IEC 61508 Functional Safety Compliant/Ready dsPIC33 DSCs

MICROCHIP

microchip.com/dsPIC33-IEC61508

Table of Contents

1. IEC 61508 Functional Safety Ready dsPIC33 DSCs

It is essential for industrial equipment or a system to be functionally safe to identify and prevent unexpected or hazardous operation and maintain a secure workplace. Developing systems that execute the required set of functions accurately as per IEC 61508 standard can help in reducing such risks. Our broad portfolio of IEC 61508 Functional Safety Ready dsPIC33 Digital Signal Controllers (DSCs) offer hardware safety features and functional safety resources to simplify designing your safety-critical industrial applications.

Dedicated hardware safety features have been integrated into dsPIC33 DSCs to help increase the reliability and monitoring in safety-critical applications. These features help ensure that end applications operate as intended, with safe shut down if any exception or issue arises.

dsPIC33 DSCs are designed for reliable operation in harsh environments and make it easy for you to develop high-performance embedded, sensor interfacing, real-time control and automation, digital power and motor control applications targeting IEC 61508 compliance. Whether you are new to IEC 61508 functional safety or a seasoned expert, you can count on our proven experience and solutions to help you meet functional safety requirements while minimizing cost, risk and development time.

2. Functional Safety Support

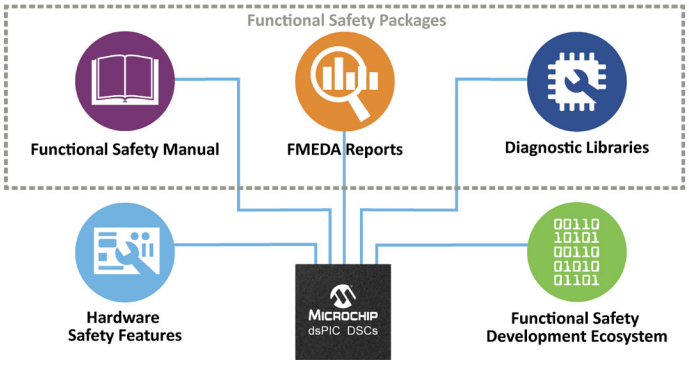
1. Select dsPIC33 DSCs which qualify as IEC 61508 “Functional Safety Compliant” devices are designed by following the IEC 61508 compliant development process
2. Failure Modes, Effects, and Diagnostic Analysis (FMEDA) report
3. Functional Safety Manual (FSM)
4. Functional safety reference application
6. TÜV Rheinland-certified functional safety development process and diagnostic libraries
7. Development ecosystem
8. Supporting safety collateral including Pin FMEA and Dependent Failure Analysis (DFA)
9. Functional safety compliant co-operative scheduler with FMEA, user manual and confirmation review files
10. Certified SAFERTOS® by WITTENSTEIN high integrity systems

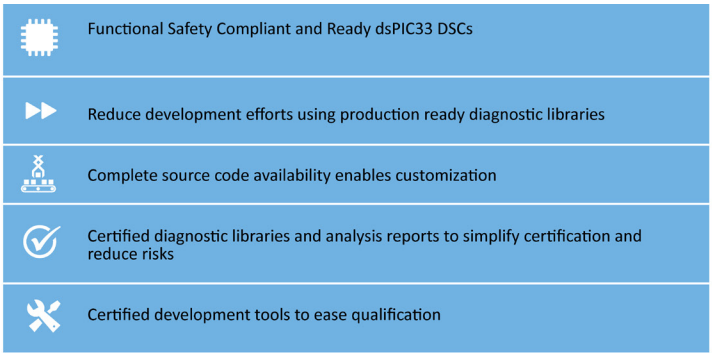
3. To simplify the development of industrial safety applications, we offer:

1. IEC 61508 Functional Safety Basic Package
2. IEC 61508 Functional Safety Starter Package
3. IEC 61508 Functional Safety Advanced Package

4. Functional Safety Support for dsPIC33 DSCs

		Functional Safety Ready	Functional Safety Compliant
Development Process	Device development flow	Quality Managed*	IEC 61508
Analysis Report	FMEDA	✓	✓
Diagnostics	Functional Safety Manual (FSM)	✓	✓
	Diagnostic software libraries and associated reports	✓	✓
Certification	For IEC 61508	TÜV Rheinland Certified Diagnostic Libraries	TÜV Rheinland Certified Hardware and Software Development Flow targeting IEC 61508 TÜV Rheinland Certified Diagnostic Libraries
Product Families		All dsPIC33C DSCs except dsPIC33CK1024MP7xx family	dsPIC33CK1024MP7xx family and All dsPIC33A DSCs except dsPIC33AK128MC1xx family





5. Certified Functional Safety Management System

Microchip implements IEC 61508 compliant Functional Safety Management System which is up to and including Safety Integrity Level 3 (SIL3) and Systematic Capability 3 (SC3) of IEC 61508. Our Functional Safety Management System has been certified by TUV-Rheinland.

6. Failure Modes, Effects, and Diagnostic Analysis (FMEDA) Report

The FMEDA report for a given Functional Safety Ready dsPIC33 DSC quantifies the device's fault modes, its Failure-In-Time (FIT) rate distribution and corresponding detection methods to help create a coverage plan.

FMEDA is a crucial tool in functional safety development because it provides a structured approach to identifying, analyzing, and mitigating risks associated with system failures. It ensures that systems are designed to meet stringent safety standards and helps improve their overall safety and reliability.

Microchip's FMEDA provides the maximum flexibility to our customers in tuning the parameters to the use case:

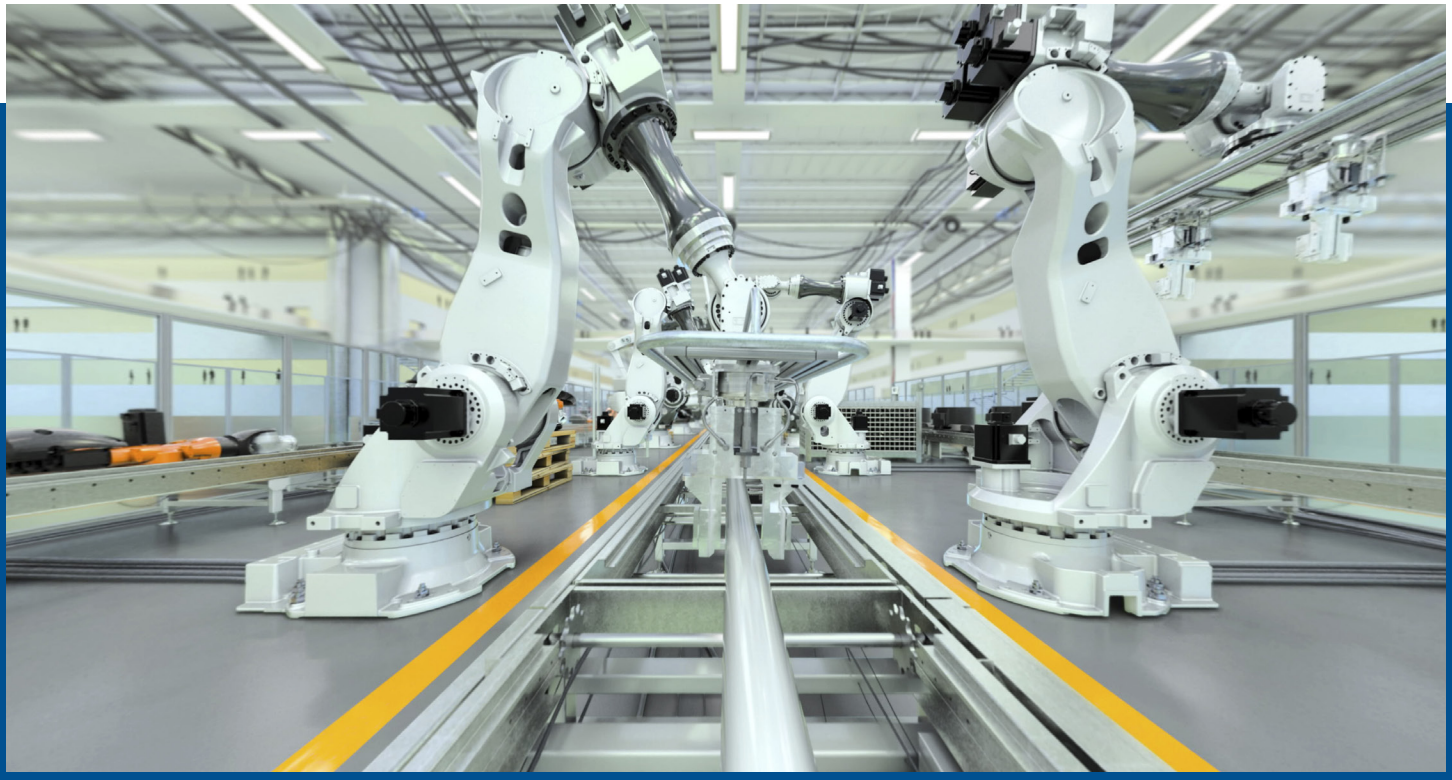
- Adjustable mission profile (includes operating temperature, lifetime, power ratings, exact device safety configuration etc.)
- Base FIT rate upon SN29500, on request for IEC 62380
- Ability to cover several safety goals

7. Functional Safety Manual (FSM)

The Functional Safety Manual for a given Functional Safety Ready dsPIC33 DSC provides details on the fault detection methods described in the FMEDA report and offers recommendations on how the device should be used for the safest operation. It includes a description of dependent failures and hardware features for detecting systematic failures, which can be used for developing diagnostic libraries.

8. Functional Safety Reference Application

If you are new to the IEC 61508 Functional Safety Standard and trying to understand how to use FMEDA report, Functional Safety Manual, Functional Safety Diagnostic libraries, and associated tools in your new safety-critical application, the Functional Safety Reference Application can help you jumpstart your design. Based on the dsPIC33 DSC, this data monitoring reference application implemented on the Explorer 16/32 Development Board (DM240001-3) with dsPIC33CH512MP508 Plug-in- Module (MA330046) serves as a reference project.



9. TÜV Rheinland Certification

We offer functional safety software mechanisms for several modules* that can detect random system failures and help achieve functional safety goals.

- Fault injection routines to test system response under a fault condition
- Static and dynamic code analysis and traceability reports to track and achieve consistency between requirements, realization, and verification of safety functionalities
- Tight integration with recommended diagnostics in the FMEDA and Functional Safety Manual
- Availability of test benches and project files on request to verify conformance of libraries to safety standards

Note: As part of the Functional Safety Advanced Packages, the latest available version of the Diagnostic libraries will be made available which can be a newer version compared to the version certified by TÜV-Rheinland or the same certified version. The latest version of the Diagnostic libraries offered may include new updates and bug fixes (if any).

*The complete list of supported modules and diagnostic functions offered within the libraries in IEC 61508 functional safety starter and advanced packages are shared under NDA.

9.1 Achieving Higher Safety Levels

Higher safety levels are typically achieved through redundancy, which can be implemented using multiple devices.

Example:

SIL 3 can be targeted using multiple devices via SIL decomposition

SIL 3 = SIL 2 (MCU) + SIL 2 (MCU), where the combination of the MCUs enables meeting the SIL 3 safety goals

10. Development Ecosystem for Functional Safety

Microchip offers TÜV SÜD-certified design tool package that supports our Functional Safety Ready dsPIC33 DSCs to make your tool qualification effort easier. The MPLAB® XC16 and XC-DSC Functional Safety Compiler Licenses include all the documentation and reports needed to have a fully qualified IEC 61508 development environment. The documentation package includes TÜV SÜD certificates, a functional safety manual, safety plan, classification and qualification reports for our tools shown below:

- TÜV SÜD-certified MPLAB XC16 Functional Safety Compiler (SW006022-FS)
- TÜV SÜD-certified MPLAB XC-DSC Functional Safety Compiler (SW006024-2)
- MPLAB X Integrated Development Environment (IDE), MPLAB debugger/programmers and associated documentation to ease safety qualification
- MPLAB Analysis Tool Suite Workstation License (SW006027-2)

10.1 Supported Third-Party Tools

Support for third-party tools from vendors such as Liverpool Data Research Associates (LDRA) Tool Suite.

To learn more, visit www.microchip.com/mplab-development-ecosystem-for-functional-safety.

10.2 Functional Safety Compliant Co-operative Scheduler

Microchip provides a functional safety compliant cooperative scheduler tailored for safety-critical applications, specifically designed to meet the stringent requirements of the IEC 61508 safety standard for automotive systems. This scheduler ensures that tasks are executed in a precise and reliable manner, offering the following key capabilities:

1. Co-operative scheduling for task management
2. Deterministic behavior for order and time of execution
3. Task prioritization for critical operations
4. Error handling, recovery and safety compliance

10.3 SAFERTOS® for Safety-Critical Applications

SAFERTOS, by WITTENSTEIN high integrity systems, is an IEC 61508 pre-certified safety Real-Time Operating System (RTOS), and it is compatible with our dsPIC33 DSCs.

To learn more about the devices supported, visit https://www.highintegritysystems.com/partners/microchip/

To learn more about the tools ecosystem, visit www.microchip.com/mplab-development-ecosystem-for-functional-safety

11. IEC 61508 Functional Safety Packages for dsPIC33 DSCs

Take advantage of our IEC 61508 Functional Safety packages for the dsPIC33 DSCs to kick-start the design of your new safety-critical application. We offer:

IEC 61508 Functional Safety Basic Package for dsPIC33 DSCs: Provides basic resources like FMEDA report and the Functional Safety Manual to get you started with the evaluation of target functional safety levels and the design of a safety-critical industrial application.

IEC 61508 Functional Safety Starter Package for dsPIC33 DSCs: Provides basic resources available as part of the Basic Package and the diagnostic source code for select modules for you to get started with your design. This package also offers the reference application that helps you understand how to approach the complex design of safety-critical application and integrate diagnostic routines into your application to achieve defined safety goals.

IEC 61508 Functional Safety Advanced Package for dsPIC33 DSCs: An advanced package for both beginners and seasoned experts to simplify the design and certification of safety-critical industrial application.

Annual Renewal: An optional annual renewal package to receive updates to the IEC 61508 Functional Safety Advanced Packages for dsPIC33 DSCs after 1 year from the date of purchase.

12. Functional Safety Package Offerings For dsPIC33 DSCs

Functional Safety Solutions for dsPIC33 DSCs	IEC 61508 Functional Safety Basic Package	IEC 61508 Functional Safety Starter Package	IEC 61508 Functional Safety Advanced Package
FMEDA Report	✓	✓	✓
Functional Safety Manual (FSM)	✓	✓	✓
Functional Safety Reference Application – Source Code and User's Guide	–	✓	✓
Functional Safety Diagnostics Overview Document	–	✓	✓
FMEA and FSM for Diagnostic Libraries	–	✓	✓
Cooperative Scheduler	–	✓	✓
Functional Safety Compliance/ Certification	–	SIL 3 compliant diagnostic libraries along with the source code for select modules*	TÜV Rheinland-certified diagnostic libraries for designs targeting up to SIL 3 (through decomposition). The libraries offer complete source code for several modules*
TÜV-Rheinland Certificate	–	–	✓
Functional Safety Analysis Reports	–	–	✓

Note: Functional Safety Basic Package, Functional Safety Starter Package, Functional Safety Advanced Packages, annual renewal and the recommended development tools are subject to commercial terms. The Functional Safety Starter Package and the Functional Safety Advanced Packages have a dependency on the corresponding Functional Safety Compiler version.

*The complete list of supported modules and diagnostic functions offered within the libraries in IEC 61508 functional safety starter and advanced packages are shared under NDA.

13. IEC 61508 Functional Safety Compliant/Ready dsPIC33 DSCs

Functional Safety Readiness	Description	Target Applications	Functional Safety Compliant/ Ready	FMEDA	Functional Safety Manual	Certified Diagnostic Library
dsPIC33AK512MPS512	200 MHz, Up to 512 KB Flash, FPU AEC Q100 Grade 0 (150°C)	High-performance Real-time Control, Motor Control, Digital Power, Capacitive Sensing, Sensor Interfacing and Measurement Control	FuSa Compliant	Now	Now	Now
dsPIC33AK512MC510	200 MHz, Up to 512 KB Flash, FPU AEC Q100 Grade 0 (150°C)		FuSa Compliant	Now	Now	Now
dsPIC33AK256MPS306	200 MHz, Up to 256 KB Flash, FPU AEC Q100 Grade 0 (150°C)		FuSa Compliant	Now	Now	Planned
dsPIC33AK128MC106	200 MHz, Up to 128 KB Flash, FPU AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Planned
dsPIC33CH512MP508 (Dual Core)	90 + 100 MHz, Up to 512 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CH128MP508 (Dual Core)	90 + 100 MHz, Up to 128 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Roadmap
dsPIC33CK1024MP710	100 MHz, Up to 1024 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Compliant	Now	Now	Now
dsPIC33CK512MPT608	100 MHz, Up to 512 KB Flash Secure DSC AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CK512MP608	100 MHz, Up to 512 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CK256MP508	100 MHz, Up to 256 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CK64MP105	100 MHz, Up to 64 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CK256MC506	100 MHz, Up to 256 KB Flash AEC Q100 Grade 0 (150°C)	High-performance Real-time Control, Motor Control, Capacitive Sensing, Sensor Interfacing and Measurement Control	FuSa Ready	Now	Now	Now
dsPIC33CK64MC105	100 MHz, Up to 64 KB Flash AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CDVC256MP506	Up to 256 KB Flash, 12V MOSFET Driver, CAN-FD Tranceiver AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CDV256MP506	Up to 256 KB Flash, 12V MOSFET Driver AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CDVL256MC506	Up to 256 KB Flash, 12V MOSFET Driver, LIN Tranceiver AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Future
dsPIC33CDV256MC506	Up to 256 KB Flash, 12V MOSFET Driver, AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Future
dsPIC33CDV64MC106	Up to 64 KB Flash, 12V MOSFET Driver AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CDVL64MC106	Up to 64 KB Flash, 12V MOSFET Driver, LIN Transceiver AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now

14. Embedded Security

Our dsPIC33 DSCs are equipped with advanced security features to ensure protection in embedded applications. These include secure boot and firmware updates, secure debug with debug entry disablement, and an Immutable Root of Trust (IRT) for implementing chain of trust. Code protection and a security module with cryptographic accelerators enhance data safety, while ICSP program/erase disable allows flash to be configured as One-Time Programmable (OTP) memory. Additionally, firmware IP and Flash write protection safeguard against unauthorized access and modifications.

Microchip Technology Inc. | 2355 W. Chandler Blvd. | Chandler AZ, 85224-6199 | microchip.com

DS00004349I