Texas Instruments (TI) Hercules™ MCU: Features Applicable to Use in High-Speed Rail

Hoiman Low
Microcontroller Business Development Manager
Texas Instruments

Since the introduction of the high speed rail in China in 2008, its network has grown to 16,000 km at the end of 2014. It is the largest high speed rail network in the world carrying 2-3 million passengers every day. These high speed trains operate around the clock carrying over 1000 people per train running at speeds over 300km/h. They operate with high frequency; for example there is a high speed train running between Shenzhen and Guangzhou every 5 to 10 minutes.

Considering the high number of travelers and the operating hours, safety is a paramount concern. The China high speed rail system has up to now demonstrated to be very safe with the exception of one fatal crash near Wenzhou due to a signaling fault in 2011 causing 40 deaths and 190 injuries. This highlights the importance of a safety signal and control system for fault detection and timely risk mitigation when a fault is detected.

High speed train signal and control systems

China's high-speed rail signal and control systems are very similar to European Train Control Systems (ETCS) which consist of a ground system and an onboard system. Information such as train location, train speed, traffic restrictions and permissible speed are exchanged continuously between the train and the ground systems. The onboard computer determines the train speed and braking pattern based on real time data.

High speed train signal and control safety requirements

China's high-speed rail safety follows CENELEC (European Committee for Electro-technical Standardization) EN 5012x railway safety standards:

- 50126: Railway Applications – The Specification and Demonstration of Reliability, Availability, maintainability and Safety (RAMS).
- 50128: Railway Applications – Communications, signaling and processing systems.
- 50129: Railway Applications – Communications, signaling and processing systems – Safety related electronic systems for signaling.

EN 5012x uses industry functional safety standard IEC 61508 as reference. EN 50126 covers the Reliability, Availability, Maintainability and Safety (RAMS) life cycle of a railway system. EN 50128 covers the software development aspect of the railway control system and EN 50129 covers railway electronics systems for signaling.

Standard	System	Safety Integrity	Architectural Metric	Architectural Requirement	Failure Rate	Specific MCU self-test requirements
IEC 61508	Programmable E/E systems	SIL – 1,2,3,4	SFF	HFT>0 for SIL 4	PFD, PFH	No
EN 50129	Railway	SIL – 1,2,3,4	N/A	Follow IEC 61508	THR	CPU, Memory

Table 1

- *Safe Failure Fraction (SFF)*
- *Hardware Failure Tolerance (HFT)*
- *Probability of Failure on Demand (PFD)*
- *Probability of Failure per Hour (PFH)*
- *Tolerable Hazard Rate (THR)*

EN 50129 risk reduction levels and failure rates are mostly harmonized to IEC 61508 – table 1.

Similar to IEC 61508, EN 50129 system risk reduction level requirement is categorized by Safety Integrity Level (SIL), SIL 1 being the lowest and SIL 4 being the highest – table 2.

However, EN 50129 specifies failure rate with THR rather than PFD/PFH in IEC 61508 – table 2.

Because of the potentially severe consequences of a high speed train system failure, the system SIL level is mostly SIL 4, i.e. failure rate of a system must be lower than 1 fail per 1E8 or 100 million operating hours.

(Note: As applied to semiconductor components, the highest SIL level attainable is SIL 3; SIL 4 is only achievable for the system itself rather than components going into the system.)

Tolerable Hazard Rate THR Per hour per function	Safety Integrity Level (SIL)
$10\text{-}9 \leq THR < 10\text{-}8$	4
$10\text{-}8 \leq THR < 10\text{-}7$	3
$10\text{-}7 \leq THR < 10\text{-}6$	2
$10\text{-}6 \leq THR < 10\text{-}5$	1

Table 2

Another notable difference between IEC 61508 and EN 50129 consists in the faults detection requirements for large integrated circuits. EN 50129 provides a list of prescribed requirements of CPU and Memory self tests, while IEC 61508 provides guidelines of techniques and measures for the faults detection.

How Texas Instruments (TI) Hercules MCUs can help customers developing products for use in high-speed train systems

Apart from the functional implementation, challenges faced by high speed train system developers regarding safety aspects are:

1. Implementing a system for SIL 4 compliance
2. Implementing specific CPU and Memory self test requirements with proven effectiveness
3. Providing a reliable inter-system communication interface
4. Providing a high speed inter-system communication interface
5. Companion analog components
6. System certification

1. System for SIL 4 compliance

As shown in table 1, EN 50129 follows IEC 61508 on hardware architectural requirements. SIL 4 requires a Hardware Failure Tolerance (HFT) = 1 (redundant architecture) and a Single Fraction Failure (SFF) >=99%

With HFT = 1 and SIL 4, it means that at least two

Maximum allowable SIL for Type B (High Demand) safety-related elements			
Safe Failure Fraction of an Element (SFF)	Hardware Fault Tolerance		
	No Redundancy	Single Redundancy	Double Redundancy
<60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Table 3: *Note: Type B products are complex products in which all failure modes are not known. Most semiconductors are considered Type B.*

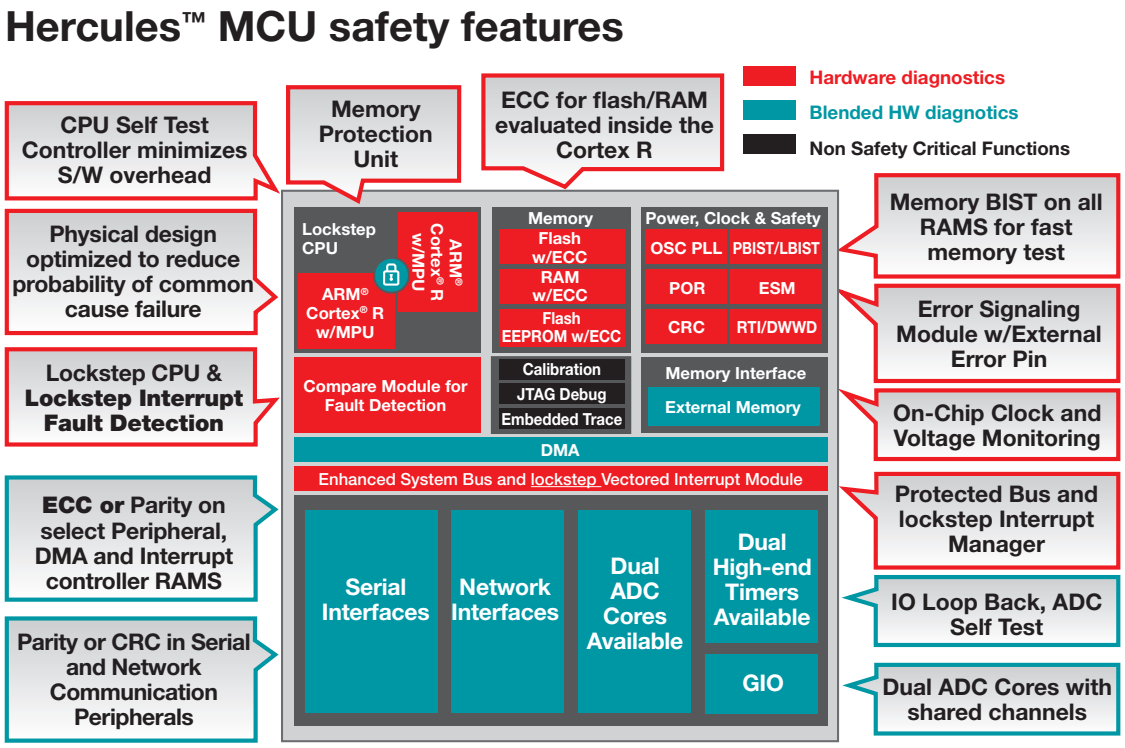
SIL 3 channels are required in a system and a dangerous failure in the system will not prevent the safety function from performing – see table 3.

TI's Hercules TMS570 MCUs are certified by TÜV SÜD as meeting IEC 61508 requirements up to SIL 3 (the highest SIL level attainable for MCUs). TÜV SÜD is an internationally recognized and independent assessor of compliance to quality and safety standards. Customers can design a dual channel system with a SIL 3 capable Hercules MCU in each channel, as a part of an overall system that must satisfy the HFT =1 and SIL 4 requirements.

2. CPU and memory self-test

EN 50129 Table D.1 specifies the fault detection measures to be implemented in large integrated circuits such as a MCU. It covers CPU, volatile memory and non-volatile memory self-test requirements.

TI Hercules TMS570 MCUs offer dual-core CPU lockstep/compare and memory Error Correction Code (ECC) real time diagnostics, as well as hardware-based CPU Logic Built-In Self Test (LBIST) and SRAM Programmable Built-In Self Test (PBIST) – see Fig. 1.



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

Figure 1

These hardware-based safety features help diagnose errors in mission-critical blocks and offer high diagnostic coverage with minimum software overhead.

- The dual ARM® Cortex® -R lockstep architecture provides cycle-to-cycle high diagnostic coverage of the CPU.
- The Error Correction Code (ECC) circuit, implemented inside the lockstep Cortex-Rx CPUs, provides bus interconnect and SRAM/Flash single bit error correction and double bit error detection (SECDED) with little to no performance impact.

D.1 requirements with high test coverage while minimizing software overhead.

Furthermore, TI also offers the Hercules SafeTI™ Diagnostic Library providing simple-to-use API functions to implement CPU and memory self-tests during the system start-up and during the system run-time. It also provides API support for initialization, exception handling, error handling and fault injection – Fig. 2.

The Hercules SafeTI Diagnostic Library can be downloaded from http://www.ti.com/tool/SAFETI_DIAG_LIB

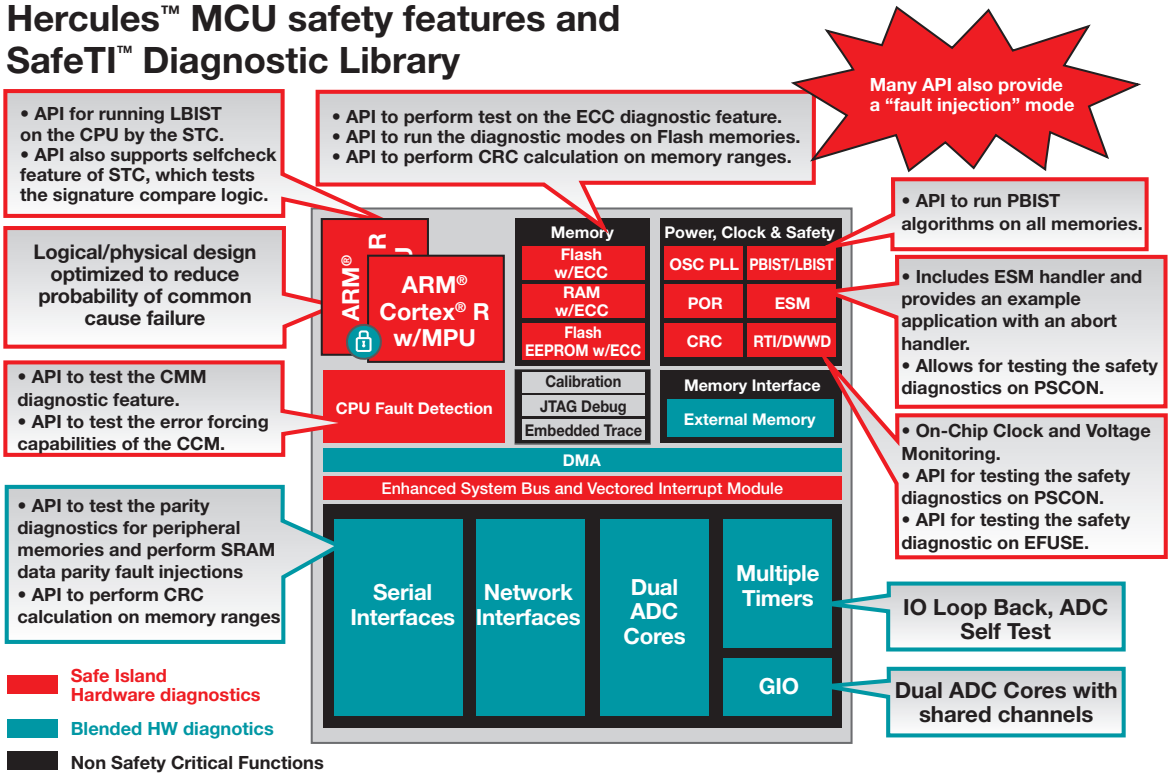


Figure 2

- The CPU LBIST and SRAM PBIST offer high coverage fault detection.

The TI Hercules MCU lockstep CPU with compare, memory ECC, LBIST and PBIST on-chip hardware-based diagnostic circuits facilitate the system implementation in compliance with EN50129 Table

3. FlexRay automotive-grade standard inter-system communication interface

Inter-MCU and inter-system communication are critical tasks in the overall train ground and onboard systems. SPI and CAN are well-established communication interfaces typically used in safety

control applications. These event driven and non-deterministic communication interfaces are efficient for many safety control applications. But they are not fault tolerant. FlexRay was developed by the automotive industry for safety applications requiring hardware fault tolerance such as Brake by Wire or Steer by Wire in the 2000's.

The FlexRay module in TI Hercules MCUs offers high speed, deterministic, fault-tolerant features for use in high speed rail signal and control systems. For more information about FlexRay, please consult TI FlexRay's training slides: www.ti.com/lit/SPRT718.

4. High-speed Ethernet inter-system communication interface

A large amount of data such as train speed, train location, traffic and track data need to be exchanged to determine the train speed and braking pattern. With trains moving at 300 km/h, high-speed communication interface is a highly desirable feature.

The Ethernet module in TI Hercules MCUs provides a standard high-speed interface for inter-system communication.

5. Analog Companion components

TI's large portfolio of analog components provides a wide selection of power supply circuits, interfaces and signal conditioning circuits connecting the Hercules MCU to the real world.

TPS65381-Q1 (Multi-Rail Automotive Power Supply for Microcontrollers in Safety-Critical Applications) is frequently used as the power supply of choice for Hercules MCU. It provides monitored power supplies for the MCU. It can also act as a watchdog supervising the MCU operation. It interfaces directly with the Hercules MCU error-signaling module for error handling outside of the MCU. Furthermore, it includes built-in self-test of internal analog and digital circuits.

For more information on TPS65381-Q1, please consult http://www.ti.com/product/TPS65381-Q1/description&lpos=Middle_Container&lid=Alternative_Devices

6. System certification

MCUs may be certified up to a particular safety integrity level (or "SIL"). A 'certified' MCU means that its development process was reviewed and meets the requirements of a functional safety system up to the specified SIL. Supporting documentation and tools such as the safety manual and failure mode effect and diagnostic analysis (FMEDA) tool are required by the standards to help system developers understand the MCU safety mechanisms and to calculate the MCU failure rate.

TI's Hercules TMS570 MCUs are certified as meeting IEC 61508 requirements up to SIL 3 as previously mentioned. The MCU development process, the management of systematic failures and the management of random failures have been examined by the certification authority. Safety documentation for these MCUs includes a safety manual available for general download (no NDA required) and a safety analysis report with the FMEDA tool available (under NDA). These documentations and tools have also been reviewed by the certification authority during the MCU certification.

Supporting the TMS570 MCUs are foundational software components such as peripheral drivers generated by HalCoGen tool and SafeTI Diagnostic Library. The software development process for these software components has been certified by TÜV NORD as meeting up to IEC 61508 SIL 3 levels of safety integrity. TÜV NORD is an internationally recognized and independent assessor of compliance to quality and safety standards. SafeTI™ Compliance Support Packages (CSP) are developed

according to TI's certified software development process and are available for HALCoGen and the SafeTI™ Diagnostic Library. These CSPs provide a helpful starting point for customers who need to provide similar evidence for their functional safety-related software during system certification. For more information on SafeTI Compliance Support Packages, please consult http://www.ti.com/lit/wp/spny007/spny007.pdf

The use of these certified MCUs and their supporting documentations and tools can help customers with their safety system development and reduce their certification efforts.

Summary

The TI Hercules MCU family offers, to help customers with their system development and industry functional safety standard certification efforts:

1. SIL 3 certified MCUs help customers to design an overall system that must satisfy the HFT =1 and SIL 4 requirements.
2. Hardware based high coverage CPU and Memory self test meeting or exceeding the EN 50129 table D.1 requirements and the Hercules SafeTI Diagnostic Library with minimum software overhead.
3. The FlexRay module providing a deterministic and fault-tolerant inter-system communication interface.
4. The Ethernet module providing a standard high-speed communication interface needed for the high-speed trains.
5. Wide selection of analog companion component including the TPS65381-Q1 Power Supply and Watchdog.
6. IEC 61508 SIL 3 certified MCUs with the safety manual and FMEDA tools as well as the foundational software components (HalCoGen peripheral drivers and SafeTI Diagnostic Library) developed with TI's IEC 61508 SIL 3 certified software development process.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265