Safety Design Packages

for STM32 & STM8 MCUs

STM32

STM8

Safety Ready

SIL Ready

ASIL Ready

ClassB Ready

life.augmented

Achieve safety certifications with ST MCUs

With its Safety Design packages based on robust built-in MCU safety features, STMicroelectronics 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 Safety Design Package**
  for industrial IEC 61508 (STM32)
- **ASIL Safety Design Package**
  for automotive ISO 26262 (STM8AF)
- **Class B Safety Design Package**
  for household electrical appliances
  IEC 60335-1/60730-1 (STM32 & STM8)

life.augmented

STM32 built-in safety features

Features	HW/ SW	STM32 F0	STM32 F1	STM32 F3	STM32 F2/F4	STM32 L0/L1	STM32 F7	STM32 L4
Dual watchdogs: Independent watchdog and system window watchdog	HW	●	●	●	●	●	●	●
Backup clock circuitry with clock security system (CSS) *for switching to back-up internal RC in case of external clock failure*	HW	●	●	●	●	●	●	●
Hardware CRC unit / Programmable polynomial *with DMA support to check embedded Flash-memory content integrity*	HW	● / *	● / -	● / -	● / -	● / *	● / ●	● / ●
Supply monitoring (POR, BOR, PVD)	HW	●	●	●	●	●	●	●
I/O function locking	HW	●	●	●	●	●	●	●
PWM critical register protections (write-once registers)	HW	●	●	●	●		●	●
Memory protection unit (MPU) *8 zones – to ensure data integrity from invalid behavior*	HW		●	●*	●	●	●	●
Multiple Flash memory protection levels	HW	●		●	●	●	●	●
PWM stop on core lockup	HW	●		●				●
Parity bit for SRAM (1bit/byte)	HW	●		●				●
Flash ECC *(1): single error correction* *(2): single error correction, double error detection*	HW					●(1)		●(2)

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

* : Depending on device

SIL Safety Design Package
for STM32 MCUs

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

SIL2/SIL3

Development

+

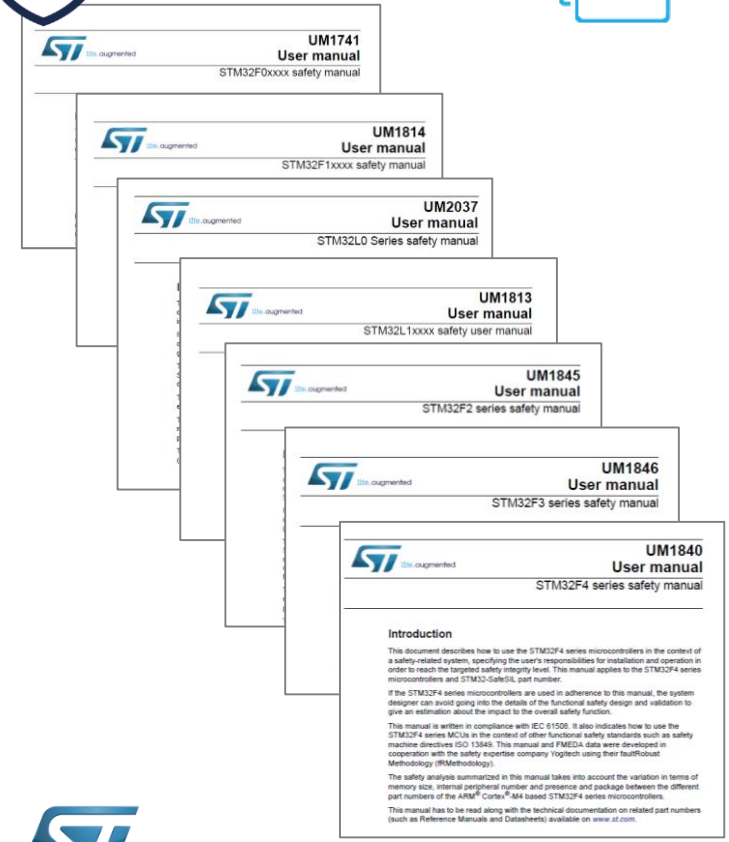
- Safety manuals
- Safety features
- Product portfolio

ST Quality foundations

life.augmented

SIL Ready

STM32 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.

Safety documentation
(e.g., FMEA/FMEDA, diagnostic coverage proof, evidence of compliance to systematic failure avoidance)

life.augmented

Achieve SIL2/SIL3 with STM32

Single STM32 (1oo1/1oo1d) 	**SIL2**
Two STM32 (1oo2/1oo2d/2oo2) 	**SIL3**

Supported STM32 series:

STM32 F0 STM32 F1 STM32 F3 STM32 L0 STM32 L1 STM32 F2 STM32 F4

Visit :
www.st.com/stm32-safesil

life.augmented

ASIL Safety Design Package
for STM8AF MCUs

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

SIL2/SIL3

Development

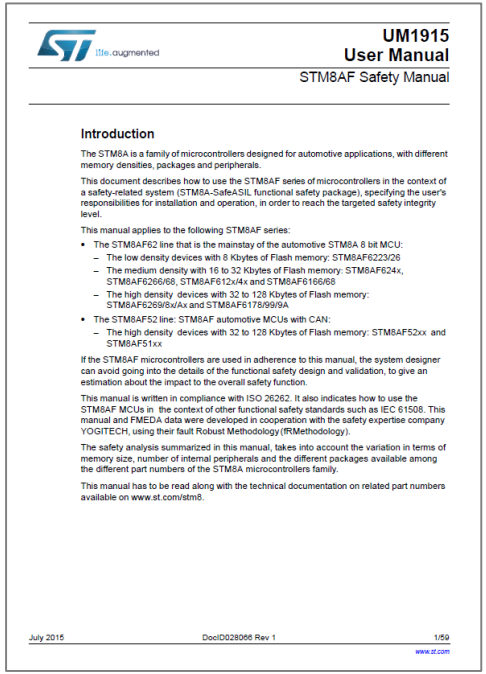
+

- Safety manuals
- Safety features
- Product portfolio

ST Quality foundations

Visit : www.st.com/stm8safety

STM8AF safety manual



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

Detailed list of safety requirements (conditions of use) and examples to guide STM8AF users to achieve Automotive Safety Integrity Level (A or B) in compliance with ISO 26262.

Safety documentation
(e.g., FMEA/FMEDA, diagnostic coverage proof, evidence of compliance to systematic failure avoidance)

Class B 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)
- Worldwide standards coverage (IEC, UL, and CSA)

life.augmented

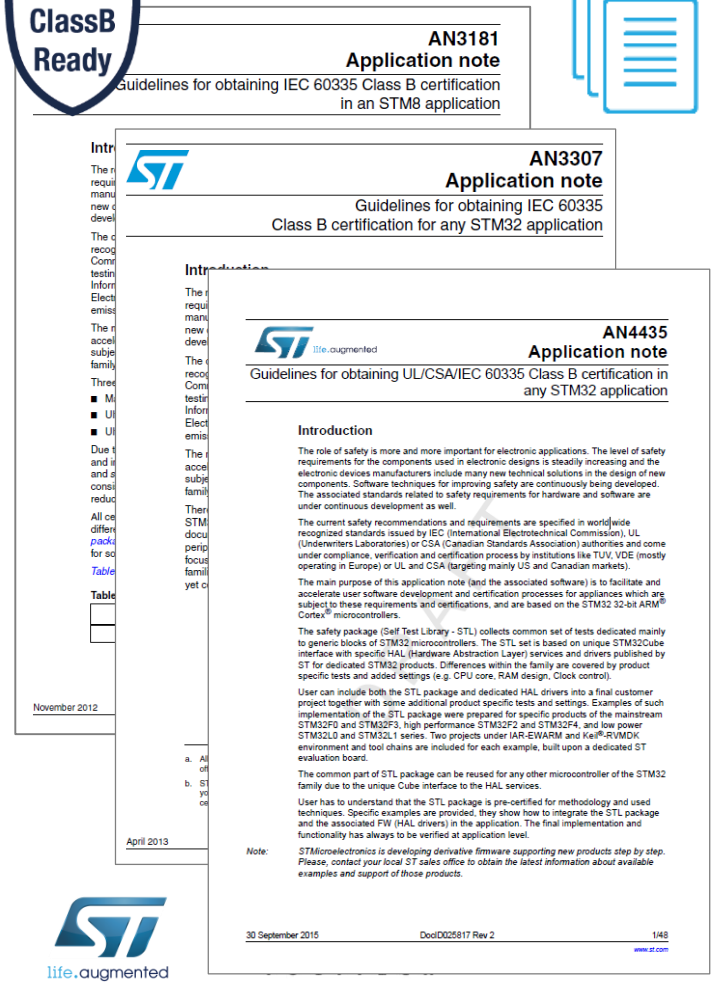
Class B Safety Design Packages

Package name	X-CUBE-CLASSB	STM32-CLASSB-SPL	STM8-SafeCLASSB
Series covered	STM32 F0 STM32 F2 STM32 F3 STM32 F4 STM32 L0 STM32 L1	STM32 F0 STM32 F1 STM32 F2 (*) STM32 F3 STM32 F4 (*)	STM8AF STM8AL STM8L STM8S
Self-test libraries based on	**STM32CubeHAL**	**STM32 Standard Peripheral Libraries**	Optimized direct access to registers
Certification	UL, 2015	VDE, 2012	
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
New series support	STM32F7 and STM32L4 will be supported	No	No

(*) Derived packages (not certified)

life.augmented

ClassB Ready



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

November 2012

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

April 2013

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 worldwide 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

life.augmented

ClassB Safety Manuals

Guidelines and examples for STM32 users to achieve Class B certification in compliance with IEC 60335-1 and 60730-1.

Safety Design Packages for STM32 & STM8 MCUs

	SIL Ready	ASIL Ready (Automotive)	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			UL CERTIFIED	DVE	
ST Firmware Platform			STM32 Cube	STM32 Standard Peripheral Libraries	Direct accesses to registers
Package name	STM32-SafeSIL	STM8A-SafeASIL	X-CUBE-CLASSB	STM32-CLASSB-SPL	STM8-SafeCLASSB

life.augmented

Safety Ready

STM32

STM8

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

life.augmented