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

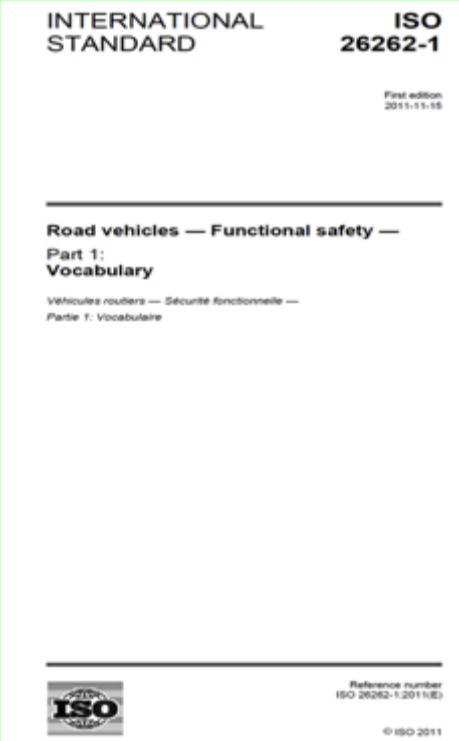
Toyota Motor Corp. vehicles sit parked ahead of shipment outside the Central Motor Corp. plant in Ohira, Miyagi Prefecture, Japan, March 7, 2014.

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

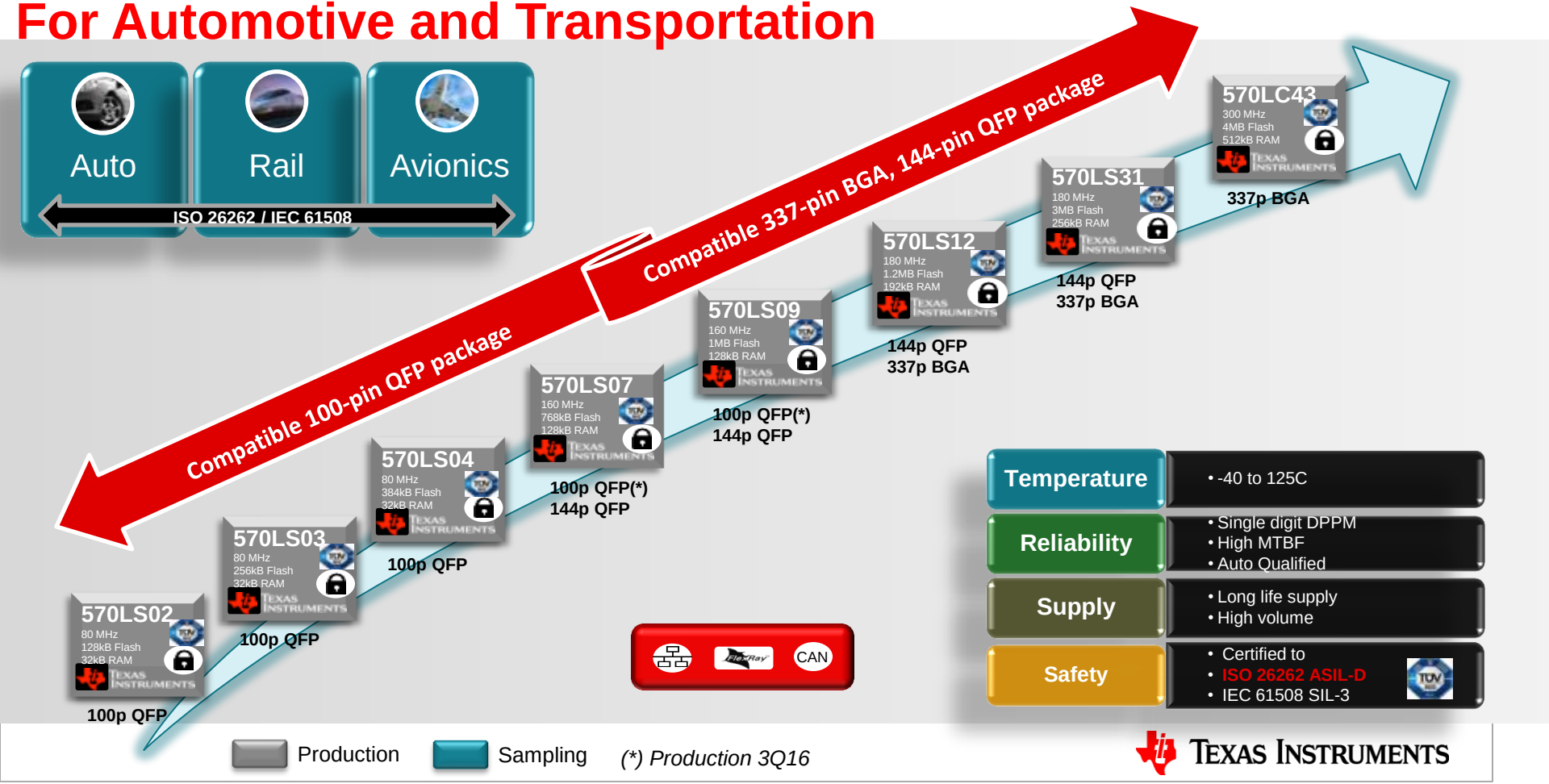
SafeTI™ Design Packages

Docs, Tools, Software

- Complementary, safety-enabled Components
- Safety Development Processes

TMS570 ARM® Cortex®-R MCU platform

For Automotive and Transportation



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

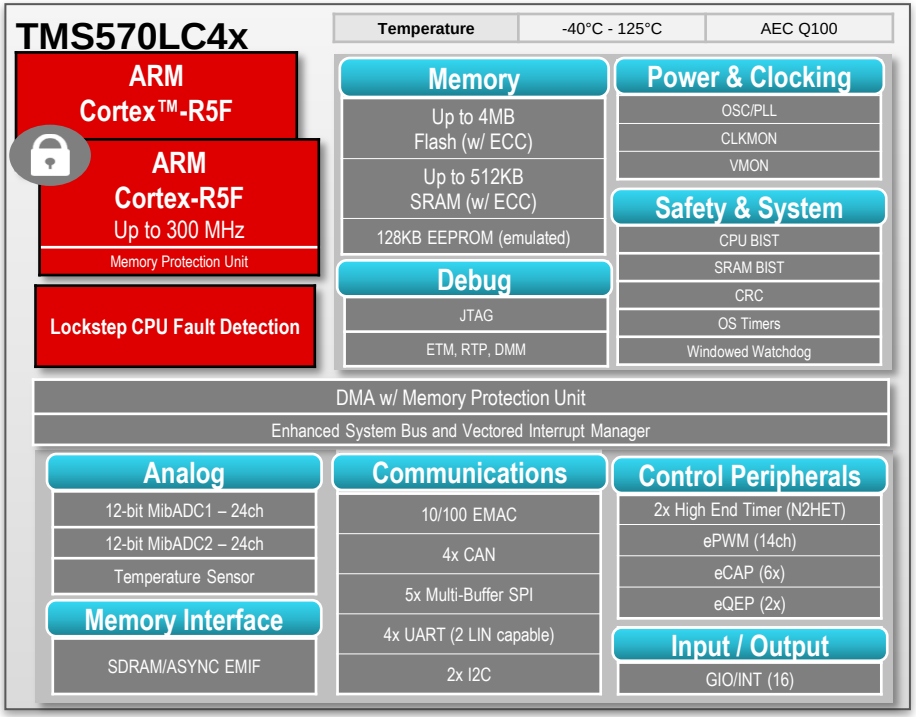
- Dual CPUs in Lockstep,CPU Logic Built in Self Test (LBIST)
- Up to 16 CPU MPU regions,Flash & RAM w/ ECC (w/ bus protection)
- Memory Built-in Self Test (PBIST),Cyclic redundancy checker module (CRC)
- Select peripheral RAMs protected by Parity/ECC

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)



Packages

337p BGA
(16x16mm)

Targeted Applications

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

Texas Instruments

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

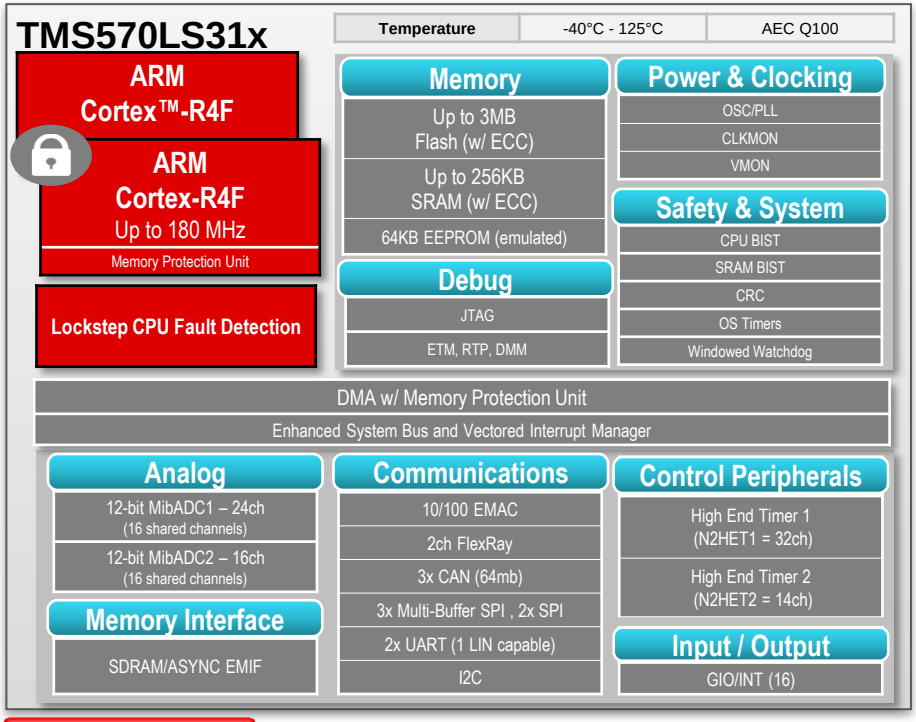
- Dual CPUs in Lockstep
- CPU Logic Built in Self Test (LBIST)
- Up to 12 CPU MPU regions
- Flash & RAM w/ ECC (w/ bus protection)
- Memory Built-in Self Test (PBIST)
- Cyclic redundancy checker module (CRC)
- Select peripheral RAMs protected by Parity

Communication Networks

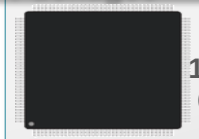
- 10/100 MAC ,FlexRay w/DMA,3 CAN Interfaces
- 5 SPI (3 Multi-Buffered),2 UART (1 LIN capable), 1 I2C

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)



Packages



144p QFP (20x20mm)

337p BGA (16x16mm)

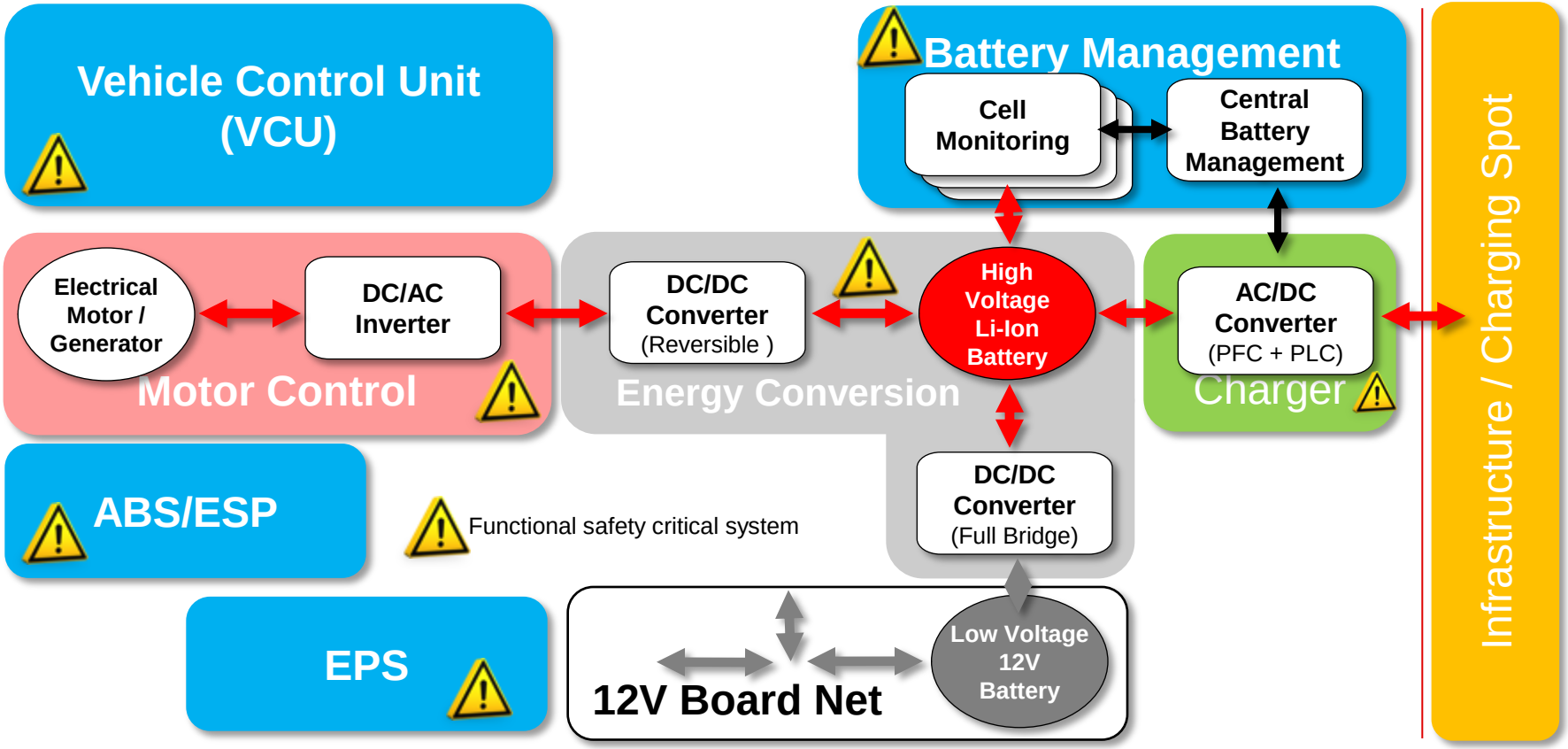
Targeted Applications

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

Texas Instruments

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

Electric Vehicle – Architecture Overview



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)

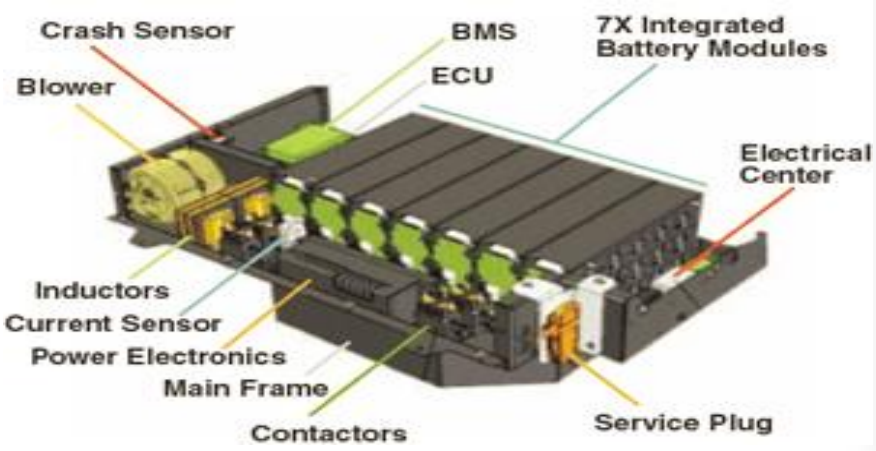


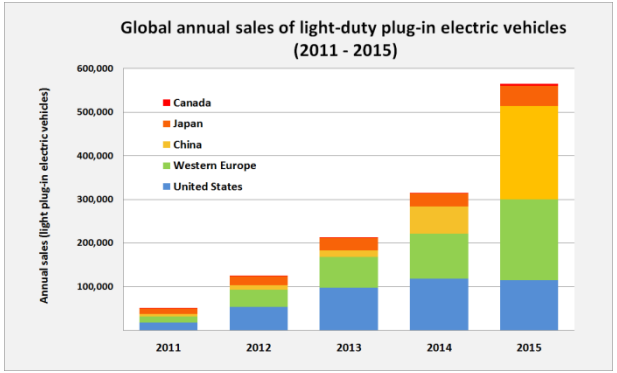
Image courtesy of A123 Systems, Watertown, Mass.

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

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.

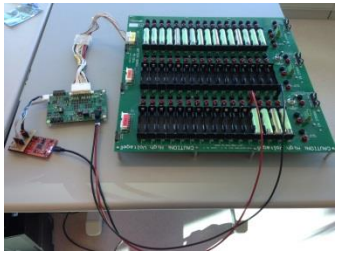
Benefits

- 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.

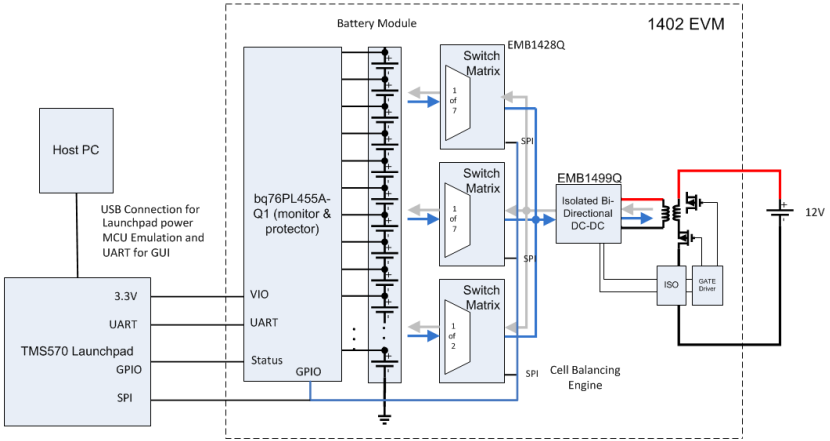
Target Applications

- 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



Safety Motor Control Block Diagram

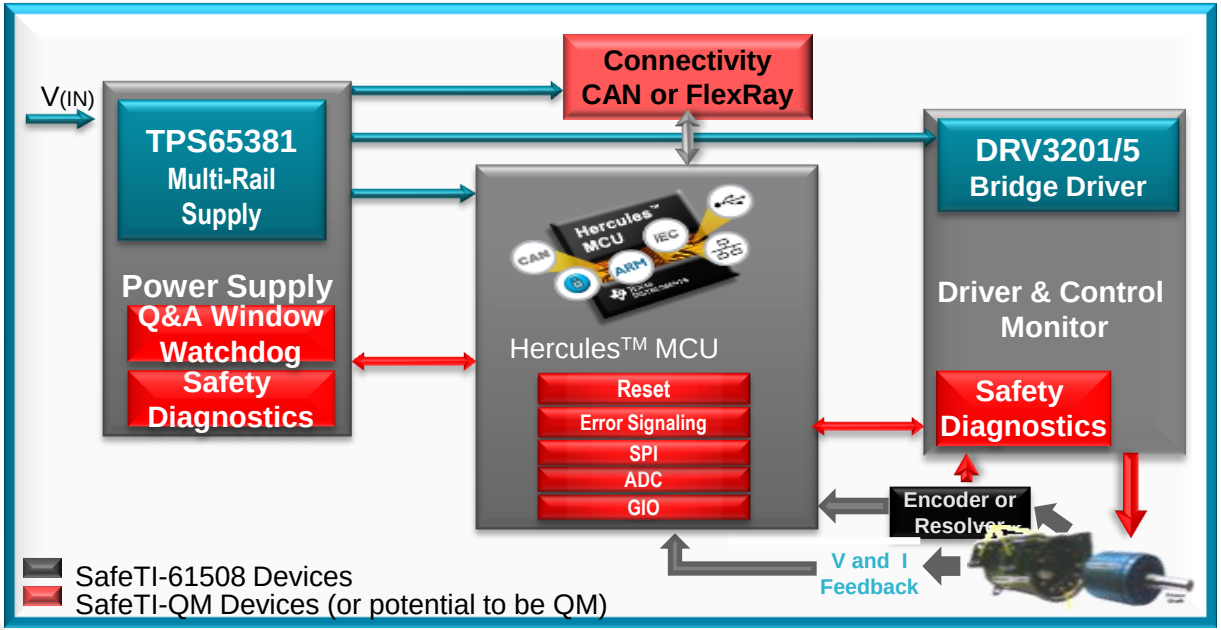
EPS

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

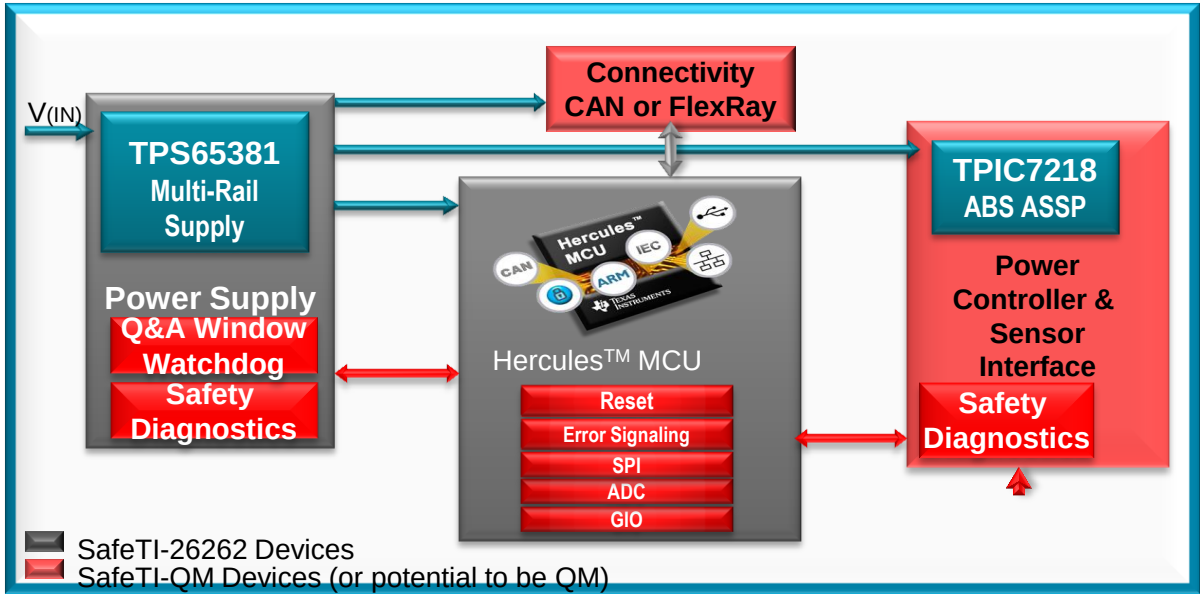
Key Software

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

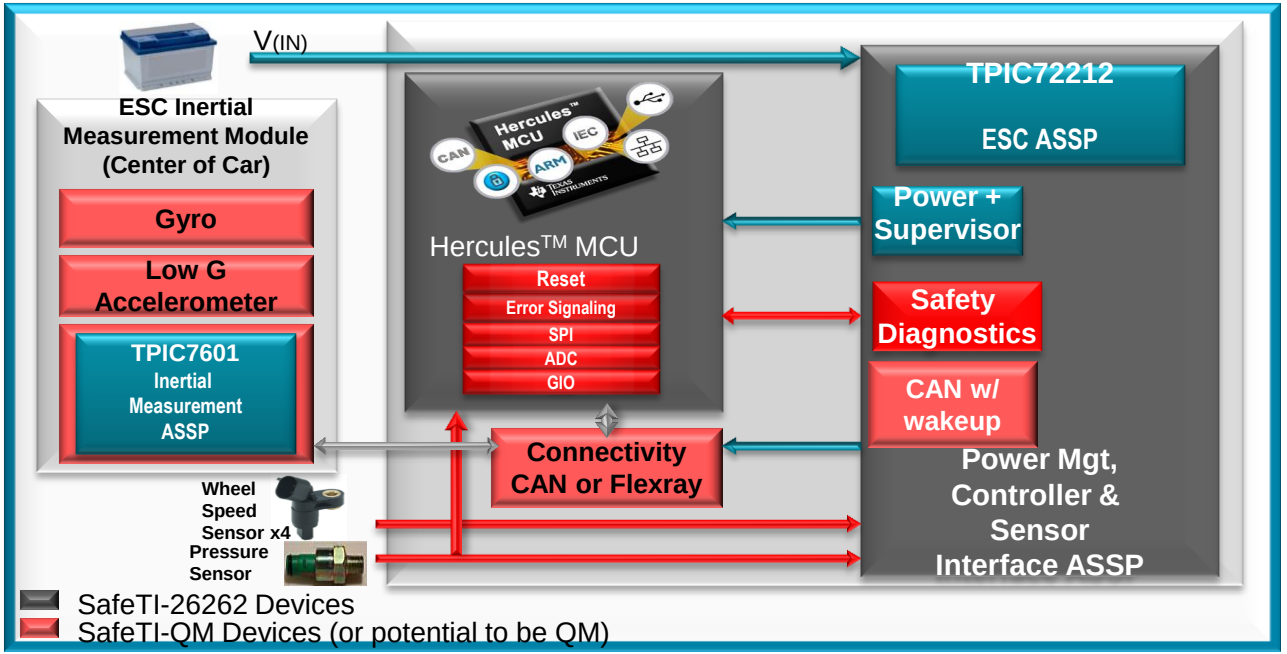
Key Software

HALCoGen
- MISRA, 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

TMS570LS07x/09x/11x/12x/21x/31x MCU
- ISO26262 ASIL-D
- AEC Q100 -40C-125C (ambient)
- LIN,CAN, Ethernet, FlexRay
- Safety docs available for all.



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

- 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

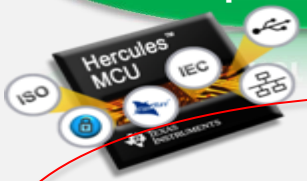
Applying Functional Safety Standards

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

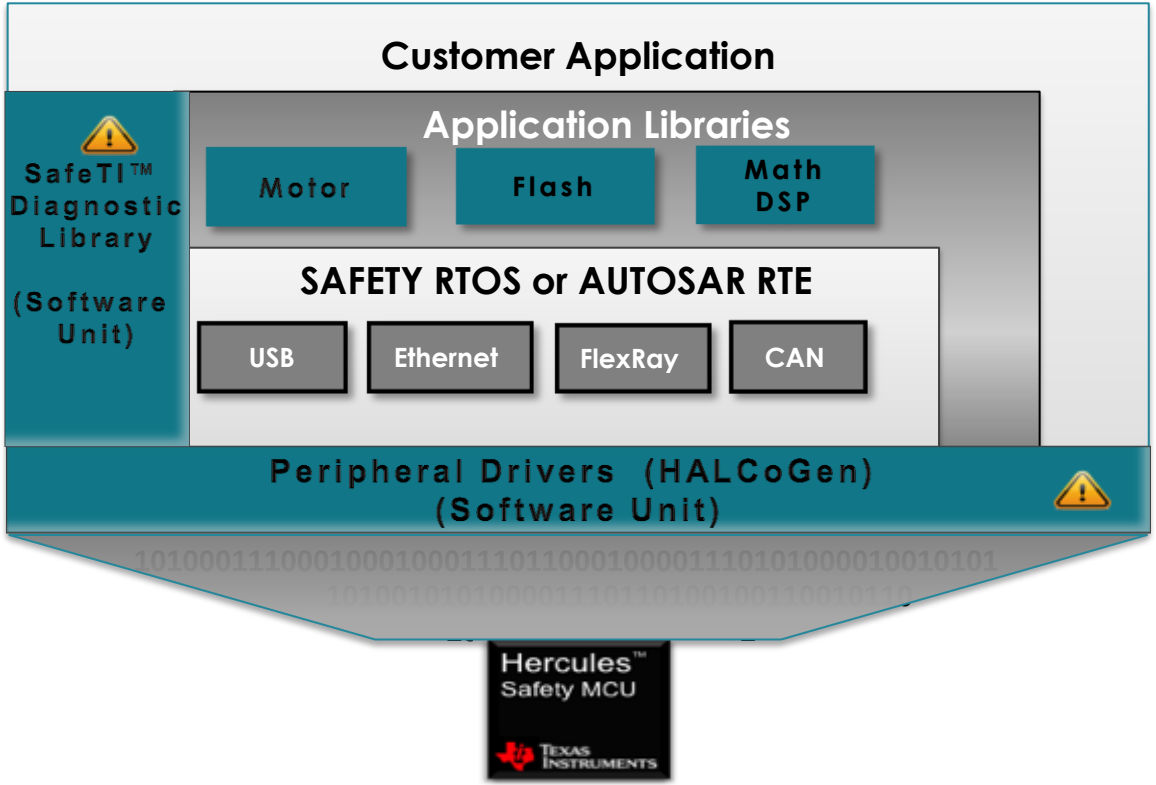


- Development processes
- Supporting processes
- Software development and V&V

CSP = Compliance Support Package

SafeTI Software Framework

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

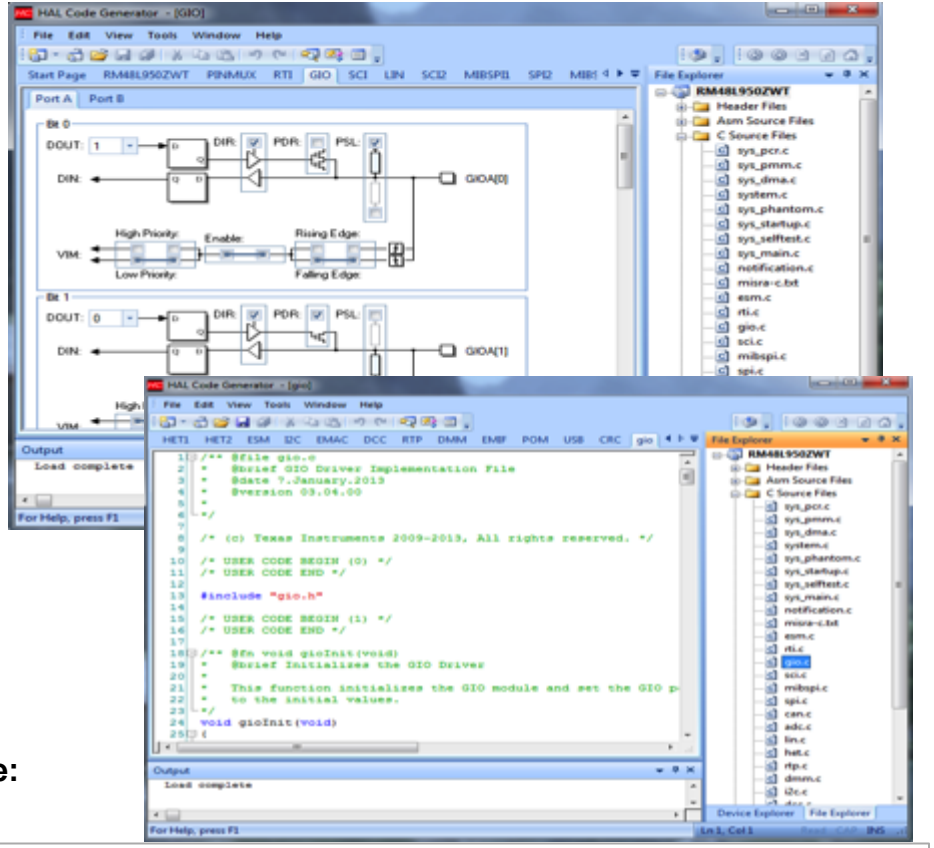


SafeTI™ Compliance Support Packages Available

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

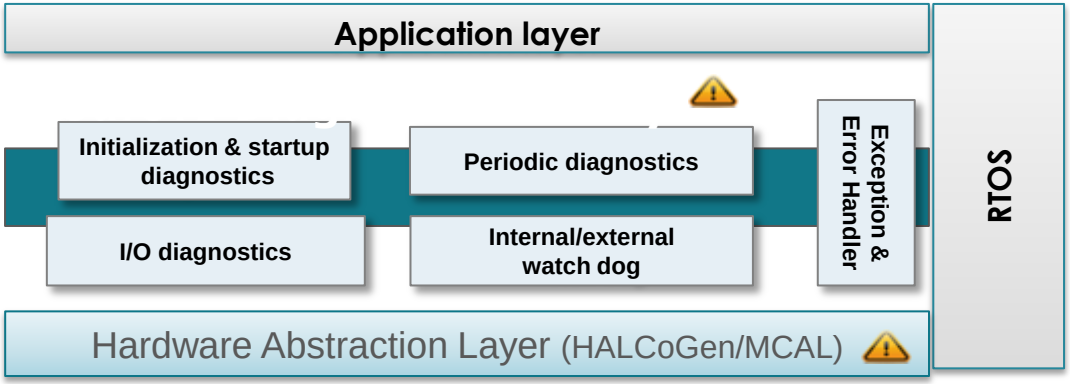


SafeTI™ HALCoGen Compliance Support Package:
www.ti.com/tool/safeti-halcogen-csp

Hercules SafeTI™ Diagnostic Library

Provides simple interfaces and a framework for

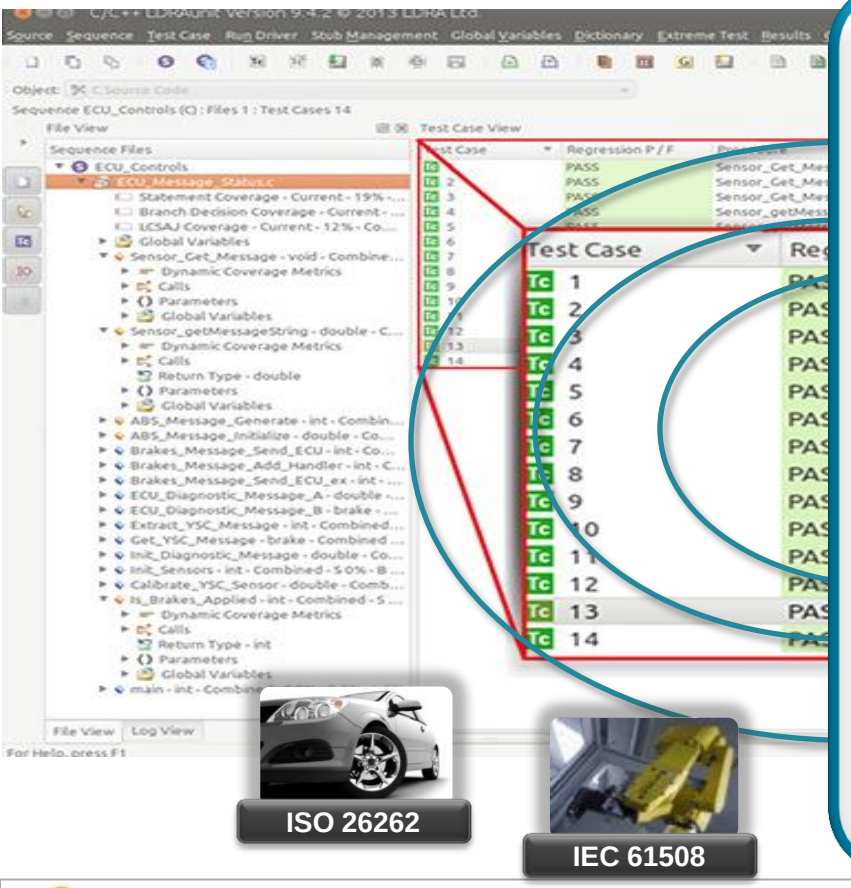
- Initializing and Enabling Safety diagnostics/Features prescribed by the Hercules Safety Manual.
- Fault injection to allow testing of application fault handling
- Error Signaling Module (ESM) handler callback routine.
- Profiling for measuring time spent in diagnostic test/fault handling



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

SafeTI™ Compliance Support Package (CSP)



- 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

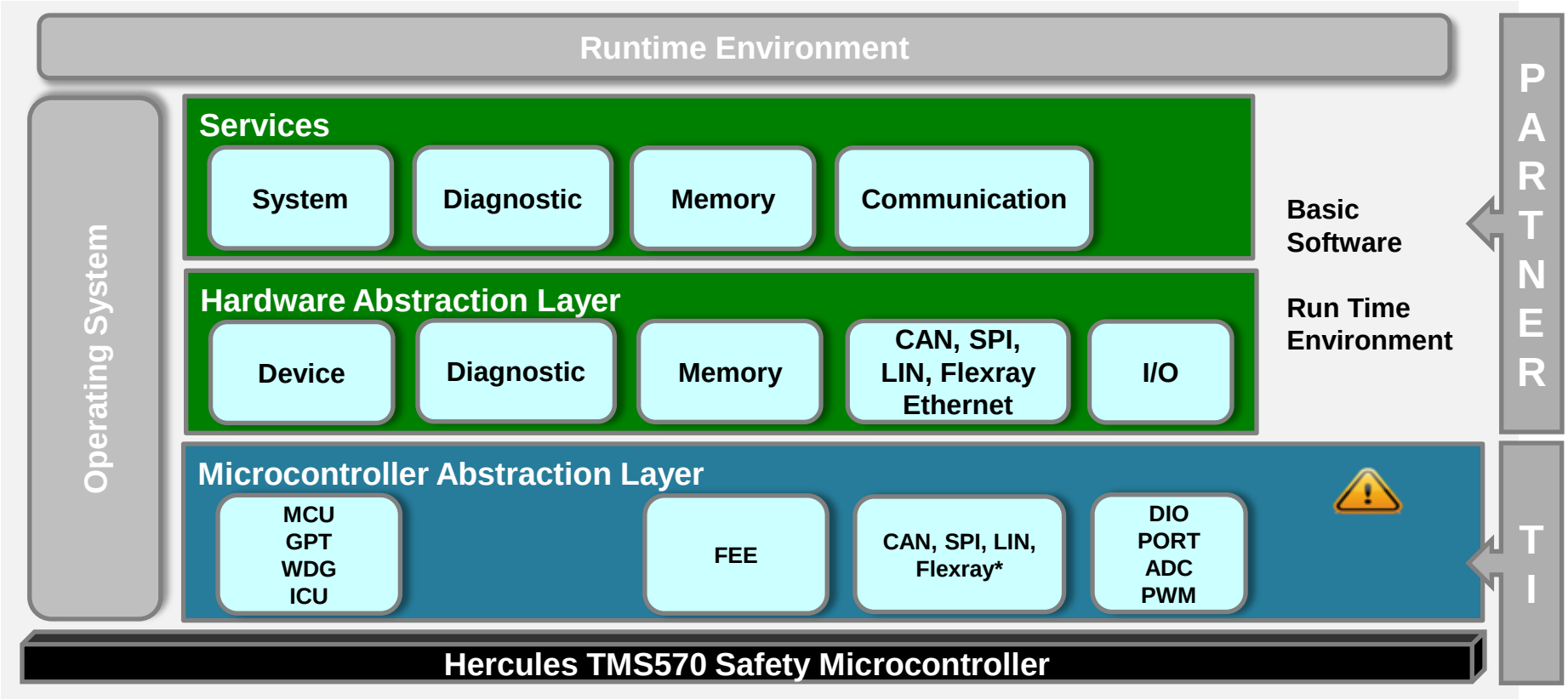
SafeTI™ Compiler Qualification Kit

- 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™ qualification suite
  - TI compiler validation test cases
  - Test Automation Unit (TAU)
  - 24hrs of Validas consulting services
  - TÜV Nord assessment report

Approved by TÜV NORD

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

Hercules TMS570 AUTOSAR v4.0 rev3 Support



*From partner

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 Trusted Process	

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

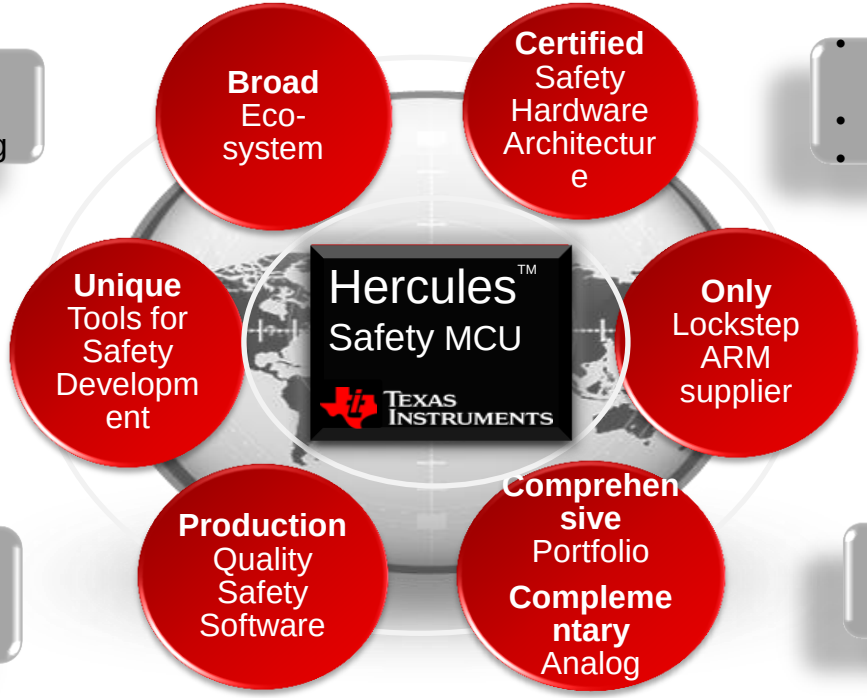
- Pre-approved for ISO 26262 (ASIL D), IEC 61508 (SIL 3)
- Proven in use
- Device FMEDA, FIT reports

- Ease development
- Aid certification

- Non-proprietary
- Market accepted
- Respected heritage

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

- 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