Functional Safety Design Packages

for STM32 & STM8 MCUs

STM32

STM8

Safety Ready

SIL Ready

ASIL Ready

ClassB Ready

life.augmented

January 2019

Achieve functional safety certifications with ST MCUs

With its **Functional Safety Design 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 Design Package**
  for industrial IEC 61508 (STM32)
- **ASIL Functional Safety Design Package**
  for automotive ISO 26262 (STM8AF)
- **Class B Functional Safety Design Package**
  for household electrical appliances
  IEC 60335-1/60730-1 (STM32 & STM8)

Safety Ready

STM32 built-in safety features

Features	F0	F1	F3	F2/F4	L0/L1	F7	H7	L4/L4+
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							●	●

life.augmented

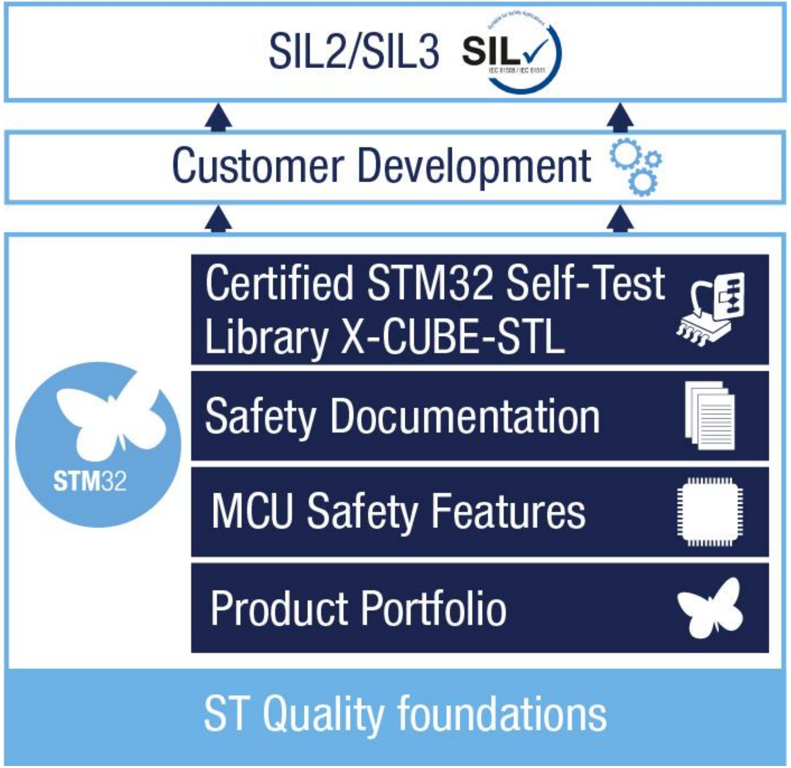
*<u>**Note**</u>: Cortex-M cores also have built-in safety features (dual stack pointer, fault exceptions, and debug module).*

* : Depending on part number

SIL
Ready

SIL Functional Safety Design Package for STM32

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



SIL2/SIL3 SIL✓

Customer Development

STM32

Certified STM32 Self-Test Library X-CUBE-STL

Safety Documentation

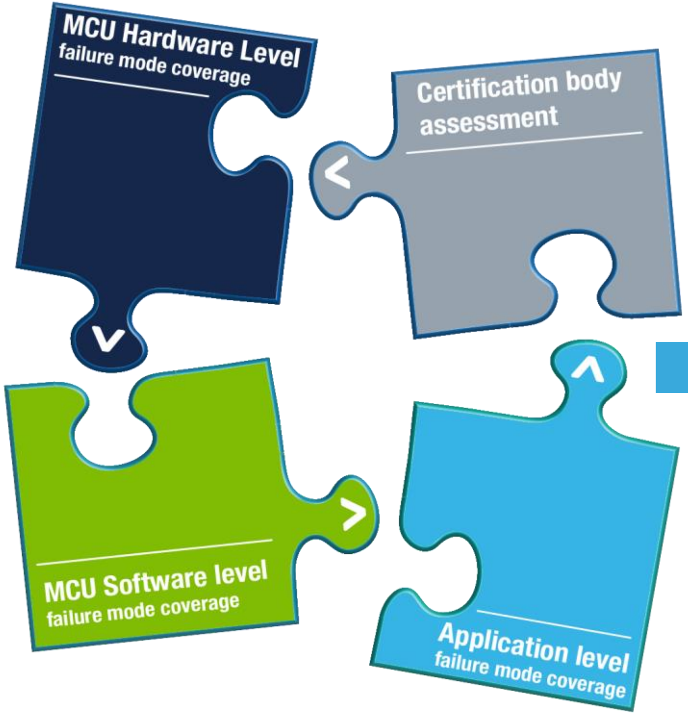
MCU Safety Features

Product Portfolio

ST Quality foundations

life.augmented

SIL Functional Safety Design Package for STM32



MCU Hardware Level
failure mode coverage

Certification body
assessment

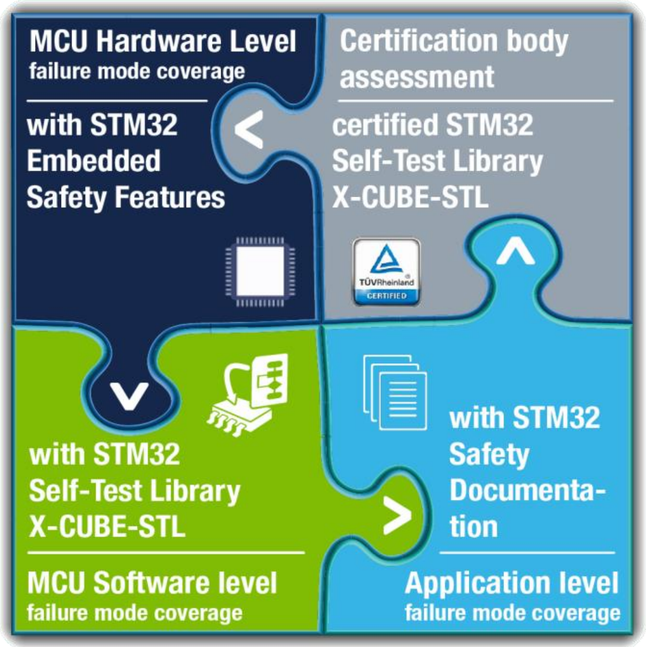
MCU Software level
failure mode coverage

Application level
failure mode coverage

without
design package

Rely on a certified comprehensive offering to

- lower your project cost
- lower your project complexity
- ease your SIL certification assessment



MCU Hardware Level
failure mode coverage
with STM32 Embedded Safety Features

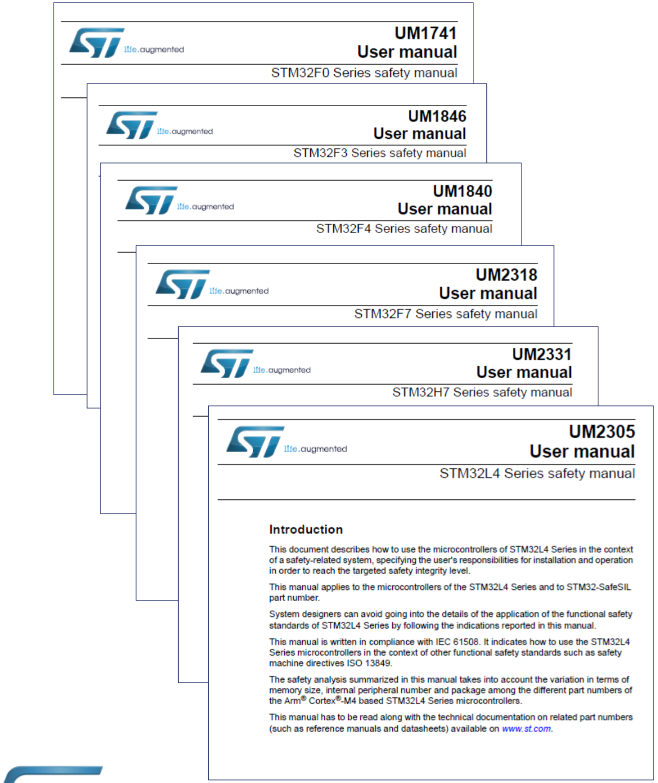
Certification body
assessment
certified STM32 Self-Test Library X-CUBE-STL

with STM32 Self-Test Library X-CUBE-STL
MCU Software level
failure mode coverage

with STM32 Safety Documenta-tion
Application level
failure mode coverage

with
design 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 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

SIL Ready

SIL Functional Safety 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 used in any end customer application
- **Compiler independent**: delivered as object code
- **Certified** by TÜV Rheinland
- **IEC 61508 SIL3 (SC3)** compliant
- Provided with **safety manual** and **user guide**

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

TÜVRheinland® CERTIFIED

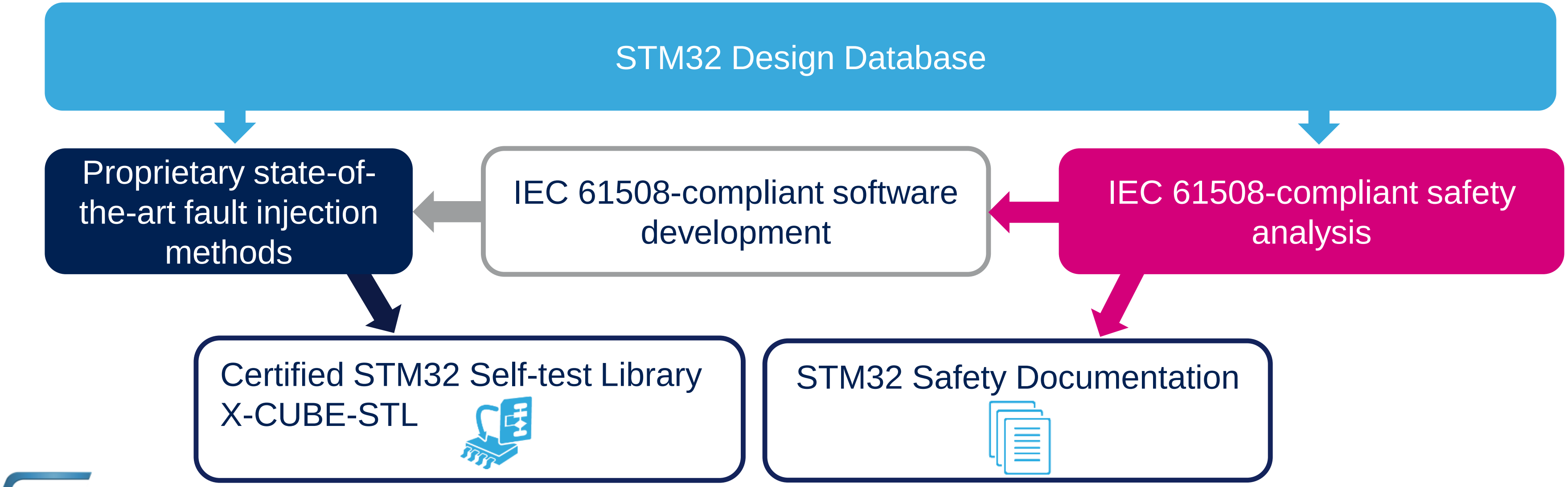
SIL IEC 61508 / IEC 61511

life.augmented

(*) submitted to NDA (**) Check the X-CUBE-STL release roadmap
(***) read the X-CUBE-STL Software License Agreement

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

SIL Ready

Achieve SIL2/SIL3 with STM32

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

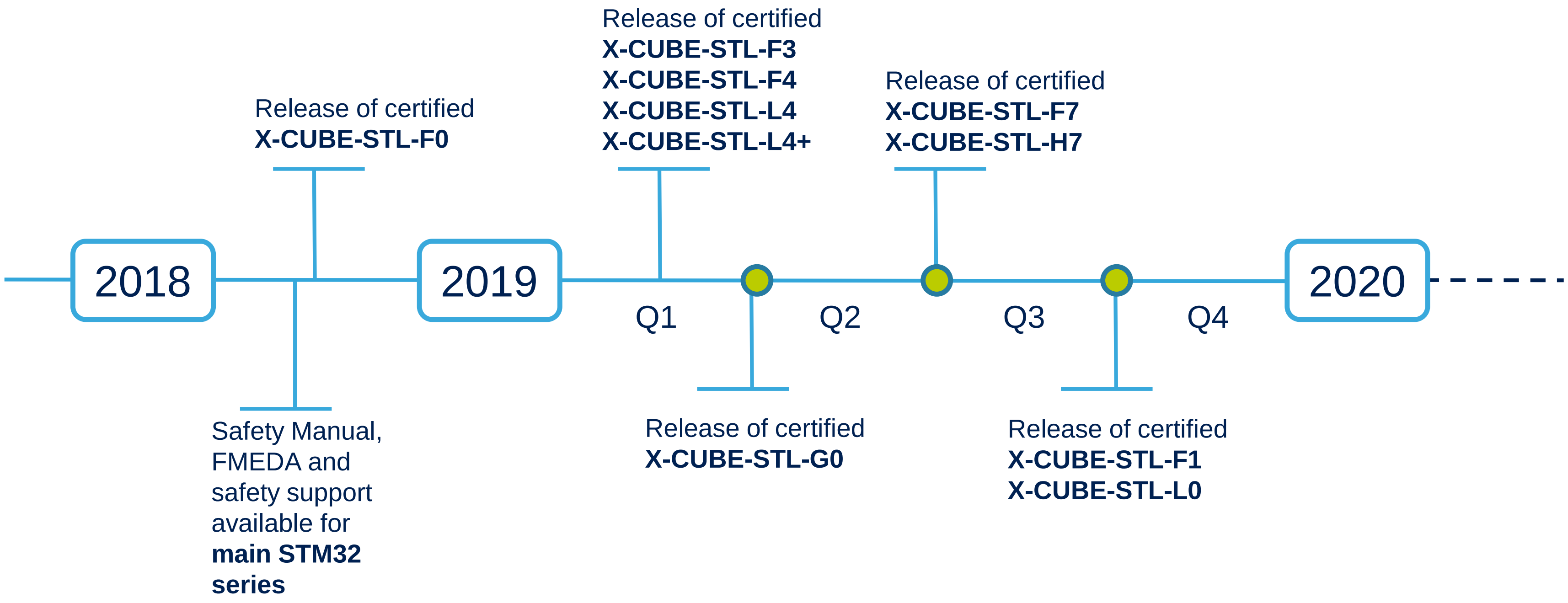
1oo1: 1 out of 1 MCU (no redundancy)

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

life.augmented

SIL Ready

X-CUBE-STL roadmap



Release of certified
X-CUBE-STL-F0

Safety Manual,
FMEDA and
safety support
available for
**main STM32
series**

Release of certified
**X-CUBE-STL-F3
X-CUBE-STL-F4
X-CUBE-STL-L4
X-CUBE-STL-L4+**

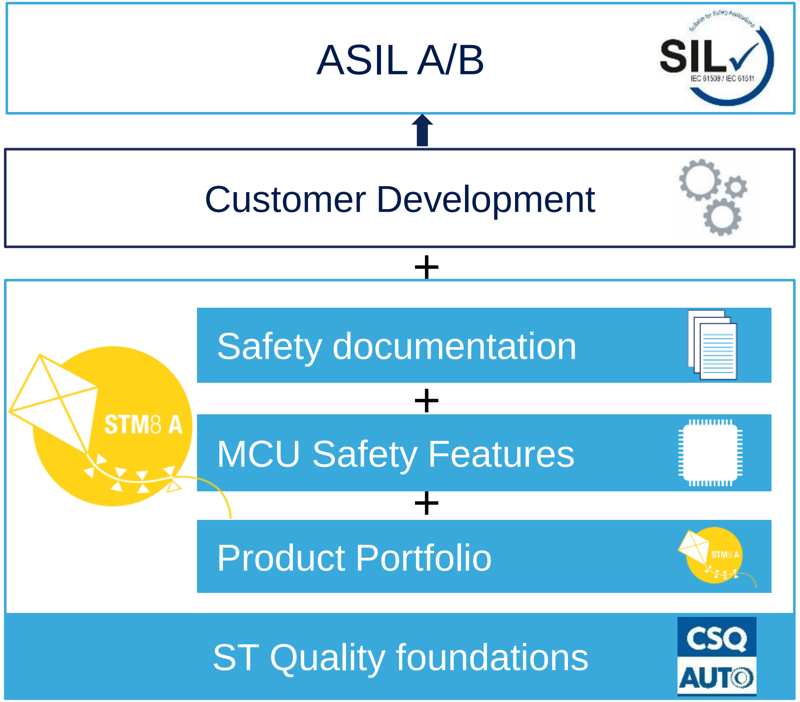
Release of certified
X-CUBE-STL-G0

Release of certified
**X-CUBE-STL-F7
X-CUBE-STL-H7**

Release of certified
**X-CUBE-STL-F1
X-CUBE-STL-L0**

STM8A-SafeASIL
Functional Safety Design Package

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



ASIL A/B

Customer Development

+

Safety documentation

+

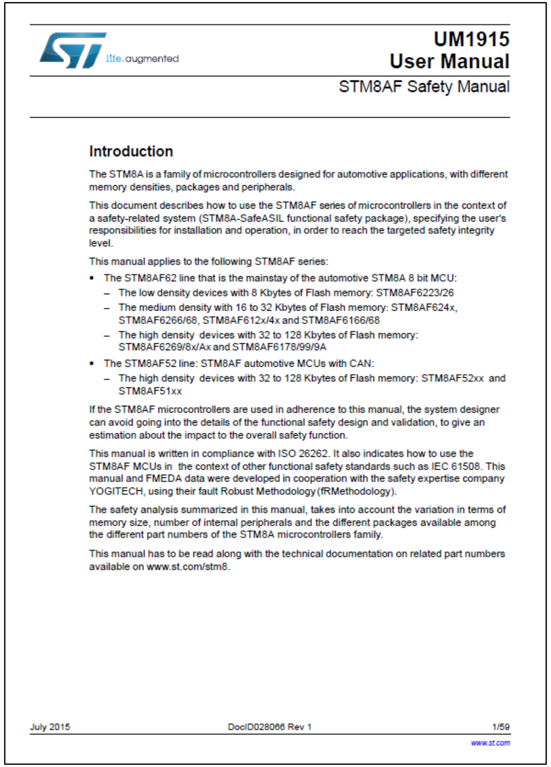
MCU Safety Features

+

Product Portfolio

ST Quality foundations

STM8A-SafeASIL
Safety Documentation



UM1915
User Manual

STM8AF Safety Manual

Introduction

The STM8A is a family of microcontrollers designed for automotive applications, with different memory densities, packages and peripherals.

This document describes how to use the STM8AF series of microcontrollers 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 series:

- The STM8AF62 line that is the mainstay of the automotive STM8A 8 bit MCU:
  - The low density devices with 8 Kbytes of Flash memory: STM8AF6223/26
  - The medium density with 16 to 32 Kbytes of Flash memory: STM8AF624x, STM8AF6266/68, STM8AF612x/4x and STM8AF6166/68
  - The 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:
  - The high density devices with 32 to 128 Kbytes of Flash memory: STM8AF52xx and STM8AF51xx

If the STM8AF microcontrollers are used in adherence to this manual, the system designer can avoid going into the details of the functional safety design and validation, to give an estimation about the impact to the overall safety function.

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. This manual and FMEDA data were developed in cooperation with the safety expertise company YOGITECH, using their fault Robust Methodology (fRMethodology).

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 the STM8A microcontrollers family.

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

July 2015 DocID028066 Rev 1 1/59

www.st.com

Safety manual: Detailed list of safety requirements (conditions of use) and examples to guide STM8AF users to achieve Automotive Safety Integrity Level (ASIL A or ASIL B) in compliance with 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.

Class B Functional Safety Design 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 or SPL
- **Safety manuals** (guidelines and examples)
- For STM32: Support of IAR™ EWARM, Keil® MDK-ARM, and System Workbench for STM32 from AC6
- **Worldwide standards coverage** (IEC, UL, and CSA)

Class B Functional Safety Design Packages

Package name	X-CUBE-CLASSB	STM32-CLASSB-SPL	STM8-SafeCLASSB
STM32 Series covered	STM32F0, F1, F3 STM32F2, F4, F7 STM32L0, L1, L4	STM32F0, F1, F3 STM32F2 (*), F4 (*)	STM8AF STM8AL STM8L STM8S
Self-test libraries based on	**STM32CubeHAL**	**STM32 Standard Peripheral Libraries**	Optimized direct access to registers
Supported development environments	**IAR™** / Arm® **Keil®** **GCC**-based AC6 compilers		
Certification	UL, 2017	VDE, 2012	(*) Derived packages (not certified)
IEC 60335-1 and 60730-1 international standards coverage	IEC, UL and CSA	IEC	
Safety manual (guidelines)	AN4435	AN3307	AN3181
Portability between MCUs	Optimized thanks to STM32Cube	Limited	Limited

life.augmented

ClassB Ready

Class B Safety Manuals

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

November 2

AN3307
Application note
Guidelines for obtaining IEC 60335 Class B certification for any STM32 application

Introducti

The role of saf requirements f manufacturers new componen 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

There are thre STM32F0xx, S document by S peripheral libra focus on main families, these yet certified (fo

a. All the Class B office.

b. STMicroelectr your local ST certification.

April 2013

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.

life.augmented

Safety Ready

Functional Safety Design Packages for STM32 & STM8 MCUs

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

life.augmented

Safety Ready

STM32

STM8

www.st.com/stm32safety
www.st.com/stm8safety