Functional safety packages
STM32 MCUs and MPUs
STM8 MCUs
“If only I could speed up the design time of safety-certified systems

This is where we come in
Free safety packages for STM32 and STM8 and an ecosystem of ST Authorized Partners
With its **Functional Safety Packages** based on robust built-in MCU/MPU safety features, ST provides a comprehensive set of certified software libraries and documentation for manufacturers to significantly reduce the development efforts, time and cost to achieve functional safety standard certifications.

- **SIL Functional Safety Package** for industrial IEC 61508 (STM32)
- **ASIL Functional Safety Package** for automotive ISO 26262 (STM8A)
- **Class B Functional Safety Package** for household electrical appliances IEC 60335-1/60730-1 (STM32 & STM8)
## STM32 built-in safety features

<table>
<thead>
<tr>
<th>Features</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>F3</th>
<th>G4</th>
<th>F2/F4</th>
<th>F7</th>
<th>H7</th>
<th>L0/L1</th>
<th>L4/L4+</th>
<th>L5</th>
<th>WB</th>
<th>MP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual watchdogs: Independent watchdog and system window watchdog</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Backup clock circuitry with clock security system (CSS)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Hardware CRC unit / Programmable polynomial</td>
<td>● / *</td>
<td>● / -</td>
<td>● /</td>
<td>● /</td>
<td>● / -</td>
<td>● /</td>
<td>● /</td>
<td>● / -</td>
<td>● /</td>
<td>● /</td>
<td>● /</td>
<td>● / *</td>
<td>● / *</td>
</tr>
<tr>
<td>Supply monitoring (POR, BOR, PVD)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>I/O function locking</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>PWM critical register protections (write-once registers)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Memory protection unit (MPU) 8 zones – to ensure data integrity from invalid behavior</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Multiple Flash memory protection levels</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>PWM stop on core lockup</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Parity bit for SRAM memory (1bit/byte)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>ECC (SECDED) for SRAM</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>ECC (SECDED) for Flash memory</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

**Note:** Cortex-M cores also have built-in safety features (dual stack pointer, fault exceptions, and debug module). *: Depending on part number
SIL functional safety package for STM32

Reduce time and cost to build STM32-based systems certified to IEC 61508 industrial safety standard

- SIL2/SIL3
- Customer Development
- Certified STM32 Self-Test Library X-CUBE-STL
- Safety Documentation
- MCU Safety Features
- Product Portfolio
- ST Quality foundations
ST provides a complete, certified offering to
- Lower project costs
- Reduce design complexity
- Ease SIL certification assessment
SIL functional safety for STM32 safety documentation

Safety manuals: detailed list of safety requirements (conditions of use) and examples to guide STM32 users to achieve safety integrity level certification in compliance with IEC 61508.

Available at STM32 series level for free download on www.st.com/x-cube-stl

FMEA: detailed list of MCU/MPU failure modes and related mitigation measures adopted

FMEDA: static snapshot reporting IEC 61508 failure rates, computed at both MCU/MPU and basic function detail levels.

Available on demand at STM32 series level (*)(**) on www.st.com/x-cube-stl

(*) submitted to NDA
(**) FMEDA snapshot is generated for a specific set of part numbers
SIL functional safety package for STM32
X-CUBE-STL self-test libraries

• Software-based diagnostic suite designed to detect random hardware failures in safety-critical STM32 core components (CPU + SRAM + Flash memory)
• Diagnostic coverage verified by state-of-the-art ST proprietary fault injection methodology
• Application independent: can be potentially used in any end customer application
• Compiler independent: delivered as object code
• Certified by TÜV Rheinland¹
• IEC 61508 SC3 compliant
• Provided with safety manual and user guide

Available on demand at STM32 series level²
www.st.com/x-cube-stl

(1) The original certificate and the updated list of certificated software versions can be downloaded from TÜV Rheinland websites: www.fsproducts.com, www.certipedia.com
(2) submitted to NDA
ST builds functional safety solutions for its STM32 Arm® Cortex®-M microcontroller family, including detailed and accurate safety analyses supported by verification activities based on state-of-the-art fault injection methods.
Achieve SIL2/SIL3 with STM32

<table>
<thead>
<tr>
<th>SIL2</th>
<th>Achievable with single STM32 (1oo1 architecture)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL3</td>
<td>Achievable with two STM32 (1oo2 architecture)</td>
</tr>
</tbody>
</table>

1oo1: 1 out of 1 MCU (no redundancy)

1oo2: 1 out of 2 MCUs (1 redundant system)
STM8A-SafeASIL Functional Safety Package

Reduce time and cost to build STM8A-based systems certified to ISO 26262 automotive functional safety standard

ASIL A/B

Customer Development

Specification for Self-Test Library
Safety documentation
MCU Safety Features
Product Portfolio

ST Quality foundations
STM8A-SafeASIL
safety documentation

Safety manual: Detailed list of safety requirements and examples to support STM8AF and STM8AL use in applications that need to fulfill functional safety requirements as defined by automotive safety integrity level ASIL B of ISO 26262.

Available for STM8AF and STM8AL series for free download on www.st.com/stm8safety

FMEA: detailed list of MCU failure modes and related mitigation measures adopted

FMEDA: static snapshot reporting ISO 26262 failure rates, computed at both MCU / basic function detail levels.

Available on demand for STM8AF and STM8AL (*)
Ask your local ST contact.

(*) submitted to NDA
full list of detailed safety requirements enabling STM8AF and STM8AL users to realize, in the framework of their ISO26262-compliant software development process, the software Self-test Library required by STM8AF or STM8AL Safety Manual to support application up to ASIL B.

The quality of the specification document allows its direct use in a development process compliant to ISO26262-6 requirements.

The specification includes the evidences and rationales behind the generation of the safety requirements for the completeness of end-user safety case.

Application independent: can be used in potentially any end-user application.

on demand for STM8AF and STM8AL series (*)
Ask your local ST contact

(*) submitted to NDA
ClassB functional safety package for STM32 and STM8 MCUs

Reduce time and cost to build STM32 & STM8 based systems certified to IEC 60335-1 and 60730-1 household electrical appliance safety standards.

- **Certified** ST self-test libraries
- **Optimized** code based on STM32CubeHAL
- **Safety manuals** (guidelines and examples)
- For STM32: Support of IAR™ EWARM, Keil® MDK-ARM, and STM32CubeIDE
- **Worldwide standards coverage** (IEC, UL, and CSA)
# ClassB functional safety package for STM32 and STM8 MCUs

<table>
<thead>
<tr>
<th>Package name</th>
<th>X-CUBE-CLASSB</th>
<th>STM8-SafeClassB</th>
</tr>
</thead>
</table>
| **STM32 Series covered**           | V2.2.0 - STM32F0, F1, F3, F2, F4, F7, STM32L0, L1, L4  
                                     | V2.3.0 - STM32G0, G4, WB, H7 | STM8AF           
                                     |                           | STM8AL           
                                     |                           | STM8L             
                                     |                           | STM8S             |
| **Self-test libraries based on**    | STM32CubeHAL  | Optimized direct access to STM8 registers |
| **Supported development environments** | IAR Embedded Workbench®, ARM KEIL®, STM32CubeIDE | IAR Embedded Workbench®, Cosmic® |
| **Certification**                   | UL@2017 & 2019 | UL & VDE@2018   |
| **IEC 60335-1 and 60730-1 international standards coverage** | IEC, UL and CSA |
| **Safety manual (guidelines)**      | AN4435         | AN3181          |
ClassB safety manuals

Guidelines and examples for STM32 and STM8 users to achieve Class B certification in compliance with IEC 60335-1 and 60730-1.
# Functional Safety Packages for STM32 & STM8 MCUs

<table>
<thead>
<tr>
<th>MCU support</th>
<th>Achievable safety standards</th>
<th>Certification</th>
<th>Package content</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32</td>
<td>IEC 61508</td>
<td></td>
<td>• Safety Documentation • Self Test Libraries</td>
<td>X-CUBE-STL</td>
</tr>
<tr>
<td>STM8A</td>
<td>ISO 26262</td>
<td></td>
<td>• Safety Documentation • Self-Test Library specification</td>
<td>STM8A-SafeASIL</td>
</tr>
<tr>
<td>STM32</td>
<td>IEC, UL, CSA 60335-1 60730-1</td>
<td></td>
<td>• Safety Documentation • Self Test Libraries</td>
<td>X-CUBE-CLASSB</td>
</tr>
<tr>
<td>STM8</td>
<td></td>
<td></td>
<td>• Safety Documentation • Self Test Libraries</td>
<td>STM8-SafeCLASSB</td>
</tr>
</tbody>
</table>
Get support from ST authorized partners

Reduce your project time and cost

Safety Requirements → HW & SW Design → Validation → Certification

Functional Safety expertise
Functional safety authorized partners

**Embedded Software**
- arm KEIL
- Embedded Office
- express logic
- SEGGER
- WITTENSTEIN

**Software Development Tools**
- arm KEIL
- IAR Systems

**Engineering, consulting, development or design services**
- EmbEx
- Hitex
- Innotec
- MESCO
- NewTec

**Training**
- Innotec
Arm Compiler for Functional Safety

Qualified toolchain for safety development

Safety Standards:
- IEC 61508 (Industrial) – SIL 3
- ISO 26262 (Automotive) – ASIL D
- EN 50128 (Railways) – SIL 4
- IEC 62304 (Medical) – CLASS C

*At any Safety Integrity Level

Safety Qualified Toolchain
Simplifies Tool Justification
- TÜV Certificate by TÜV SUD
- Qualification Kit
  - Safety Manual
  - Defect Report

Licensed as ‘Standalone’ or via Arm IDE Toolkits:
- Arm Development Studio
  - Gold/Platinum Edition
- Keil MDK-Professional

Baseline toolchain for Arm Safety Software development:
- Certified C Library
- Arm FuSa Run-Time System
- Arm Software-Test Libraries
Arm FuSa RTS: Run-Time System for Functional Safety

Software components certified for safety-critical applications

User Application code
- FuSa RTX RTOS
- FuSa Event Recorder
- Software test library (STL)
  - Self-test code for run-time verification
- FuSa CMSIS-Core (Arm-Core specific)
- Certified C library (Cortex-M)

Covered safety standards:
- Automotive: ISO 26262, ASIL D
- Industrial: IEC 61508, SIL 3
- Railways: EN 50128, SIL 4
- Medical: IEC 62304, Class C

Supported processors:
- Cortex-M0/M0+
- Cortex-M3
- Cortex-M4
- Cortex-M7

FuSa RTS components certified with Arm Compiler for Functional Safety
5 Steps to Your Safety Platform

1. Safety Concept
   Analyze system needs and provide a safety concept

2. Select Software
   ST Microcontroller & Embedded Office products or whatever the system needs

3. Setup Safety Platform
   Integrate software components and realize missing parts

4. Pre-Certification
   Harmonize safety manuals, certify remaining parts, assessment with authority

5. Long-term Maintenance
   Active functional safety management, workshops and training
5 Steps to Your Safety Platform

Safety & Cyber Security Engineers
TÜV Rheinland certified engineers

300+ Successful Customer Projects
Aerospace, Industrial, Automotive, Rail, Medical

70+ Satisfied Customers Worldwide
Products, Development Services, Mentoring

Certified Software Components
Safety RTOS, Safety AddOns, HW Selftests
Development of Turn-Key Certified Products

Main Industrial Sectors

System Engineering
- Software
- Hardware
- Mechanics
- Certification
- Production
- Prod. Life Cycle Management

More than 150 Experts - 20 years of Experience
TÜV Rheinland awarded the first Functional Safety Management (FSM) certificate with the **highest maturity level** (5) to embeX.

- Offering
  - **Development and of turn-key certified safety products and safety sub-systems**
  - **Transfer** of development processes and know-how to customers
  - **Consulting**
Thus, embeX offers:
• Risk Analysis
• Consultancy
• Developments achieving SIL 3 (IEC 61508) and SL 4 (IEC 62443)
• Verification including pen tests and fuzzing
Consulting & Engineering

- Excellent know-how in leading micro controller architectures for automotive & industrial
- STM32 functional safety experts
- Consulting & Development and Certification support according to standards: IEC 61508, ISO 26262, ISO 13849 ... and more

- Consulting for process, system & concept
- Architecture and design specification
- Hardware and software development
- Unit testing & system verification
Expertise out of our Customer projects

DC/DC converters
Implementing security requirements

Safety integration & certification
Emulator for special micro controllers

IoT implementation and integration

eDrive development

Battery management

Functional Safety process consulting

ECUs for powertrain & combustion engine
IAR Embedded Workbench for safety-critical applications

World leading embedded development tools

- More than 30 years of experience as a compiler vendor
- More than 1 million embedded devices built with our tools
- More than 150,000 users worldwide

The build chains are certified by TÜV SÜD as compliant with the international umbrella standards and the certification validates the quality of IAR Systems’ entire development processes, as well as the delivered software.

Certified toolchain
- A special functional safety edition of IAR Embedded Workbench

Simplified validation
- Functional Safety certificate from TÜV SÜD
- Safety report from TÜV SÜD
- Safety guide

Guaranteed support through the product life cycle
- Prioritized support
- Validated service packs
- Regular reports of known problems

Validated according to:
- IEC 61508
- ISO 26262
- EN 50128, EN 50657
- IEC 62304

Available for Arm and STM8
Our obsession is SafeWare Engineering!

- Hard and Software (IEC61508)
- Machinery (ISO13849, IEC62061)
- Factory automation (IEC61131-3, IEC61800-5-2)
- Railway Technology (IEC 50126, IEC 50128, IEC 50129)
- Process industry (IEC 61511)
- Nuclear, Wind and Solar Energy
- Automotive Systems (ISO26262)
- Farming Machines (EN16590, ISO25119)

Consulting
- Training
- Development Support
- Project Implementation
- Standardization, Approval and Certification
- Safety Management
- Specifications and Mathematical Methods

INNOTEC GMBH
WWW.INNOTECSAFETY.COM
ERLENWEG 12
49324 MELLE
GERMANY
+49 (5422) 9811-350
Our range of services: Factory & Process Automation

Tailor-made Development Solutions
Customized hardware and software development with flexible use of design packages.

Directly applicable DESIGN PACKAGES
Proven circuits and software components for rapid implementation of your development project.

Development Consulting
Development accompanying consulting and coaching in the areas of functional safety, explosion-proof and industrial communication.
Our offering: Your success is our driving force

**Consulting**
- Technology Consulting
- Functional Safety Management
- Explosion-proof trainings
- Industrial Communication
- Support in the creation of Requirements

**Concept – Architecture**
- Creation of the Functional Safety Concept
- Creation of the Explosion-proof Concept
- System Architecture
- Quality Assurance Measures

**Development – Design/Implementation/Prototyping**
- Hardware Development
- Software Development
- Safety Development
- PCB Layout
- Prototyping
- Type Testing
- Integration Test
- Use of existing Safety Design Packages
- Support of product launching into production

**Certification**
- Comprehensive Support of the Certification
MESCO Safety Design Packages

Build-up with a base board & expansion boards

Design Packages based on **ST solutions**

Built up with a main board & expansion boards as a reference design, our Design Packages simplify and accelerate the development in both safety- and non-safety-related environments.

Expansion boards
Azure RTOS Functional Safety

- ThreadX, FileX, GUIX, NetX Duo pre-certified by TUV to IEC 61508 SIL 4, IEC 62304 Class C, ISO 26262 ASIL D, EN 50128 SW-SIL 4
- USBX certification by TUV to IEC 61508 SIL 4, IEC 62304 Class C, ISO 26262 ASIL D, EN 50128 SW-SIL 4 in progress
- ThreadX, FileX, and NetX Duo pre-certified by UL to UL/IEC 60730, UL/IEC 60335, and UL 1998
- New Azure RTOS versions (ThreadX, FileX, GUIX, NetX Duo, and USBX) TUV and UL re-certifications available in 2021
NTSafetySolutions

**Training & Consulting**
- Varied range of seminars for functional safety in practice
- Safety workshops for individual customers

**Products, e.g.**
- SafeFlex – Reference platform for safety development
- NTSafeDriveMonitor – Safety module for monitoring of drives
- NTBMS – Safety reference platform for Battery Management Systems

**Expert services to do with all aspects of product development**
- Safety management assessment
- Safety risk assessment
- Safety requirement analysis
- Licensing strategy
- Safety planning
- Safety concept
- Concept examination
- Functional safety management

**Managed Services in Product Lifecycle**
- Safety system development
- Safety engineering
- Safety software development
- Safety hardware development
- Integration, verification & validation
- Documentation & traceability
embOS-Safe

Deployed and proven in several billion devices

embOS is deployed in several billion devices and is a proven choice for embedded products. It has been deployed in all kinds of applications, such as home appliances, IoT, transportation, industrial, medical or automotive.

More than 27 years of continuous development

SEGGER started to offer embOS in the early 90s as a product and has continued to develop the RTOS and add device support until today. It has become the core for SEGGER’s own products as well as a multitude of customer products.

Easy transition from standard to certified

While any application benefits from a reliable operating environment, in some cases, prove in form of certification is required. In markets where certification might become a requirement, embOS is the ideal choice, as it uses the same code base as embOS-Safe making a later conversion as easy as possible.

embOS features

- Guarantees 100% deterministic real-time operation
- Highest performance with lowest use of memory
- Powerful and easy to use API
- Kernel awareness plugins available
- Zero interrupt latency
- Cycle Precise System Time
- MadeForSTM32
embOS-Safe

Safety with Certificate
TÜV Süd has verified the embOS development process and confirms, that embOS-Safe is ideally suited as fundamental component for safety products. embOS-Safe is certified for functional safety according to IEC 61508 SIL 3 and IEC 62304 Class C.

Consistent interface
The Application Programming Interface (API) is unchanged in relation to embOS. Therefore existing software parts can be (re-)used easily. This helps to use embOS-Safe in existing applications.

Certification Kit
The embOS-Safe certification kit includes all necessary documents, including the comprehensive embOS Safety Manual.

One-Stop-Solution
The certified RTOS embOS-Safe is also available for SEGGER's IDE Embedded Studio, offering a one-stop-solution. Naturally, embOS-Safe is fully suited for usage with SEGGER's extensive portfolio of outstanding middleware, debug probes and production tools, too.

embOS is labelled MadeForSTM32
SAFERTOS® is a pre-certified safety Real Time Operating System (RTOS) for embedded processors. It delivers superior performance and dependability, whilst utilizing minimal resources.

SAFERTOS is a safety critical upgrade to FreeRTOS:
- Based on the FreeRTOS functional model
- Rebuilt to comply with **SIL 3 requirements**
- No open source code

**SAFERTOS can be found in:**
- Dialysis machines
- Prostheses
- Control systems found on trains
- Safety critical servo controllers
- Industrial control systems and many more

<table>
<thead>
<tr>
<th>Industry</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial</td>
<td>IEC 61508</td>
</tr>
<tr>
<td>Automotive</td>
<td>ISO 26262</td>
</tr>
<tr>
<td>Medical</td>
<td>IEC 62304/FDA 510K</td>
</tr>
<tr>
<td>Railway</td>
<td>EN 50128</td>
</tr>
</tbody>
</table>

100% success rate certifying with TÜV SÜD across Industry sectors:
SAFERTOS Support for ST

SAFERTOS Supported Platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>Cortex Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32F3, STM32F4, STM32L4</td>
<td>ARM Cortex-M4</td>
</tr>
<tr>
<td>STM32F2, STM32F1, STM32L1, STM32W</td>
<td>ARM Cortex-M3</td>
</tr>
<tr>
<td>STM32F0</td>
<td>ARM Cortex-M0</td>
</tr>
<tr>
<td>STM32F7, H7</td>
<td>ARM Cortex-M7</td>
</tr>
<tr>
<td>STM32H7 Dual Core</td>
<td>ARM Cortex-M7 &amp; ARM Cortex-M4</td>
</tr>
</tbody>
</table>

SAFERTOS supports:
- X-CUBE-STL;
- STM32Cube embedded software;
- STM32 SIL Functional Safety Package;
- Secure boot.

SAFERTOS Demos for ST are available:
- 30-days evaluation packages with full source code on request. Download Demos here.

Free White Paper:
Based on the X-CUBE-STL Functional Safety Package. Free to Download
WITTENSTEIN high integrity systems (WHIS) are safety RTOS specialists, part of The WITTENSTEIN Group. WHIS specialize in high integrity and safety critical embedded systems design.

**SAFERTOS® Source Code**

- Royalty Free, Perpetual Licensing
- 12 Months Free Support & Maintenance
- Smooth path to certification

**Design Assurance Pack**

- Middleware
- Safety Components
- Tools

**Training & Support**

WHIS also offer Board Support Packages, Training Courses and more…
Thank you