life.augmented

Functional safety packages for STM32 MCUs and MPUs, and STM8 MCUs

STM32

STM8

Safety Ready

SIL Ready

ClassB Ready

Partner Program

“If only

I could speed up the design 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 and MPU safety features, ST provides a full **set of certified software libraries and documentation** for manufacturers to significantly **reduce the development effort, time and cost** to achieve functional safety standard certifications.

- **SIL functional safety package**
  for industrial IEC 61508 (STM32)

  SIL Ready

- **Class B functional safety package**
  for household electrical appliances
  IEC 60335-1/60730-1 (STM32 & STM8)

  ClassB Ready

life.augmented

STM32 built-in safety features

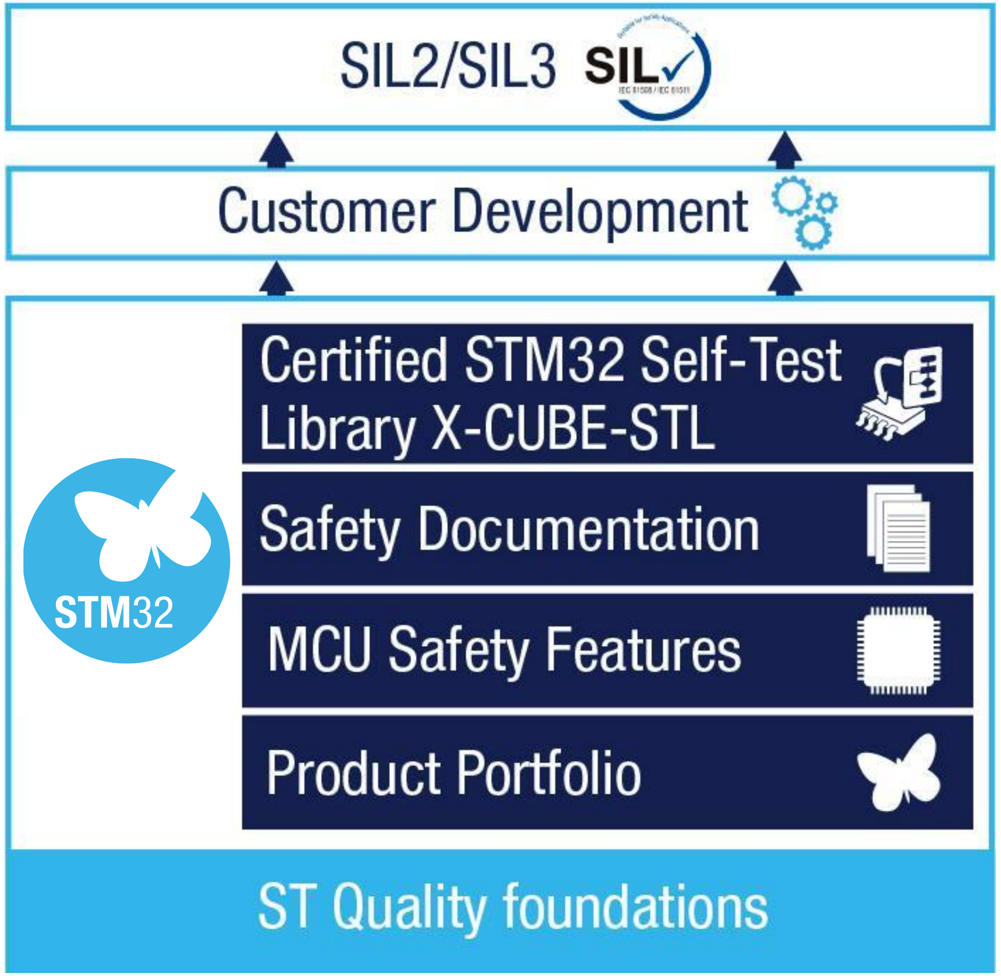
- Dual watchdogs: Independent watchdog and system window watchdog
- Backup clock circuitry with clock security system (CSS)
- Supply monitoring (POR, BOR, PVD)
- I/O function locking
- PWM critical register protections with write-once registers (except on STM32L0/L1)
- Memory protection unit (MPU) with 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)

Other features	C0	F0	F1	G0	F3	G4	F2 F4	H5	F7	H7	H7RS	L0 L1	U0	L4/L4+	L5	U5	WB	WBA	WL	MP1
Nb of Hardware CRC unit	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
Programmable polynomial in CRC unit	●	(1)		●		●		●	●	●	●	(1)	●	●	●	●	●	●	●	●
Multiple Flash memory protection levels	●	●		●	●	●	●	●	●	●	N.A.	●	●	●	●	●	●	●	●	N.A.
PWM stop on core lockup	●	●		●	●	●		●		●	●			●	●	●	●	●	●	●
Parity bit for SRAM memory (1bit/byte)	●	●		●	●	●							●	●	●		●	●	●	
ECC (SECDED) for SRAM								●		●	●					●				
ECC (SECDED) for Flash memory				●		●		●		●	N.A.		●	●	●	●	●	●	●	N.A.

(1) Depending on part number
N.A. Not Applicable

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

SIL functional safety package

SIL Ready

SIL functional safety package for STM32

MCU Hardware Level
failure mode coverage

Certification body assessment

MCU Software level
failure mode coverage

Application level
failure mode coverage

without Package

ST provides a complete, certified offering to

- Lower project costs
- Reduce design complexity
- Ease SIL certification assessment

MCU Hardware Level
failure mode coverage

with STM32 Embedded Safety Features

Certification body assessment

Certified STM32 Self-Test Library X-CUBE-STL

with STM32 Self-Test Library X-CUBE-STL

MCU Software level
failure mode coverage

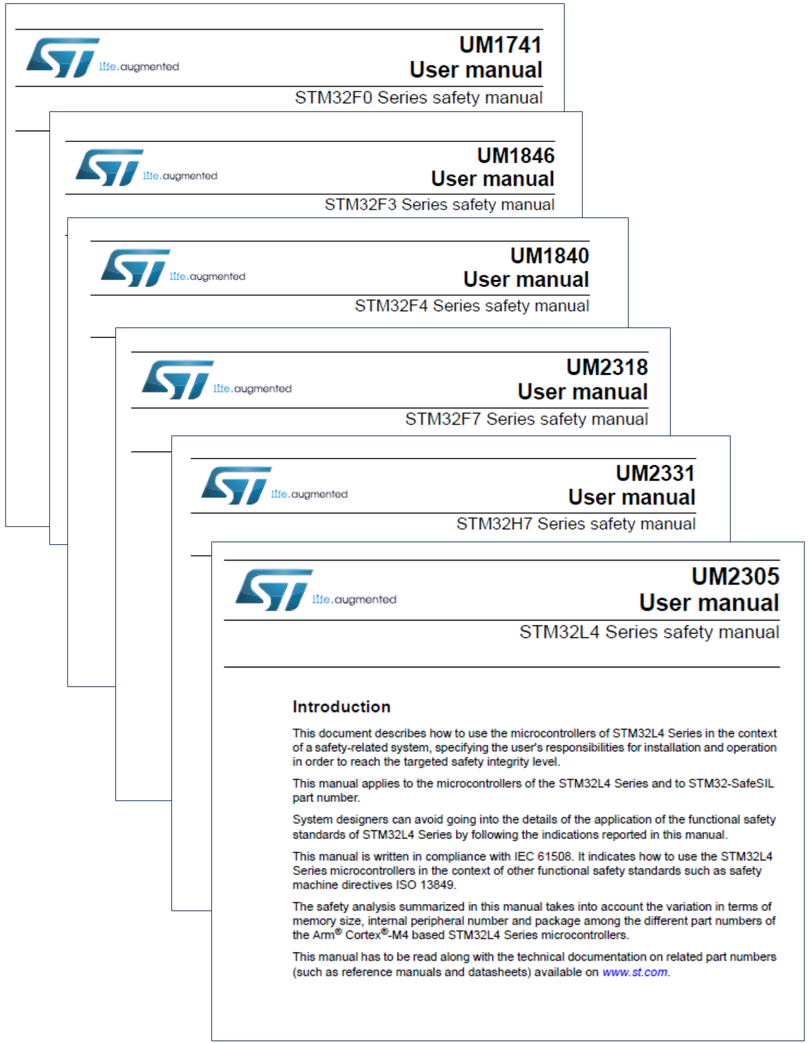
with STM32 Safety Documentation

Application level
failure mode coverage

TÜVRheinland
CERTIFIED

with Package

SIL functional safety for STM32 safety documentation



UM1741
User manual
STM32F0 Series safety manual

UM1846
User manual
STM32F3 Series safety manual

UM1840
User manual
STM32F4 Series safety manual

UM2318
User manual
STM32F7 Series safety manual

UM2331
User manual
STM32H7 Series safety manual

UM2305
User manual
STM32L4 Series safety manual

Introduction

This document describes how to use the microcontrollers of STM32L4 Series in the context of a safety-related system, specifying the user's responsibilities for installation and operation in order to reach the targeted safety integrity level.

This manual applies to the microcontrollers of the STM32L4 Series and to STM32-SafeSIL part number.

System designers can avoid going into the details of the application of the functional safety standards of STM32L4 Series by following the indications reported in this manual.

This manual is written in compliance with IEC 61508. It indicates how to use the STM32L4 Series microcontrollers in the context of other functional safety standards such as safety machine directives ISO 13849.

The safety analysis summarized in this manual takes into account the variation in terms of memory size, internal peripheral number and package among the different part numbers of the Arm® Cortex®-M4 based STM32L4 Series microcontrollers.

This manual has to be read along with the technical documentation on related part numbers (such as reference manuals and datasheets) available on *www.st.com*.

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

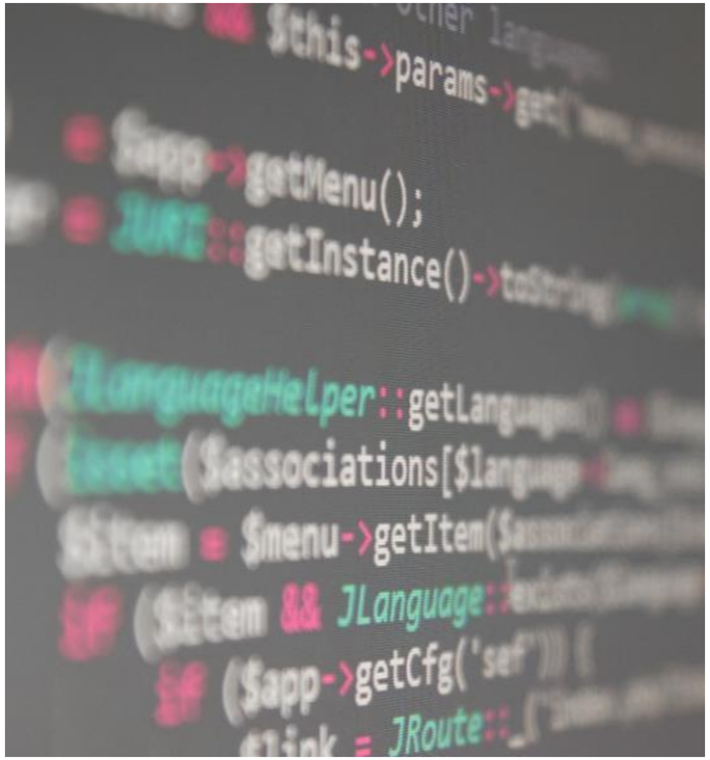
FMEA: detailed list of MCU/MPU failure modes and related mitigation measures adopted

FMEDA: static snapshot reporting IEC 61,508 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



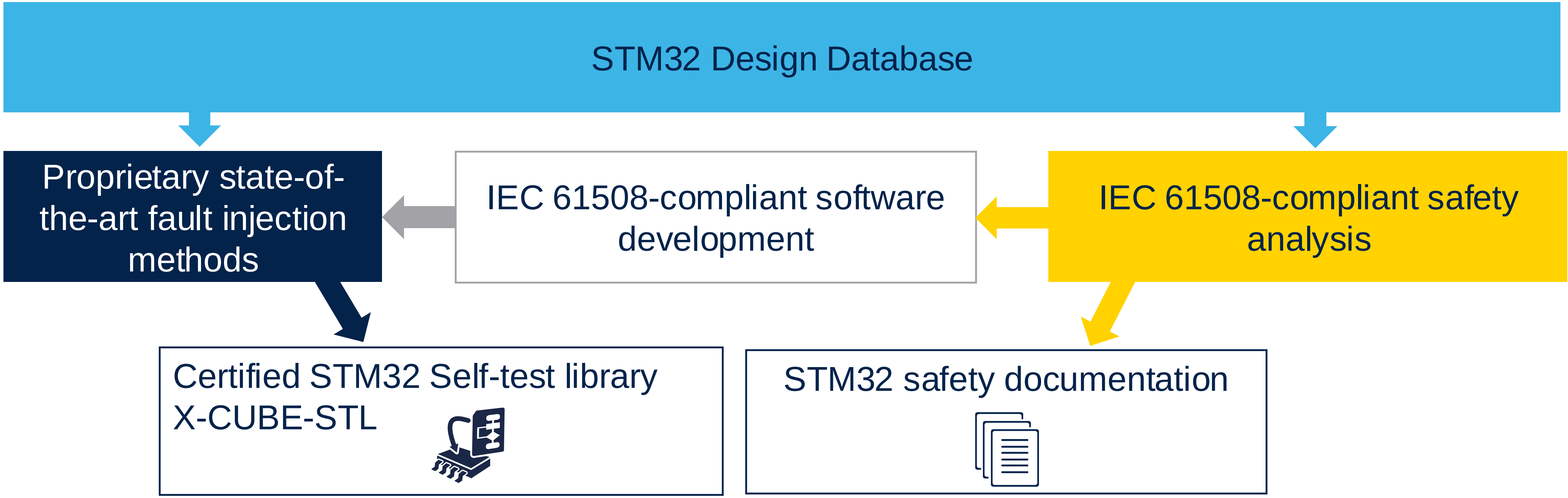
- A software diagnostic suite designed to detect random hardware failures in safety-critical STM32 core components (CPU + SRAM + flash memory)
- Diagnostic coverage verified by state-of-the-art ST proprietary fault injection methodology
- Application independent: can be potentially used in any end customer application
- Compiler independent: delivered as object code
- Certified by TÜV Rheinland [1]
- IEC 61508 SC3 compliant
- Provided with safety manual and user guide

Available on demand at STM32 series level[2]
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 functional safety methodology

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.



STM32 Design Database

Proprietary state-of-the-art fault injection methods

IEC 61508-compliant software development

IEC 61508-compliant safety analysis

Certified STM32 Self-test library X-CUBE-STL

STM32 safety documentation

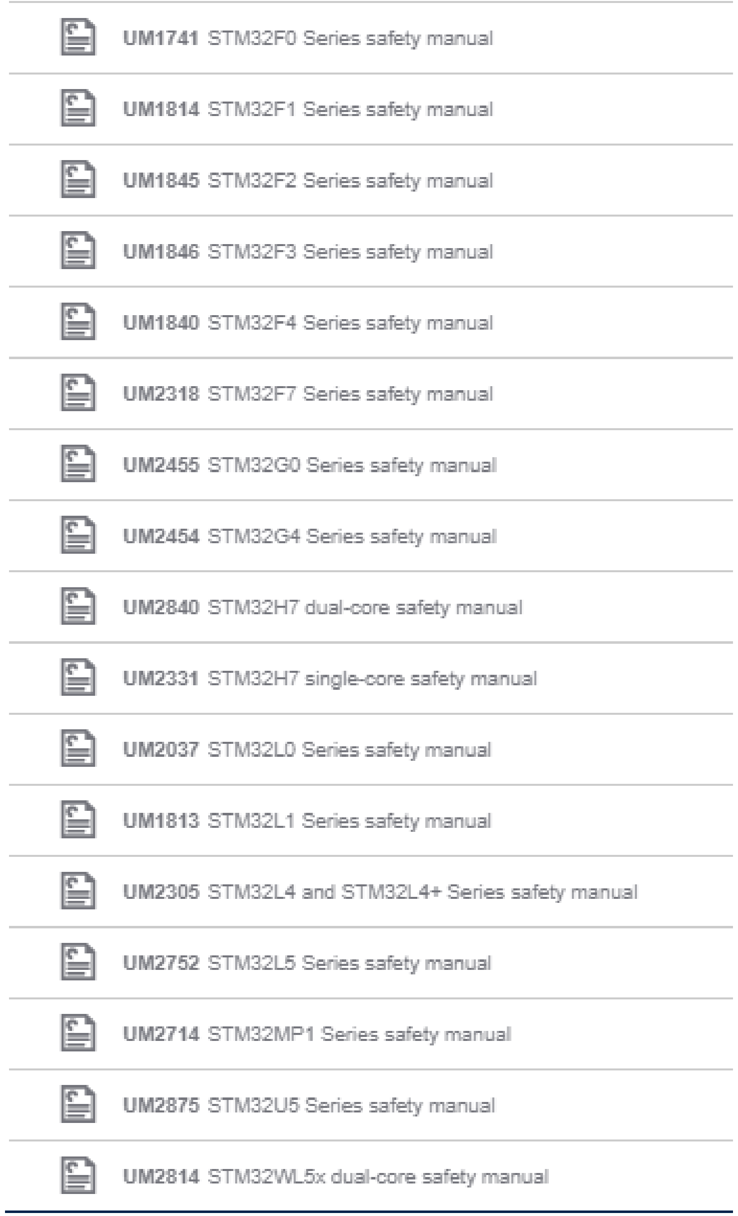
Achieve SIL2/SIL3 with STM32

SIL2	**Achievable with single STM32** (1oo1 architecture)
SIL3	**Achievable with two STM32** (1oo2 architecture)

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

1oo2: 1 out of 2 MCUs (1 redundant system)

STM32 Safety Concepts



UM1741	STM32F0 Series safety manual
UM1814	STM32F1 Series safety manual
UM1845	STM32F2 Series safety manual
UM1846	STM32F3 Series safety manual
UM1840	STM32F4 Series safety manual
UM2318	STM32F7 Series safety manual
UM2455	STM32G0 Series safety manual
UM2454	STM32G4 Series safety manual
UM2840	STM32H7 dual-core safety manual
UM2331	STM32H7 single-core safety manual
UM2037	STM32L0 Series safety manual
UM1813	STM32L1 Series safety manual
UM2305	STM32L4 and STM32L4+ Series safety manual
UM2752	STM32L5 Series safety manual
UM2714	STM32MP1 Series safety manual
UM2875	STM32U5 Series safety manual
UM2814	STM32WL5x dual-core safety manual

STM32 MCU single Cortex®-M core

Refer to STM32F0, F1, F2, F3, F4, F7, H7 single core, G0, G4, L0, L1, U0 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

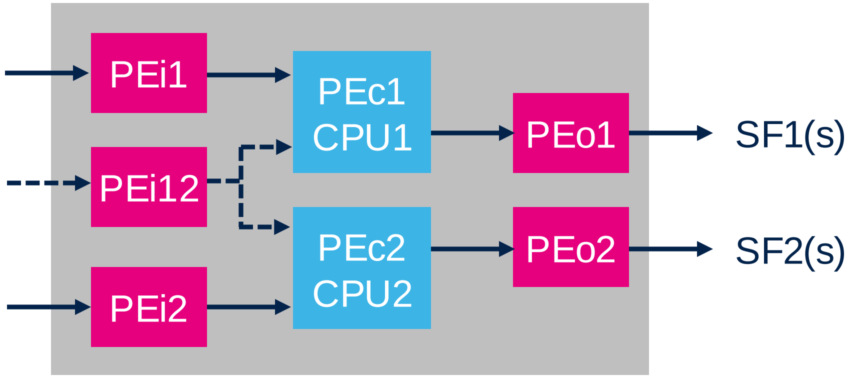
STM32MP1 MPU dual Cortex®-A7 and Cortex®-M4

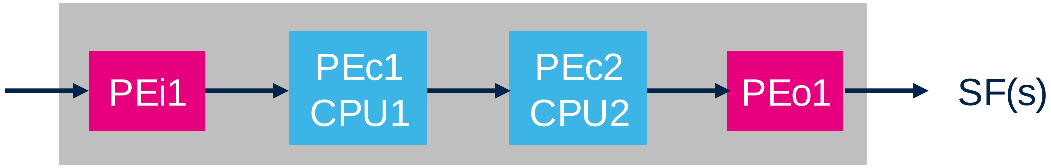
Refer to the STM32MP1 safety manual for details

TÜV Rheinland dual core certificate

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

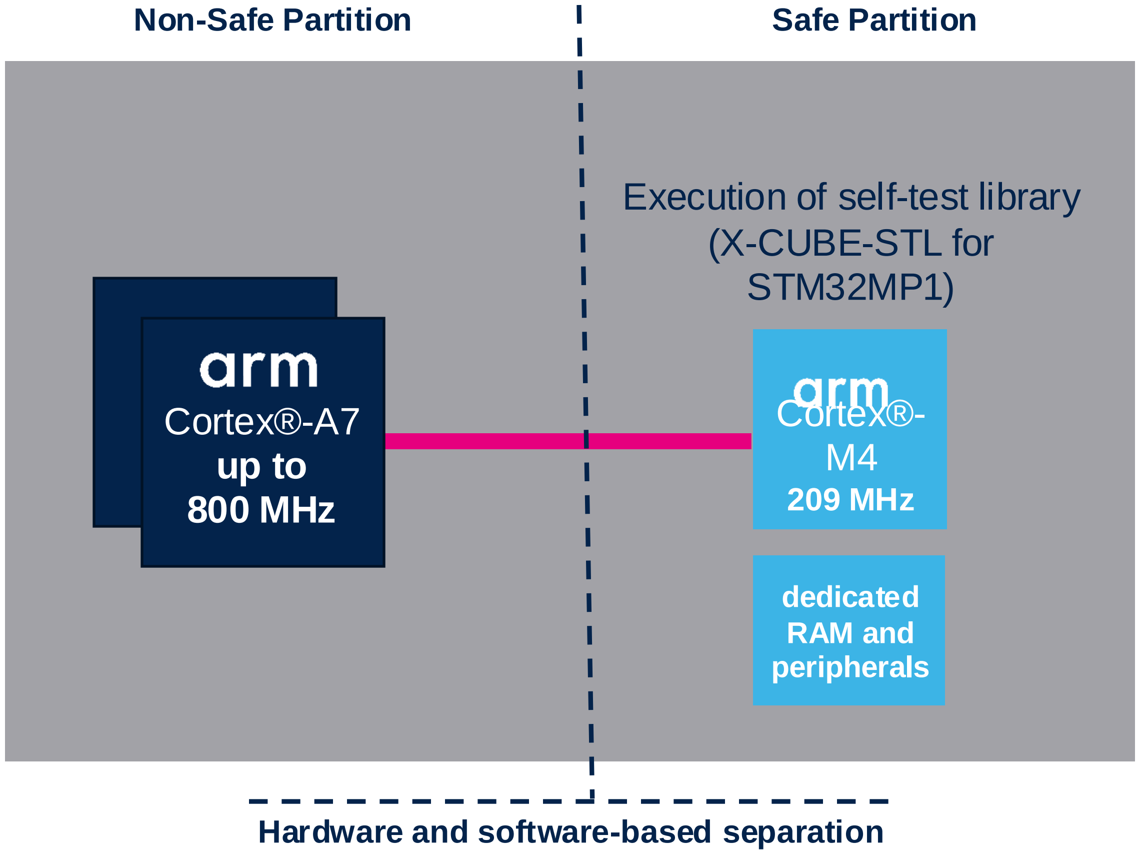
Collaborative scheme
The 2 CPUs collaborate for the implementation of the same safety function

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
Execution of self-test library (X-CUBE-STL for STM32MP1)
arm
Cortex®-M4
209 MHz
dedicated RAM and peripherals
Hardware and software-based separation

The coexistence with non-safety related software on Cortex®-A7 (for example, Linux) is possible

More details in UM2714 STM32MP1 Series safety manual

CLASS B Functional Safety Package

ClassB functional safety package for STM32 and STM8 MCUs

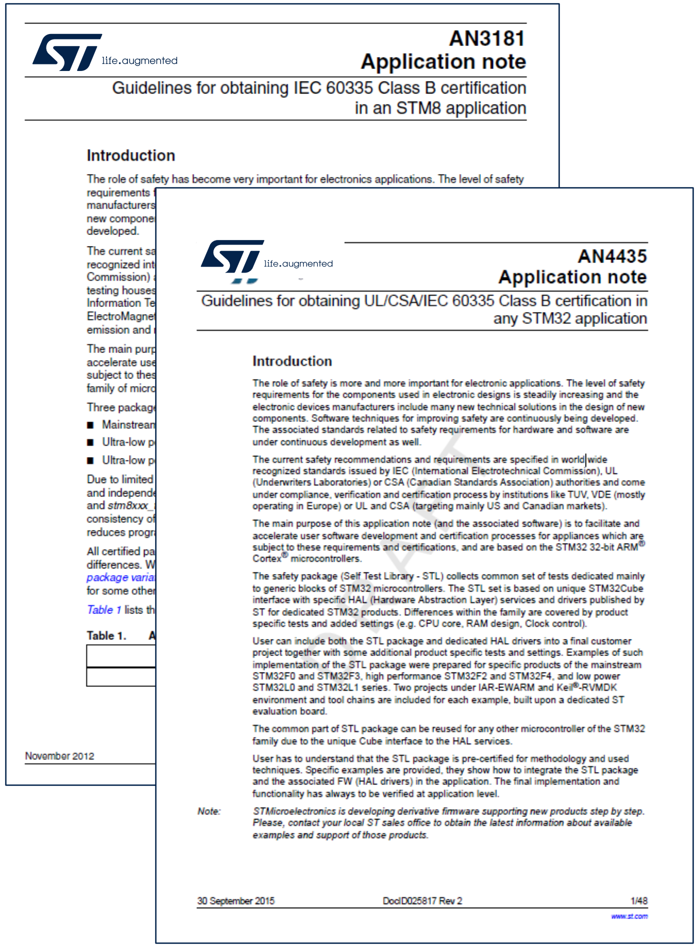
Reduce time and cost to build STM32 & STM8 based systems certified to IEC 60335-1 and 60730-1 household electrical appliance safety standards.

- **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

Package name	X-CUBE-CLASSB	STM8-SafeClassB
STM32 series covered	**V2.2.0 -** STM32F0, F1, F3, F2, F4, F7, STM32L0, L1, L4 **V2.3.0** - STM32G0, G4, WB, H7 single core **V2.4.0** - STM32L5 **V3.0.0, 3.0.1** - STM32H7 dual core **V4.0.0** – STM32C0, STM32F7, STM32G0, STM32G4, STM32H5, STM32H7 (Cortex®-M7 core only), STM32L4, STM32L4+, STM32U5, STM32WL, STM32MP15	STM8AF STM8AL STM8L STM8S
Supported development environments	**IAR Embedded Workbench®, Arm® Keil®, STM32CubeIDE**	**IAR Embedded Workbench®, Cosmic®**
Certification	**UL@2016-2021**	**UL & VDE@2018**
IEC 60335-1 and 60730-1 international standards coverage	IEC, UL and CSA	
Safety manual (guidelines)	AN4435	AN3181

ClassB safety manuals



AN3181
Application note

Guidelines for obtaining IEC 60335 Class B certification
in an STM8 application

Introduction

The role of safety has become very important for electronics applications. The level of safety
requirements
manufacturers
new compone
developed.

The current sa
recognized int
Commission)
testing houses
Information Te
ElectroMagnet
emission and

The main purp
accelerate use
subject to thes
family of micro

Three package

- Mainstream
- Ultra-low p
- Ultra-low p

Due to limited
and independe
and *stm8xxx_*
consistency of
reduces progra

All certified pa
differences. W
package varia
for some other

Table 1 lists th

Table 1. A

November 2012

AN4435
Application note

Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in
any STM32 application

Introduction

The role of safety is more and more important for electronic applications. The level of safety requirements for the components used in electronic designs is steadily increasing and the electronic devices manufacturers include many new technical solutions in the design of new components. Software techniques for improving safety are continuously being developed. The associated standards related to safety requirements for hardware and software are under continuous development as well.

The current safety recommendations and requirements are specified in world wide recognized standards issued by IEC (International Electrotechnical Commission), UL (Underwriters Laboratories) or CSA (Canadian Standards Association) authorities and come under compliance, verification and certification process by institutions like TUV, VDE (mostly operating in Europe) or UL and CSA (targeting mainly US and Canadian markets).

The main purpose of this application note (and the associated software) is to facilitate and accelerate user software development and certification processes for appliances which are subject to these requirements and certifications, and are based on the STM32 32-bit ARM® Cortex® microcontrollers.

The safety package (Self Test Library - STL) collects common set of tests dedicated mainly to generic blocks of STM32 microcontrollers. The STL set is based on unique STM32Cube interface with specific HAL (Hardware Abstraction Layer) services and drivers published by ST for dedicated STM32 products. Differences within the family are covered by product specific tests and added settings (e.g. CPU core, RAM design, Clock control).

User can include both the STL package and dedicated HAL drivers into a final customer project together with some additional product specific tests and settings. Examples of such implementation of the STL package were prepared for specific products of the mainstream STM32F0 and STM32F3, high performance STM32F2 and STM32F4, and low power STM32L0 and STM32L1 series. Two projects under IAR-EWARM and Keil®-RVMDK environment and tool chains are included for each example, built upon a dedicated ST evaluation board.

The common part of STL package can be reused for any other microcontroller of the STM32 family due to the unique Cube interface to the HAL services.

User has to understand that the STL package is pre-certified for methodology and used techniques. Specific examples are provided, they show how to integrate the STL package and the associated FW (HAL drivers) in the application. The final implementation and functionality has always to be verified at application level.

Note: STMicroelectronics is developing derivative firmware supporting new products step by step. Please, contact your local ST sales office to obtain the latest information about available examples and support of those products.

30 September 2015 DocID025817 Rev 2 1/48

www.st.com

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

Safety Ready

Functional safety packages for STM32 & STM8 MCUs

	SIL Ready	ClassB Ready	
MCU support	STM32	STM32	STM8
Achievable safety standards	IEC 61508	IEC, UL, CSA 60335-1 60730-1	
Certification	TÜVRheinland CERTIFIED	UL CERTIFIED	VDE UL CERTIFIED
Package content	• Safety documentation • Self-Test libraries	• Safety documentation • Self-Test libraries	• Safety documentation • Self-Test libraries
Package name	X-CUBE-STL	X-CUBE-CLASSB	STM8-SafeCLASSB

Functional safety ecosystem

Get support from ST authorized partners

Reduce your project time and cost

Safety Requirements → HW & SW Design → Validation → Certification

Partner Program

life.augmented

Functional safety expertise

Partner Program

life.augmented

Functional safety Authorized Partners

Embedded software

- arm KEIL
- Embedded Office
- SCIOPTA
- SEGGER It simply works!
- TUXERA
- WITTENSTEIN

Software development tools

- arm KEIL
- IAR SYSTEMS

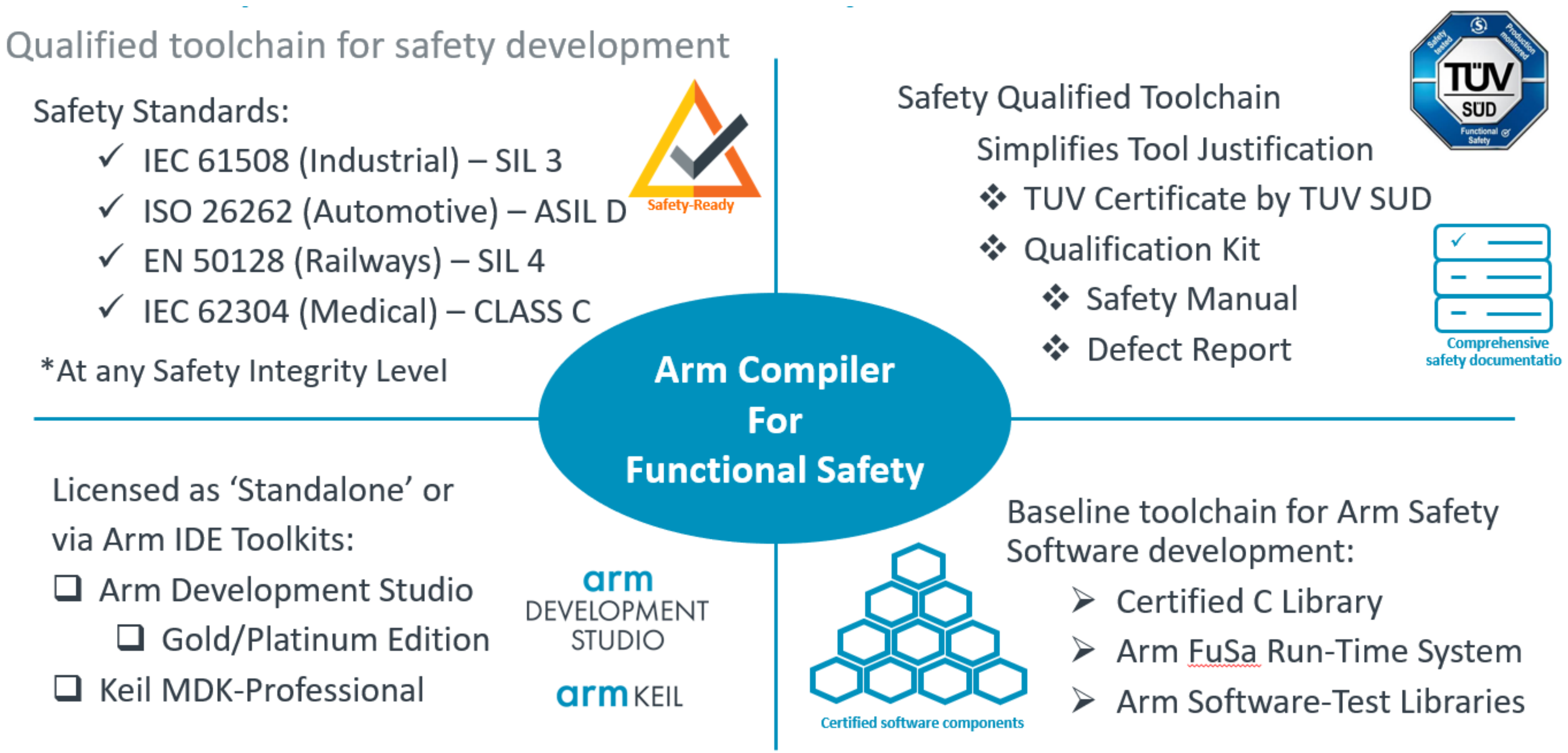
Engineering, consulting, development or design services

- Embedded Office
- embeX Your embedded experts
- 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:

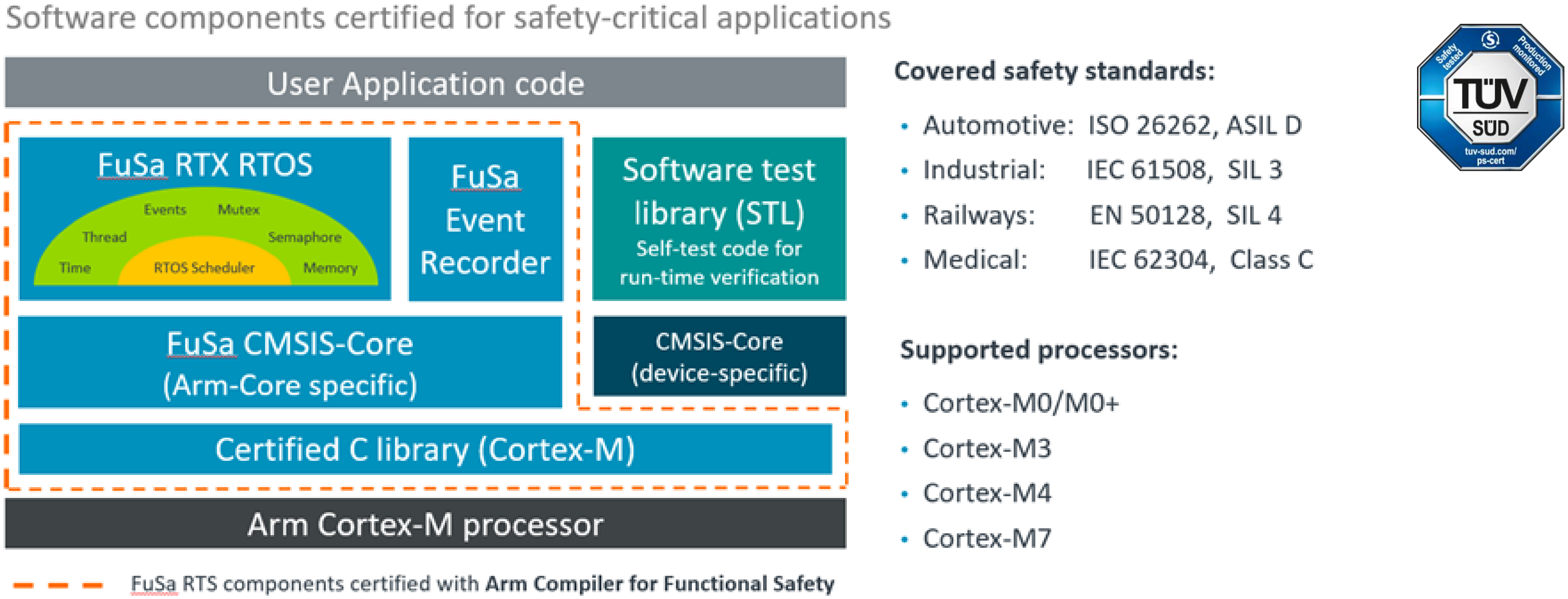
- ❑ Arm Development Studio
  - ❑ Gold/Platinum Edition
- ❑ Keil MDK-Professional

Baseline toolchain for Arm Safety Software development:

- ➢ Certified C Library
- ➢ Arm FuSa Run-Time System
- ➢ Arm Software-Test Libraries

Safety-Ready
TÜV SÜD
Comprehensive safety documentatio
arm DEVELOPMENT STUDIO
arm KEIL
Certified software components

Arm FuSa RTS: runtime 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)

CMSIS-Core
(device-specific)

Certified C library (Cortex-M)

Arm Cortex-M processor

FuSa RTS components certified with **Arm Compiler for Functional Safety**

Covered safety standards:

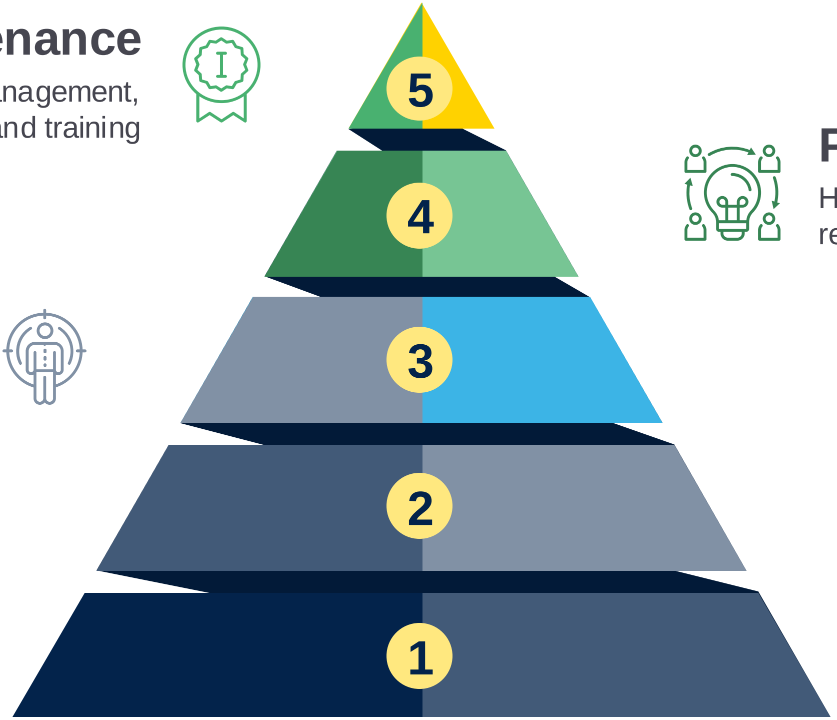
Automotive:	ISO 26262, ASIL D
Industrial:	IEC 61508, SIL 3
Railways:	EN 50128, SIL 4
Medical:	IEC 62304, Class C

Supported processors:

- Cortex-M0/M0+
- Cortex-M3
- Cortex-M4
- Cortex-M7

Embedded Office

5 steps to your safety platform



Long-term maintenance

Active functional safety management,
workshops, and training

Pre-certification

Harmonize safety manuals, certify
remaining parts, assessment with authority

Setup safety platform

Integrate software components
and realize missing parts

Select software

ST microcontroller & embedded office
products or whatever the system needs

Safety concept

Analyze system needs and
provide a safety concept

Embedded Office

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

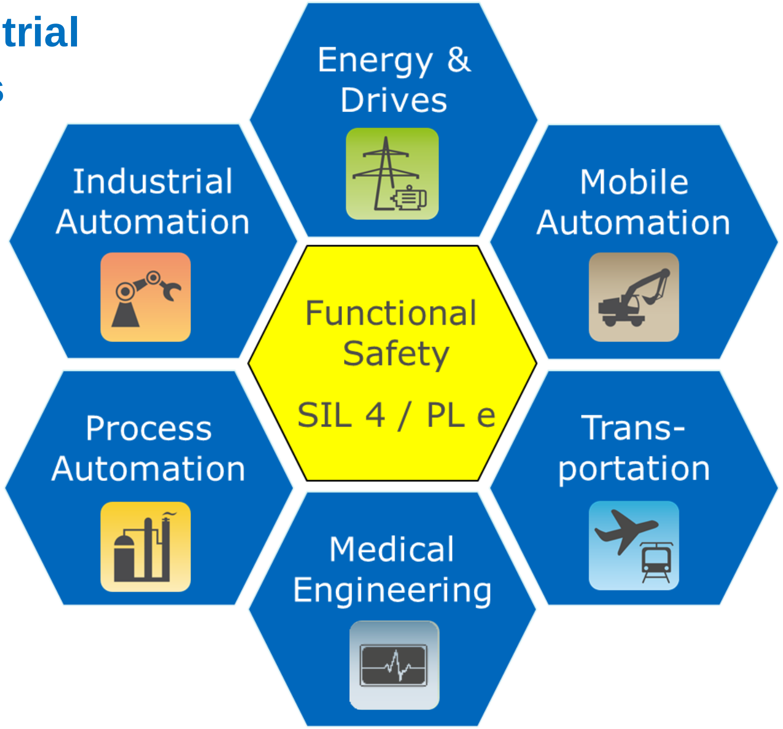
Safety RTOS, safety AddOns, HW Selftests

life.augmented

Development of turnkey certified products

- System engineering
- Software
- Hardware
- Mechanics
- Certification
- Production
- Prod. life cycle management

Main industrial sectors



Functional Safety

SIL 4 / PL e

Energy & Drives

Industrial Automation

Mobile Automation

Process Automation

Trans-portation

Medical Engineering

More than 150 experts - 20 years of experience

Recognized company in functional safety worldwide

- TÜV Rheinland awarded the first Functional Safety Management (FSM) certificate with the **highest maturity level** (5) to embeX

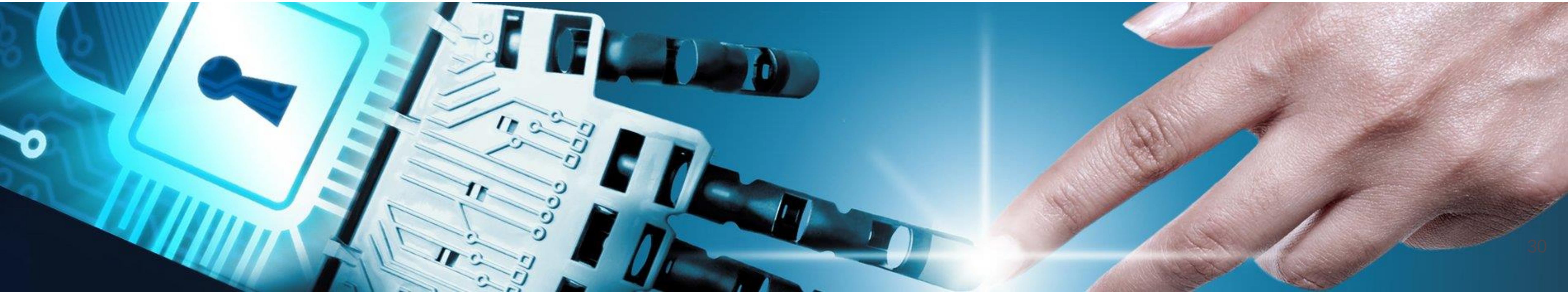
- Offering
  - **Development of certified turnkey safety products and subsystems**
  - **Transfer** of development processes and know-how to customers
  - **Consulting**

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:
https://www.embex-engineering.com/en/competencies-technologies/safety-security/



IAR Systems

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

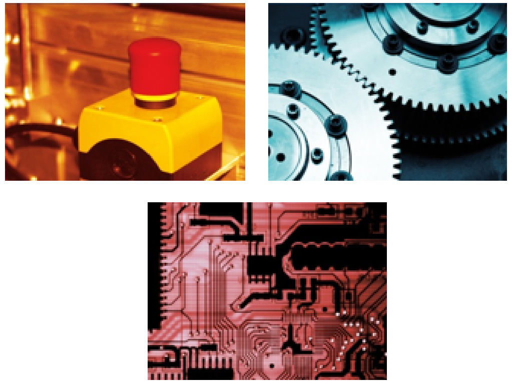
Validated according to:
IEC 61508
ISO 26262
EN 50128, EN 50657
IEC 62304

Arm Functional Safety Partner
Software & Tools

Available for Arm and STM8

Innotec

Our obsession is SafeWare engineering!



- 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)

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

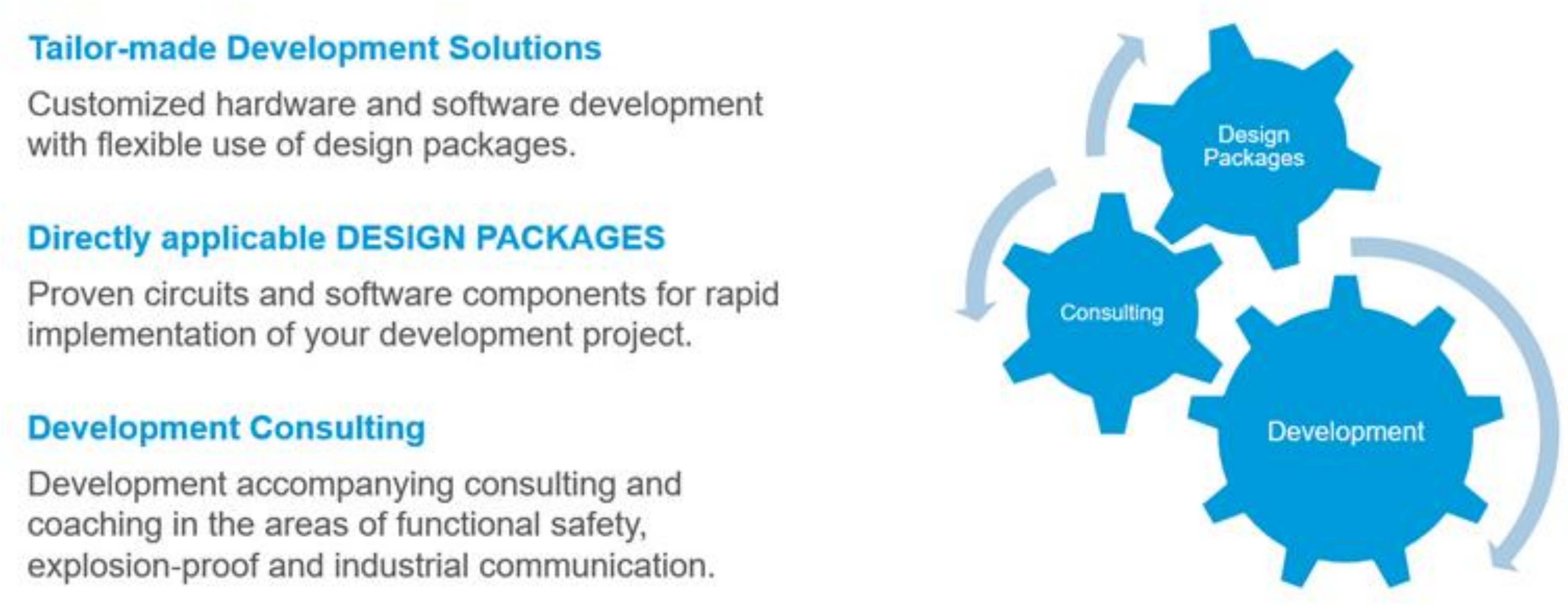
INNOTEC GMBH
WWW.INNOTECSAFETY.COM

ERLENWEG 12
49324 MELLE
GERMANY

+49 (5422) 9811-350

MESCO

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

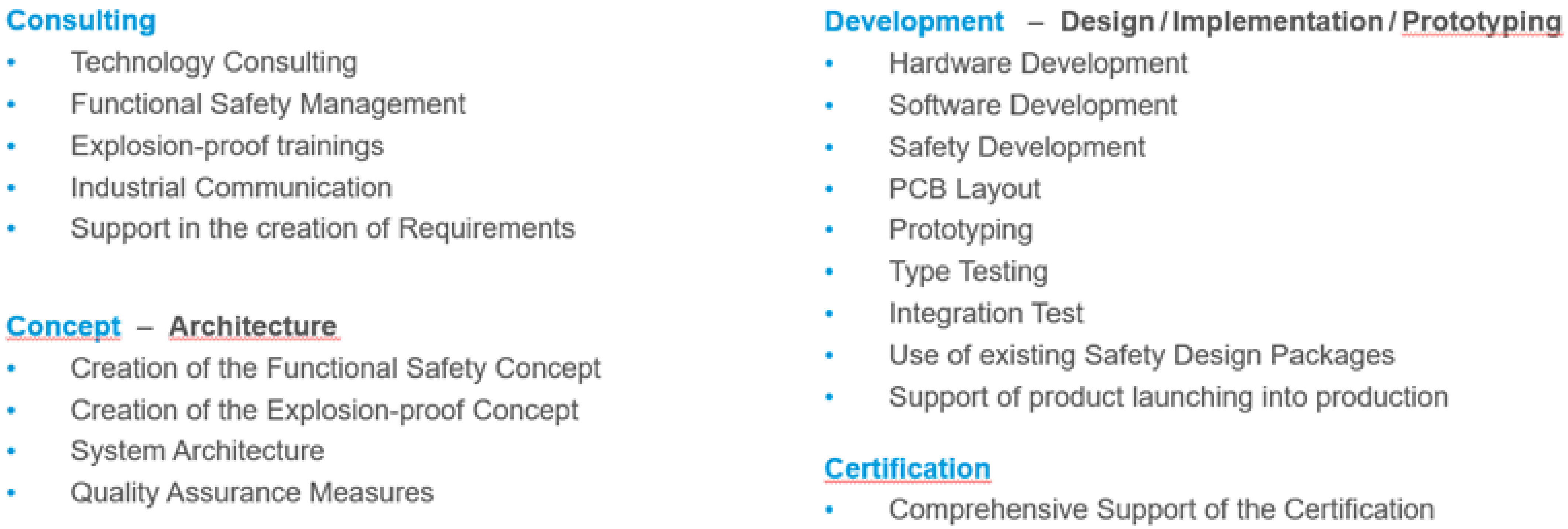
Proven circuits and software components for rapid implementation of your development project.

Development Consulting

Development accompanying consulting and coaching in the areas of functional safety, explosion-proof and industrial communication.

MESCO

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

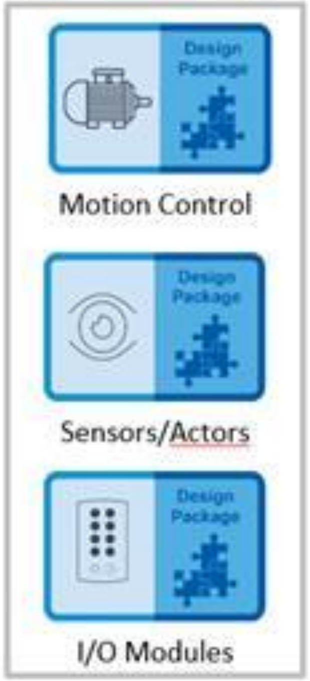
- Hardware Development
- Software Development
- Safety Development
- PCB Layout
- Prototyping
- Type Testing
- Integration Test
- Use of existing Safety Design Packages
- Support of product launching into production

Certification

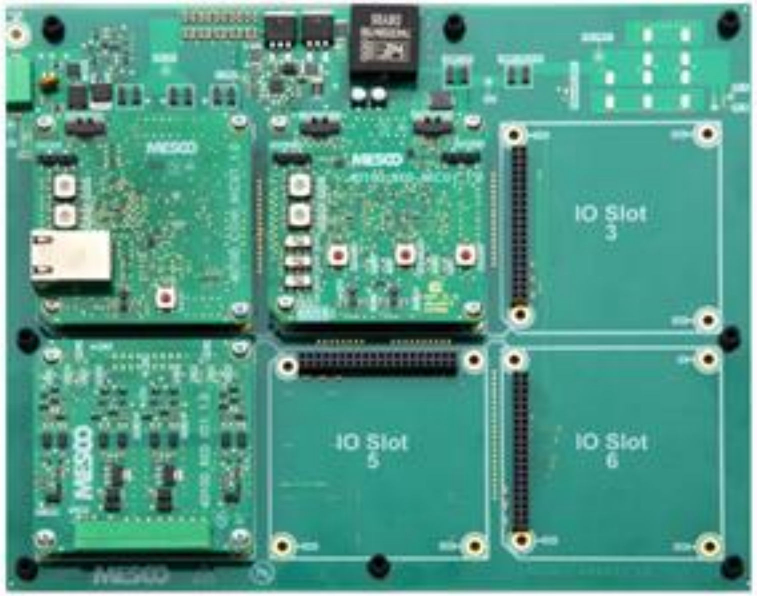
- Comprehensive Support of the Certification

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

NewTec

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

NTSafeFlex STM32

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 MCUs 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

SCIOPTA

SCIOPTA RTOS

SAFE

SCIOPTA RTOS is designed with safety in mind.

CERTIFIED

SCIOPTA RTOS is certified according to following standards: IEC61508 (SIL 3), EN50128/129 (SIL 3/4) and ISO26262 (ASIL D).

MIGRATION NON SAFE – SAFE

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

FAST

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

SMALL

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

DYNAMIC

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

SCHEDULING

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

EASY TO USE

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

FUTURE PROOF

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

USE CASES

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

SEGGER microcontroller

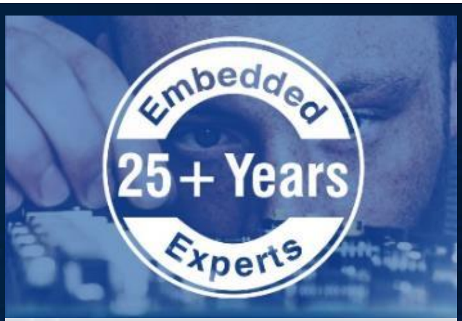
embOS-Safe

- 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 is deployed in many applications, such as home appliances, IoT, transportation, industrial, medical or automotive.



More than 27 years of continuous development

SEGGER started offering 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, proof 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

embOS is MadeForSTM32

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.

Tuxera

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

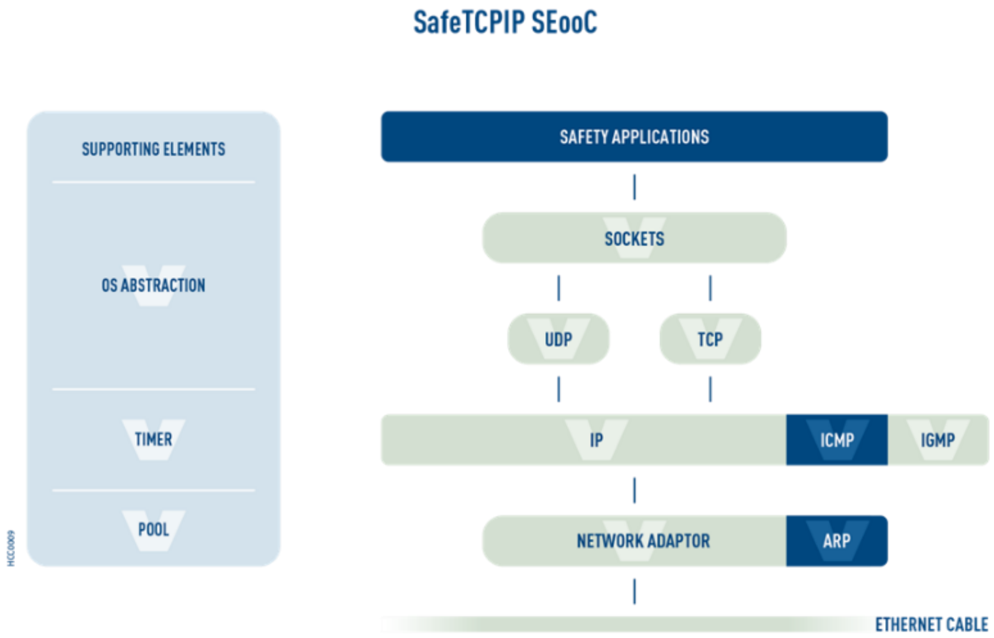
Accelerating Safety Development

- SEooC
- Integration TestBench
- SafeTCPIP

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

- More information: https://www.tuxera.com/products/safetcpip/



WITTENSTEIN high integrity systems

SAFERTOS®: safety critical RTOS

100% success rate certifying with TÜV SÜD across Industry sectors:

Industrial	**IEC 61508**
Automotive	**ISO 26262**
Medical	**IEC 62304/FDA 510K**
Railway	**EN 50128**

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

SAFE**RTOS** is a safety critical upgrade to FreeRTOS:

- Based on the FreeRTOS functional model
- Rebuilt to comply with **SIL 3 requirements**
- No open source code

SAFE**RTOS can be found in:**

- Dialysis machines
- Prostheses
- Control systems found on trains
- Safety critical servo controllers
- Industrial control systems and many more

life.augmented

WITTENSTEIN high integrity systems

SAFERTOS Support for ST

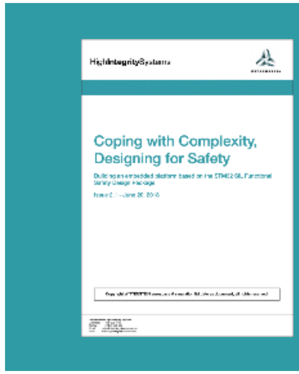
SAFERTOS Supported Platforms	
STM32F3, STM32F4, STM32L4	Arm Cortex®-M4
STM32F2, STM32F1, STM32L1, STM32W	Arm Cortex®-M3
STM32F0	Arm Cortex®-M0
STM32F7, H7	Arm Cortex®-M7
STM32H7 Dual Core	Arm Cortex®-M7 & Arm Cortex®-M4

SAFE**RTOS** supports:

- X-CUBE-STL;
- STM32Cube embedded software;
- STM32 SIL functional safety package;
- Secure boot.

SAFE**RTOS** demos for ST are available:

- 30-days evaluation packages with full source code on request. Download demos here.



HighIntegritySystems

Coping with Complexity, Designing for Safety

Building an embedded platform based on the STM32 SIL Functional Safety Design Package

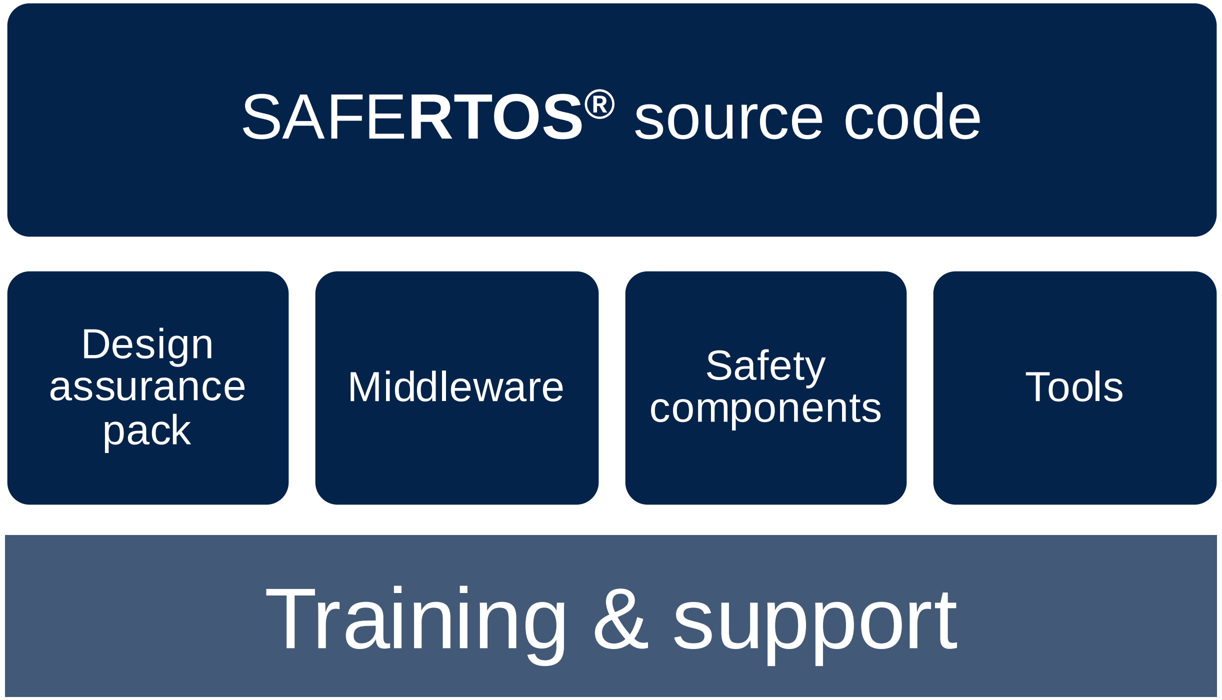
[illegible]

Free White Paper:
Based on the X-CUBE-STL Functional safety Package.
Free to Download

WITTENSTEIN high integrity systems

WITTENSTEIN high integrity systems standard offer

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

Training & support

- ✓ Royalty free, perpetual licensing
- ✓ 12 months free support & maintenance
- ✓ Smooth path to certification

WHIS also offers board support packages, training courses and more.

Our technology starts with You

Find out more at www.st.com/functionalsafety

life.augmented