How to improve system availability and minimize down time with Hercules™ MCUs?

Hoiman Low
MCU Business Development Manager
Texas Instruments

We are living in a world full of electronics. It's a nuisance when our electronic watch stops working. On the other hand, it could be a major disaster if a data center is down. Factories typically run continuously. System down time is costly and should be avoided. Equipment operating 24/7 and/or performing mission critical tasks need to be highly AVAILABLE.

What is System Availability

Per Wikipedia, "availability is the probability that a system will work as required when required during the period of a mission" – https://en.wikipedia.org/wiki/Availability_(system)

Availability can be calculated as follow:

Availability = **MTTF / (MTTF + MTTR)**

where

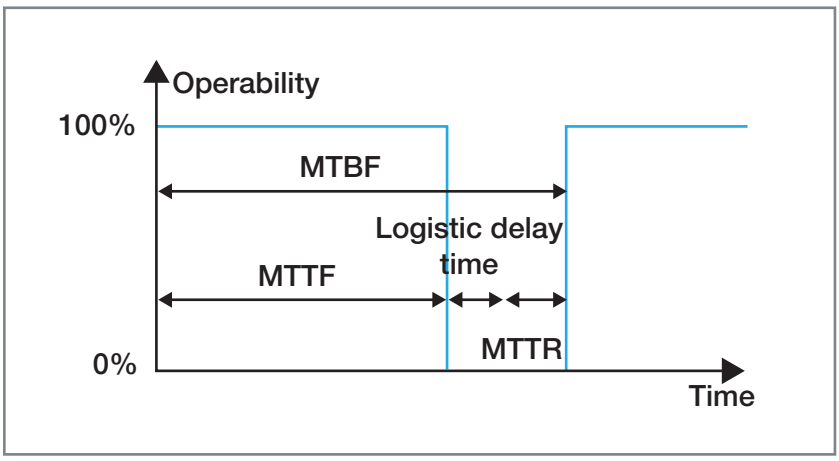
MTTF = Mean Time To Failure

MTTR = Mean Time To Repair

MTBF = Mean Time Between failure = MTTF + MTTR

Examples:

1. Equipment is operational for 7884 hours (0.9 years) per year and requires 876 hours to repair, the availability is 90%.
2. Equipment is operational for 8672.4 hours (0.99 years) per year and requires 87.6 hours to repair, the availability is 99%.



Importance of Availability

Here are typical Mean Time Between Failure (MTBF) numbers for different equipments:

- Wind Turbine: 0.7-1 year
- Industrial control PLC: 40 – 50 years
- Telecom/Medical equipments power supply: 200-600 years
- Industrial transmitter or motor speed encoder: 500-800 years
- Avionics: 100,000 years

It is obvious why 100K years of MTBF is required for avionics. In order to achieve this kind of MTBF, a redundant system architecture is required.

For wind turbines, the low MTBF means that they breakdown often and can take days to repair if located in a remote inaccessible region.

Semiconductor Reliability MTBF

We often hear the comments that electronic components are much more reliable than mechanical components. The reliability of a system is determined by its weakest component. If an electronic component such as a Microcontroller (MCU) is so much more reliable than the mechanical parts it controls, why are we talking about improving system availability with TI's Hercules MCU?

Indeed modern electronic components are very reliable. The MTBF of a MCU quoted by semiconductor suppliers are typically >50K years at 55c. Higher temperature will reduce the MTBF somewhat, but it is still significantly higher than the few hundred years of industrial equipments.

Unfortunately, this is only part of the story. There are different failure modes affecting a MCU. There are permanent failures as a result of operational wear-out. There are transient failures caused by external disturbance such as Electromagnetic Interference (EMI) or radiation induced soft error.

Understanding Semiconductor Failures

There are 3 phases of MCU failures; early life, steady state and wearout. This is commonly referred to as the 'bath tub' curve which is used to represents instantaneous failure rates over time in semiconductor products. The Hercules MCU family is an automotive grade design with zero Defect Parts Per Million (DPPM) design methodology and manufactured with zero defect process technology minimizing early life failures and ensuring long MTBF. The MCU MTBF due to permanent failure is very high as quoted by all semiconductor suppliers. However, the MCU MTBF due to transient failure is several orders of magnitude lower depending on the technology used and the size of the memory.

Example:
A MCU with 2 million logic gates, 2MB Flash and 256KB SRAM, permanent failure MTBF is ~50K years and transient failure MTBF is ~50 years.

Therefore, the most critical aspect of MCU availability is transient failure.

How Hercules MCUs Provide High System Availability

Hercules MCU architecture includes several diagnostic and repair features that can detect and respond to transient failures (Fig.1).

Error Correction Circuit (ECC) protects flash and SRAM memory. They are also designed to minimize multi-bit errors within a logical word. Single bit error can be detected and repaired on the fly with no impact to MCU performance.

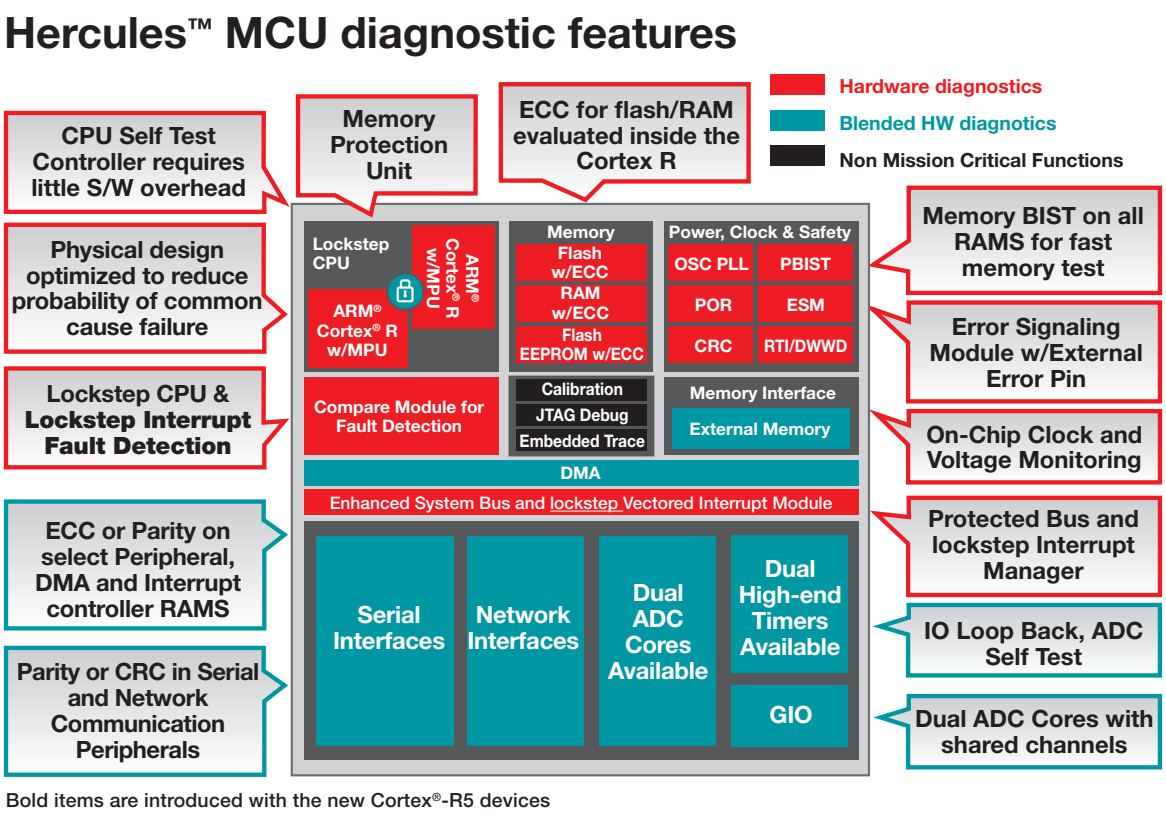


Figure 1: *Hercules MCU diagnostic features*

CPU is protected against transient logic error by lock-step CPU architecture. Upon the detection of a CPU failure, the hardware based and high coverage CPU self-test can be run to determine if the failure is transient or permanent. If the failure is transient, the system can be re-started avoiding unnecessary downtime.

There are many papers on radiation induced soft error and its impact to SRAM and logic storage elements such as flip-flops. Please refer to TI application note (http://www.ti.com/lit/wp/spna109/spna109.pdf) for details. Basically, neutron and alpha particles can cause a state change when they strike a MCU. The memory or logic state change can potentially cause mal-function of a system.

Hercules Memory Availability

Hercules MCUs include ECC circuitry on the SRAM and FLASH memories enabling detection of errors in the memory. The ECC is checked in the CPU core providing an end to end diagnostic on the transmissions between the CPU and FLASH memory. The following use case (Fig.2) illustrates how the Hercules MCU SRAM ECC feature helps to increase system availability and to avoid unnecessary shut down.

Hercules CPU Availability

Here is another example (Fig 3) to illustrate how a transient failure in the CPU can be detected, ‘repaired’ and restarted in real time.

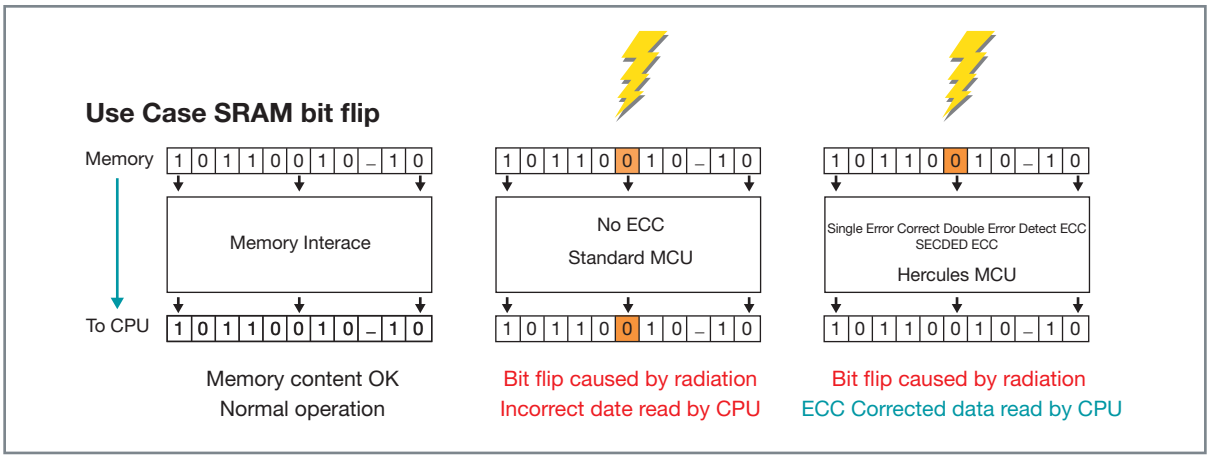


Figure 2: *Hercules memory availability vs transient failure example*

In a standard CPU, if an internal CPU register bit is flipped due to radiation, it can cause a malfunction.

Hercules' MCU lock-step CPU architecture allows real time detection of the CPU fault when one of the CPU register bits is flipped. Upon detection, a hardware based CPU self-test can be executed.

If the CPU self-test fails, the detected CPU fault is confirmed and the system should shut down. However, if the CPU self-test passes, the detected CPU fault is likely to be transient in nature, the MCU can go through a reset cycle making the system available again.

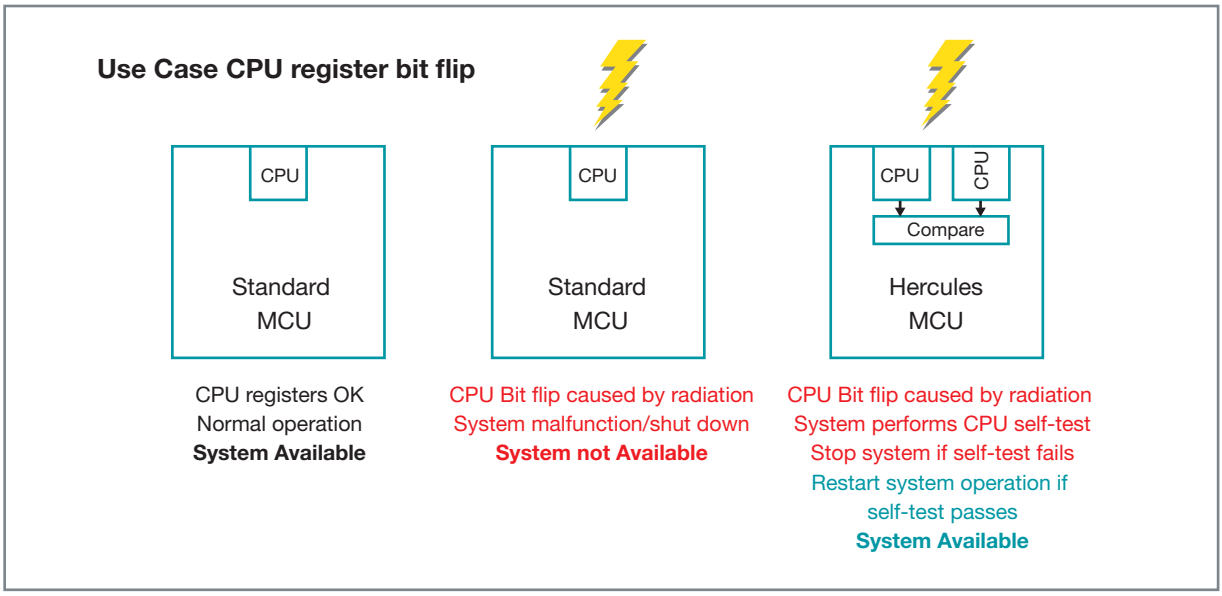


Figure 3: *Hercules CPU availability vs transient failure example*

Conclusion

Hercules MCUs provide Flash/SRAM memory protection with ECC, CPU protection with lock-step compare, hardware based memory and CPU self test as well as redundant peripherals such as timers and CANs. These are unique features supporting real-time diagnostics and repair enhancing system availability. In addition, the SRAM ECC error profiling feature allows implementation of defect analytics to schedule predictive maintenance if required.

TI offers a scalable platform of Hercules MCUs with the same architecture and pin to pin / SW compatibility across the family. It is widely used in automotive and industrial safety applications with automotive grade quality and reliability. For customers where operational availability is a key requirement, the unique diagnostics and self-repair features help to enhance the system availability and minimize costly down time.

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