

ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSCs



Table of Contents

ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSCs.....	3	Development Ecosystem for Functional Safety	8
Functional Safety Solution	3	Supported Third-Party Tools	8
To simplify development of your safety-critical applications, we offer:.....	3	Functional Safety Compliant Co-operative Scheduler	8
Functional Safety Support for dsPIC33 DSCs	4	SAFERTOS® for Safety-Critical Applications	8
Certified Functional Safety Management System.....	5	ISO 26262 Functional Safety Packages for dsPIC33 DSCs.....	9
Failure Modes, Effects, and Diagnostic Analysis (FMEDA) Report.....	5	Functional Safety Package Offerings For dsPIC33 DSCs.....	10
Functional Safety Manual (FSM).....	5	ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSC	11
Functional Safety Reference Application	5	Functional Safety Compliant MCALs, AUTOSAR and OSEK for the Functional Safety Compliant/Ready dsPIC33 DSCs	12
Application Note: ISO 26262 Functional Safety: Implementation of a Safety Element out of Context (AN3864)	6	ISO 26262 Functional Safety Touch	12
Achieving Higher Safety Levels.....	6	Embedded Security	12
TÜV Rheinland Certification.....	7		



1. ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSCs

Designing automotive applications that are safety-critical is a challenge as they demand reliable operation and must ensure user safety. Microchip's dsPIC33 Digital Signal Controllers (DSCs) can be used in safety-critical high-performance embedded, sensor interfacing, capacitive touch, digital power, and motor control applications for the automotive market targeting ISO 26262 compliance.

Whether you are new to the ISO 26262 functional safety or a seasoned expert, you can count on Microchip's proven experience to help you meet functional safety requirements while minimizing cost, risk, and development time. Our Functional Safety Compliant/Ready dsPIC33 DSCs offer the following resources to simplify ISO 26262 ASIL B certification of your automotive designs.



2. Functional Safety Solution

1. Select dsPIC33 DSCs which qualify as "Functional Safety Compliant" devices are designed by following the TÜV Rheinland-certified ISO 26262 compliant development process
2. Failure Modes, Effects, and Diagnostic Analysis (FMEDA) report
3. Functional Safety Manual (FSM)
4. Functional safety reference application
5. Application note - ISO 26262 Functional Safety: Implementation of a Safety Element out of Context (AN3864)
6. TÜV Rheinland-certified functional safety 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
11. Functional safety compliant MCALs, AUTOSAR and OSEK
12. ISO 26262 Functional Safety Touch packages

3. To simplify development of your safety-critical applications, we offer:

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



4. Functional Safety Support for dsPIC33 DSCs

		Functional Safety Ready	Functional Safety Compliant
Development Process	Device development flow	Quality Managed*	ISO 26262
Analysis Report	FMEDA	✓	✓
Diagnostics	Functional Safety Manual (FSM)	✓	✓
	Diagnostic software libraries and associated reports	✓	✓
Certification	For ISO 26262	TÜV Rheinland Certified Diagnostic Libraries	TÜV Rheinland Certified Hardware and Software Development Flow targeting ISO 26262 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 ISO 26262 compliant Functional Safety Management System which is up to and includes Automotive Safety Integrity Level ASIL D. 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 Compliant/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:

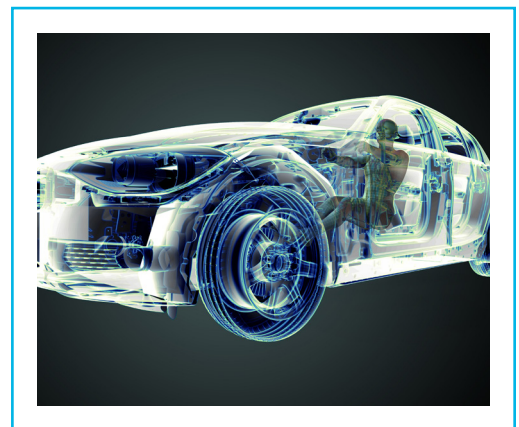
- Adjustable mission profile (includes operating temperature, lifetime, power ratings, exact device safety configuration etc.)
- Base FIT rate upon SN29500, on request for IEC 62380
- Ability to cover several safety goals

7. Functional Safety Manual (FSM)

The Functional Safety Manual for a given Functional Safety Compliant/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 ISO 26262 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) can serve as an example project.





9. Application Note: ISO 26262 Functional Safety: Implementation of a Safety Element out of Context (AN3864)

The ISO 26262 Functional Safety Application Note (AN3864) introduces the main concepts of the ISO 26262 safety standard and focuses on the implementation of a “Safety Element out of Context” (SEooC), covering the hardware and software aspects viewed from the very specific perspective of safety. The application note helps you with the following:

- A general overview of the main aspects/parts of the ISO 26262 Standard and help understand the basics, with a specific focus on safety element out of context
- Provide guidelines in the development of a system using a functional safety reference application
- Show the steps required by a development compliant with the ISO 26262 Standard and the information and artifacts that must be generated by the designer for compliance

9.1 Achieving Higher Safety Levels

Higher safety levels are typically achieved by redundancy. This can be implemented by multiple dsPIC33 devices. Example: ASIL C or ASIL D can be targeted using multiple devices via ASIL decomposition

ASIL C = ASIL B(C) + ASIL A(C)

ASIL D = ASIL B(D) + ASIL B(D), where the combination of the DSCs enables meeting the ASIL C or ASIL D safety goals.



10. TÜV Rheinland Certification

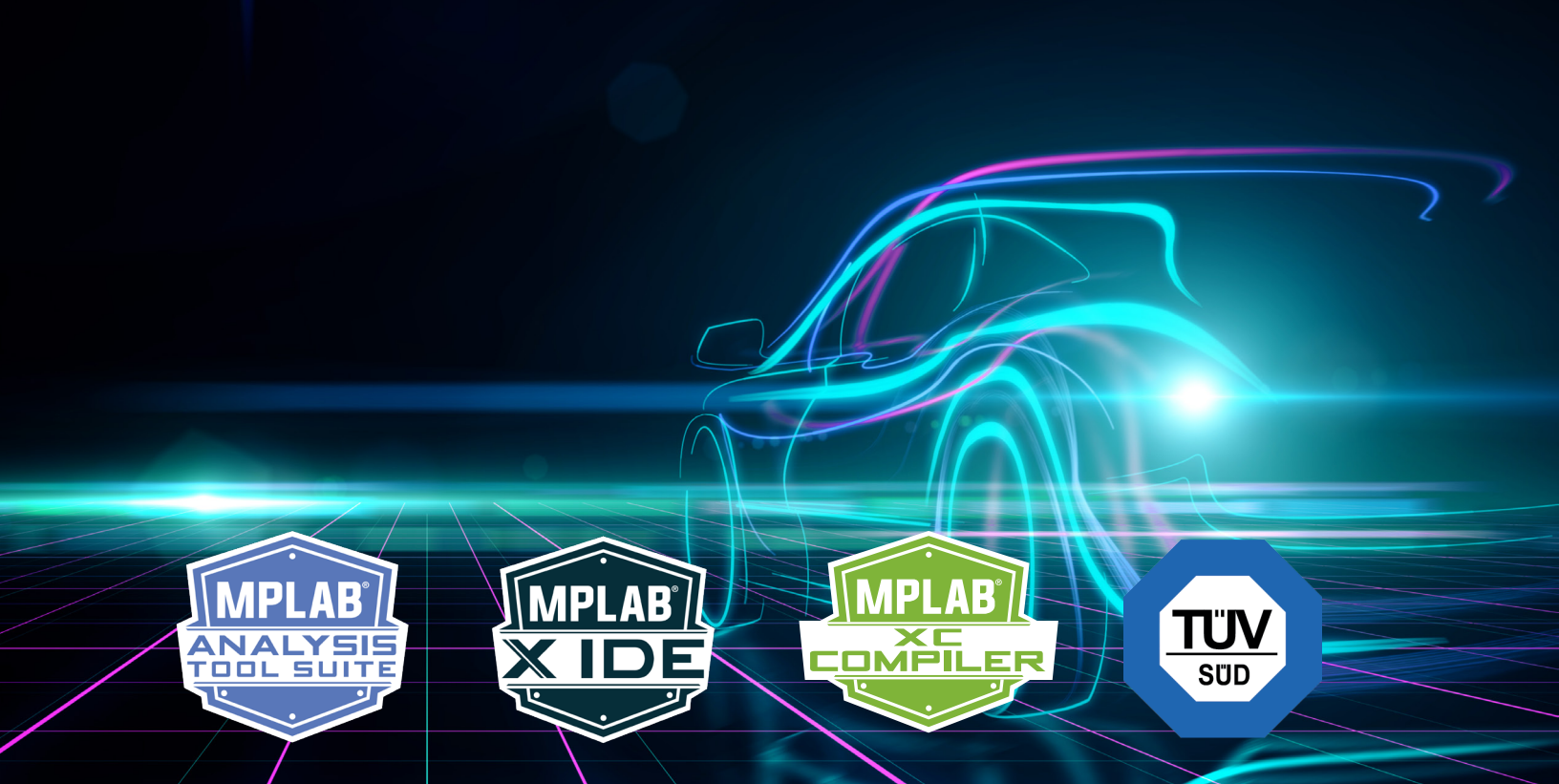
We offer functional safety software mechanisms for several modules* that can detect random system failures and help achieve functional safety goals.

- 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 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 ISO 26262 functional safety starter and advanced packages are shared under NDA.



11. Development Ecosystem for Functional Safety

Microchip offers TÜV SÜD-certified design tool package that supports our Functional Safety Compliant/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 ISO 26262 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)

11.1 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

11.2 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 ISO 26262 safety standard for automotive systems. This scheduler ensures that tasks are executed in a precise and reliable manner, offering the following key capabilities:

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

11.3 SAFERTOS® for Safety-Critical Applications

SAFERTOS, by WITTENSTEIN high integrity systems, is an ISO 26262 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



12. ISO 26262 Functional Safety Packages for dsPIC33 DSCs

Take advantage of our ISO 26262 Functional Safety packages for the dsPIC33 DSCs to kick-start the design of your new safety-critical application. We offer:

- **ISO 26262 Functional Safety Basic Package for dsPIC33 DSCs:** Offers basic resources to get started with designing your functional safety application
- **ISO 26262 Functional Safety Starter Package for dsPIC33 DSCs:** Helps to kick-start the design of new safety-critical application by enabling you to understand the overall steps required for the development
- **ISO 26262 Functional Safety Advanced Package for dsPIC33 DSCs:** An advanced package for beginners and seasoned experts to simplify the design and certification of safety-critical application
- **Annual Renewal:** An optional annual renewal package to receive updates to the ISO 26262 Functional Safety Advanced Packages for dsPIC33 DSCs after 1 year from the date of purchase



13. Functional Safety Package Offerings For dsPIC33 DSCs

Functional Safety Solutions for dsPIC33 DSCs	ISO 26262 Functional Safety Basic Package	ISO 26262 Functional Safety Starter Package	ISO 26262 Functional Safety Advanced Package
FMEDA Report	✓	✓	✓
Functional Safety Manual (FSM)	✓	✓	✓
Functional Safety Reference Application – Source Code and User's Guide	-	✓	✓
Functional Safety Reference Application Note (AN3864)	-	✓	✓
Functional Safety Diagnostics Overview Document	-	✓	✓
Functional Safety Compliance/Certification	-	ASIL C compliant diagnostic libraries along with the source code for select modules*	TÜV Rheinland-certified diagnostic libraries for designs targeting up to ASIL C (through decomposition). The libraries offer complete source code for several modules*
FMEA and FSM for Diagnostic Libraries	-	✓	✓
Cooperative Scheduler	-	✓	✓
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 ISO 26262 functional safety starter and advanced packages are shared under NDA.

14. ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSC

ISO 26262 Functional Safety Compliant/Ready dsPIC33 DSCs	Description	Target Applications	Functional Safety Compliant/Ready	FMEDA Report	Functional Safety Manual	Diagnostic Libraries
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 AEC Q100 Grade 1 (125°C) Secure DSC		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 Transceiver AEC Q100 Grade 0 (150°C)	Motor Control	FuSa Ready	Now	Now	Now
dsPIC33CDV256MP506	Up to 256 KB Flash, 12V MOSFET Drivers AEC Q100 Grade 0 (150°C)		FuSa Ready	Now	Now	Now
dsPIC33CDVL256MC506	Up to 256 KB Flash, 12V MOSFET Driver, LIN Transceiver 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
dsPIC33EV256GM106 dsPIC33EV128GM106	70 MHz, 5V Up to 256 KB Flash AEC Q100 Grade 0 (150°C)	5V Robust Designs, Motor Control, High-performance Real-time Control, Capacitive Sensing, Sensor Interfacing and Measurement Control	FuSa Ready	Now	Now	-

15. Functional Safety Compliant MCALs, AUTOSAR and OSEK for the Functional Safety Compliant/Ready dsPIC33 DSCs

AUTOSAR addresses the challenge of increasing software complexity by providing an open and exchangeable solution to standardize software architecture for automotive Electronic Control Units (ECUs). This enables automotive designers to create innovative electronic systems that offer improved quality, performance, safety, and security.

As an associate partner of the AUTOSAR standard, we offer production ready Microcontroller Abstraction Layer (MCAL) software for our Functional Safety Compliant/Ready dsPIC33 DSCs. This software development solution complies with Automotive SPICE® and ISO 26262 standards. In addition to this, you can also take advantage of:

- Vector's MICROSAR supporting the dsPIC33 DSCs
- KPIT's AUTOSAR OS supporting the dsPIC33 DSCs

The Functional Safety Compliant MCALs from Microchip are subject to commercial terms. Solutions from our partners including Vector's MICROSAR and KPIT's AUTOSAR OS are subject to 3rd party terms and conditions.

16. ISO 26262 Functional Safety Touch

The ISO26262 Functional Safety Touch packages for core independent touch DSCs enable to develop automotive safety-compliant touch applications. The Functional Safety Touch packages* include:

- ASIL-B and ASPICE L1-compliant functional safety touch library
- Functional safety manual
- Functional safety touch reference application with user's guide
- Functional safety library integration guide
- Static and dynamic code reports (advanced package)
- Safety analysis reports

Learn more: <https://www.microchip.com/en-us/products/microcontrollers/dspic-dscs/applications/capacitive-touch>

*Note: Functional safety packages for TÜV Rheinland certified diagnostic software libraries for dsPIC33 DSCs must be purchased separately. The ISO 26262 Functional Safety Touch packages are currently available for dsPIC33C family of devices.

Please contact your local [Microchip Sales Office](#) for additional information or our [Client Success Team](#) who can assist you with sales, product inquiries and support on new designs.

Please contact dsPIC33.functionalsafety@microchip.com for assistance

17. 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.