life.augmented

Functional safety packages for STM32 & STM8 MCUs

STM32

STM8

Safety Ready

SIL Ready

ASIL Ready

ClassB Ready

life.augmented

Partner Program

“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

Achieve functional safety certification with ST MCUs

With its **Functional Safety Packages** based on robust built-in MCU 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 (STM8AF)
- **Class B Functional Safety Package**
  for household electrical appliances
  IEC 60335-1/60730-1 (STM32 & STM8)

life.augmented

STM32 built-in safety features

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

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

life.augmented

SIL functional safety package for STM32

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

SIL Functional Safety Package for STM32

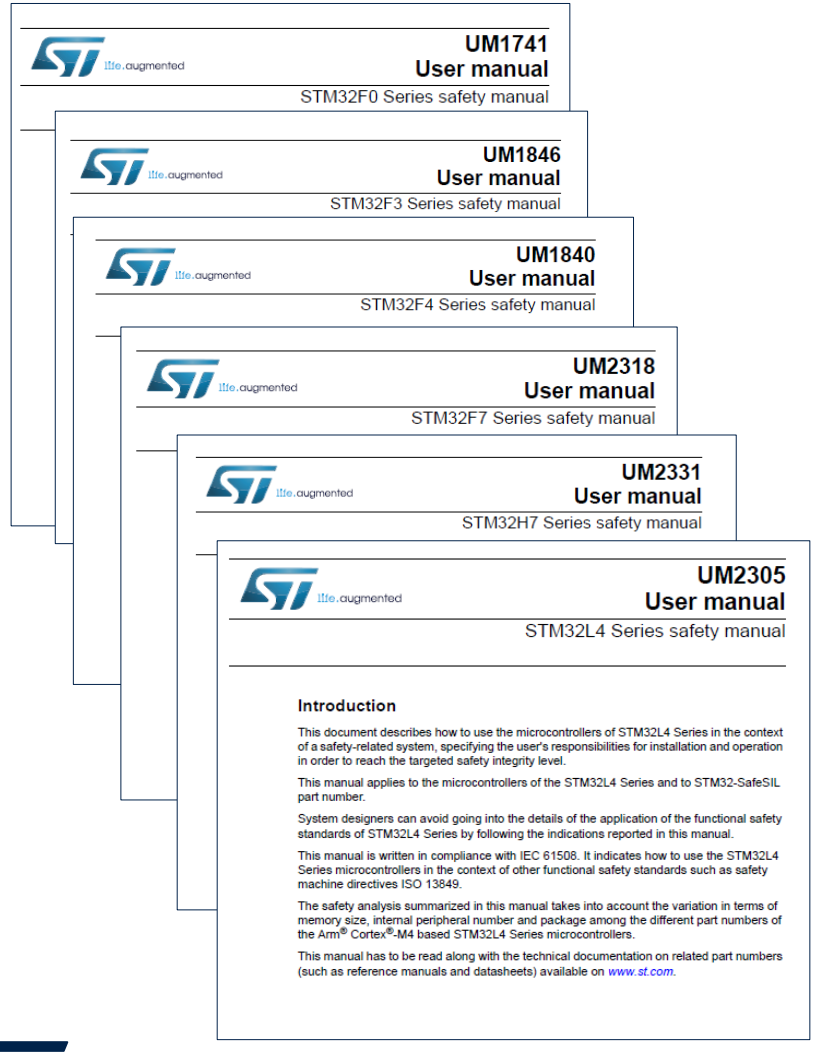
without design package

ST provides a complete, certified offering to

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

with design package

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 failure modes and related mitigation measures adopted

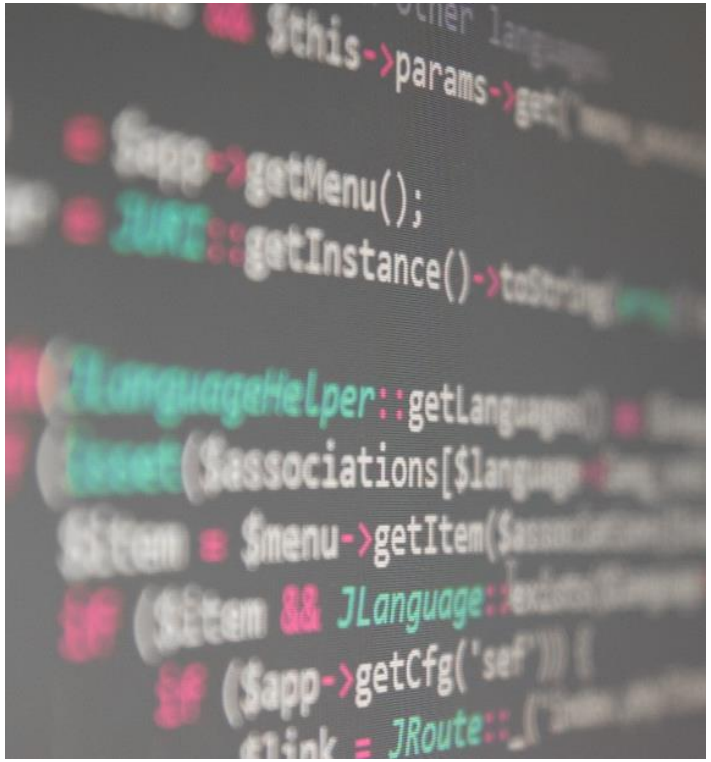
FMEDA: static snapshot reporting IEC 61508 failure rates, computed at both MCU and basic function detail levels.

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

life.augmented

SIL functional safety package for STM32 X-CUBE-STL self-test libraries



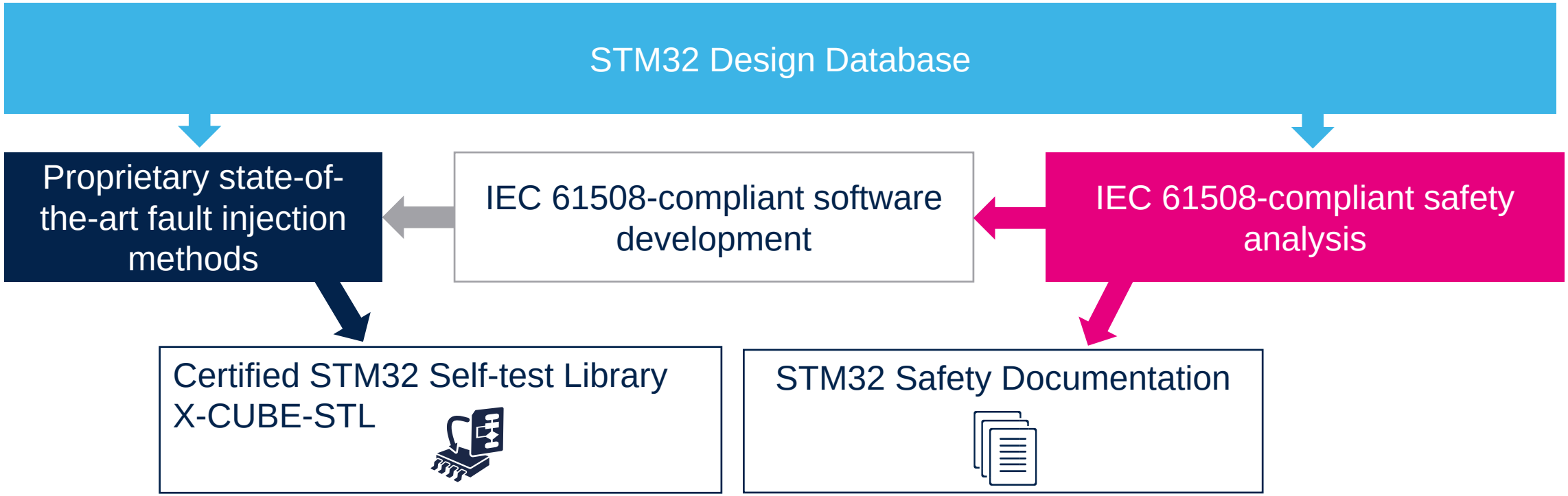
- Software-based diagnostic suite designed to detect random hardware failures in safety-critical STM32 core components (CPU + SRAM + Flash memory)
- Diagnostic coverage verified by state-of-the-art ST proprietary fault injection methodology
- Application independent: can be potentially used in any end customer application
- Compiler independent: delivered as object code
- Certified by TÜV Rheinland [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.



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)

life.augmented

STM8A-SafeASIL Functional Safety Package

Reduce time and cost to build STM8AF-based systems certified to ISO 26262 automotive functional safety standard

ASIL A/B

Customer Development

+

Specification for Self-Test Library

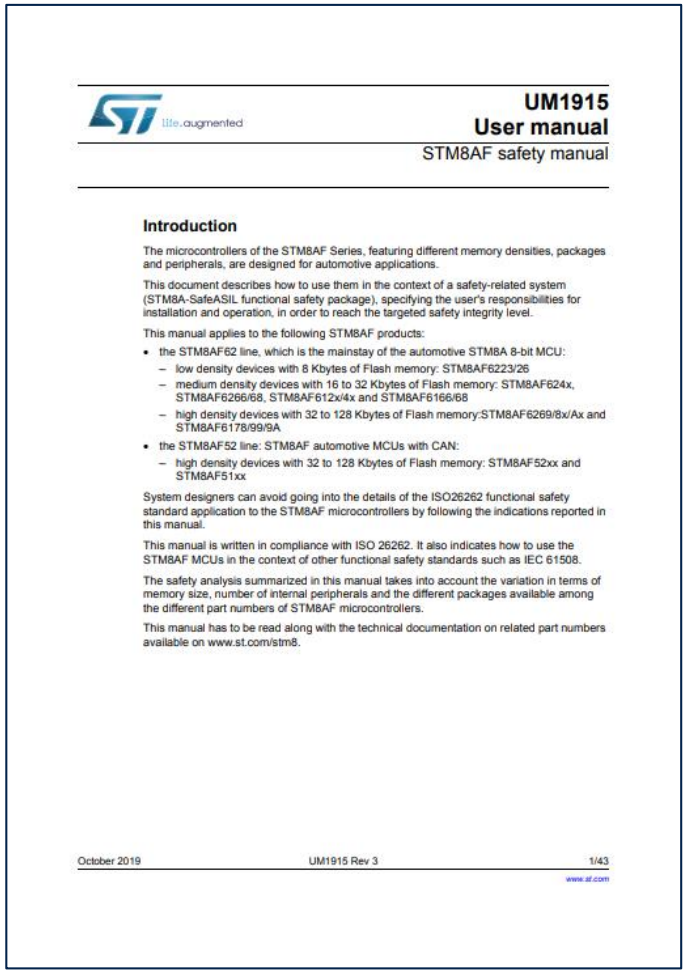
Safety documentation

MCU Safety Features

Product Portfolio — STM8A

ST Quality foundations

STM8A-SafeASIL safety documentation



UM1915
User manual
STM8AF safety manual

Introduction

The microcontrollers of the STM8AF Series, featuring different memory densities, packages and peripherals, are designed for automotive applications.

This document describes how to use them in the context of a safety-related system (STM8A-SafeASIL functional safety package), specifying the user's responsibilities for installation and operation, in order to reach the targeted safety integrity level.

This manual applies to the following STM8AF products:

- the STM8AF62 line, which is the mainstay of the automotive STM8A 8-bit MCU:
  - low density devices with 8 Kbytes of Flash memory: STM8AF6223/26
  - medium density devices with 16 to 32 Kbytes of Flash memory: STM8AF624x, STM8AF6266/68, STM8AF612x/4x and STM8AF6166/68
  - high density devices with 32 to 128 Kbytes of Flash memory:STM8AF6269/8x/Ax and STM8AF6178/99/9A
- the STM8AF52 line: STM8AF automotive MCUs with CAN:
  - high density devices with 32 to 128 Kbytes of Flash memory: STM8AF52xx and STM8AF51xx

System designers can avoid going into the details of the ISO26262 functional safety standard application to the STM8AF microcontrollers by following the indications reported in this manual.

This manual is written in compliance with ISO 26262. It also indicates how to use the STM8AF MCUs in the context of other functional safety standards such as IEC 61508.

The safety analysis summarized in this manual takes into account the variation in terms of memory size, number of internal peripherals and the different packages available among the different part numbers of STM8AF microcontrollers.

This manual has to be read along with the technical documentation on related part numbers available on www.st.com/stm8.

October 2019 UM1915 Rev 3 1/43

Safety manual: Detailed list of safety requirements and examples to support STM8AF 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 series level 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 at STM8AF part number level. (*)
Ask your local ST contact.

(*) submitted to NDA

life.augmented

STM8A-SafeASIL specification for self-test library

AN5482

full list of detailed safety requirements enabling STM8AF users to realize, in the framework of their ISO26262-compliant software development process, the software Self-test Library required by STM8AF 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 series(*)
Ask your local ST contact

(*) submitted to NDA

ClassB functional safety package for STM32 and STM8 MCUs

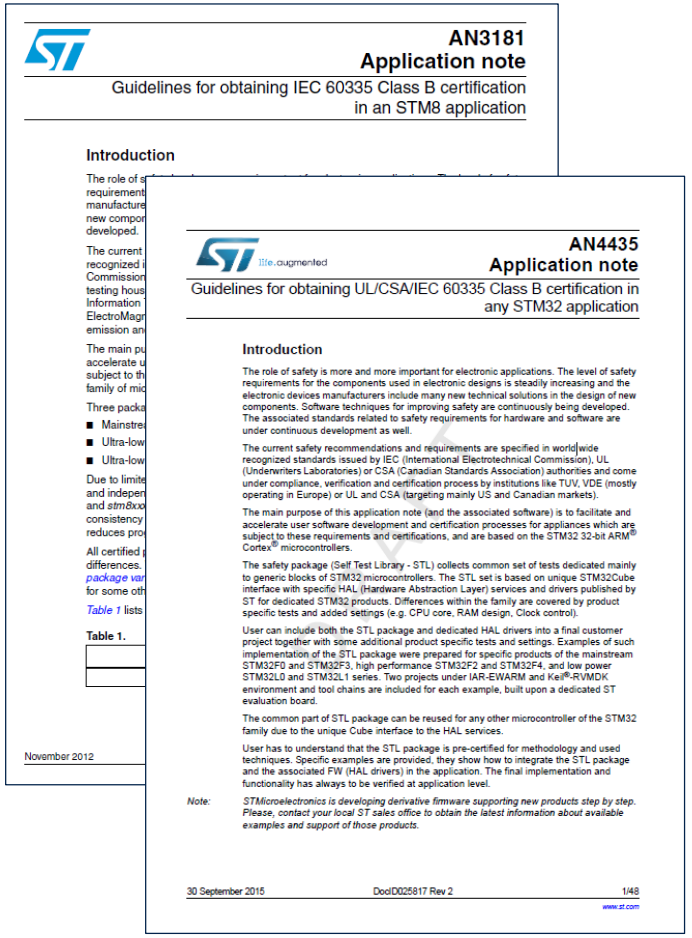
Reduce time and cost to build STM32 & STM8 based systems certified to IEC 60335-1 and 60730-1 household electrical appliance safety standards.

- **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

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	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



AN3181
Application note
Guidelines for obtaining IEC 60335 Class B certification in an STM8 application

Introduction

November 2012

life.augmented

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 for STM32 & STM8 MCUs

	SIL Ready	ASIL Ready	ClassB Ready	
MCU support	STM32	STM8AF	STM32	STM8
Achievable safety standards	IEC 61508	ISO 26262	IEC, UL, CSA 60335-1 60730-1	
Certification	TÜVRheinland CERTIFIED		UL CERTIFIED	DVE UL CERTIFIED
Package content	• Safety Documentation • Self Test Libraries	• Safety Documentation • Self-Test Library specification	• Safety Documentation • Self Test Libraries	• Safety Documentation • Self Test Libraries
Package name	**X-CUBE-STL**	**STM8A-SafeASIL**	**X-CUBE-CLASSB**	**STM8-SafeCLASSB**

Get support from ST authorized partners

Reduce your project time and cost

Safety Requirements → HW & SW Design → Validation → Certification

life.augmented

Partner Program

Functional Safety expertise

life.augmented

Functional safety authorized partners

Embedded Software

- arm KEIL
- Embedded Office
- expresslogic
- SEGGER It simply works!
- WITTENSTEIN

Software Development Tools

- arm KEIL
- IAR SYSTEMS

Engineering, consulting, development or design services

- Embedded Office
- hitex EMBEDDED TOOLS & SOLUTIONS
- 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-Ready

Safety Qualified Toolchain

Simplifies Tool Justification

- TUV Certificate by TUV SUD
- Qualification Kit
  - Safety Manual
  - Defect Report

Comprehensive safety documentatio

Arm Compiler For Functional Safety

Licensed as 'Standalone' or via Arm IDE Toolkits:

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

arm DEVELOPMENT STUDIO

arm KEIL

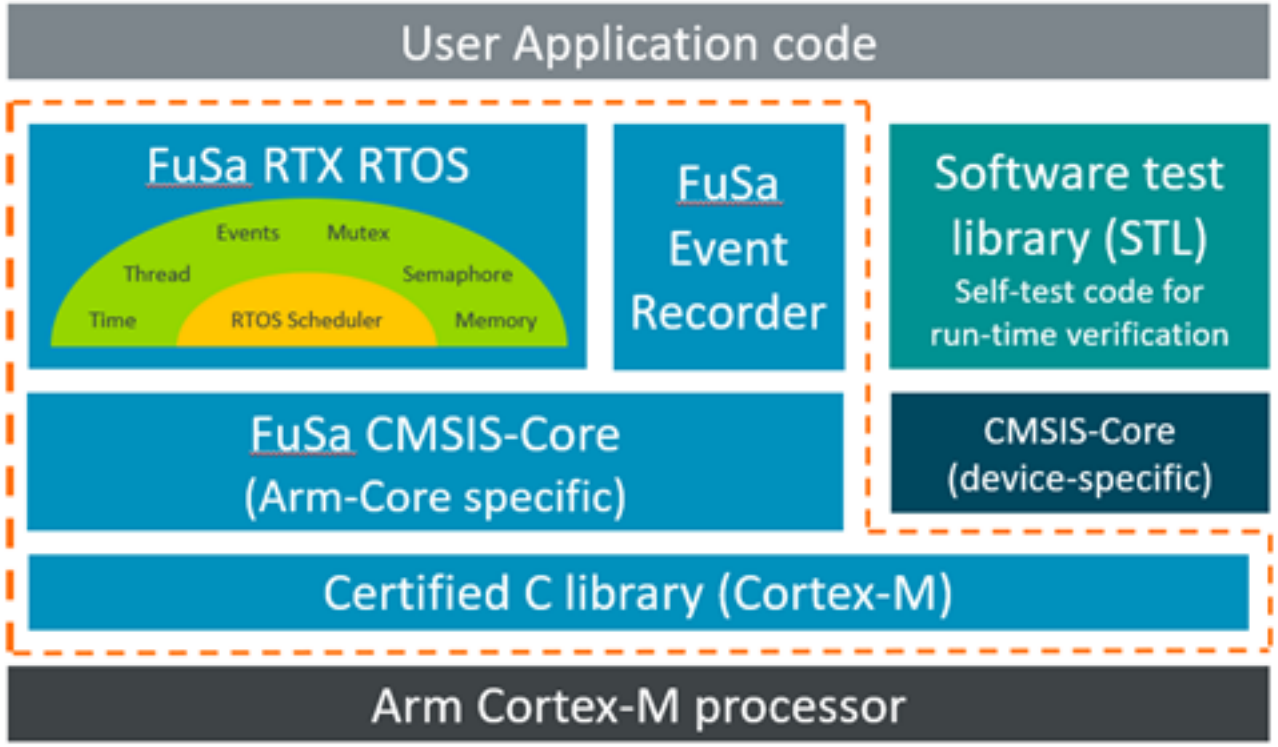
Baseline toolchain for Arm Safety Software development:

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

Certified software components

Arm FuSa RTS: Run-Time System for Fonctional Safety

Software components certified for safety-critical applications



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

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

hitex
EMBEDDED TOOLS & SOLUTIONS

Hitex

Consulting & Engineering

life.augmented

Expertise out of our Customer projects

DC/DC converters

Safety integration & certification

Implementing security requirements

Emulator for special micro controllers

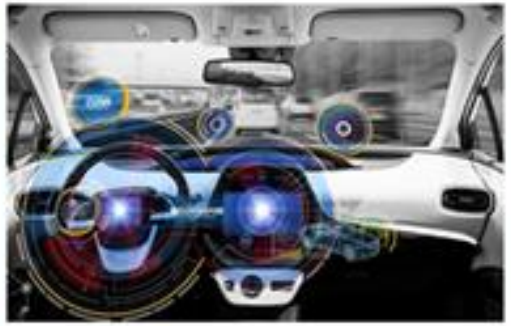
IoT implementation and integration

eDrive development

Functional Safety process consulting

Battery management

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

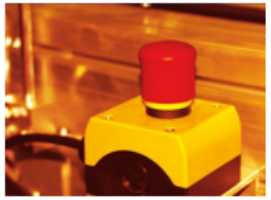
Arm Functional Safety Partner
Software & Tools

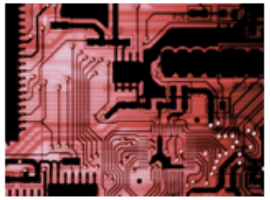
Available for Arm and STM8

innotec

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

life.augmented

Our range of services: Factory & Process Automation

Tailor-made Development Solutions

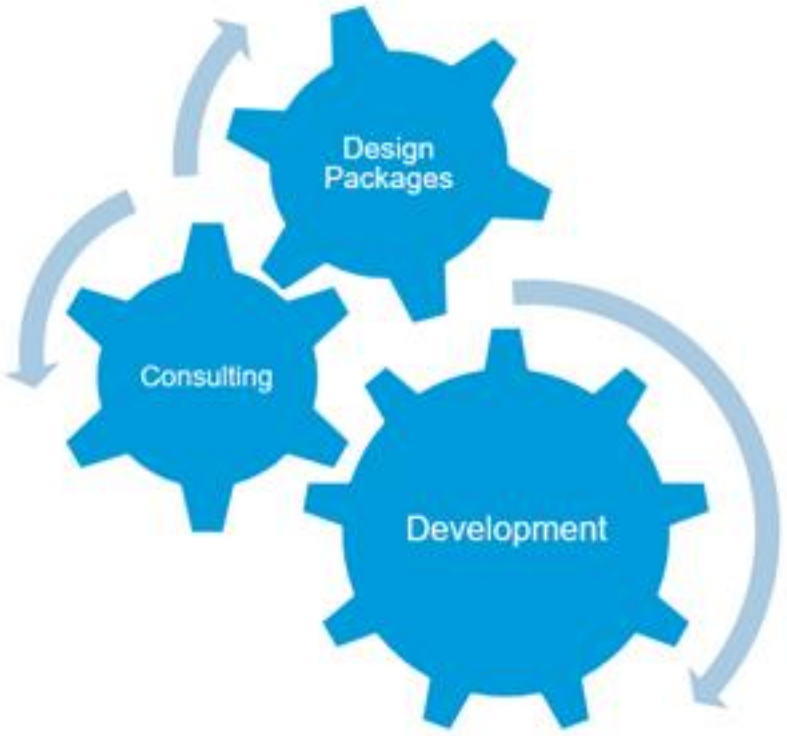
Customized hardware and software development with flexible use of design packages.

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

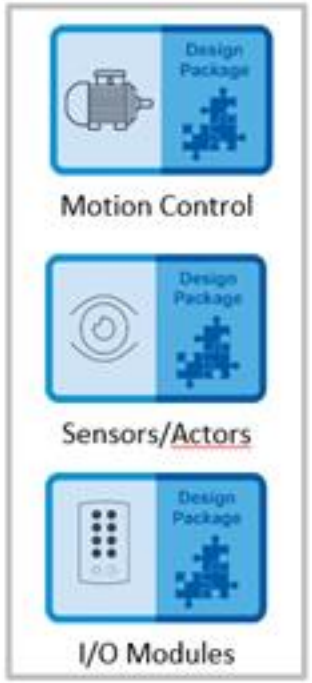
- Hardware Development
- Software Development
- Safety Development
- PCB Layout
- Prototyping
- Type Testing
- Integration Test
- Use of existing Safety Design Packages
- Support of product launching into production

Certification

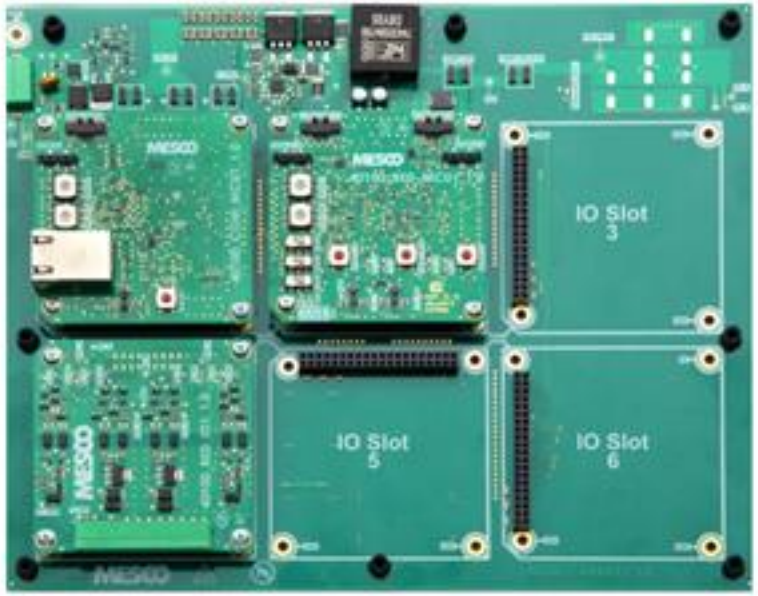
- Comprehensive Support of the Certification

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

expresslogic

Microsoft

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 fall 2020

life.augmented

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

life.augmented

SEGGER Microcontroller

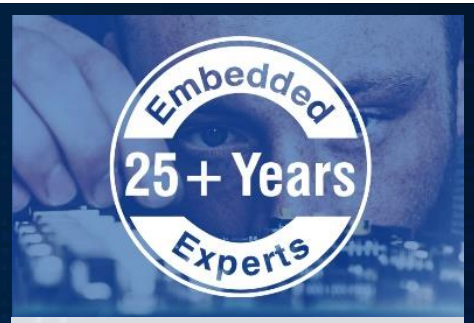
embOS-Safe

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

embOS-Safe

embOS is labelled 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.

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

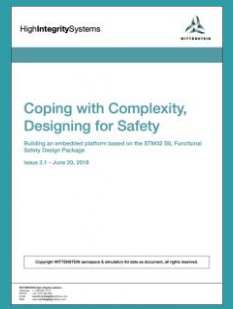
SAFERTOS Supported Platforms	
STM32F3, STM32F4, STM32L4	ARM Cortex-M4
STM32F2, STM32F1, STM32L1, STM32W	ARM Cortex-M3
STM32F0	ARM Cortex-M0
STM32F7, H7	ARM Cortex-M7
STM32H7 Dual Core	ARM Cortex-M7 & ARM Cortex-M4

SAFE**RTOS** supports:

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

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

- 30 day 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

life.augmented

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 specialise **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 offer Board Support Packages, Training Courses and more…

Safety Ready

STM32

STM8

www.st.com/functionalsafety

life.augmented

Thank you

life.augmented