

Addressing Systematic and Random hardware faults using C2000™ SafeTI™ Products



Introduction

Functional safety standards help minimize the risk of physical injury resulting from dangerous failures.

These dangerous failures can arise from:

- Systematic faults
- Random hardware faults

The challenge that engineers often face is to design systems in a way that addresses both systematic and random hardware faults in order to prevent dangerous failures from occurring. Inability to do so could hinder the system from achieving a safe state in the event of a system failure. C2000 SafeTI products are designed to meet up to the highest standards in managing both systematic as well as random hardware faults. These products are mainly classified as C2000 SafeTI automotive and industrial products and C2000 SafeTI quality managed products.

C2000 SafeTI automotive and industrial products are developed following TI's rigorous and robust hardware development process that has been independently assessed and certified by TUV-SUD. These products are mainly targeted towards automotive and industrial applications that require compliance to the ISO 26262 and IEC 61508 standards.

C2000 SafeTI quality managed products on the other hand are developed following TI's ISO 9001/IATF 16949 compliant HW development process and are mainly targeted towards white goods, household goods and appliances. Although these products mainly support compliance to the IEC 60730, UL 1998 and IEC 60335 standards, it is important to note that these quality managed products also come with a functional safety manual and an FMEDA that can be leveraged to assist with compliance to a wide range of other standards for customers' end applications which include automotive and industrial systems.

Manage & Mitigate Systematic Faults

Systematic faults are caused by human error and can result from mistakes in the design or manufacturing process of an element, subsystem or system. These faults may be managed and mitigated with a robust and rigorous development process.

SafeTI Advantage

- Independent functional safety management process and safety culture established at TI
- C2000 SafeTI quality managed products are developed using our enterprise wide ISO 9001/IATF 16949 compliant development process
- C2000 SafeTI automotive and industrial hardware products are developed using our certified **QRAS AP00210 process**
 - Independently assessed and certified by TUV SUD to meet a systematic capability of ASIL D/SIL 3
 - Certification revalidated on an annual basis and recertified every 3 years by TUV SUD

Detect & Prevent Random Hardware Faults

Unpredictable failures that occur during the lifetime of a hardware element are characterized as random hardware faults. These faults may be detected and prevented with the help of built-in functional safety mechanisms or diagnostics.

C2000 SafeTI Advantage

Safety Mechanisms

Safety Mechanisms play a key role in the overall safety of a system by detecting potentially dangerous failures and consequently helping place the system in a safe state.

- With over 300 built-in safety mechanisms, C2000 SafeTI MCUs provide the required diagnostic coverage to meet a random hardware capability of ASIL B/SIL 2 at a component level
- Functional safety manuals provide detailed information on the safety mechanisms to aid customers in the development of compliant systems up to ASIL D/SIL 3
- C2000 microcontroller based **tunable FMEDA** provides increased flexibility with features such as package FIT estimation, product function tailoring, safety mechanism tailoring and custom diagnostics allowing customers to tune the FMEDA to their own application specific needs

Key safety mechanisms on C2000 MCUs are shown in **figure 1**.

C2000 Safety Mechanisms

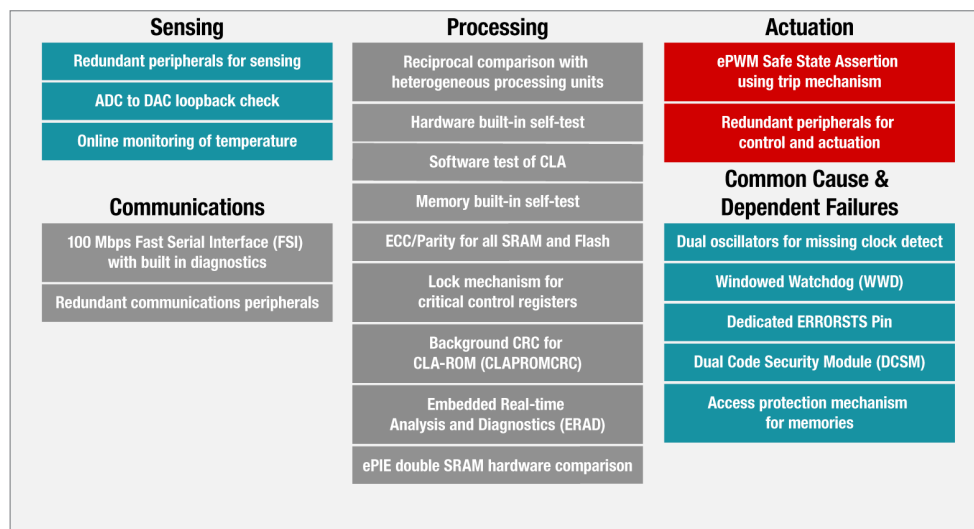


Figure 1. Key C2000 functional safety mechanisms

SafeTI Software Enablers

SafeTI Software packages help simplify certification for functional safety applications

C2000 IEC 60730 Software Package

- UL Recognized under UL 1998, UL 60730-1 and CAN/CSA-E60730-1:02
- It is also VDE certified according to IEC 60335-1 (5. Ed) and IEC 60730-1 (4. Ed)
- The accompanying functional safety manuals describe the safety mechanisms that can be used in the development of IEC 60730-1 and/or IEC 60335-1 compliant systems
- Included SW self-test library (STL) can help assist customers develop systems compliant with other functional safety standards
 - The software library can be called upon power-on initialization and/or periodically within the application to achieve the periodic self-test safety requirements in UL IEC 60730-1 Annex H.11.12 for software/control Class B and/or ANSI/UL 1998 software class 1
 - STL meets the requirements of Annex H of the IEC 60730-1 and Annex R of the IEC 60335-1 standards

SafeTI Diagnostic Library (SDL)

- SDL provides simple interfaces and a framework for
 - Initializing and enabling the safety mechanisms described in the functional safety manuals
 - Fault injection to allow testing of application fault handling
 - Profiling for measuring time spent in diagnostic test/fault handling
- Accompanying Compliance Support Packages (CSP) provide necessary documentation and reports to assist with compliance to a wide range of standards for end systems in automotive, industrial and other applications

Conclusion

A big challenge with developing functional safety compliant systems is to design in a way to minimize the risk associated with dangerous failures in causing physical injury to people or damage to the environment or property. Addressing both systematic and random hardware faults becomes critical in the design of such functionally safe systems. C2000 SafeTI MCUs are developed using a certified hardware development process to meet the stringent requirements of applicable standards and possess a wide range of built in functional safety mechanisms that can be leveraged to help place the system in a safe state. This makes C2000 SafeTI MCUs an ideal building block in the development of functional safety compliant systems.

Additional Resources

1. [Click here to view all available Functional Safety collateral for C2000](#)
2. [C2000 based Tunable FMEDA Whitepaper](#)
3. [Tunable FMEDA 5-part video training series](#)
4. [Safety mechanisms brochure](#)
5. To learn more about C2000 Functional Safety, please visit www.ti.com/c2000safeTI

TI Worldwide Technical Support

Internet

TI Semiconductor Product Information Center Home Page
support.ti.com

TI E2E™ Community Home Page
e2e.ti.com

Product Information Centers

| | | |
|-----------------|----------------|------------------------------------|
| Americas | Phone | +1(512) 434-1560 |
| Brazil | Phone | 0800-891-2616 |
| Mexico | Phone | 0800-670-7544 |
| | Fax | +1(972) 927-6377 |
| | Internet/Email | support.ti.com/sc/pic/americas.htm |

Europe, Middle East, and Africa

| | |
|--------------------|--------------------------------------|
| Phone | |
| European Free Call | 00800-ASK-TEXAS (00800 275 83927) |
| International | +49 (0) 8161 80 2121 |
| Russian Support | +7 (4) 95 98 10 701 |

Note: The European Free Call (Toll Free) number is not active in all countries. If you have technical difficulty calling the free call number, please use the international number above.

| | |
|--------------|------------------------|
| Fax | +(49) (0) 8161 80 2045 |
| Internet | www.ti.com/asktexas |
| Direct Email | asktexas@ti.com |

Japan

| | | |
|----------------|---------------|---------------------------------|
| Phone | Domestic | 0120-92-3326 |
| Fax | International | +81-3-3344-5317 |
| | Domestic | 0120-81-0036 |
| Internet/Email | International | support.ti.com/sc/pic/japan.htm |
| | Domestic | www.tij.co.jp/pic |

Asia

| | |
|---|-------------------------|
| Phone | |
| International | +91-80-41381665 |
| Domestic | <u>Toll-Free Number</u> |
| Note: Toll-free numbers do not support mobile and IP phones. | |
| Australia | 1-800-999-084 |
| China | 800-820-8682 |
| Hong Kong | 800-96-5941 |
| India | 1-800-425-7888 |
| Indonesia | 001-803-8861-1006 |
| Korea | 080-551-2804 |
| Malaysia | 1-800-80-3973 |
| New Zealand | 0800-446-934 |
| Philippines | 1-800-765-7404 |
| Singapore | 800-886-1028 |
| Taiwan | 0800-006800 |

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

B090712

The platform bar and E2E are trademarks of Texas Instruments. All other trademarks are the property of their respective owners.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to TI's Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2019, Texas Instruments Incorporated