Functional Safety Design Packages for STM32 & STM8 MCUs

July 2019
Achieve Functional Safety Certification 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)
### STM32 built-in safety features

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

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

Certified STM32 Self-Test Library X-CUBE-STL
Safety Documentation
MCU Safety Features
Product Portfolio

ST Quality foundations
SIL Functional Safety Design Package
for STM32

Rely on a certified comprehensive offering to
• lower your project cost
• lower your project complexity
• ease your SIL certification assessment
SIL Functional Safety for STM32

Safety Documentation

Safety manuals: detailed list of safety requirements (conditions of use) and examples to guide STM32 users to achieve safety integrity level certification in compliance with IEC 61508.

Available at STM32 series level for free download on www.st.com/x-cube-stl

FMEA: detailed list of MCU 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 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](http://www.st.com/x-cube-stl)

(*) submitted to NDA  
(**) Check the X-CUBE-STL release roadmap  
(***) read the X-CUBE-STL Software License Agreement
ST builds functional safety solutions for its STM32 Arm® Cortex®-M microcontroller family, including detailed and accurate safety analyses supported by verification activities based on state-of-the-art fault injection methods.
Achieve SIL2/SIL3 with STM32

<table>
<thead>
<tr>
<th>SIL2</th>
<th>Achievable with single STM32 (1oo1 architecture)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL3</td>
<td>Achievable with two STM32 (1oo2 architecture)</td>
</tr>
</tbody>
</table>

1oo1: 1 out of 1 MCU (no redundancy)
1oo2: 1 out of 2 MCUs (1 redundant system)
X-CUBE--STL Roadmap

- **2018**
  - Safety Manual, FMEDA and safety support available for main STM32 series

- **2019**
  - Q1: Release of certified X-CUBE-STL-F0
  - Q2: Release of certified X-CUBE-STL-F3, X-CUBE-STL-F4, X-CUBE-STL-L4, X-CUBE-STL-L4+

- **2020**
  - Q3: Release of certified X-CUBE-STL-G0
  - Q4: Release of certified X-CUBE-STL-F7, X-CUBE-STL-H7
  - 2020:
    - X-CUBE-STL-G0
    - X-CUBE-STL-F3
    - X-CUBE-STL-F4
    - X-CUBE-STL-L4
    - X-CUBE-STL-L4+
    - X-CUBE-STL-G0
    - X-CUBE-STL-F7
    - X-CUBE-STL-H7

---
STM8A-SafeASIL
Functional Safety Design Package

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

STM8A

ASIL A/B
Customer Development

Safety documentation
MCU Safety Features
Product Portfolio
ST Quality foundations

ASIL Ready

STM8 Ready

Visit www.st.com/stm8safety
Available on demand at STM8AF part number level.
Ask your local ST contact.

STM8A-SafeASIL
Safety Documentation

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.
ClassB 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

<table>
<thead>
<tr>
<th>Package name</th>
<th>X-CUBE-CLASSB</th>
<th>STM32-CLASSB-SPL</th>
<th>STM8-SafeCLASSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32 Series covered</td>
<td>STM32F0, F1, F3</td>
<td>STM32F0, F1, F3</td>
<td>STM8AF, STM8AL, STM8L, STM8S</td>
</tr>
<tr>
<td></td>
<td>STM32F2, F4, F7</td>
<td>STM32F2 (<em>) , F4 (</em>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STM32L0, L1, L4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-test libraries based on</td>
<td>STM32CubeHAL</td>
<td>STM32 Standard Peripheral Libraries</td>
<td>Optimized direct access to registers</td>
</tr>
<tr>
<td>Supported development environments</td>
<td>IAR™ / Arm® Keil® GCC-based AC6 compilers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certification</td>
<td><strong>UL, 2017</strong></td>
<td><strong>VDE, 2012</strong></td>
<td>(*) Derived packages (not certified)</td>
</tr>
<tr>
<td>IEC 60335-1 and 60730-1 international standards coverage</td>
<td>IEC, UL and CSA</td>
<td>IEC</td>
<td></td>
</tr>
<tr>
<td>Safety manual (guidelines)</td>
<td>AN4435</td>
<td>AN3307</td>
<td>AN3181</td>
</tr>
<tr>
<td>Portability between MCUs</td>
<td>Optimized thanks to STM32Cube</td>
<td>Limited</td>
<td>Limited</td>
</tr>
</tbody>
</table>
Guidelines and examples for STM32 and STM8 users to achieve Class B certification in compliance with IEC 60335-1 and 60730-1.
<table>
<thead>
<tr>
<th>MCU support</th>
<th>Achievable safety standards</th>
<th>Certification</th>
<th>Package content</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32</td>
<td>IEC 61508</td>
<td>IEC, UL, CSA 60335-1 60730-1</td>
<td>• Safety Documentation • Self Test Libraries (X-CUBE-CLASSB)</td>
<td>X-CUBE-CLASSB</td>
</tr>
<tr>
<td>STM32</td>
<td>ISO 26262</td>
<td>IEC 60335-1</td>
<td>• Safety Documentation • Self Test Libraries for STM32 SPL</td>
<td>STM32-CLASSB-SPL</td>
</tr>
<tr>
<td>STM8A</td>
<td>IEC, UL, CSA 60335-1 60730-1</td>
<td></td>
<td>• Safety Documentation • Self Test Libraries</td>
<td>STM8-SafeCLASSB</td>
</tr>
</tbody>
</table>
www.st.com/stm32safety
www.st.com/stm8safety