 022/SC 03/WG16
  - ISO/NP PAS 19451

Hercules™ TMS570 safety MCUs for automotive and transportation motor control

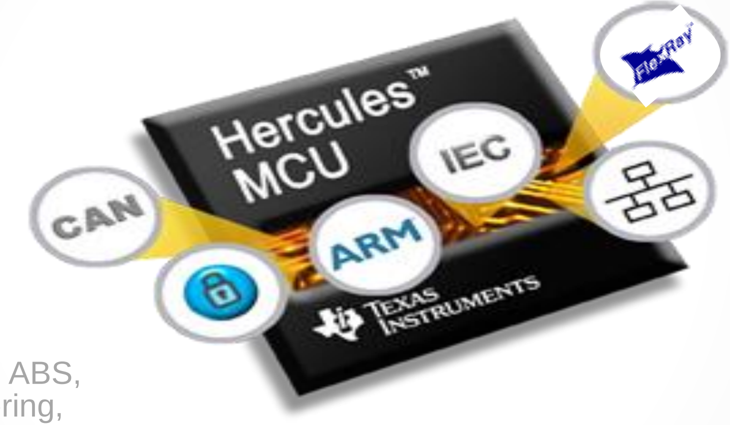
Automotive

HEV/EV cars



Radar/collision avoidance (ADAS)

Active suspension, ABS, electric power steering, airbag and more!



Transportation

Railway systems

Aerospace

Bus

Extending Hercules TMS570 safety MCU platform

- From 120 MIPS to 500 DMIPs lockstep ARM Cortex-R core
- From 128KB to 4 MB flash
- Cortex-R4 and Cortex-R5 options
- Fixed- and floating-point options

Proven safety architecture

- ISO26262, IEC61508
- Lockstep CPUs
- CPU and RAM built-in self test
- Flash & RAM ECC
- Clock, Voltage monitoring

Expanded motor control support

- Enhanced PWMs, capture and Quadrature Encoder Interface
- New MotorWare™-enabled Kits
- New DSP Library

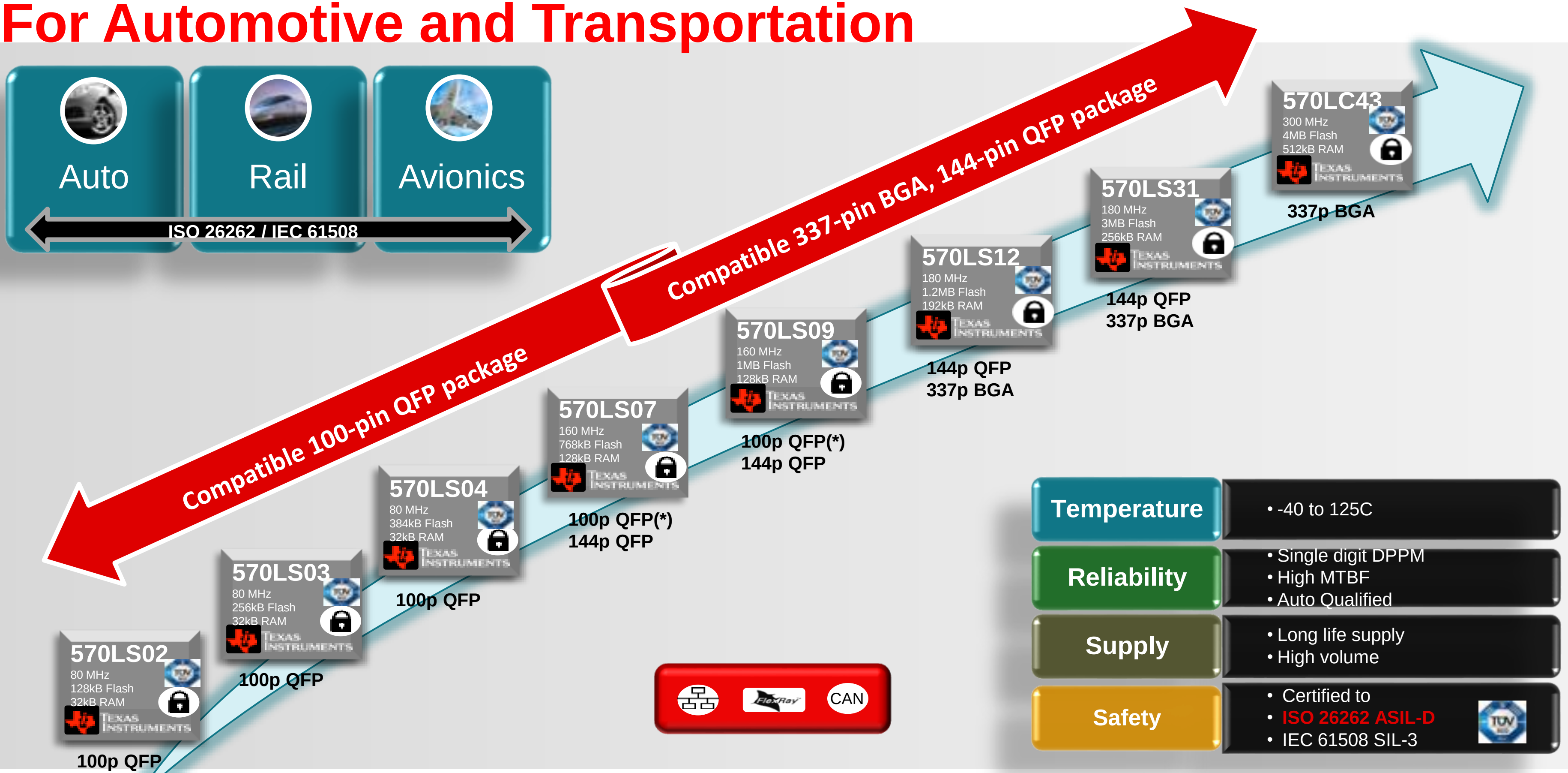
SafeTI™ Design Packages

Docs, Tools, Software

- Complementary, safety-enabled Components
- Safety Development Processes

TMS570 ARM® Cortex®-R MCU platform

For Automotive and Transportation



Auto

Rail

Avionics

ISO 26262 / IEC 61508

Compatible 100-pin QFP package

Compatible 337-pin BGA, 144-pin QFP package

570LS02
80 MHz
128kB Flash
32kB RAM
100p QFP

570LS03
80 MHz
256kB Flash
32kB RAM
100p QFP

570LS04
80 MHz
384kB Flash
32kB RAM
100p QFP

570LS07
160 MHz
768kB Flash
128kB RAM
100p QFP(*)
144p QFP

570LS09
160 MHz
1MB Flash
128kB RAM
100p QFP(*)
144p QFP

570LS12
180 MHz
1.2MB Flash
192kB RAM
144p QFP
337p BGA

570LS31
180 MHz
3MB Flash
256kB RAM
144p QFP
337p BGA

570LC43
300 MHz
4MB Flash
512kB RAM
337p BGA

Temperature	• -40 to 125C
Reliability	• Single digit DPPM • High MTBF • Auto Qualified
Supply	• Long life supply • High volume
Safety	• Certified to • ISO 26262 ASIL-D • IEC 61508 SIL-3

▨ Production ▨ Sampling *(*) Production 3Q16*

Texas Instruments

TMS570LC4x Block Diagram

Lockstep ARM Cortex-R5F Cached Floating Point MCU

Features

IEC ISO CAN

Performance / Memory

- Up to 300 MHz ARM Cortex-R5F w/ Floating Point
- Up to 4MB Flash and 512KB Data SRAM w/ECC
- 32KB Instruction & 32KB Data Cache w/ECC
- Dedicated 128KB Data Flash (EEPROM Emulation)
- 16 Channel DMA

Safety

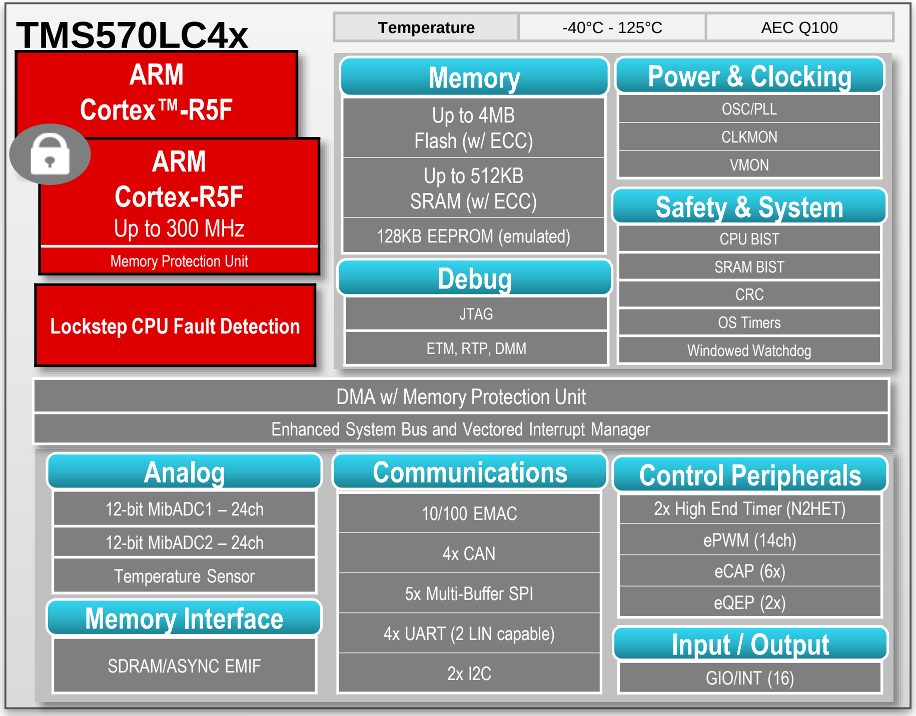
- Dual CPUs in Lockstep,CPU Logic Built in Self Test (LBIST)
- Up to 16 CPU MPU regions,Flash & RAM w/ ECC (w/ bus protection)
- Memory Built-in Self Test (PBIST),Cyclic redundancy checker module (CRC)
- Select peripheral RAMs protected by Parity/ECC

Communication Networks

- 10/100 MAC ,4 CAN Interfaces
- 5 Multi-Buffered SPI,4 UART (2 LIN capable), 2 I2C

Enhanced I/O Control

- 2x Timer Coprocessor (N2HET) w/DMA
  - Up to 64 total channels (2x32)
  - Pins can be used as Hi-Res PWM or Input Capture
- Motor Control Timers
  - ePWM, eCAP, eQEP
- 2 x12-bit Multi-Buffered ADC
  - Up to 48 total input channels
  - Calibration and Self Test
- Up to 145 GPIO pins (16 dedicated)



TMS570LC4x

Temperature	-40°C - 125°C	AEC Q100

ARM Cortex™-R5F

ARM Cortex-R5F
Up to 300 MHz
Memory Protection Unit

Lockstep CPU Fault Detection

Memory
Up to 4MB Flash (w/ ECC)
Up to 512KB SRAM (w/ ECC)
128KB EEPROM (emulated)

Power & Clocking
OSC/PLL
CLKMON
VMON

Debug
JTAG
ETM, RTP, DMM

Safety & System
CPU BIST
SRAM BIST
CRC
OS Timers
Windowed Watchdog

DMA w/ Memory Protection Unit
Enhanced System Bus and Vectored Interrupt Manager

Analog
12-bit MibADC1 – 24ch
12-bit MibADC2 – 24ch
Temperature Sensor

Memory Interface
SDRAM/ASYNC EMIF

Communications
10/100 EMAC
4x CAN
5x Multi-Buffer SPI
4x UART (2 LIN capable)
2x I2C

Control Peripherals
2x High End Timer (N2HET)
ePWM (14ch)
eCAP (6x)
eQEP (2x)

Input / Output
GIO/INT (16)

Packages

337p BGA
(16x16mm)

Targeted Applications

- High End IEC61508 and ISO26262 Safety Applications
- Automotive, Rail, Aerospace (COTS), Off Road

Note: Above reflects max configuration of each module – some functions are multiplexed.

TMS570LS31x/21x Block Diagram

Lockstep ARM Cortex-R4F w/ Floating Point

Features

IEC ISO FlexRay CAN

Performance / Memory

- Up to 180 MHz ARM Cortex-R4F w/ Floating Point
- Up to 3MB Flash and 256KB Data SRAM
- Dedicated 64KB Data Flash (EEPROM Emulation)
- 16 Channel DMA

Safety

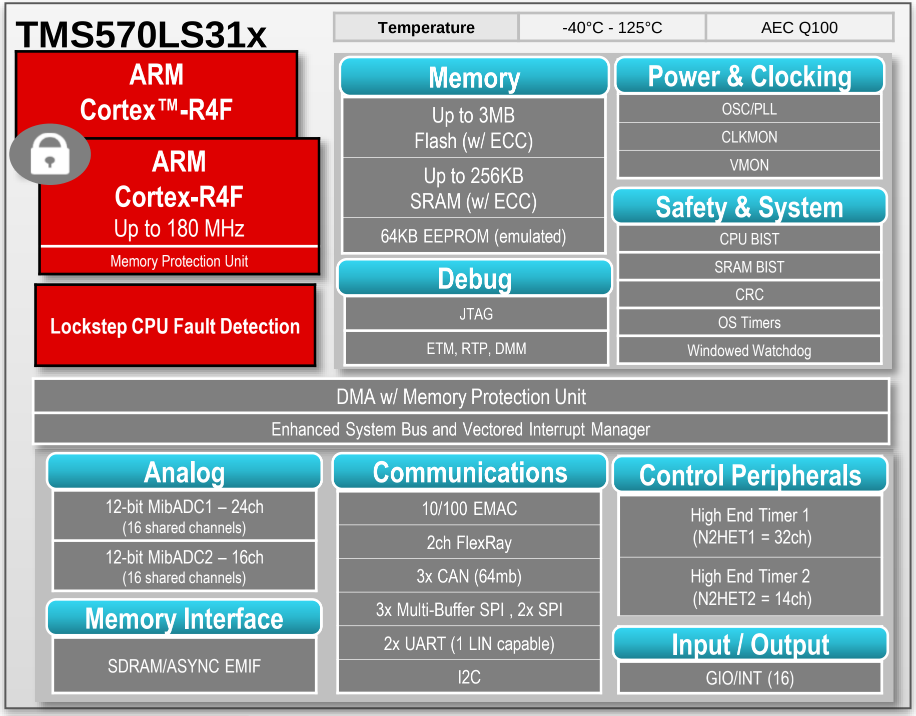
- Dual CPUs in Lockstep
- CPU Logic Built in Self Test (LBIST)
- Up to 12 CPU MPU regions
- Flash & RAM w/ ECC (w/ bus protection)
- Memory Built-in Self Test (PBIST)
- Cyclic redundancy checker module (CRC)
- Select peripheral RAMs protected by Parity

Communication Networks

- 10/100 MAC ,FlexRay w/DMA,3 CAN Interfaces
- 5 SPI (3 Multi-Buffered),2 UART (1 LIN capable), 1 I2C

Enhanced I/O Control

- 2x Timer Coprocessor (N2HET) w/DMA
  - Up to 44 pins plus 6 monitor channels
  - Pins can be used as Hi-Res PWM or Input Capture
- 2 x12-bit Multi-Buffered ADC
  - 24 total input channels (16 shared)
  - Calibration and Self Test
- Up to 120 GPIO pins (16 dedicated)



TMS570LS31x

Temperature	-40°C - 125°C	AEC Q100

ARM Cortex™-R4F

ARM Cortex-R4F
Up to 180 MHz
Memory Protection Unit

Lockstep CPU Fault Detection

Memory
Up to 3MB Flash (w/ ECC)
Up to 256KB SRAM (w/ ECC)
64KB EEPROM (emulated)

Power & Clocking
OSC/PLL
CLKMON
VMON

Debug
JTAG
ETM, RTP, DMM

Safety & System
CPU BIST
SRAM BIST
CRC
OS Timers
Windowed Watchdog

DMA w/ Memory Protection Unit
Enhanced System Bus and Vectored Interrupt Manager

Analog
12-bit MibADC1 – 24ch (16 shared channels)
12-bit MibADC2 – 16ch (16 shared channels)

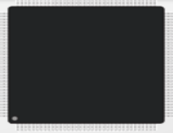
Memory Interface
SDRAM/ASYNC EMIF

Communications
10/100 EMAC
2ch FlexRay
3x CAN (64mb)
3x Multi-Buffer SPI , 2x SPI
2x UART (1 LIN capable)
I2C

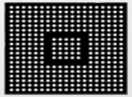
Control Peripherals
High End Timer 1 (N2HET1 = 32ch)
High End Timer 2 (N2HET2 = 14ch)

Input / Output
GIO/INT (16)

Packages



144p QFP (20x20mm)



337p BGA (16x16mm)

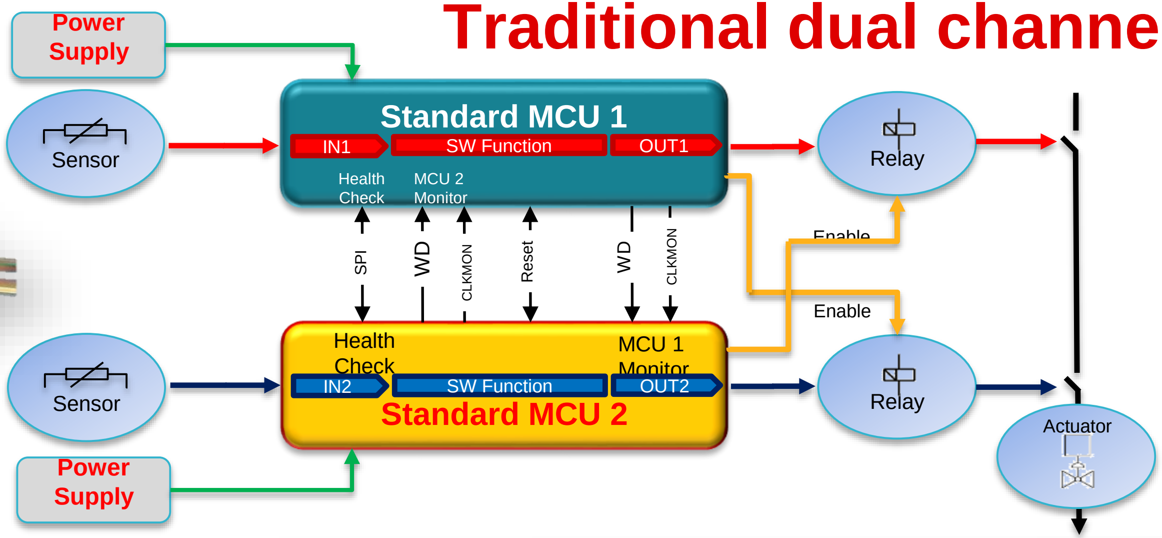
Targeted Applications

- IEC 61508 and ISO 26262 Safety Applications
- Automotive, Rail, Aerospace (COTS), Off Road

Note: Above reflects max configuration of each module – some functions are multiplexed.

Traditional dual channel vs. Lockstep

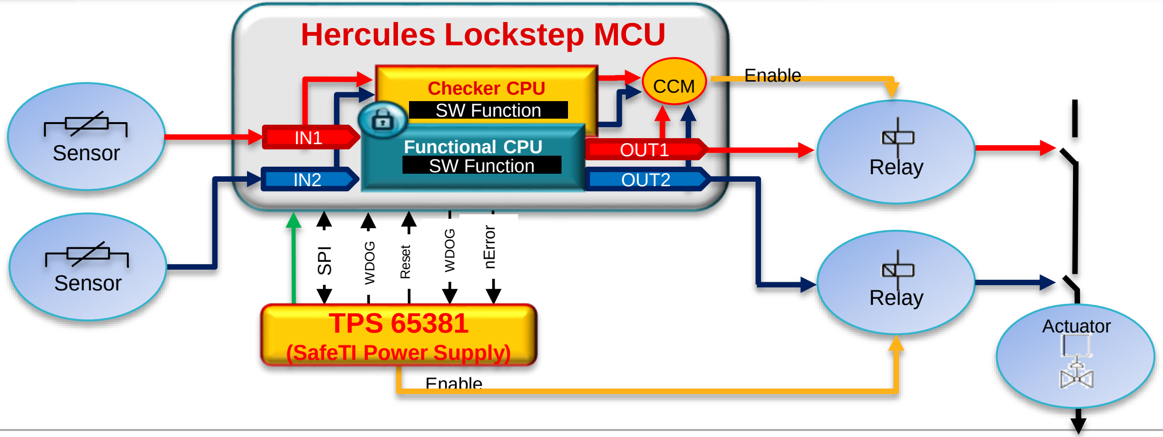
Standard Controller Approach



- + Traditional physical 2 channel system
- + MCU component level diversity possible

- − Fault detection depends on software latency
- − Fault coverage depends on software
- − Memory corruption protected by mirroring
- − Extra software developed
  1. CPU Sync
  2. Safety checks
  3. Self Test

Lockstep Controller Approach

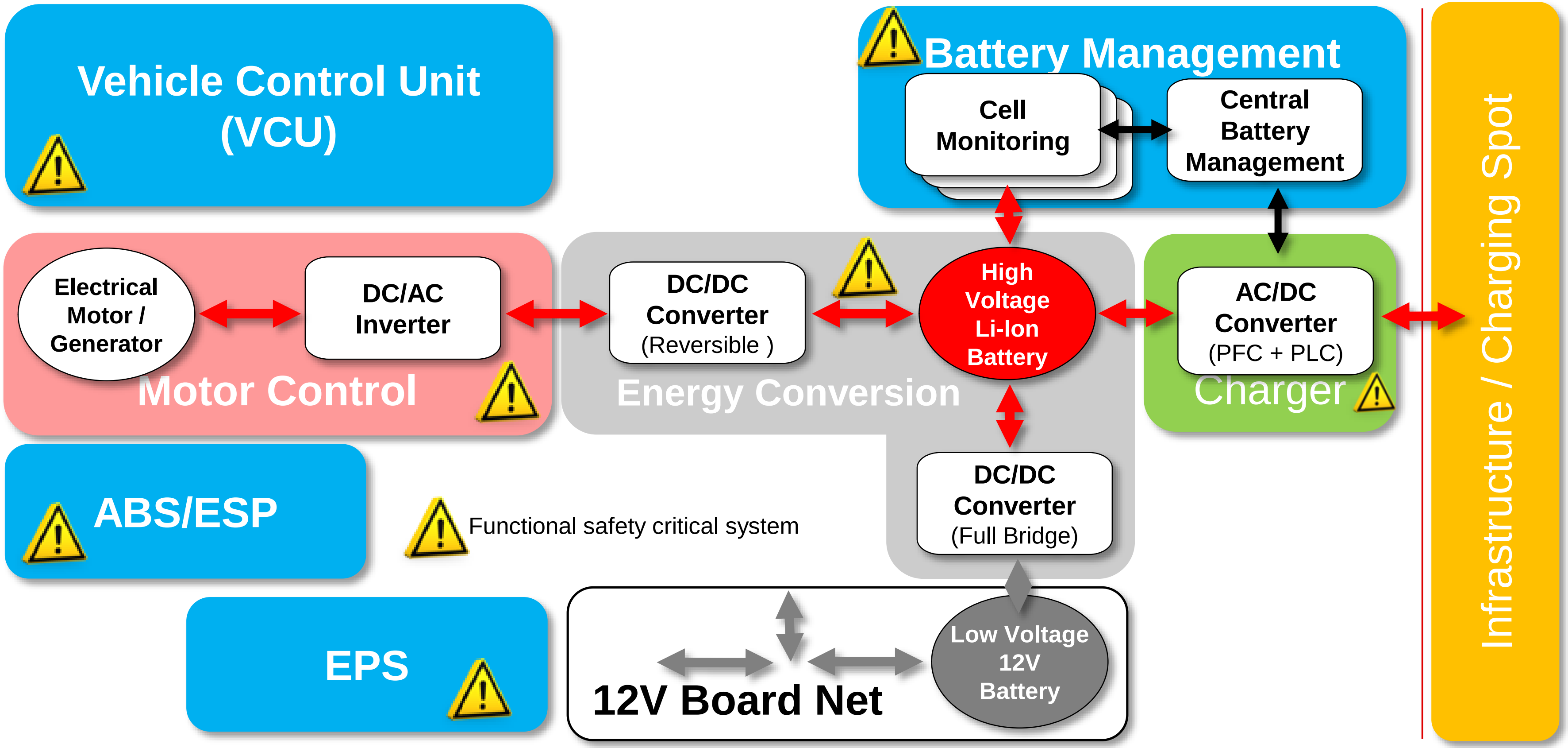


- + Fault detection in 2 cycles
- + Hard, Transient, AC faults detected
- + Memory corruption detected by ECC
- + Minimal software developed for safety checks
- + Self Test by Hardware
- + Module level diversity possible
- + Software isolation via Memory Protection Unit

- − Non-traditional logical 2 channel system

🟧 Diagnostics   CCM Core Compare Module

Electric Vehicle – Architecture Overview



Vehicle Control Unit (VCU)
Battery Management
Cell Monitoring
Central Battery Management
Electrical Motor / Generator
DC/AC Inverter
Motor Control
DC/DC Converter (Reversible)
High Voltage Li-Ion Battery
Energy Conversion
AC/DC Converter (PFC + PLC)
Charger
Infrastructure / Charging Spot
ABS/ESP
Functional safety critical system
DC/DC Converter (Full Bridge)
EPS
12V Board Net
Low Voltage 12V Battery

Battery Management System (BMS)

What is the Battery Management System?

- In an electric vehicle (EV) or hybrid electric vehicle, the battery management system monitors and controls the high-voltage battery stack. This includes:
  - Measuring the cells' charge, voltage, and health
  - Measuring the temperature of the cells
  - Controlling the current among cells to avoid over- or under-charging (cell balancing)

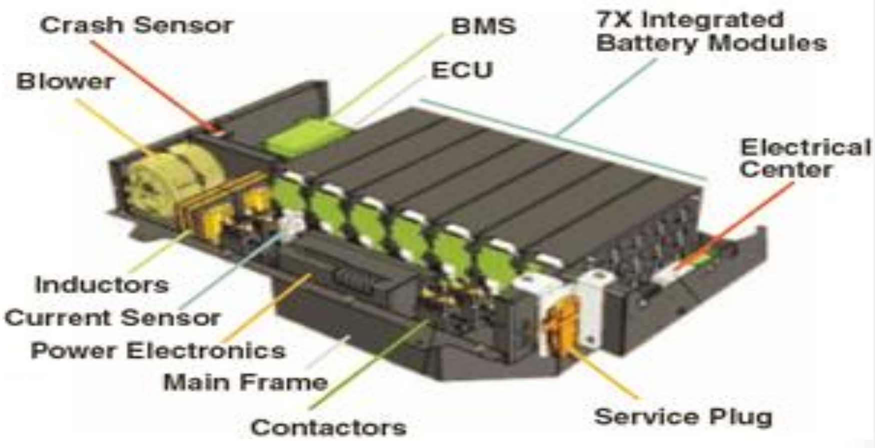


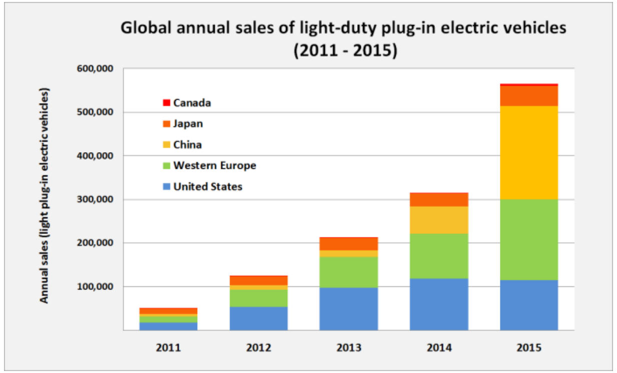
Image courtesy of A123 Systems, Watertown, Mass.

What does this EE consist of?

- **Passive cell balancing**
  - The technique places a bleed resistor across a cell when its state of charge exceeds that of its neighbors. This extends the useful lifetime (number of cycles) of the battery.
  - Simple but has resistive losses
- **Active cell balancing**
  - Shuttles energy among individual cells using FET matrix to direct energy from higher-charged cells to lower-charged cells
  - High efficiency, but requires more circuitry
- **Thermal management**
  - Monitors temperature and controls heat/cooling for battery pack
  - Maintains battery pack within temperature range for best operation of cell chemistry
- **Disconnect unit**
  - Disconnects high voltage from the rest of the car
  - Disconnects during servicing or in case of crash
- **Fuel cell management**
  - Monitors and controls the operation of fuel cell unit in fuel cell vehicle
  - Controls high voltage generated by chemical reaction within the fuel cell

BMS: Functional Safety is Required

- Primary concern with Lithium Ion Batteries is potential for thermal runaway caused by internal short in a cell or due to manufacturing flaw or an accident.
- BMS systems monitor the cell voltages and temperatures and alerts the vehicle control unit of any abnormalities.
- Car manufactures require BMS development be done according to the ISO 26262 functional safety standard up to ASIL C/D level.
- Battery Management Systems are expected to continue to grow!!
- ISO 26262 is automotive functional safety standard. Hercules MCUs are certified to ISO 26262 ASIL-/D!!



Source - http://energy.gov/eere/vehicles/fact-918-march-28-2016-global-plug-light-vehicle-sales-increased-about-80-2015

TMS570 *Active Cell-Balancing Battery-Management*: TIDM-TMS570 TIDesigns

Features

- The diagnostic features of TMS570LS0432 microcontroller (MCU) are enabled to monitor and report TMS570LS0432 status during run time.
- The TMS570LS0432 MCU configures BQ76PL455A-Q1 for monitoring cell voltages and checking BQ76PL455A-Q1 status during run time.
- The TMS570LS0432 MCU analyzes the data from all battery cells and generates active cell balancing command.
- The TMS570LS0432 MCU commands EMB1428Q for cell balancing and monitors EMB1428 and EMB1499 status during run time.

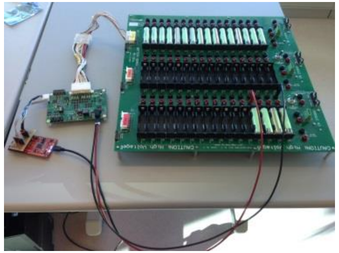
Benefits

- Demonstrate TMS570LS0432 (an ISO 26262 capable MCU) supporting active cell balancing between one cell in a 16 cell battery module and a 12V supply for emulation of HEV/EV application.
- Demonstrate building the system example using the off shelf TI evaluation kits: TMSLS0432 Launchpad and EM1402 BMS EVM.

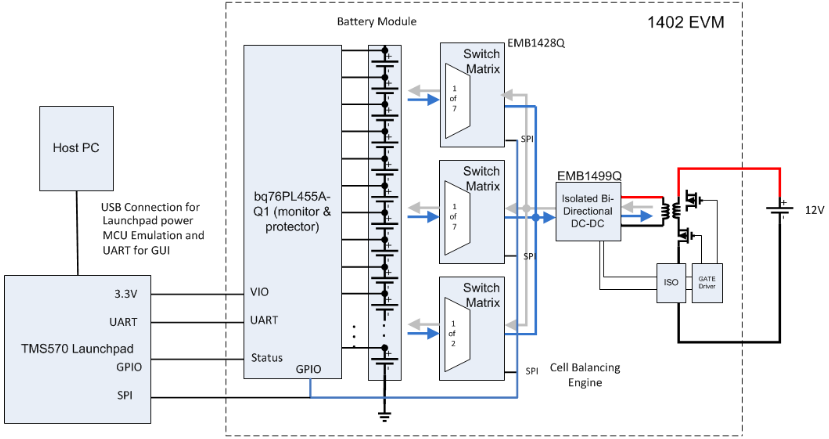
Target Applications

- Electric and Hybrid Electric Vehicles (EVs, HEVs, PHEVs, and mild hybrids)
- Energy Storage (ESS)
- Uninterruptible Power Supplies (UPSs)
- E-Bikes and E-Scooters

Tools & Resources



- **TIDM-TMS570BMS TI Design Folder**
  - User Guide
  - Relevant Design Files
- **Device Datasheets:**
  - TMS570LS0432
  - BQ76PL455A-Q1
  - EMB1428Q
  - EMB1499Q



TEXAS INSTRUMENTS

Safety Motor Control Block Diagram

EPS

Key Reference Designs

- DRV8301-LS31-KIT

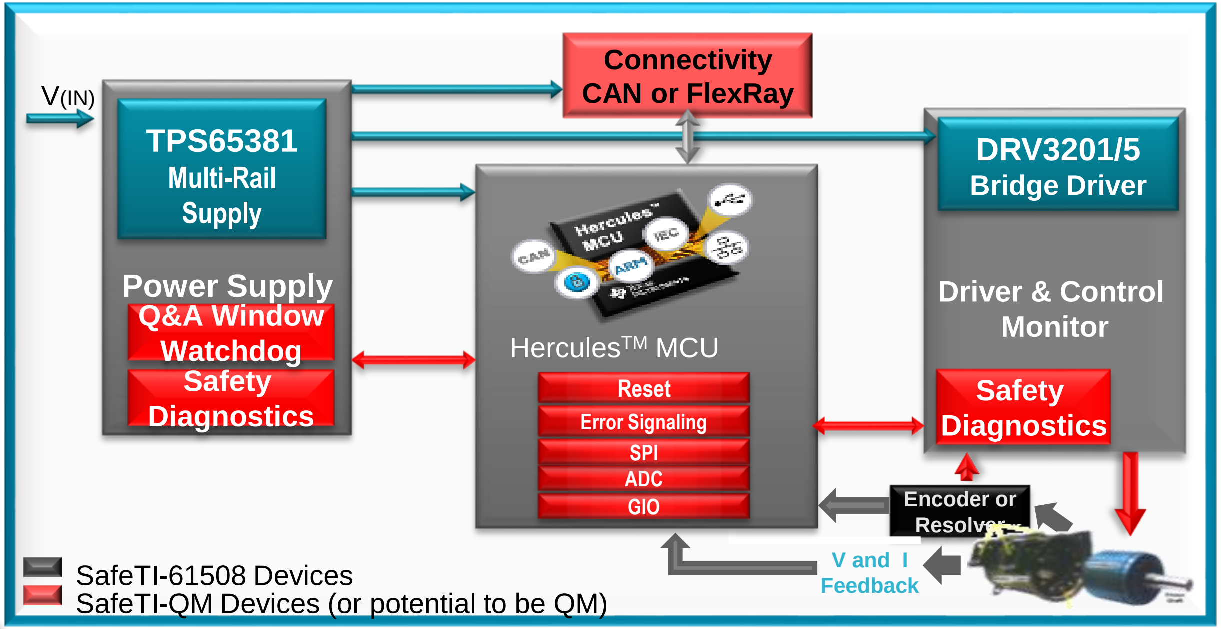
Key Software

smo_enc Hercules MotorWare

- Combines sensorless feedback redundant/safety channel with sensor

HALCoGen

- MISRA, IEC 61508 driver code



Key Safety Processors

TMS570LS03x/04x/07x/09x/11x/12x MCU

- ISO26262, ASIL-D, 125C
- CAN, Ethernet, FlexRay
- Over 250 MIPs
- Floating Point
- 384KB to 3MB Options
- Safety docs available for all

Key Bridge/Gate Drivers

DRV3201/5 Safing FET Driver

- 3x FET Safing Monitor
- Diagnostics: Temp, Voltage, Short, VDS
- Protection: CLK, Shoot through, Dead Time
- Auto temp, ISO2626, IEC 61508

Key Power Management

TPS6538x – Integrated Safety

- DRV & MCU Safing Monitor & Diags
- Robust, internal supply paths
- Integrated, protected sensor supply
- 40V compliant supply inputs!
- Built for Hercules MCUs
- Suitable for use in ISO26262 apps

Key Interface/Connectivity

CAN (ISO) Transceiver : ISO1050

- Isolation up to 5000VRMS
- Failsafe outputs

Ehternet PHY: DP83848VYB

- -40 to 105C, 3.3V

Anti-Lock Braking Block Diagram

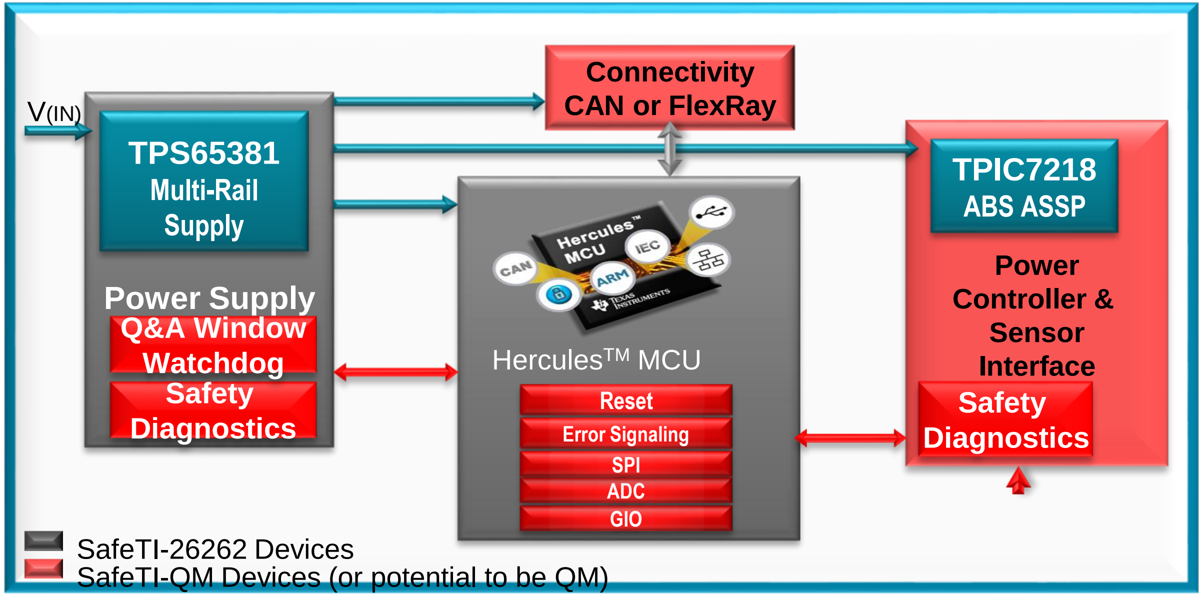
Key Software

HALCoGen

- MISRA, IS026262 driver code

AUTOSAR OS/RTE:

- Vector MICROSAR Safe
- ElektroBit tresos
- ETAS RTA-OS & RTA-RTE
- TI MCAL available for AUTOSAR v4.0.3



Key Safety Processors

TMS570LS03x/04x/07x/09x//11x/12x MCU

- ISO26262 ASIL-D
- AEC Q100 -40C-125C (ambient)
- LIN,CAN, Ethernet, FlexRay
- Safety docs available for all.

Key Power Control and Sensor Interface

TPIC7218 ABS ASSP

- Auto temp, ISO2626, IEC 61508

Key Power Management

TPS6538x – Integrated Safety

- Robust, internal supply paths
- Integrated, protected sensor supply
- 40V compliant supply inputs!
- Built for Hercules™ MCUs
- Suitable for use in ISO26262 apps

Key Interface/Connectivity

CAN (ISO) Transceiver : ISO1050

- Isolation up to 5000VRMS
- Failsafe outputs

Electronic Stability Control Block Diagram

Key Software

HALCoGen

- MISRA, ISO26262 driver code

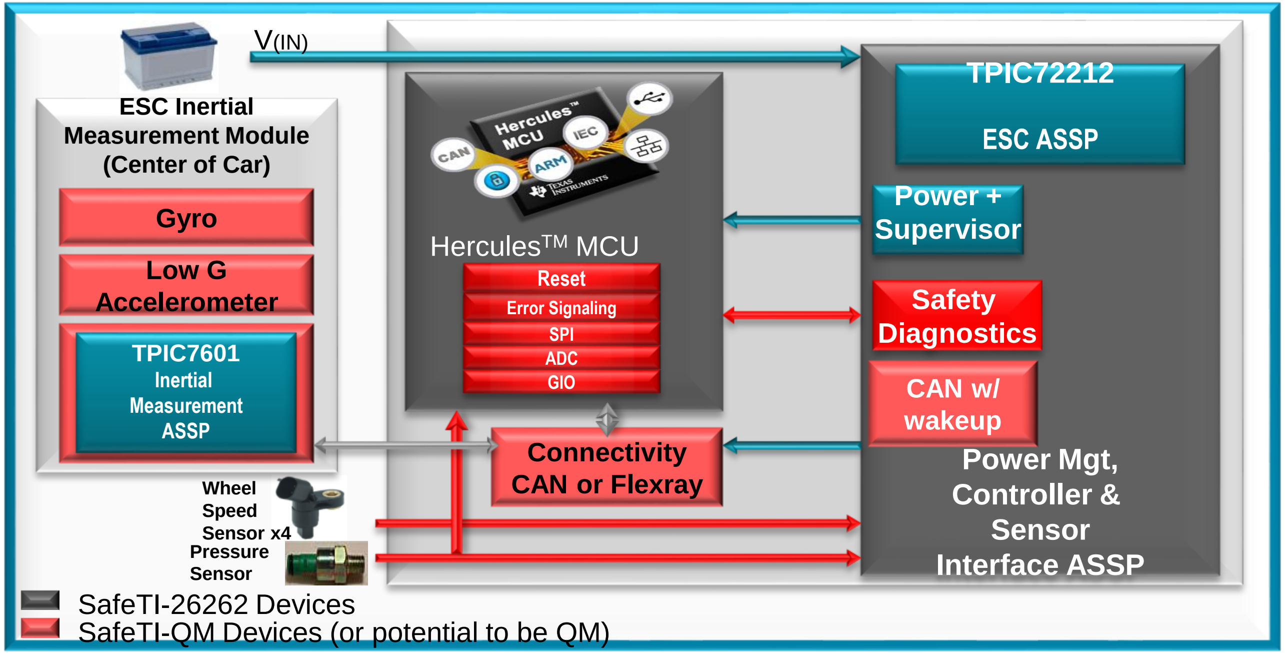
AUTOSAR OS/RTE:

- Vector MICROSAR Safe
- ElektroBit tresos
- ETAS RTA-OS & RTA-RTE
- TI MCAL available for AUTOSAR v4.0.3

Key Safety Processors

TMS570LS07x/09x/11x/12x/21x/31x MCU

- ISO26262 ASIL-D
- AEC Q100 -40C-125C (ambient)
- LIN,CAN, Ethernet, FlexRay
- Safety docs available for all.



V(IN)

ESC Inertial Measurement Module (Center of Car)

Gyro

Low G Accelerometer

TPIC7601 Inertial Measurement ASSP

Hercules™ MCU

Hercules™ MCU

Reset

Error Signaling

SPI

ADC

GIO

Connectivity CAN or Flexray

Wheel Speed Sensor x4

Pressure Sensor

TPIC72212

ESC ASSP

Power + Supervisor

Safety Diagnostics

CAN w/ wakeup

Power Mgt, Controller & Sensor Interface ASSP

▨ SafeTI-26262 Devices

🟥 SafeTI-QM Devices (or potential to be QM)

Key Power Control and Sensor Interface

TPIC72212 ESC ASSP

- Auto temp, ISO2626, IEC 61508

TPIC7601 Inertial Measurement ASSP

- Auto temp, ISO2626, IEC 61508

Key Power Management

Included in TPIC72212

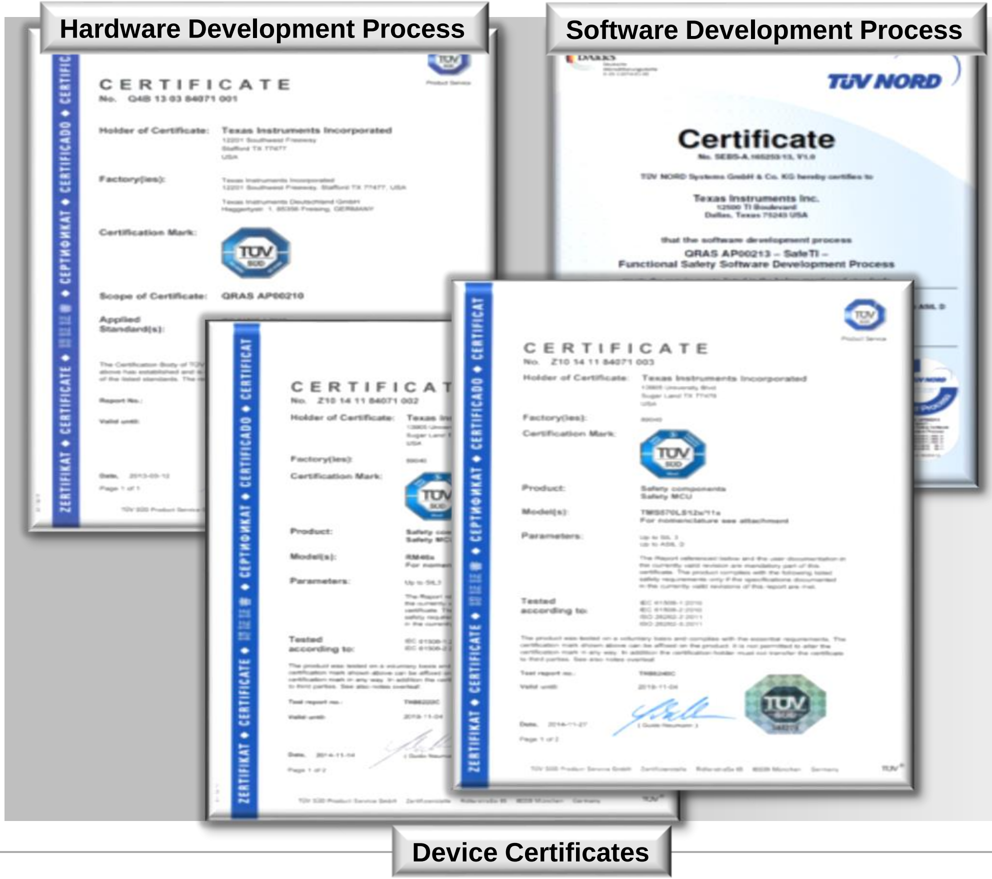
- Power + Supervisor
- Safety Diagnostics
- Suitable for use in ISO26262 apps

Key Interface/Connectivity

CAN (ISO) Transceiver : ISO1050

- Isolation up to 5000VRMS
- Failsafe outputs

Hercules Product & Process Certification



Hardware Development Process

CERTIFICATE
No. Q4B 13 03 84071 001

Holder of Certificate: Texas Instruments Incorporated
12201 Southwest Freeway
Stafford TX 77477
USA

Factory(ies): Texas Instruments Incorporated
12201 Southwest Freeway, Stafford TX 77477, USA
Texas Instruments Deutschland GmbH
Haggertystr. 1, 85356 Freising, GERMANY

Certification Mark:

Scope of Certificate: QRAS AP00210

Applied Standard(s):

Report No.:

Valid until:

Date, 2013-03-12

Page 1 of 1

Software Development Process

TÜV NORD

Certificate
No. SEBS-A.165253/13, V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies to

Texas Instruments Inc.
12500 TI Boulevard
Dallas, Texas 75243 USA

that the software development process
QRAS AP00213 – SafeTI –
Functional Safety Software Development Process

CERTIFICATE
No. Z10 14 11 84071 002
Holder of Certificate: Texas Instruments Incorporated
Factory(ies):
Certification Mark:
Product: Safety components
Safety MCU
Model(s): RM46x
Parameters: Up to SIL3
Tested according to:
Test report no.:
Valid until:
Date, 2014-11-04
Page 1 of 2

CERTIFICATE
No. Z10 14 11 84071 003

Holder of Certificate: Texas Instruments Incorporated
13905 University Blvd
Sugar Land TX 77479
USA

Factory(ies): 89040

Certification Mark:

Product: Safety components
Safety MCU

Model(s): TMS570LS12x/11x
For nomenclature see attachment

Parameters: Up to SIL 3
Up to ASIL D

Tested according to: IEC 61508-1:2010
IEC 61508-2:2010
ISO 26262-2:2011
ISO 26262-5:2011

Test report no.:

Valid until: 2019-11-04

Date, 2014-11-27

(Guido Neumann)

Page 1 of 2

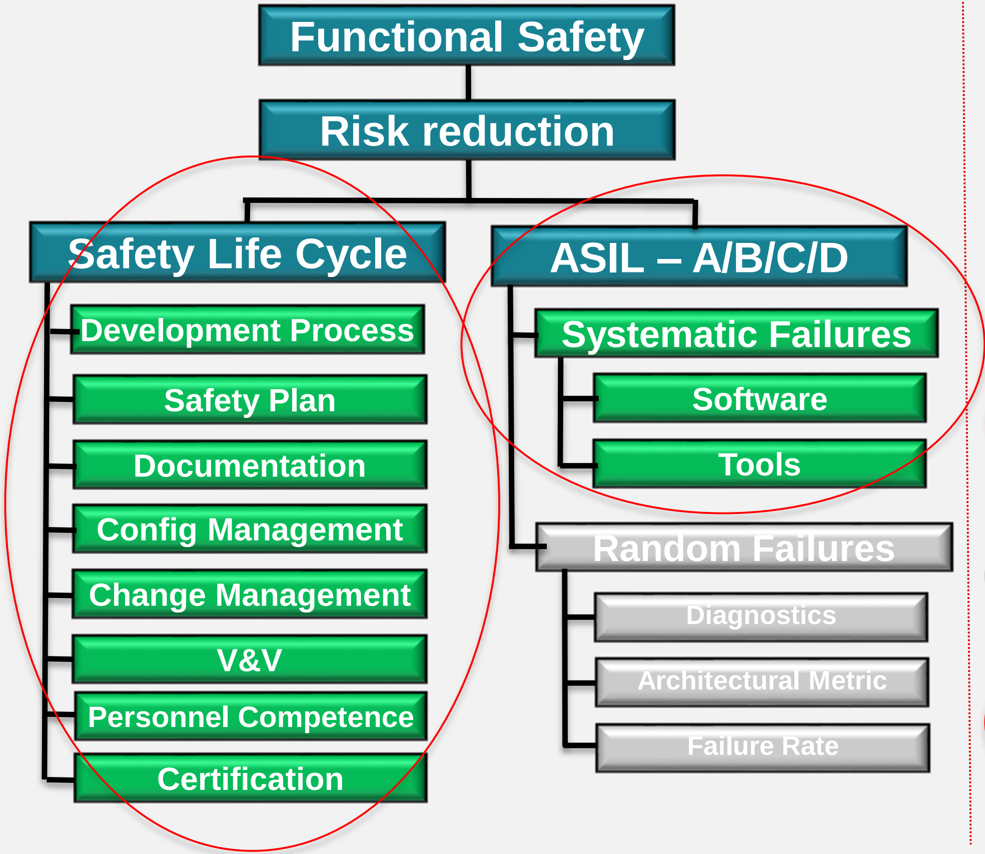
TÜV SÜD Product Service GmbH Zertifizierstelle Ridlerstraße 65 80339 München Germany

Device Certificates

- First devices certified by Exida for IEC 61508 SIL-3 use in 2011
- TÜV-SÜD certified the SafeTI Hardware functional safety development process in 2013 for:
  - ➢ IEC 61508 SIL-3
  - ➢ ISO 26262 ASIL-D
- Hercules MCUs certified for IEC 61508 SIL-3, ISO 26262 ASIL-D:
  - ➢ Hercules MCU Safety Architecture
  - ➢ Device (RM42, RM46x, RM48x)
  - ➢ Device (TMS570LS03x/04x/11x/12x/21x/31x)
- TÜV-Nord certified the SafeTI Software functional safety development process in 2015 for
  - ➢ IEC 61508 SIL-3
  - ➢ ISO 26262 ASIL-D
- TÜV-SÜD concept assessment in 2014 for ISO 13849:
  - ➢ Lockstep MCU + Safety Companion Power Supply

Applying Functional Safety Standards

SafeTI™ Design Packages for Functional Safety



Functional Safety

Risk reduction

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

ASIL – A/B/C/D
- Systematic Failures
  - Software
  - Tools
- Random Failures
  - Diagnostics
  - Architectural Metric
  - Failure Rate

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

Process Certification
Software CSP
Compiler Qual. Kit

CERTIFICATE

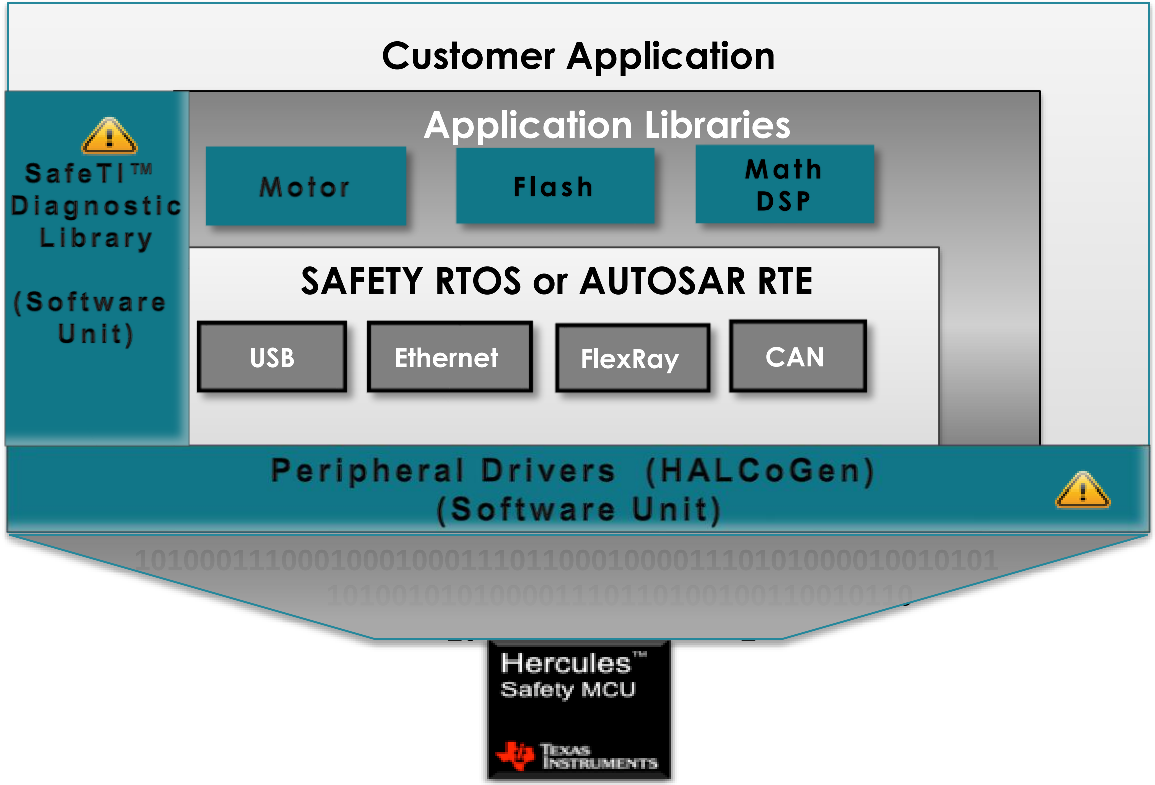
- Development processes
- Supporting processes
- Software development and V&V

CSP = Compliance Support Package

SafeTI Software Framework

SafeTI™ Software Development Process Certified by TÜV NORD meeting ISO 26262 and IEC 61508 requirements

TÜV NORD
TÜV NORD Systems GmbH & Co.KG
Trusted Process
QRAS AP00213
- Safe TI -
Functional Safety Software Development Process
ISO 26262-2:2011, ASIL D
ISO 26262-6:2011, ASIL D
ISO 26262-8:2011, ASIL D
IEC 61508-1:2010, SIL 3
IEC 61508-3:2010, SIL 3
SEBS-A.165253/13

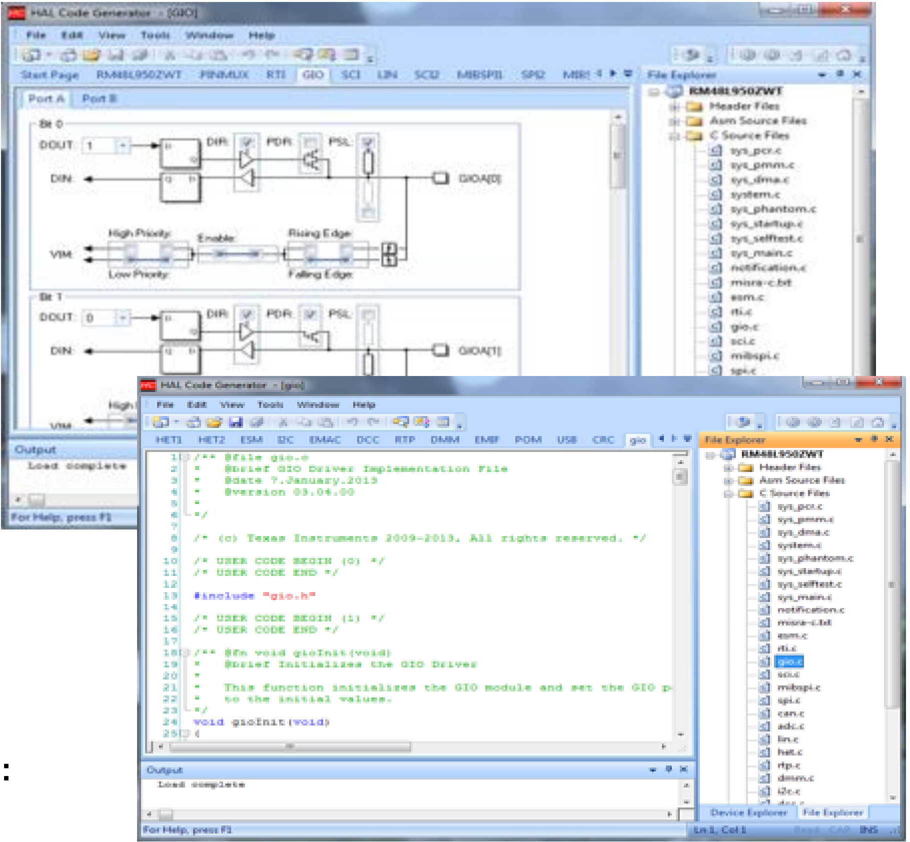


⚠ SafeTI™ Compliance Support Packages Available

HALCoGen - Hardware Abstraction Layer Code Generator

HALCoGen Features

- User Input on High Abstraction Level
- Generates C Source Code for Hercules™ MCU
  - Peripheral Drivers
  - Device Initialization
- Native support for CCS, ARM, IAR and GHS IDEs
- Interactive Help System with example code



```
/** @file gio.c
 *   @brief GIO Driver Implementation File
 *   @date 7.January.2013
 *   @version 03.04.00
 *
 */

/* (c) Texas Instruments 2009-2013, All rights reserved. */

/* USER CODE BEGIN (0) */
/* USER CODE END */

#include "gio.h"

/* USER CODE BEGIN (1) */
/* USER CODE END */

/** @fn void gioInit(void)
 *   @brief Initializes the GIO Driver
 *
 *   This function initializes the GIO module and set the GIO p
 *   to the initial values.
 */
void gioInit(void)
{
```

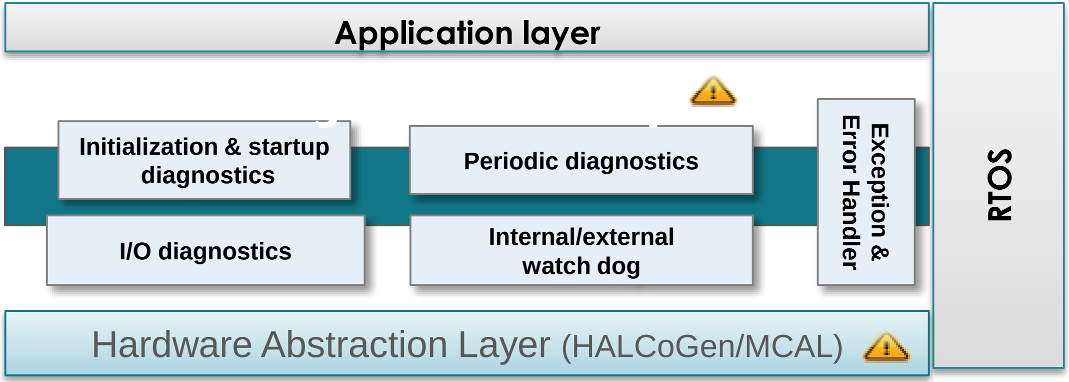
```
Load complete
```

SafeTI™ HALCoGen Compliance Support Package:
www.ti.com/tool/safeti-halcogen-csp

Hercules SafeTI™ Diagnostic Library

Provides simple interfaces and a framework for

- Initializing and Enabling Safety diagnostics/Features prescribed by the Hercules Safety Manual.
- Fault injection to allow testing of application fault handling
- Error Signaling Module (ESM) handler callback routine.
- Profiling for measuring time spent in diagnostic test/fault handling


Application layer
Initialization & startup diagnostics
Periodic diagnostics
I/O diagnostics
Internal/external watch dog
Exception & Error Handler
RTOS
Hardware Abstraction Layer (HALCoGen/MCAL)

Device Partition	Unique Identifier	Safety Feature or Diagnostic	API Name
Cortex-R4F CPU	CPU1	Lockstep compare	SL_SelfTest_CCMR4F
	CPU2A	Boot time execution of LBIST STC	SL_SelfTest_STC
	CPU2B	Periodic execution of LBIST STC	SL_SelfTest_STC
	CPU7	Software readback of written configuration	SL_Read_Compare
Error Signaling	ESM1	Periodic software readback of static configuration registers	SL_Read_Compare
	ESM3	Use of status shadow registers	SL_Init_ResetReason_XInfo
	ESM4	Software readback of written configuration	SL_Read_Compare

Functions map directly to the Hercules Safety Manual

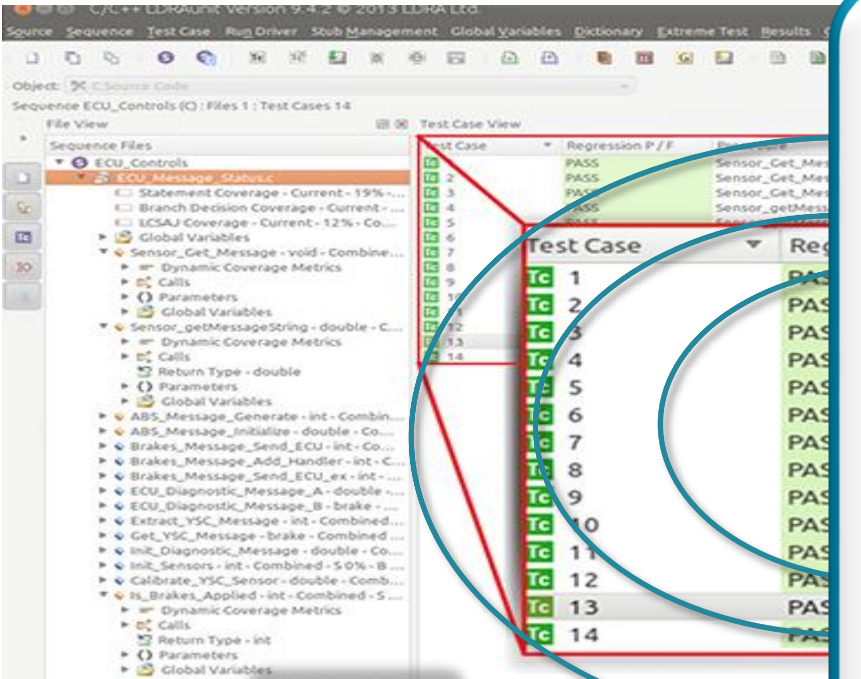
Safety Manual for TMS570LS31x/21x and RM48x Hercules™ ARM® Safety Critical Microcontrollers

User's Guide

SafeTI Compliance Support Package
www.ti.com/tool/safeti-hercules-diag-lib-csp

Texas Instruments

SafeTI™ Compliance Support Package (CSP)



Sequence ECU_Controls (C) : Files 1 : Test Cases 14

- ECU_Controls
  - ECU_Message_Status.c
    - Statement Coverage - Current - 19% -...
    - Branch Decision Coverage - Current - ...
    - LCSAJ Coverage - Current - 12% - Co...
    - Global Variables
    - Sensor_Get_Message - void - Combine...
      - Dynamic Coverage Metrics
      - Calls
      - Parameters
      - Global Variables
    - Sensor_getMessageString - double - C...
      - Dynamic Coverage Metrics
      - Calls
      - Return Type - double
      - Parameters
      - Global Variables
    - ABS_Message_Generate - int - Combin...
    - ABS_Message_Initialize - double - Co...
    - Brakes_Message_Send_ECU - int - Co...
    - Brakes_Message_Add_Handler - int - C...
    - Brakes_Message_Send_ECU_ex - int - ...
    - ECU_Diagnostic_Message_A - double -...
    - ECU_Diagnostic_Message_B - brake - ...
    - Extract_YSC_Message - int - Combined...
    - Get_YSC_Message - brake - Combined ...
    - Init_Diagnostic_Message - double - Co...
    - Init_Sensors - int - Combined - 50% - B ...
    - Calibrate_YSC_Sensor - double - Comb...
    - Is_Brakes_Applied - int - Combined - S ...
      - Dynamic Coverage Metrics
      - Calls
      - Return Type - int
      - Parameters
      - Global Variables
    - main - int - Combine

Test Case	Regression P / F	Procedure
1	PASS	Sensor_Get_Mes
2	PASS	Sensor_Get_Mes
3	PASS	Sensor_Get_Mes
4	PASS	Sensor_getMess
5	PASS	
6	PAS	
7	PAS	
8	PAS	
9	PAS	
10	PAS	
11	PAS	
12	PAS	
13	PAS	
14	PAS	

ISO 26262

IEC 61508

- Assists customers using Hercules software components to comply to functional safety standards
- SafeTI software development process certified by TUV NORD to IEC 61508 and ISO 26262
- CSPs Include:
  - Documentation:
    - Safety Requirements
    - Safety Manual
    - Static and Dynamic test results
    - Code coverage reports
    - MISRA-C results
    - Traceability report
  - Unit Test Capability:
    - TI unit level test cases
    - Test Automation Unit (TAU) based on LDRAunit®
- Available NOW! for HALCoGen and SafeTI Hercules Diagnostic Library
  - www.ti.com/tool/safeti-halcogen-csp
  - www.ti.com/tool/safeti-hercules-diag-lib-csp
  - Customers can download the demo or submit request for production version

TÜV NORD

LDRA

SafeTI Compliance Support Packages available now!

Texas Instruments

SafeTI™ Compiler Qualification Kit

Use Case Definition for qualification in Tool Chain Analyzer

Define your use-case for qualification: Enter use-case name and select used tool features of Tool Chain Analyzer

Use Case TCA with 1 Feature 1 Error 7 Tests

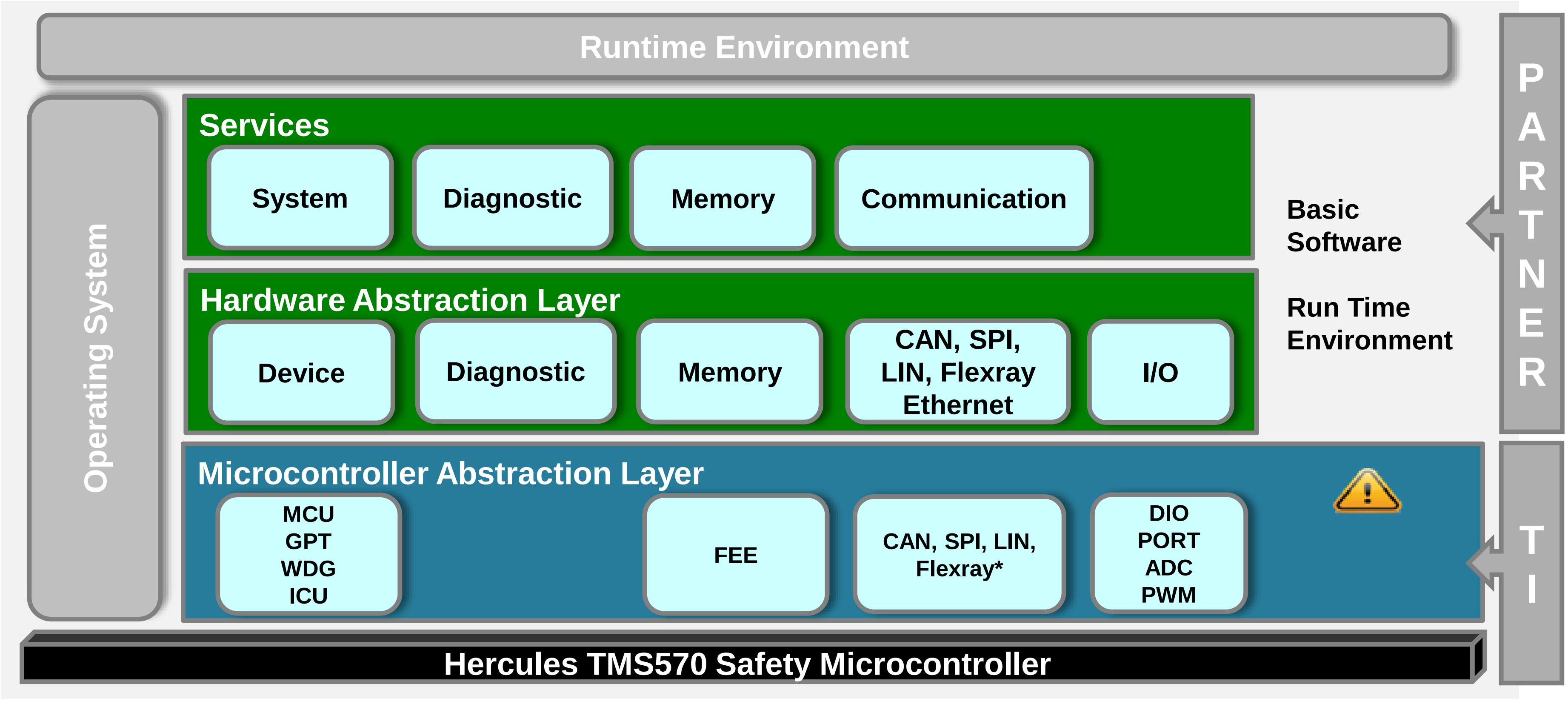
http://www.ti.com/tool/safeti_cqkit

- Assists in qualifying TI C/C++ Compiler s to functional safety standards
- Flexible integration into development processes due to the model-based qualification method
- 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
  - Solid Sands SuperTest^{TM} qualification suite
  - TI compiler validation test cases
  - Test Automation Unit (TAU)
  - 24hrs of Validas consulting services
  - TÜV Nord assessment report

Approved by

TÜV NORD

Hercules TMS570 AUTOSAR v4.0 rev3 Support



Runtime Environment

Operating System

Services

System

Diagnostic

Memory

Communication

Hardware Abstraction Layer

Device

Diagnostic

Memory

CAN, SPI,
LIN, Flexray
Ethernet

I/O

Microcontroller Abstraction Layer

MCU
GPT
WDG
ICU

FEE

CAN, SPI, LIN,
Flexray*

DIO
PORT
ADC
PWM

Hercules TMS570 Safety Microcontroller

Basic
Software

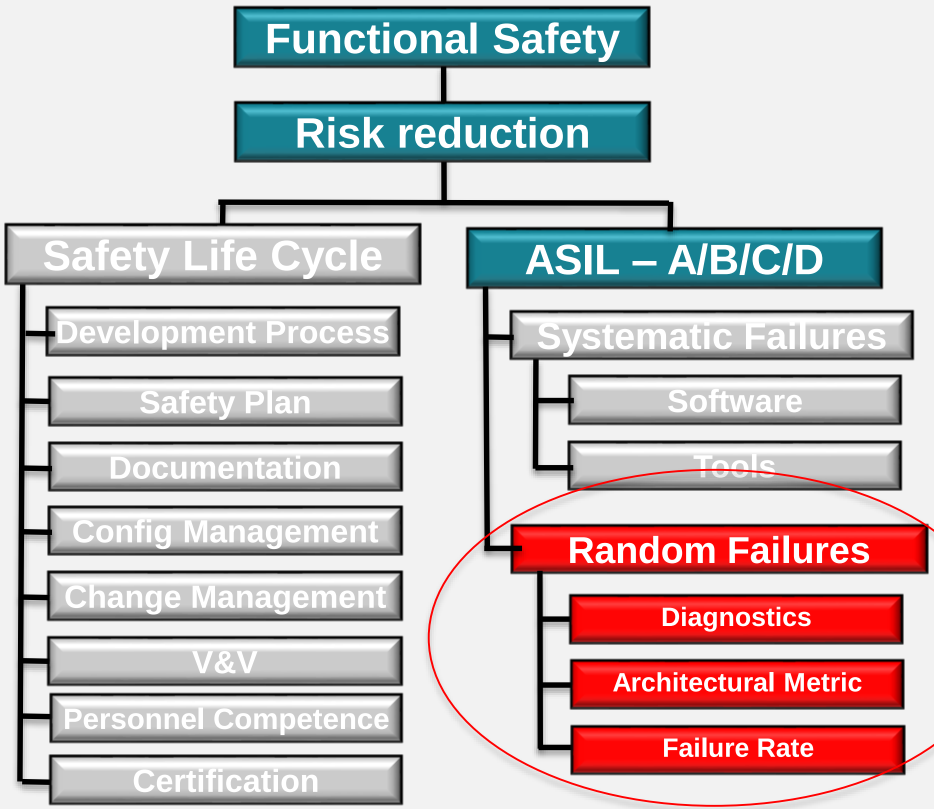
Run Time
Environment

PARTNER

TI

*From partner

Applying Functional Safety Standards



- Functional Safety
  - Risk reduction
    - Safety Life Cycle
      - Development Process
      - Safety Plan
      - Documentation
      - Config Management
      - Change Management
      - V&V
      - Personnel Competence
      - Certification
    - ASIL – A/B/C/D
      - Systematic Failures
        - Software
        - Tools
      - Random Failures
        - Diagnostics
        - Architectural Metric
        - Failure Rate

SafeTI™ Design Packages for Functional Safety

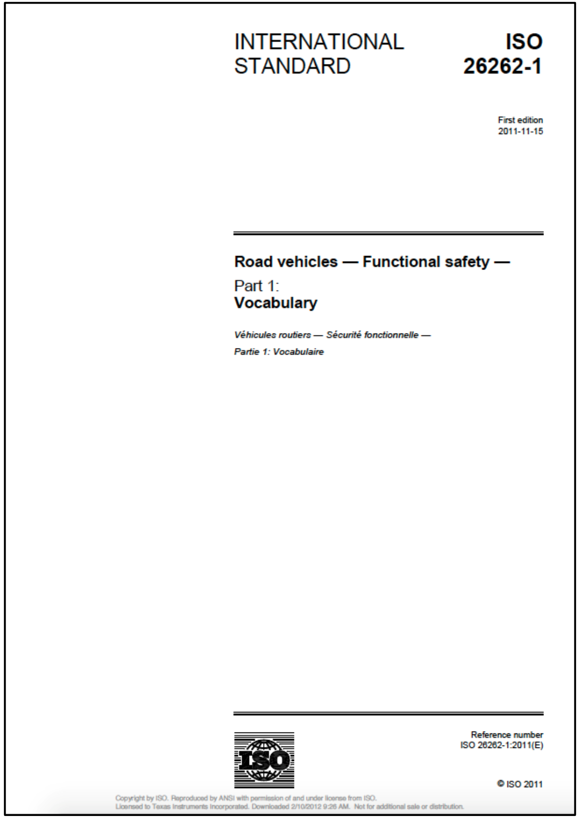
SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

- How to manage MCU hardware random failures
- How to estimate failure rate vs ASIL requirements

Hercules™ Architecture (FMEDA)

CSP = Compliance Support Package

ISO 26262 - Management of Random Failures



INTERNATIONAL STANDARD

ISO 26262-1

First edition
2011-11-15

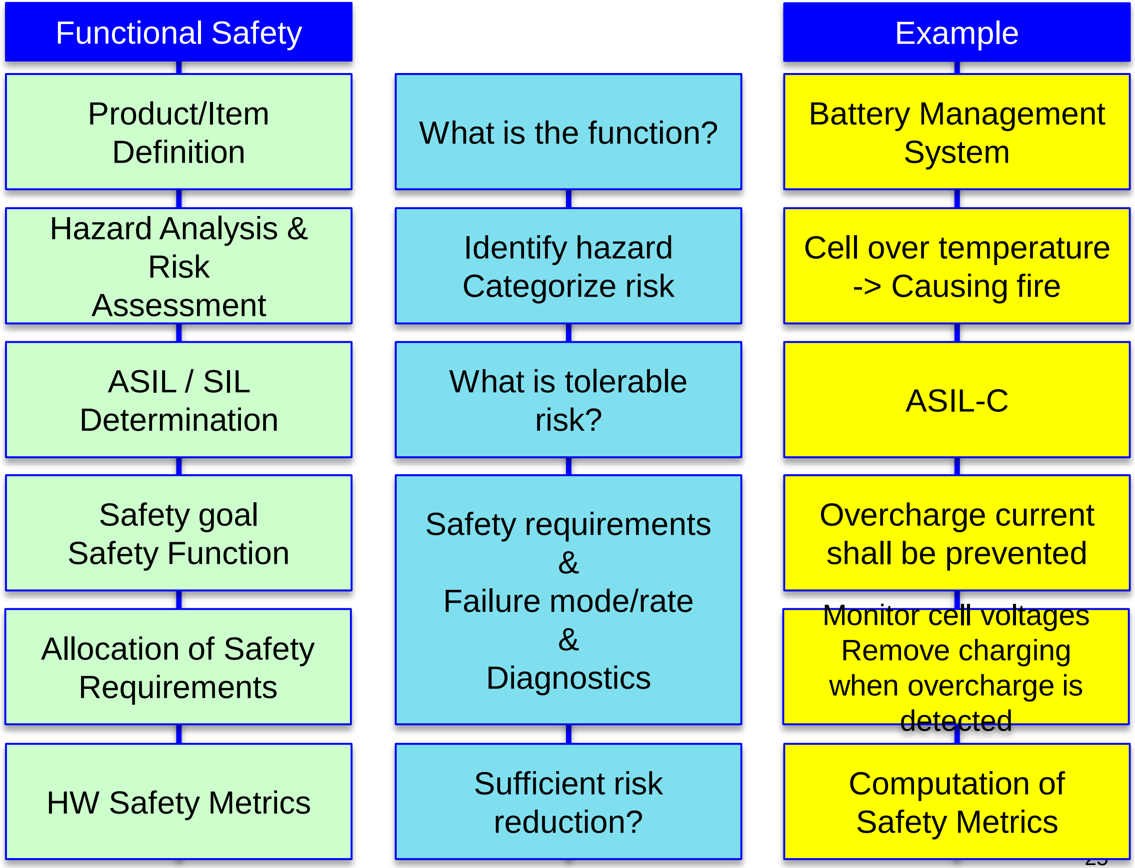
Road vehicles — Functional safety —

Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2011(E)

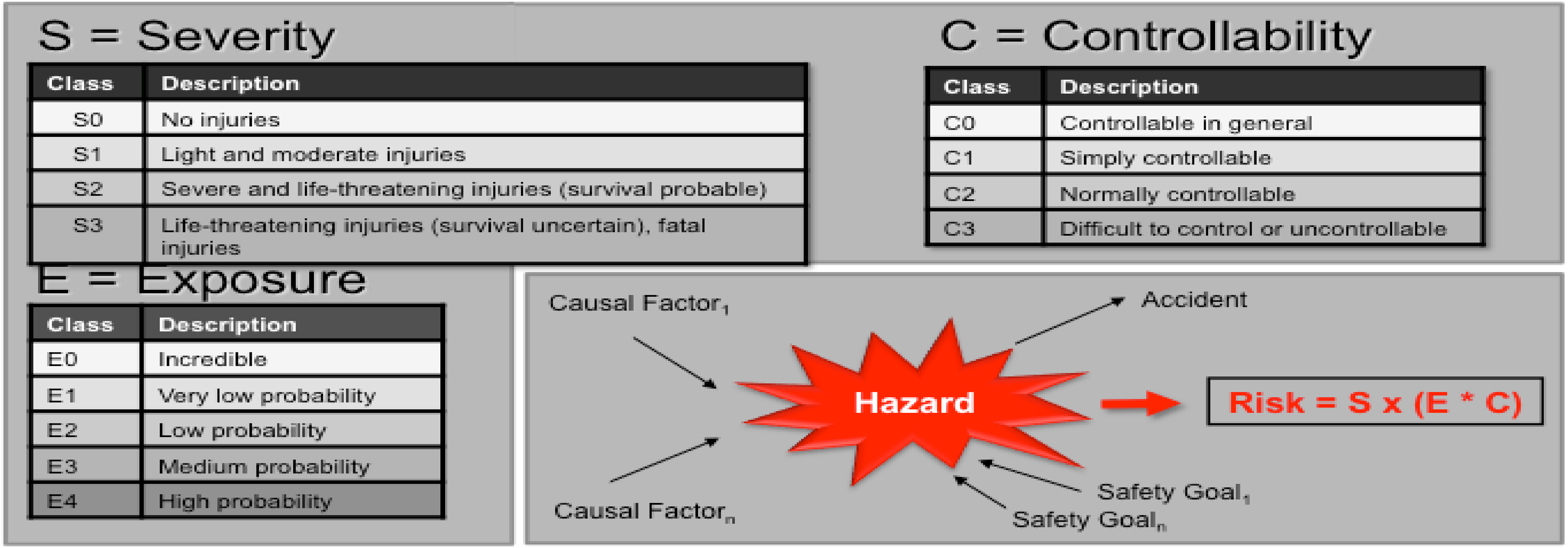
© ISO 2011



Functional Safety		Example
Product/Item Definition	What is the function?	Battery Management System
Hazard Analysis & Risk Assessment	Identify hazard Categorize risk	Cell over temperature -> Causing fire
ASIL / SIL Determination	What is tolerable risk?	ASIL-C
Safety goal Safety Function	Safety requirements & Failure mode/rate & Diagnostics	Overcharge current shall be prevented
Allocation of Safety Requirements		Monitor cell voltages Remove charging when overcharge is detected
HW Safety Metrics	Sufficient risk reduction?	Computation of Safety Metrics

Determining ISO 26262 ASIL Level

- To determine the ASIL level of a system a Risk Assessment must be performed for all Hazards identified.
- Risk is comprised if three components: **Severity, Exposure & Controllability**



S = Severity

Class	Description
S0	No injuries
S1	Light and moderate injuries
S2	Severe and life-threatening injuries (survival probable)
S3	Life-threatening injuries (survival uncertain), fatal injuries

C = Controllability

Class	Description
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

E = Exposure

Class	Description
E0	Incredible
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

Risk = S x (E * C)

ASIL Determination Table

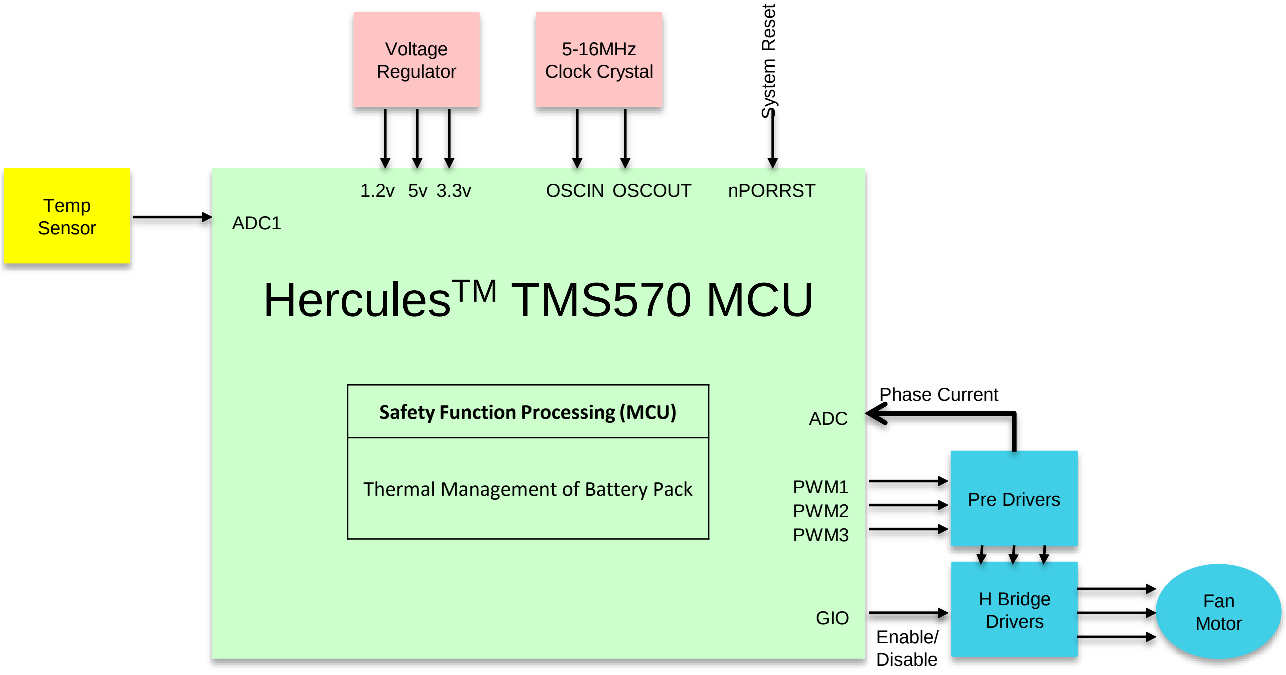
Risk = Severity x (Exposure * Controllability)

		Controllability		
Severity	Exposure	C1Simply	C2 Normal	C3 Difficult
S1 Light and moderate injuries	E1 Very Low	QM	QM	QM
	E2			QM
	E3			ASIL A
	E4			ASIL B
S2 Severe and life-threatening injuries (survival probable)	E1 Very Low	QM	QM	QM
	E2 Low	QM	QM	ASIL A
	E3 Medium	QM	ASIL A	ASIL B
	E4 High	ASIL A	ASIL B	ASIL C
S3 Life-threatening injuries (survival uncertain), fatal injuries	E1 Very Low	QM	QM	ASIL A
	E2 Low	QM	ASIL A	ASIL B
	E3 Medium	ASIL A	ASIL B	ASIL C
	E4 High	ASIL B	ASIL C	ASIL D

Overcharge current -> Over temperature -> Smoke/Fire
Severity: Life threatening injury (S2)
Exposure: City road or highway high probability (E4)
Controllability: difficult for driver to control (C3)

Application Example

BMS Function: Manage battery cell charging status and thermal management of battery pack

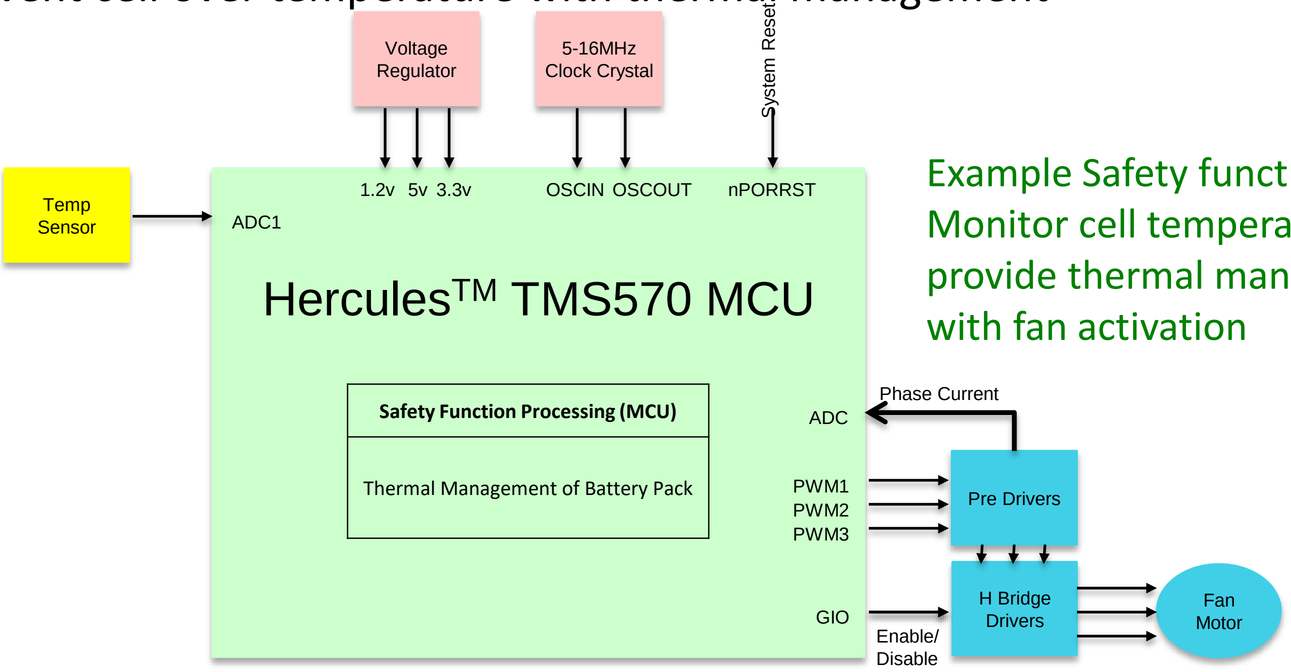


Simplified diagram for illustration purpose only

Application Example

Hazard: Cell over temperature-> Risk: Fire-> ASIL-C

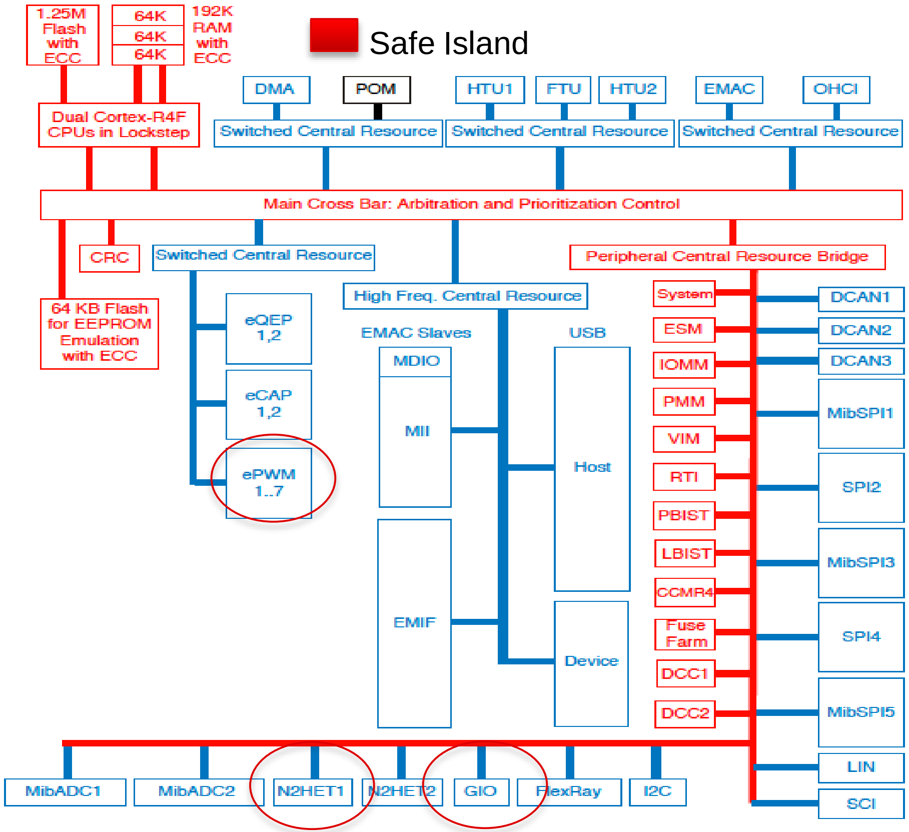
Safety Goal: Prevent cell over temperature with thermal management



Example Safety function: Monitor cell temperature and provide thermal management with fan activation

Simplified diagram for illustration purpose only

MCU Safety Critical Elements per Safety Function



- Safety Critical Elements are elements within MCU the implement the safety function

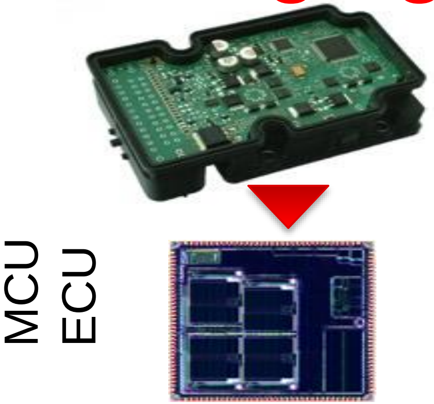
- Diagnostics are necessary to detect safety related failures

- Sufficient diagnostics coverage (DC) is needed to meet required IEC 26262 HW metrics per ASIL level

- In this example, safety critical elements are: Safe Island, ADC, PWM, GIO

Simplified diagram for illustration purpose only

Managing Hardware Random Failures

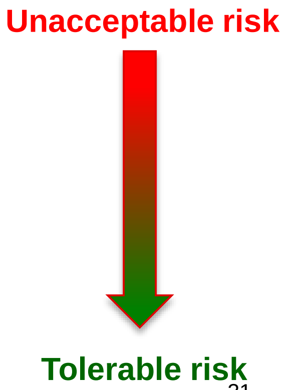


- Millions of transistors, metal lines, resistors, capacitors..
- Each component could fail (permanent and/or transient)
- A component failure could lead to a system failure

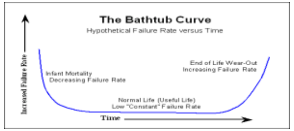
- Failure rate is measured in **F**ailure **I**n **T**ime (FIT)
- 1 FIT is 1 fail in 10^9 operating hours
- Assuming 1 million cars on the road with 4 driving hours per day per car on average:
  - 100 FIT => ~150 failures per year

ASIL	SPFM	PMHF (FIT)
ASIL B	>90%	<100
ASIL C	>97%	<100
ASIL D	>99%	<10

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

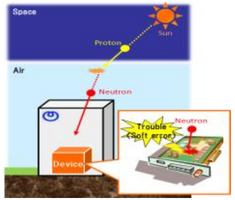


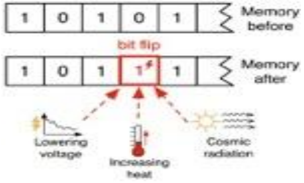
MCU Failure Mode and Failure Rate



- **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^{TM} MCU safety diagnostic features

🟥 Safe Island Hardware diagnostics

🟦 Blended HW diagnostics

⬛ Non Safety Critical Functions

CPU Self Test Controller requires little S/W overhead

Physical design optimized to reduce probability of common cause failure

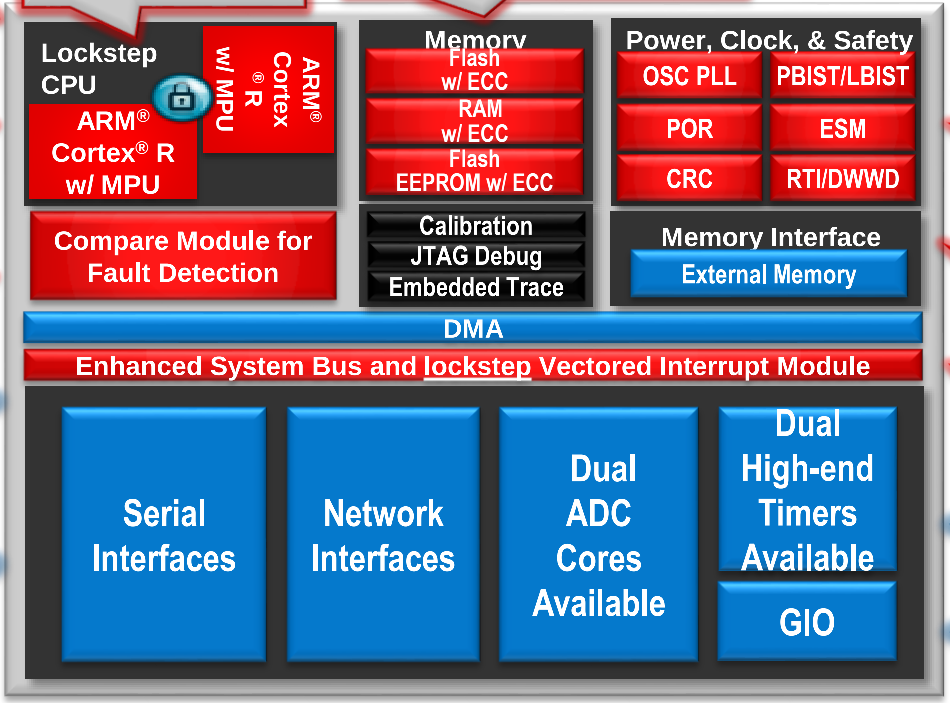
Lockstep CPU & **Lockstep Interrupt Fault Detection**

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

Parity or CRC in Serial and Network Communication Peripherals

Memory Protection Unit

ECC for flash / RAM evaluated inside the Cortex R



Lockstep CPU

ARM® Cortex® R w/ MPU

ARM® Cortex® R w/ MPU

Compare Module for Fault Detection

Memory

Flash w/ ECC

RAM w/ ECC

Flash EEPROM w/ ECC

Calibration

JTAG Debug

Embedded Trace

Power, Clock, & Safety

OSC PLL

PBIST/LBIST

POR

ESM

CRC

RTI/DWWD

Memory Interface

External Memory

DMA

Enhanced System Bus and lockstep Vectored Interrupt Module

Serial Interfaces

Network Interfaces

Dual ADC Cores Available

Dual High-end Timers Available

GIO

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

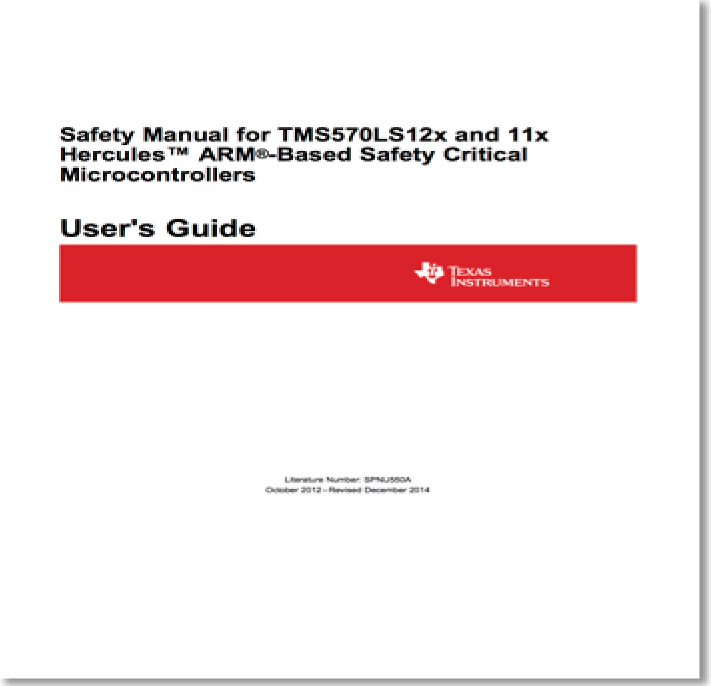
IO Loop Back, ADC Self Test, …

Dual ADC Cores with shared channels

Bold items are introduced with the new Cortex®-R5 devices

How to implement Applicable Diagnostics?

Hercules^{TM} Safety Manual



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

User's Guide

Literature Number: SPNU550A
October 2012 – Revised December 2014

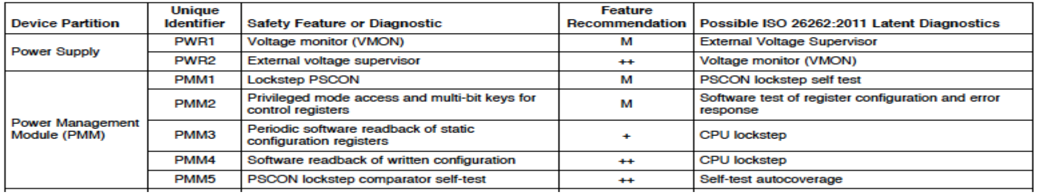


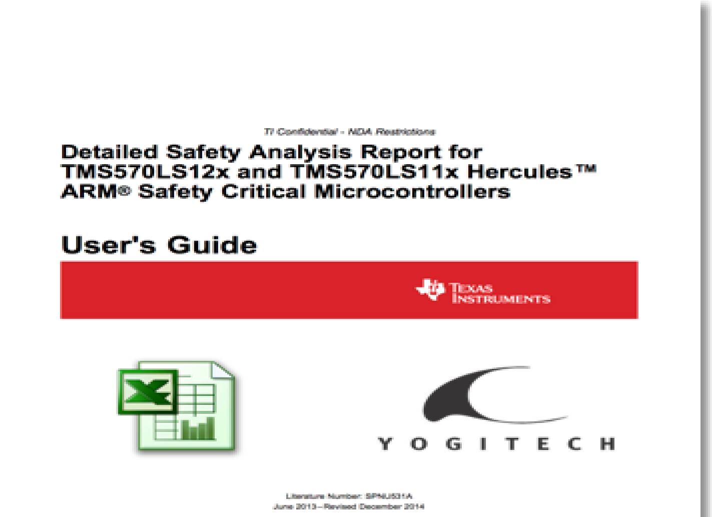
Table 2. Summary of Safety Features and Diagnostics

Device Partition	Unique Identifier	Safety Feature or Diagnostic	Feature Recommendation	Possible ISO 26262:2011 Latent Diagnostics
Power Supply	PWR1	Voltage monitor (VMON)	M	External Voltage Supervisor
	PWR2	External voltage supervisor	++	Voltage monitor (VMON)
Power Management Module (PMM)	PMM1	Lockstep PSCON	M	PSCON lockstep self test
	PMM2	Privileged mode access and multi-bit keys for control registers	M	Software test of register configuration and error response
	PMM3	Periodic software readback of static configuration registers	+	CPU lockstep
	PMM4	Software readback of written configuration	++	CPU lockstep
	PMM5	PSCON lockstep comparator self-test	++	Self-test autocoverage

- 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 Safe Island, SPI, ADC …

TMS570LS12x Safety manual spnu550a

Detailed Safety Analysis Report & FMEDA worksheet



TI Confidential - NDA Restrictions

Detailed Safety Analysis Report for TMS570LS12x and TMS570LS11x Hercules™ ARM® Safety Critical Microcontrollers

User's Guide

Literature Number: SPNU531A
June 2013–Revised December 2014

- 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

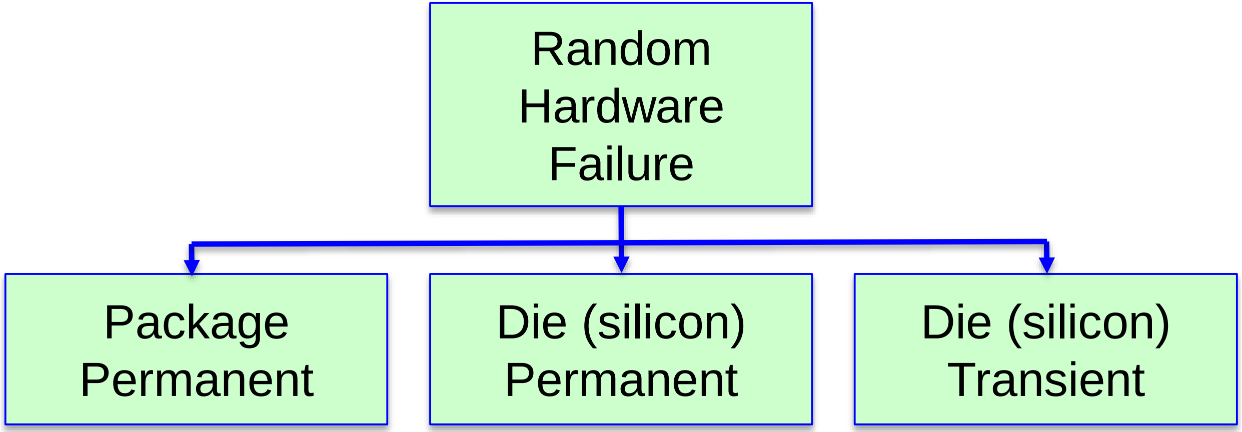
Available under NDA

TMS570LS12x Detailed Analysis Report spnu531a

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.

ISO 26262 HW Metrics Calculation Failure Rate / Mission Profiles

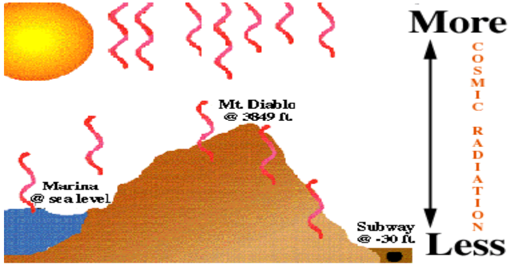


Random Hardware Failure

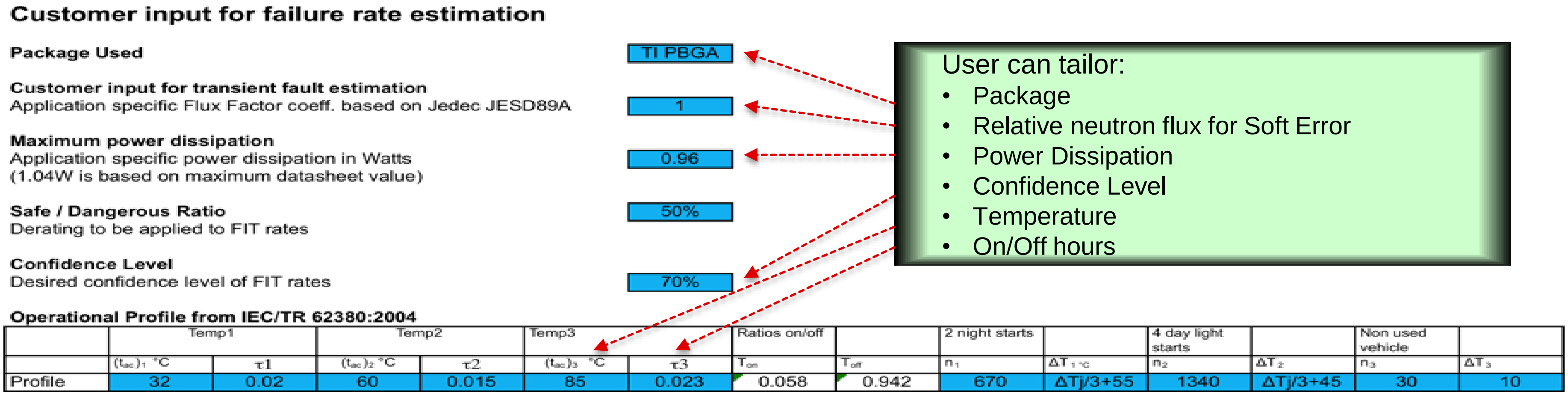
Package Permanent

Die (silicon) Permanent

Die (silicon) Transient



ISO 26262/IEC61508 HW Metrics Calculation Mission Profiles



Customer input for failure rate estimation

Package Used — 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
(1.04W is based on maximum datasheet value) — 0.96

Safe / Dangerous Ratio
Derating to be applied to FIT rates — 50%

Confidence Level
Desired confidence level of FIT rates — 70%

Operational Profile from IEC/TR 62380:2004

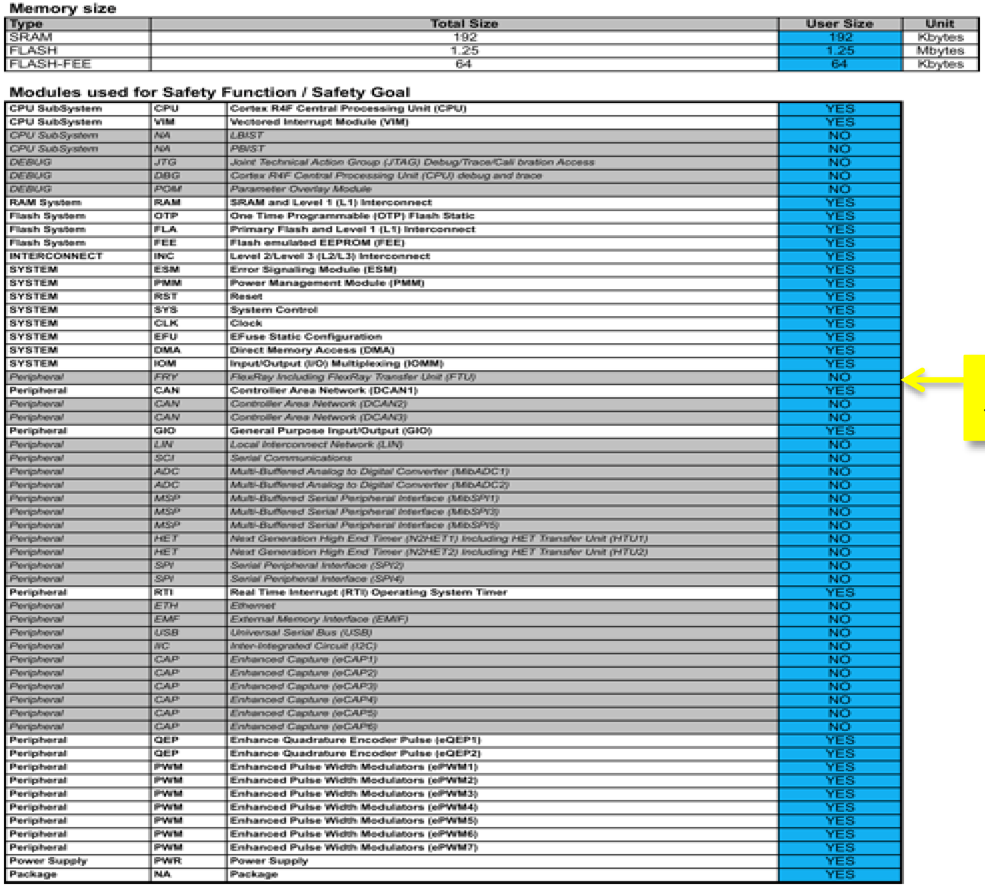
	Temp1		Temp2		Temp3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
	$(t_{ac})_1$ °C	τ1	$(t_{ac})_2$ °C	τ2	$(t_{ac})_3$ °C	τ3	T_{on}	T_{off}	n_1	ΔT_1 °C	n_2	ΔT_2	n_3	ΔT_3
Profile	32	0.02	60	0.015	85	0.023	0.058	0.942	670	ΔTj/3+55	1340	ΔTj/3+45	30	10

User can tailor:
- Package
- Relative neutron flux for Soft Error
- Power Dissipation
- Confidence Level
- Temperature
- On/Off hours

- 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



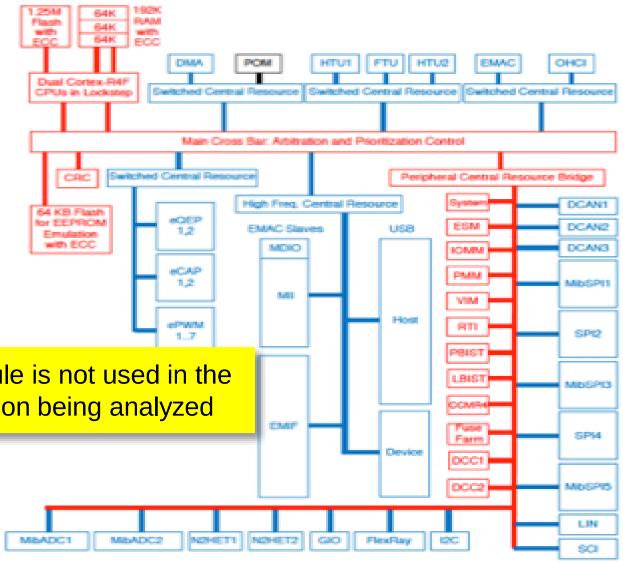
Memory size

Type	Total Size	User Size	Unit
SRAM	192	192	Kbytes
FLASH	1.25	1.25	Mbytes
FLASH-FEE	64	64	Kbytes

Modules used for Safety Function / Safety Goal

CPU SubSystem	CPU	Cortex R4F Central Processing Unit (CPU)	YES
CPU SubSystem	VIM	Vectored Interrupt Module (VIM)	YES
CPU SubSystem	*NA*	*LBIST*	NO
CPU SubSystem	*NA*	*PBIST*	NO
DEBUG	*JTG*	*Joint Technical Action Group (JTAG) Debug/Trace/Cali bration Access*	NO
DEBUG	*DBG*	*Cortex R4F Central Processing Unit (CPU) debug and trace*	NO
DEBUG	*POM*	*Parameter Overlay Module*	NO
RAM System	RAM	SRAM and Level 1 (L1) Interconnect	YES
Flash System	OTP	One Time Programmable (OTP) Flash Static	YES
Flash System	FLA	Primary Flash and Level 1 (L1) Interconnect	YES
Flash System	FEE	Flash emulated EEPROM (FEE)	YES
INTERCONNECT	INC	Level 2/Level 3 (L2/L3) Interconnect	YES
SYSTEM	ESM	Error Signaling Module (ESM)	YES
SYSTEM	PMM	Power Management Module (PMM)	YES
SYSTEM	RST	Reset	YES
SYSTEM	SYS	System Control	YES
SYSTEM	CLK	Clock	YES
SYSTEM	EFU	EFuse Static Configuration	YES
SYSTEM	DMA	Direct Memory Access (DMA)	YES
SYSTEM	IOM	Input/Output (I/O) Multiplexing (IOMM)	YES
Peripheral	*FRY*	*FlexRay Including FlexRay Transfer Unit (FTU)*	NO
Peripheral	CAN	Controller Area Network (DCAN1)	YES
Peripheral	*CAN*	*Controller Area Network (DCAN2)*	NO
Peripheral	*CAN*	*Controller Area Network (DCAN3)*	NO
Peripheral	GIO	General Purpose Input/Output (GIO)	YES
Peripheral	*LIN*	*Local Interconnect Network (LIN)*	NO
Peripheral	*SCI*	*Serial Communications*	NO
Peripheral	*ADC*	*Multi-Buffered Analog to Digital Converter (MibADC1)*	NO
Peripheral	*ADC*	*Multi-Buffered Analog to Digital Converter (MibADC2)*	NO
Peripheral	*MSP*	*Multi-Buffered Serial Peripheral Interface (MibSPI1)*	NO
Peripheral	*MSP*	*Multi-Buffered Serial Peripheral Interface (MibSPI3)*	NO
Peripheral	*MSP*	*Multi-Buffered Serial Peripheral Interface (MibSPI5)*	NO
Peripheral	*HET*	*Next Generation High End Timer (N2HET1) Including HET Transfer Unit (HTU1)*	NO
Peripheral	*HET*	*Next Generation High End Timer (N2HET2) Including HET Transfer Unit (HTU2)*	NO
Peripheral	*SPI*	*Serial Peripheral Interface (SPI2)*	NO
Peripheral	*SPI*	*Serial Peripheral Interface (SPI4)*	NO
Peripheral	RTI	Real Time Interrupt (RTI) Operating System Timer	YES
Peripheral	*ETH*	*Ethernet*	NO
Peripheral	*EMF*	*External Memory Interface (EMIF)*	NO
Peripheral	*USB*	*Universal Serial Bus (USB)*	NO
Peripheral	*IIC*	*Inter-Integrated Circuit (I2C)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP1)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP2)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP3)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP4)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP5)*	NO
Peripheral	*CAP*	*Enhanced Capture (eCAP6)*	NO
Peripheral	QEP	Enhance Quadrature Encoder Pulse (eQEP1)	YES
Peripheral	QEP	Enhance Quadrature Encoder Pulse (eQEP2)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM1)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM2)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM3)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM4)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM5)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM6)	YES
Peripheral	PWM	Enhanced Pulse Width Modulators (ePWM7)	YES
Power Supply	PWR	Power Supply	YES
Package	NA	Package	YES

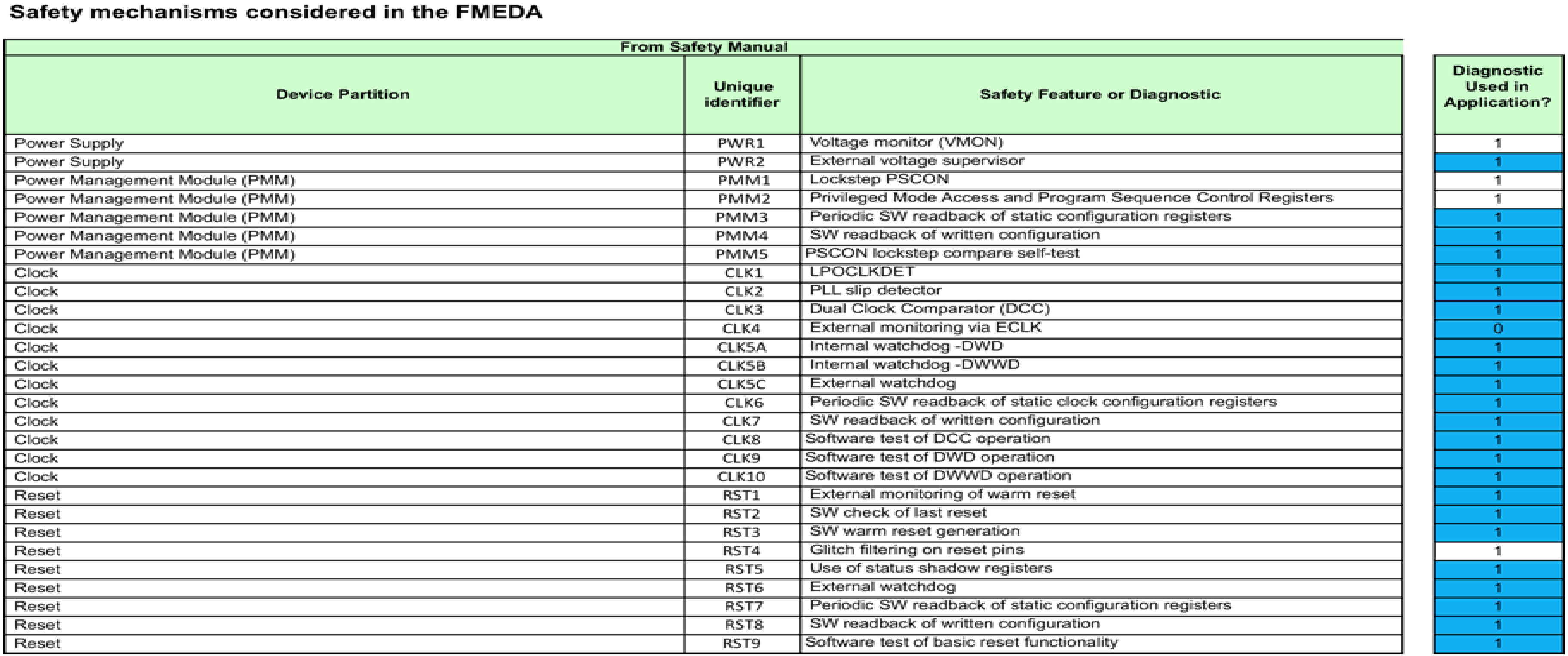
Module is not used in the function being analyzed


1.25M Flash with ECC
64K
64K
64K
192K RAM with ECC
DMA
POM
HTU1
FTU
HTU2
EMAC
OHCI
Dual Cortex-R4F CPUs in Lockstep
Switched Central Resource
Switched Central Resource
Switched Central Resource
Main Cross Bar: Arbitration and Prioritization Control
CRC
Switched Central Resource
Peripheral Central Resource Bridge
64 KB Flash for EEPROM Emulation with ECC
High Freq. Central Resource
eQEP 1,2
eCAP 1,2
ePWM 1..7
EMAC Slaves
MDIO
MII
EMIF
USB
Host
Device
System
ESM
IOMM
PMM
VIM
RTI
PBIST
LBIST
CCMR4
Fuse Farm
DCC1
DCC2
DCAN1
DCAN2
DCAN3
MibSPI1
SPI2
MibSPI3
SPI4
MibSPI5
LIN
SCI
MibADC1
MibADC2
N2HET1
N2HET2
GIO
FlexRay
I2C

- 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

FMEDA worksheet – Safety Mechanisms Tailoring



Safety mechanisms considered in the FMEDA

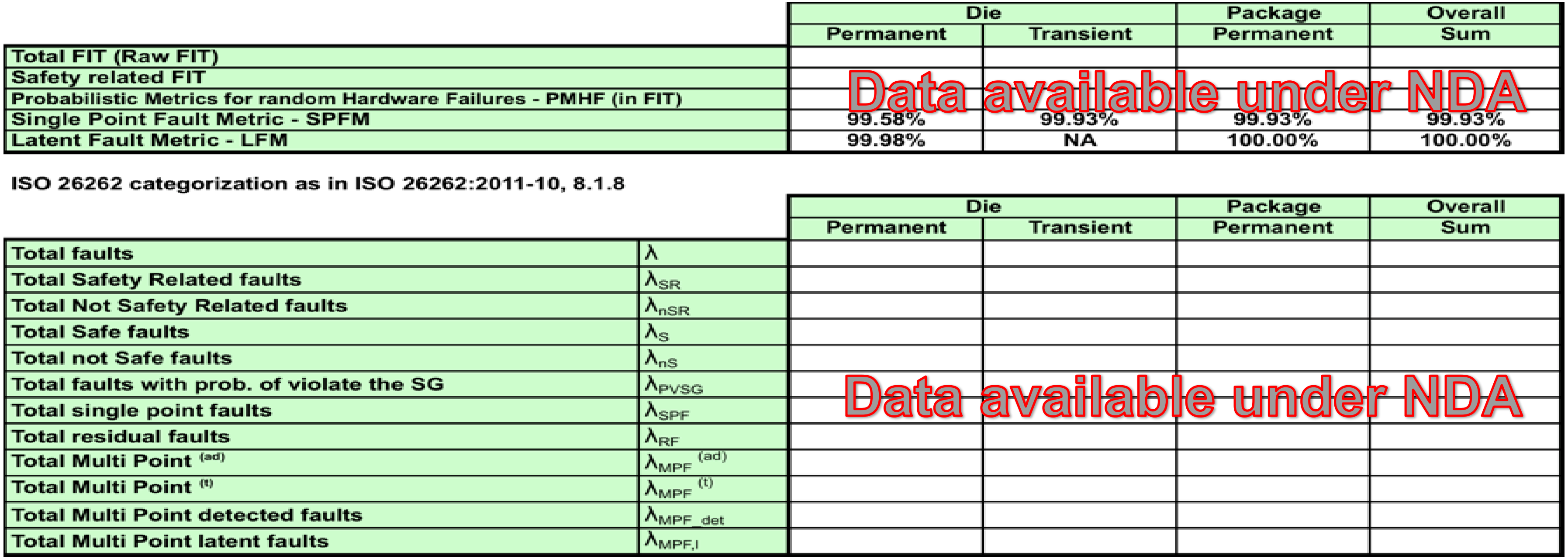
From Safety Manual			
Device Partition	Unique identifier	Safety Feature or Diagnostic	Diagnostic Used in Application?
Power Supply	PWR1	Voltage monitor (VMON)	1
Power Supply	PWR2	External voltage supervisor	1
Power Management Module (PMM)	PMM1	Lockstep PSCON	1
Power Management Module (PMM)	PMM2	Privileged Mode Access and Program Sequence Control Registers	1
Power Management Module (PMM)	PMM3	Periodic SW readback of static configuration registers	1
Power Management Module (PMM)	PMM4	SW readback of written configuration	1
Power Management Module (PMM)	PMM5	PSCON lockstep compare self-test	1
Clock	CLK1	LPOCLKDET	1
Clock	CLK2	PLL slip detector	1
Clock	CLK3	Dual Clock Comparator (DCC)	1
Clock	CLK4	External monitoring via ECLK	0
Clock	CLK5A	Internal watchdog -DWD	1
Clock	CLK5B	Internal watchdog -DWWD	1
Clock	CLK5C	External watchdog	1
Clock	CLK6	Periodic SW readback of static clock configuration registers	1
Clock	CLK7	SW readback of written configuration	1
Clock	CLK8	Software test of DCC operation	1
Clock	CLK9	Software test of DWD operation	1
Clock	CLK10	Software test of DWWD operation	1
Reset	RST1	External monitoring of warm reset	1
Reset	RST2	SW check of last reset	1
Reset	RST3	SW warm reset generation	1
Reset	RST4	Glitch filtering on reset pins	1
Reset	RST5	Use of status shadow registers	1
Reset	RST6	External watchdog	1
Reset	RST7	Periodic SW readback of static configuration registers	1
Reset	RST8	SW readback of written configuration	1
Reset	RST9	Software test of basic reset functionality	1

- 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:



	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)				
Safety related FIT				
Probabilistic Metrics for random Hardware Failures - PMHF (in FIT)				
Single Point Fault Metric - SPFM	99.58%	99.93%	99.93%	99.93%
Latent Fault Metric - LFM	99.98%	NA	100.00%	100.00%

Data available under NDA

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

		Die		Package	Overall
		Permanent	Transient	Permanent	Sum
Total faults	λ				
Total Safety Related faults	λ_{SR}				
Total Not Safety Related faults	λ_{nSR}				
Total Safe faults	λ_{S}				
Total not Safe faults	λ_{nS}				
Total faults with prob. of violate the SG	λ_{PVSG}				
Total single point faults	λ_{SPF}				
Total residual faults	λ_{RF}				
Total Multi Point $^{(ad)}$	λ_{MPF} $^{(ad)}$				
Total Multi Point $^{(t)}$	λ_{MPF} $^{(t)}$				
Total Multi Point detected faults	λ_{MPF_det}				
Total Multi Point latent faults	$\lambda_{MPF,l}$				

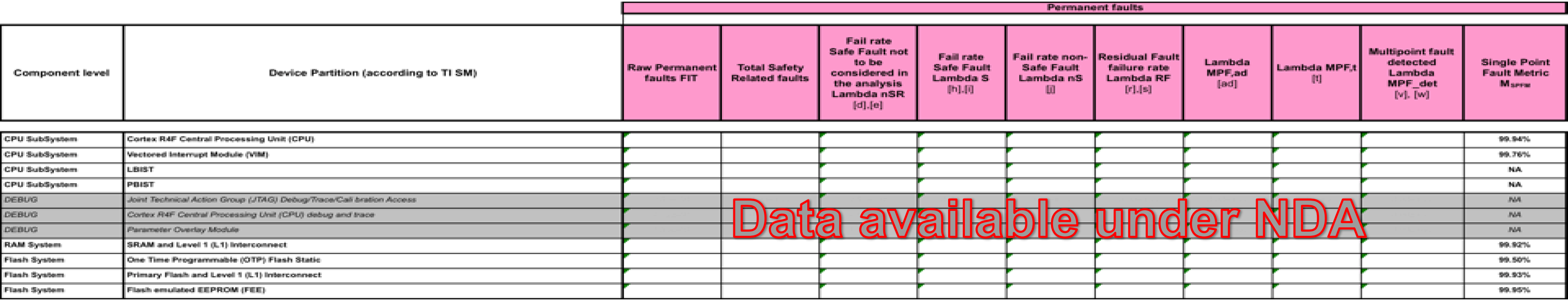
Data available under NDA

FMEDA worksheet is available under NDA

Based on TMS570LS12x v1.0 FMEDA worksheet

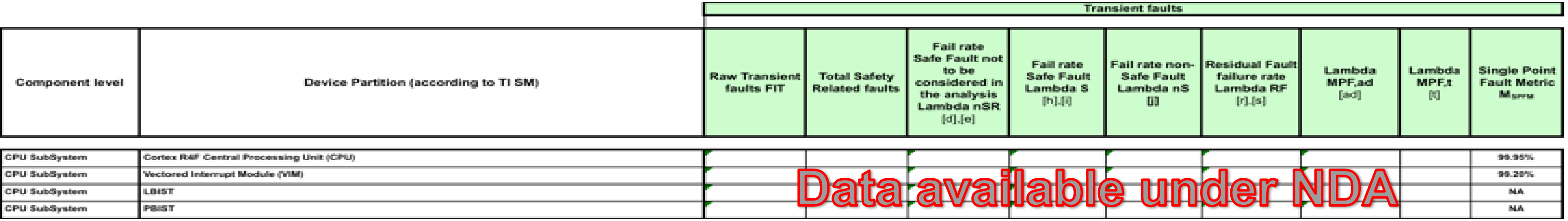
FMEDA worksheet – Metrics Summary / Details

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



		Permanent faults									
Component level	Device Partition (according to TI SM)	Raw Permanent faults FIT	Total Safety Related faults	Fail rate Safe Fault not to be considered in the analysis Lambda nSR [d].[e]	Fail rate Safe Fault Lambda S [h].[i]	Fail rate non-Safe Fault Lambda nS [j]	Residual Fault failure rate Lambda RF [r].[s]	Lambda MPF,ad [ad]	Lambda MPF,t [t]	Multipoint fault detected Lambda MPF_det [v]. [w]	Single Point Fault Metric M_{SPFM}
CPU SubSystem	Cortex R4F Central Processing Unit (CPU)										99.94%
CPU SubSystem	Vectored Interrupt Module (VIM)										99.76%
CPU SubSystem	LBIST										NA
CPU SubSystem	PBIST										NA
DEBUG	*Joint Technical Action Group (JTAG) Debug/Trace/Cali bration Access*										NA
DEBUG	*Cortex R4F Central Processing Unit (CPU) debug and trace*										NA
DEBUG	*Parameter Overlay Module*										NA
RAM System	SRAM and Level 1 (L1) Interconnect										99.92%
Flash System	One Time Programmable (OTP) Flash Static										99.50%
Flash System	Primary Flash and Level 1 (L1) Interconnect										99.93%
Flash System	Flash emulated EEPROM (FEE)										99.95%

Data available under NDA



		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 nSR [d].[e]	Fail rate Safe Fault Lambda S [h].[i]	Fail rate non-Safe Fault Lambda nS [j]	Residual Fault failure rate Lambda RF [r].[s]	Lambda MPF,ad [ad]	Lambda MPF,t [t]	Single Point Fault Metric M_{SPFM}
CPU SubSystem	Cortex R4F Central Processing Unit (CPU)									99.95%
CPU SubSystem	Vectored Interrupt Module (VIM)									99.20%
CPU SubSystem	LBIST									NA
CPU SubSystem	PBIST									NA

Data available under NDA

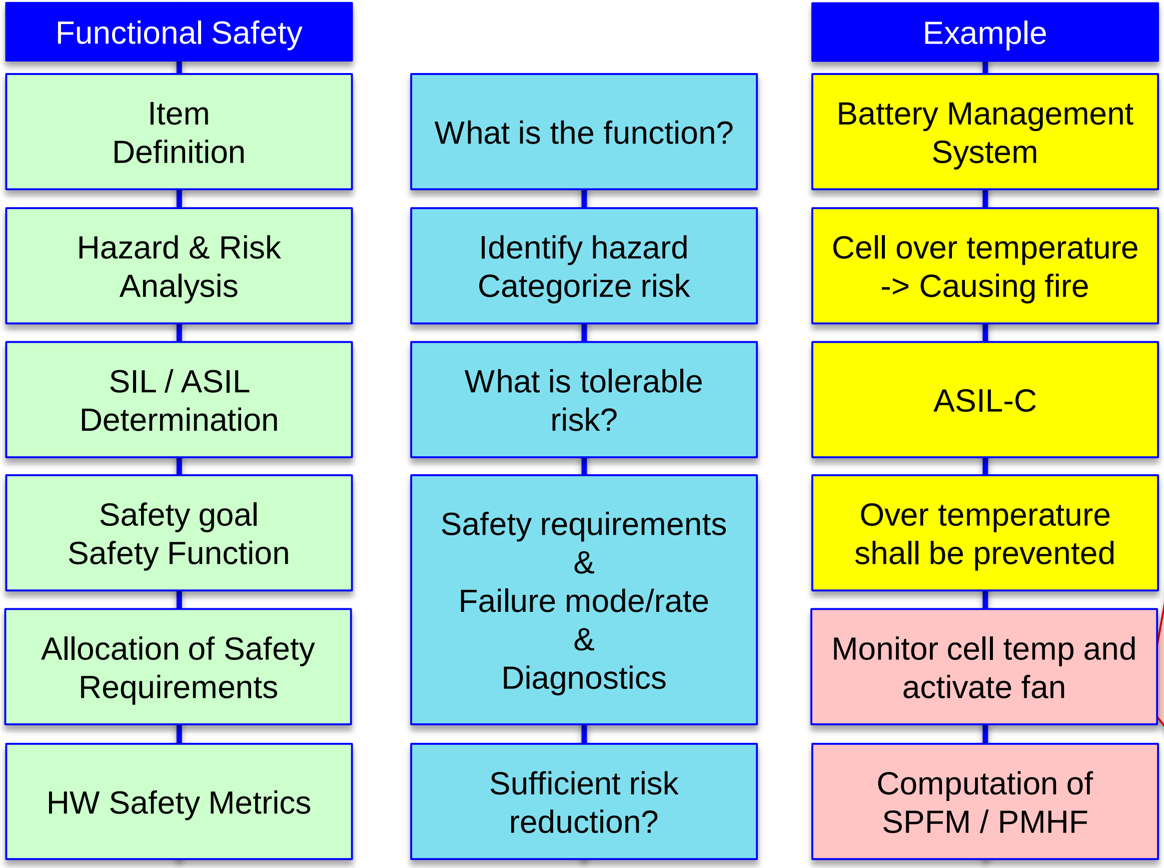
Details of ISO 26262 Metrics:

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

FMEDA worksheet is available under NDA

Based on TMS570LS12x v1.0 FMEDA worksheet

ISO 26262 Risk reduction



Functional Safety		Example
Item Definition	What is the function?	Battery Management System
Hazard & Risk Analysis	Identify hazard Categorize risk	Cell over temperature -> Causing fire
SIL / ASIL Determination	What is tolerable risk?	ASIL-C
Safety goal Safety Function	Safety requirements & Failure mode/rate & Diagnostics	Over temperature shall be prevented
Allocation of Safety Requirements		Monitor cell temp and activate fan
HW Safety Metrics	Sufficient risk reduction?	Computation of SPFM / PMHF

- 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

Product	Standard	Assessor	Certificate
RM48x (20 Devices)	IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3	TÜV SÜD	
RM46x (12 Devices)	IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3	TÜV SÜD	
TMS570LS31x/21x (14 Devices)	IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3 ISO 26262-2:2011; ASIL D ISO 26262-5:2011; ASIL D	TÜV SÜD	
TMS570LS12x/11x (10 Devices)	IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3 ISO 26262-2:2011; ASIL D ISO 26262-5:2011; ASIL D	TÜV SÜD	
SafeTI Development Process for IEC 61508 and ISO 26262 Compliant Hardware Components	IEC 61508-1:2010; SIL 3 IEC 61508-2:2010; SIL 3 ISO 26262-2:2011; ASIL D ISO 26262-5:2011; ASIL D	TÜV SÜD	
SafeTI Functional Safety Software Development Process	IEC 61508-1:2010; SIL 3 IEC 61508-3:2010; SIL 3 ISO 26262-2:2011; ASIL D ISO 26262-6:2011; ASIL D ISO 26262-8:2011; ASIL D	TÜV NORD TÜV NORD Systems GmbH & Co.KG Trusted Process QRAS AP00213 - Safe TI - Functional Safety Software Development Process ISO 26262-2:2011, ASIL D ISO 26262-6:2011, ASIL D ISO 26262-8:2011, ASIL D IEC 61508-1:2010, SIL 3 IEC 61508-3:2010, SIL 3 SEBS-A.165253/13	

56 Hercules products certified and counting!!

RM48x, RM46x and RM42x certified to IEC 61508 SIL 3 for Industrial functional safety applications.

TMS570LS31x/21x, TMS570LS12x/11x and TMS570LS04/03/02x certified to ISO 26262 ASIL D for Automotive functional safety applications.

SafeTI Hardware and Software development processes also certified.

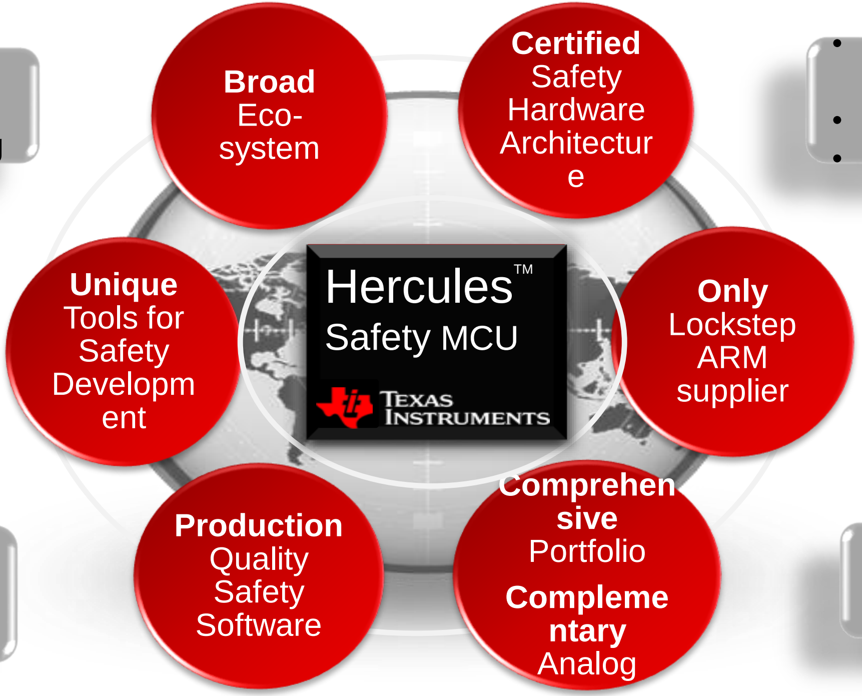
Reduce time and effort to certify your end system!!

Hercules MCUs Accelerating Safety Products to Market

- Software
- Development Tools
- Consulting & Training

- Ease development
- Aid certification

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



Broad Eco-system

Certified Safety Hardware Architecture

Unique Tools for Safety Development

Hercules™ Safety MCU

Texas Instruments

Only Lockstep ARM supplier

Production Quality Safety Software

Comprehensive Portfolio

Complementary Analog

- Pre-approved for ISO 26262 (ASIL D), IEC 61508 (SIL 3)
- Proven in use
- Device FMEDA, FIT reports

- Non-proprietary
- Market accepted
- Respected heritage

- Pin & SW Compatible
- Safety Chipset
- SafeTI Program

Why TI for Battery Management System

MCU leadership in automotive safety applications:

- Braking -- 65% share,
- Airbag – 40% share
- EPS - >20% and growing

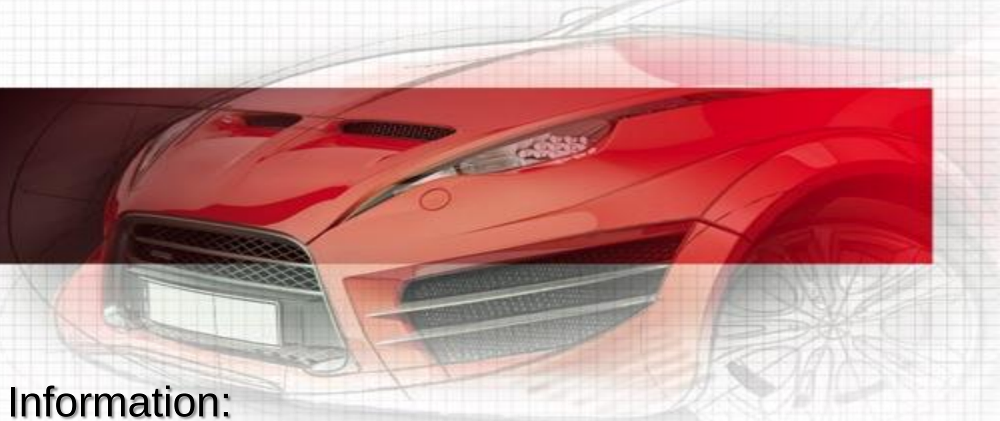
20+ years automotive experiences:

- Q100 qualification
- Zero defect (0 dppm)
- Product supply longevity
- -40c to 125c temp specification

SafeTI chip set (TMS570 + bq76PL455A + EMB14xx) for integrated safety BMS system

ISO 26262 certified MCU with documentation and tools ease system certification effort

Thank You



Contact Information:
Hoiman Low: hm-low@ti.com
Loyal Bao:loyal-bao@ti.com