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 with an ecosystem of ST Authorized Partners
Achieve functional safety certification with ST MCUs and MPUs

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

- Dual watchdogs: Independent watchdog and system window watchdog
- Backup clock circuitry with clock security system (CSS)
- Supply monitoring (POR, BOR, PVD)
- I/O function locking
- PWM critical register protections with write-once registers (except on STM32L0/L1)
- Memory protection unit (MPU) with 8 or 16 regions to ensure data integrity from invalid behavior (except on STM32F0)
- Built-in safety features in Cortex-M cores (dual stack pointer, fault exceptions, debug module)

<table>
<thead>
<tr>
<th>Other features</th>
<th>C0</th>
<th>F0</th>
<th>F1</th>
<th>G0</th>
<th>F3</th>
<th>G4</th>
<th>F2/F4</th>
<th>H5</th>
<th>F7</th>
<th>H7</th>
<th>L0/L1</th>
<th>L4/L4+</th>
<th>L5</th>
<th>U5</th>
<th>WB</th>
<th>WBA</th>
<th>WL</th>
<th>MP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nb of Hardware CRC unit</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Programmable polynomial in CRC unit</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>
<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>
<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>
<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>
<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>
<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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SIL Functional Safety Package
Reduce time and cost to build STM32-based systems certified to IEC 61508 industrial safety standard
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 Rheinland
- IEC 61508 SC3 compliant
- Provided with safety manual and user guide

Available on demand at STM32 series level
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></td>
<td><img src="image" alt="STM32 Chip" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIL3</th>
<th>Achievable with two STM32 (1oo2 architecture)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Two STM32 Chips" /></td>
</tr>
</tbody>
</table>

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

1oo2: 1 out of 2 MCUs (1 redundant system)
# STM32 Safety Concepts

## STM32 MCU single Cortex-M core

Refer to STM32F0, F1, F2, F3, F4, F7, H7 single core, G0, G4, L0, L1, L4/L4+, L5, U5 safety manuals for details.

TÜV Rheinland single core certificate

## STM32 MCU dual Cortex-M core

Refer to STM32H7 dual-core and STM32WL5x dual-core safety manuals for details.

TÜV Rheinland dual core certificate

## STM32MP1 MPU dual Cortex-A7 and Cortex-M4

Refer to STM32MP1 safety manual for details.

TÜV Rheinland dual core certificate

<table>
<thead>
<tr>
<th>Document Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UM1741</td>
<td>STM32F0 Series safety manual</td>
</tr>
<tr>
<td>UM1818</td>
<td>STM32F1 Series safety manual</td>
</tr>
<tr>
<td>UM1845</td>
<td>STM32F2 Series safety manual</td>
</tr>
<tr>
<td>UM1886</td>
<td>STM32F3 Series safety manual</td>
</tr>
<tr>
<td>UM1840</td>
<td>STM32F4 Series safety manual</td>
</tr>
<tr>
<td>UM2316</td>
<td>STM32F7 Series safety manual</td>
</tr>
<tr>
<td>UM2455</td>
<td>STM32G0 Series safety manual</td>
</tr>
<tr>
<td>UM2454</td>
<td>STM32G4 Series safety manual</td>
</tr>
<tr>
<td>UM2640</td>
<td>STM32H7 dual-core safety manual</td>
</tr>
<tr>
<td>UM2331</td>
<td>STM32H7 single-core safety manual</td>
</tr>
<tr>
<td>UM2027</td>
<td>STM32L0 Series safety manual</td>
</tr>
<tr>
<td>UM1813</td>
<td>STM32L1 Series safety manual</td>
</tr>
<tr>
<td>UM2306</td>
<td>STM32L4 and STM32L4+ Series safety manual</td>
</tr>
<tr>
<td>UM2792</td>
<td>STM32L5 Series safety manual</td>
</tr>
<tr>
<td>UM2714</td>
<td>STM32L4P1 Series safety manual</td>
</tr>
<tr>
<td>UM2675</td>
<td>STM32L5 Series safety manual</td>
</tr>
<tr>
<td>UM2614</td>
<td>STM32WL5x dual-core safety manual</td>
</tr>
</tbody>
</table>
STM32 MCU dual Cortex-M core Safety Concept

2 possible schemes for acquisition, execution and transfer of result

**Individual scheme**
Each CPU implements a specific safety function, no collaboration

**Collaborative scheme**
The 2 CPUs collaborate for the implementation of the same safety function

PEi = input processing element  
PEC = computation processing element  
PEo = input processing element  
SF(s) = on or multiple safety Functions

More details in UM2840 STM32H7 dual-core safety manual and UM2814 STM32WL5x dual-core safety manual
STM32MP1 MPU dual Cortex-A7 and Cortex-M4 Safety Concept

Safety function implementation confined in Cortex-M4 real-time side

Non-Safe Partition  |  Safe Partition
--- | ---
arm Cortex-A7 up to 800 MHz | arm Cortex-M4 209 MHz

Execution of self-test library (X-CUBE-STL for STM32MP1)

Hardware and software-based separation

The coexistence with non-safety related software on Cortex-A7 (e.g. Linux) is possible

More details in UM0714 STM32MP1 Series safety manual
ASIL Functional Safety Package
Reduce time and cost to build STM8A-based systems certified to ISO 26262 automotive functional safety standard.
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](http://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
CLASS B Functional Safety Package
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
- **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>
<tbody>
<tr>
<td><strong>STM32 Series covered</strong></td>
<td><strong>V2.2.0</strong> - STM32F0, F1, F3, F2, F4, F7, STM32L0, L1, L4</td>
<td>STM8AF</td>
</tr>
<tr>
<td></td>
<td><strong>V2.3.0</strong> - STM32G0, G4, WB, H7 single core</td>
<td>STM8AL</td>
</tr>
<tr>
<td></td>
<td><strong>V2.4.0</strong> - STM32L5</td>
<td>STM8L</td>
</tr>
<tr>
<td></td>
<td><strong>V3.0.0, 3.0.1</strong> - STM32H7 dual core</td>
<td>STM8S</td>
</tr>
<tr>
<td></td>
<td><strong>V4.0.0</strong> – STM32U5, STM32C0, STM32G0</td>
<td></td>
</tr>
<tr>
<td><strong>Supported development environments</strong></td>
<td>IAR Embedded Workbench®, ARM KEIL®, STM32CubeIDE</td>
<td>IAR Embedded Workbench®, Cosmic®</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td><strong>UL@2016-2021</strong></td>
<td><strong>UL &amp; VDE@2018</strong></td>
</tr>
<tr>
<td>IEC 60335-1 and 60730-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International standards coverage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety manual (guidelines)</td>
<td>AN4435</td>
<td>AN3181</td>
</tr>
</tbody>
</table>
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 summary
<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>IEC, UL, CSA</td>
<td>Safety Documentation</td>
<td>X-CUBE-STL</td>
</tr>
<tr>
<td>STM8A</td>
<td>ISO 26262</td>
<td>60335-1, 60730-1</td>
<td>Self-Test Libraries</td>
<td>STM8A-SafeASIL</td>
</tr>
<tr>
<td>STM32</td>
<td></td>
<td></td>
<td>Safety Documentation</td>
<td>X-CUBE-CLASSB</td>
</tr>
<tr>
<td>STM8</td>
<td></td>
<td></td>
<td>Self-Test Libraries</td>
<td>STM8-SafeCLASSB</td>
</tr>
</tbody>
</table>
Functional Safety Ecosystem
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
- Microsoft
- SCIOPTA
- SEGGER
- TUXERA
- WITTENSTEIN

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

**Engineering, consulting, development or design services**
- Embedded Office
- embex
- innotec
- MESCO
- NewTec

**Training**
- innotec
- MESCO
- NewTec
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
  - TUV Certificate by TUV SUD
  - Qualification Kit
    - Safety Manual
    - Defect Report

Arm Compiler For Functional Safety

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)

Arm Cortex-M processor

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
Embedded Office

5 Steps to Your Safety Platform

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

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

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

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

5. Long-term Maintenance
   Active functional safety management, workshops and training
Embedded Office

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

More than 150 Experts - 20 years of Experience

Main Industrial Sectors

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

Energy & Drives
Industrial Automation
Mobile Automation
Functional Safety
SIL 4 / PL e
Process Automation
Medical Engineering
Transportation
TÜV Rheinland awarded the first Functional Safety Management (FSM) certificate with the highest maturity level (5) to embeX.

Offering
- Development of certified turnkey safety products and subsystems
- Transfer of development processes and know-how to customers
- Consulting

Recognized Company in Functional Safety Worldwide
Cyber Security is an essential Prerequisite for Safety

Thus, embeX offers:

• Risk Analysis
• Consultancy
• Developments achieving SIL 3 (IEC 61508) and SL 4 (IEC 62443)
• Verification including pen tests and fuzzing

Further information:
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!

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

- Hard and Software (IEC61508)
- Machinery (ISO13849, IEC62061)
- Factory automation (IEC61131-6, 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)
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

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.

Design Packages based on ST solutions

Expansion boards
Azure RTOS Functional Safety

- **Azure RTOS ThreadX & ThreadX SMP**
  A high-performance real-time operating system

- **Azure RTOS FileX**
  An embedded FAT file system that offers optional fault tolerant features

- **Azure RTOS NetX and NetX Duo**
  A TCP/IP IPv4/IPv6 embedded network stack that includes cloud connectivity and IPsec and TLS/DTLS security protocols

- **Azure RTOS USBX**
  A USB stack that provides host, device, and on-the-go support

- **Azure RTOS GUIX Studio and GUIX**
  A complete design environment and run-time to create and maintain 2D graphical user interfaces
Azure RTOS Functional Safety

- ThreadX, FileX, GUIX, NetX Duo, USBX pre-certified by TUV to IEC 61508 SIL 4, IEC 62304 Class C, ISO 26262 ASIL D, EN 50128 SW-SIL 4, UL 1998, UL/IEC 60730, UL/IEC 60335
- Azure RTOS pre-certification covers generic C code
- Same source code whether or not certification is needed
- Pre-certification artifacts are licensed separately
**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
Reduce cost and time-to-market of your safety application development with NTSafeFlex STM32 evaluation board and Safety Software Library

- The board is based on two STM32G070 with additional Software Library for functional safety solutions up to SIL 3 and PLe, Cat4.
- Typical applications: safety control logic, motor supervision, general safety applications with low performance standards, etc.
SCIOPTA RTOS is designed with safety in mind. SCIOPTA RTOS is certified according following standards: IEC61508 (SIL 3), EN50128/129 (SIL 3/4) and ISO26262 (ASIL D).

SCIOPTA RTOS’ certified API does not differ from the non-certified version. All system call are certified.

SCIOPTA RTOS is tailored to the specific CPU exploiting all its features to provide short latencies, small overhead and deterministic execution.

SCIOPTA RTOS is designed to be compact and still offering a wide range of system calls to enable almost any kind of application.

SCIOPTA RTOS can be used in a complete dynamic manner so that the application can react on upcoming needs.

SCIOPTA RTOS uses pre-emptive scheduling based on priorities and round-robin scheduling with optional time slice.

SCIOPTA RTOS hides many of the burden other RTOSs put on the developer. A set of six system calls is sufficient for 80% of an application.

SCIOPTA RTOS’s asynchronous direct message passing fits perfect future challenges like many-core SoCs or distributed systems.

SCIOPTA RTOS is successfully used in different areas like Automotive, Defense, Rail Way, Medical, Industrial Automation and Consumer Electronics.
embOS-Safe

- Medical
- Industrial
- Home Appliances
- Transportation
- Automotive
- and more ..

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
SEGGER Microcontroller

**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
Tuxera Certifiable SafeTCPIP™ Stack

A complete TCP/IP v4 stack for safety-critical automotive, industrial, or medical embedded systems. SafeTCPIP™ is developed to the ISO 26262 ASIL B standard, and mappable to other standards such as IEC 61508 and ISO 62304.

• The stack is suitable for integration into any system that requires a high level of safety-integrity
• Supports TCP, UDP, ARP, ICMP, IGMP, Socket, and Ethernet Interface
• Built with Tuxera's Software SEooC Development Process
• Advanced extra modules: IPsec/IKEv2, MACsec, MQTT, TLS, EAPol, SNMP, SSH, HTTP, FTP, NTP, EST, and many more
• CryptoCore™ software feature supports AES, Base64, ChaCha20, MD5, RSA, SHA, and others

• Supports STMicroelectronics STM32 microcontroller series
• Integrates with both RTOS and non-RTOS based systems
SEooC: Reusing Embedded Software in Safety-Critical Systems

- SEooC is defined as a method for using software or hardware components in a vehicle that were not originally designed for that specific project.
- Developed to a safety standard, such as ISO 26262, which means that it is developed with all the processes of a full software safety life cycle and within the design constraints of a safety system.
  - “Safety” – indicates that this module is specifically developed in the context of a set of safety requirements.
  - “Element” – indicates that this is a unit or module with a specific range of functionality.
  - “out of Context” – software components are developed to provide a specific function, with no awareness of how the component will actually be used in the target system.
- Tuxera is the first embedded software module vendor to use the SEooC approach to build commercial software Elements, beginning with its SafeTCPIP product.
SAFERTOS®: safety critical RTOS

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

### Industry sectors:

<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>
SAFERTOS Support for ST

SAFERTOS Supported Platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>Cortex Architecture</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

WITTENSTEIN high integrity systems (WHIS) are safety RTOS specialists, part of The WITTENSTEIN Group. WHIS specialize high integrity and safety critical embedded systems design.

SAFE
RTOS
Source Code

Design Assurance Pack  Middleware  Safety Components  Tools

Royalty Free, Perpetual Licensing

12 Months Free Support & Maintenance

Smooth path to certification

Training & Support

WHIS also offer Board Support Packages, Training Courses and more…
Our technology starts with You

Find out more at www.st.com/functionalsafety