SafeTI™ Functional Safety: A tunable FMEDA for C2000™ MCUs

Jitin George
Product Marketing Engineer
C2000™ Microcontrollers,
Texas Instruments

With the ever-increasing focus on functional safety in industrial and automotive markets, product manufacturers are constantly challenged to minimize risks due to system malfunctions.

Designing systems targeted at safety-critical applications involves adhering to a rigorous hardware development process, along with the implementation of safety mechanisms/diagnostics to increase robustness against systematic and random hardware faults. Safety analysis is an equally important step in the design of such systems to mitigate the risk of a violation of the functional safety goal due to hardware component malfunctions.

A failure mode, effects and diagnostic analysis (FMEDA) provides data on failure modes – data that's required when quantifying risk reduction for the violation of a functional safety goal. An FMEDA is used in the development stage of a customer's system and provides a detailed analysis of different failure modes, the associated effects of failure modes, diagnostics and the impact of any implemented diagnostics/safety mechanisms in terms of diagnostic coverage.

A Texas Instruments (TI) C2000 microcontroller (MCU)-based FMEDA comes with the added benefit of tunability, with features such as package failures in time (FIT) estimation, product function tailoring, safety mechanism tailoring and custom diagnostics, allowing customers to tune the FMEDA to the application-specific use of a TI MCU in their systems.

The need for a tunable FMEDA

Microcontrollers are usually developed as a safety element out of context (SEooC), i.e. development takes place without any knowledge of the end application. TI creates the associated FMEDA without knowledge of the final application and is based on assumed functional safety requirements. Once the end application and associated functional safety requirements are known, the FMEDA needs to be tailored to match the desired configuration of the application in order for it to yield accurate results. With most static/non-tunable FMEDAs, only the MCU manufacturer can perform tailoring of the FMEDA.

This approach might sound feasible, but has its own drawbacks. First, it might not be the best option for customers wanting to protect their intellectual property; the MCU manufacturer may require the disclosure of certain application-specific details to tailor the FMEDA to a particular need. Second, there is the inconvenience of reaching out to the MCU manufacturer to tune the FMEDA every time there is a change in application design that results in a change in functional safety requirements.

To support functional safety system designers, TI provides a truly customizable solution that gives customers complete control, allowing them to tailor the FMEDA to their own application-specific needs without having to rely on anyone else.

Benefits of the C2000 MCU FMEDA

As stated earlier, an MCU FMEDA is created based on assumed functional safety requirements. As these requirements change, the FMEDA needs

to be tailored accordingly. The C2000 FMEDA provides a variety of different options to tailor the FMEDA based on the end application in which the MCU is used. Let's explore some of these features and associated benefits by looking at the F2837x/F2807x FMEDA as an example.

Product function tailoring

The product function tailoring feature allows customers to select only those parts and sub-parts of the MCU that are used in their end application and mark them yes if they are functional safety-related or no if they are not, as shown in **Figure 1**. This includes on-chip memories (static random access memory [SRAM] and flash) as well as on-chip peripherals.

The F2837x/F2807x FMEDA sets the default utilization of on-chip resources at 100%, although in reality, the application may not even use all of the peripherals and memories available on the device. Product function tailoring enables customers to easily select the required on-chip resources in the FMEDA to exactly match the end application use case, thereby yielding accurate results.

Package FIT estimation

There may be situations where there is a change in the operating mission profile of the end application. The default setting in the FMEDA may not accurately represent this application use case. For example, the operational profile on the F2837x/F2807x FMEDA is set to the mission profile for automotive motor control applications by default. However, if the MCU were used in any other application, chances are that MCU parameters such as package type and maximum power dissipated

Inputs for application specific tailoring of failure rates

Type	Total size	User size	Unit
CPU1-Mx	4	4	Kbytes
CPU1-Dx	8	8	Kbytes
CPU1-LSx	24	24	Kbytes
CPU2-Mx	4	4	Kbytes
CPU2-Dx	8	8	Kbytes
CPU2-LSx	24	24	Kbytes
GSx	128	128	Kbytes
FLASH	1	1	Mbytes

Modules used for Safety Function/Safety Goal

CPU subsystem	CPU1_CORE	Yes
CPU subsystem	CPU2_CORE	Yes
CPU subsystem	MCLA1	Yes
CPU subsystem	MCLA2	Yes
CPU subsystem	CPU1_DCSM	Yes
CPU subsystem	CPU2_DCSM	Yes
System	CPU1 TIMER0	Yes
System	CPU1 TIMER1	Yes
System	CPU1 TIMER2	Yes
System	CPU2 TIMER0	Yes
System	CPU2 TIMER1	Yes

Figure 1. *Product function tailoring using the F2837x/F2807x FMEDA. All highlighted fields are user customizable.*

Customer input for failure rate estimation

Package used	TI ZWT
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 (0.8 W is based on maximum datasheet value)	1.4
Safe/dangerous ratio Derating to be applied to FIT rates	0%
Confidence level Desired confidence level of FIT rates	70%

Operation 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	$\tau 1$	$(t_{ac})_2$°C	$\tau 2$	$(t_{ac})_3$°C	$\tau 3$	T_{ON}	T_{OFF}	n_1	$\Delta T_{1°C}$	n_2	ΔT_2	n_3	ΔT_3
Profile	32	0.02	60	0.015	85	0.023	0.058	0.942	670	$\Delta T_J/3+55$	1340	$\Delta T_J/3+45$	30	10

Figure 2. *FIT estimation using the F2837x/F2807x FMEDA. All highlighted fields are user customizable.*

would also change, thus requiring the FMEDA to be tuned accordingly.

The FIT estimation feature on the F2837x/F2807x FMEDA enables this level of customization by allowing customers to enter values specific to their own application-specific operational profile, as shown in **Figure 2**.

The F2837x/F2807x FMEDA gives customers the ability to update parameters such as package type and confidence level that affect the rate of permanent failures. Additionally, it enables input for transient fault estimation, which allows user configuration of the neutron flux factor value according to the Joint Electron Device Engineering Council (JEDEC) JESD89A standard.

Safety mechanism tailoring and custom diagnostics

Hardware functional safety requirements at the MCU level are satisfied by implementing safety mechanisms described in the safety manual. However, existing safety mechanisms with their diagnostic coverages may not be adequate when there is a change in functional safety requirements at the application level. In such situations, additional safety mechanisms may need to be defined for the MCU to meet the new functional safety goal. These new safety mechanisms would then need to be associated with the failure modes of the respective parts of the MCU, and the effect of this action would need to be verified by re-computing hardware metrics at the MCU level.

The safety mechanism tailoring feature enables customers to view all available safety mechanisms and provides a way to select required safety mechanisms depending on the functional safety requirements of the end application, as shown in **Figure 3.**

The custom diagnostics feature on the F2837x/F2807x FMEDA is an extension of safety mechanism tailoring and enables customers to view selected safety mechanisms as well as their resulting diagnostic coverage values. The added benefit of this feature is that it provides the ability to add additional custom safety mechanisms and input the corresponding diagnostic coverage values depending on the functional safety concept implemented in the end application. The custom

Safety mechanisms considered in the FMEDA

From safety manual			
Device partition	**Unique identifier**	**Safety feature or diagnostic**	**Diagnostic used in application?**
Power supply	PWR1	External voltage supervisor	1
Power supply	PWR2	External watchdog	1
Clock	CLK1	Missing clock detect	1
Clock	CLK2	Clock integrity check using CPU timer	1
Clock	CLK3	Clock integrity check using HRPWM	1
Clock	CLK5	External monitoring of clock via XCLKOUT	1
Clock	CLK6	Internal watchdog - WD	1
Clock	CLK7	External watchdog	1
Clock	CLK8	Periodic software read back of static configuration registers	1
Clock	CLK9	Software read back of written configuration	1
Clock	CLK10	Software test of watchdog (WD) operation	1
Clock	CLK12	Software test of MCD functionality	1
Clock	CLK13	PII lock profiling using on chip timer	1
Clock	CLK14	Peripheral clock gating (PCLKCR)	1

Figure 3. *Safety mechanism tailoring using the F2837x/F2807x FMEDA. All highlighted fields are user customizable.*

diagnostics feature provides added flexibility by giving customers the option to define their own custom diagnostics in situations where the available safety mechanisms are not sufficient for the application.

Conclusion

An FMEDA plays a key role in application-level safety analysis and provides information on the different failure modes of parts/subparts, the corresponding failure rates and failure mode distribution, and safety mechanisms and their effectiveness. Additionally, it also provides hardware architectural metrics such as single-point fault metric (SPFM), latent fault metric (LFM) and probabilistic metric for random hardware failures (PMHF).

Since an MCU FMEDA is usually not created for any specific end application, there is always the need to tailor the FMEDA once that end application is known. The need for tuning an FMEDA becomes even greater when there are changes in application-specific functional safety requirements, environment parameters or other use-case constraints that the MCU manufacturer may not be able to predict.

A C2000 MCU FMEDA such as the F2837x/F2807x FMEDA provides a flexible and robust solution with features such as product function tailoring, FIT estimation, safety mechanism tailoring and custom diagnostics, enabling customers to independently tune the MCU FMEDA to satisfy their application-specific functional safety requirements with ease.

Additional resources:

C2000™ SafeTI™ Tunable FMEDA Training

C2000 functional safety page

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources 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.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

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