

---

## Adapting the X-CUBE-STL functional safety package for STM32 (IEC 61508 compliant) to other safety standards

### Introduction

The safety analysis reported in STM32 MCU/MPU safety manuals is executed in accordance with the IEC 61508 safety norm. This document reports the outcome of a change impact analysis with respect to different safety standards. For each new safety standard addressed, the following items are considered:

- Differences in the suggested hardware architecture (architectural categories), and how to map to safety architectures of IEC 61508.
- Differences in the safety integrity level definitions and metrics computation methods, and how to recompute and judge the safety performances of the devices according to the new standard.

The safety standards examined within this change impact analysis are:

- ISO 13849-1:2015, ISO13849-2:2012: Safety of machinery and Safety, related parts of control systems
- IEC 61800-5-2:2016: Adjustable speed electrical power drive systems (related parts Safety requirements, functional).

# 1 About this document

## 1.1 Purpose and scope

The safety analysis reported in STM32 MCU/MPU safety manuals is executed according to the IEC 61508 safety norm.

This document includes the outcome of a change impact analysis with respect to different safety standards, applied to the IEC61508 compliant safety analysis of STM32 MCU/MPU and included in related safety manuals.

This document applies to STM32 MCUs and MPUs Arm®-based devices.

*Note:* Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.



## 1.2 Terms and abbreviations

**Table 1. Terms and abbreviations**

Acronym	Definition
CoU	Conditions of use
CPU	Central processing unit
DC	Diagnostic coverage
FIT	Failure in time
FMEA	Failure mode effect analysis
FMEDA	Failure mode effect diagnostic analysis
ITRS	International technology roadmap for semiconductors
MCU	Microcontroller unit
MPU	Microprocessor unit
SFF	Safe failure fraction
SIL	Safety integrity level

## 1.3 Reference safety standards

[1] ISO 13849-1:2015, ISO13849-2:2012 – Safety of machinery and Safety-related parts of control systems,

[2] IEC 61800-5-2:2016 –Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

[3] IEC61508:1-7© IEC:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems

## 2 ISO 13849-1:2015, ISO 13849-2:2012

ISO 13849-1 is a type B1 standard. It provides a guideline for the development of Safety-related parts of machinery control systems (SRP/CS) including programmable electronics, hardware and software.

### 2.1 ISO 13849 architectural categories

The diagrammatic representation of the typical safety function is reported in ISO 13849-1:2015, [4.4]. Under the assumption that *Compliant item* as defined in related section of MCU Safety Manual is used to implement the block *b* (logic), the equivalence of the ISO 13849 representation with the one in safety manual is evident. The mapping of ISO 13849 architectures with the one indicated in MCU Safety Manual for the definition of the *Compliant item* is therefore possible.

ISO 13849-1:2015 in [Section 2 ISO 13849-1:2015, ISO 13849-2:2012](#) defines in details five different categories. The following table lists for each category the possible implementation by one of the IEC 61508 compliant architectures described in the relevant section of MCU Safety Manual. It is worth to note that for each category, the achievable *PL* is decided by the specific values of diagnostic coverage  $(DC)_{avg}$  and mean time to dangerous failure (MTTFd) (refer to ISO 13849 safety metrics computation for details on computations).

**Table 2. ISO 13849 architectural categories**

ISO13849-1:2015		Link to IEC61508-compliant safety architectures	Notes/constraints
Category	Clause		
B	6.2.3	Possible with 1oo1 architecture	No requirements for <i>MTTFd</i> and $(DC)_{avg}$ are given for category B, anyway it is recommended to follow MCU safety manual recommendation.
1	6.2.4	Not recommended	Category not recommended (see IEC13849-1).
2	6.2.5	Possible with 1oo1 architecture (external WDT is mandatory)	The adoption of external WDT (CPU_SM_5) acting as TE is mandatory. Constraints on $(DC)_{avg}$ and <i>MTTFd</i> can be satisfied but computations are needed. <sup>(1)</sup> Constraints on <i>CCF</i> are satisfied. <sup>(2)</sup>
3	6.2.6	Possible with 1oo2 architecture + DUAL_SM_0	Constraints on $DC_{avg}$ and <i>MTTFd</i> can be satisfied but computations are needed. <sup>(1)</sup> Constraints on <i>CCF</i> are satisfied. <sup>(2)</sup>
4	6.2.7	Possible with 1oo2 architecture + DUAL_SM_0	Implementation of DUAL_SM_0 scheme is mandatory to mitigate fault accumulation. Constraints on $DC_{avg}$ and <i>MTTFd</i> can be satisfied but computations are needed. <sup>(1)</sup> Constraints on <i>CCF</i> are satisfied. <sup>(2)</sup>

1. Computations related to  $DC_{avg}$  and *MTTFd* can involve also other components than device because used in the safety function implementation (sensors, actuators, etc). The figures need therefore to be evaluated at system level.
2. *CCF* additional requirements expressed in ISO13849-1, Annex F table F.1 are basically enforcing the system implementation and therefore outside the scope of the MCU safety manual. It is worth to note that the complete safety analysis resulting as output of the IEC61508 compliance activity (MCU safety manual) helps to claim the score for item #4 in Table F.1.

## 2.2 ISO13849 safety metrics computation

Appendix C of ISO 13849 presents tables of standardized mean time to dangerous failure (MTTFd) for the various electric or electronics components. However, table C.3 in ISO 13849 points to ICs manufacturer's data while attempting to classify MTTFd for programmable ICs. As a consequence, safety analysis results of MCU Safety Manual can be re-mapped in ISO 13849 domain, because even computed for IEC 61508 they are definitely more and more accurate in the definition of dangerous failures identification.

When for a certain component  $PFH \ll 1$ , then it can be assumed that  $MTTFd = 1 / PFH$ .

It is worth to note that according ST methodology, FMEDA data includes failure rate related to transient faults without any assumption about their potential partial safeness. Because of this assumption, PFH values in Device FMEDA leads to very conservative values for computed MTTFd.

In ISO 13849-1 the DC for each single component has the same meaning of the IEC 61508 metric; results of MCU safety manual and related FMEA/FMEDA can therefore be reused. However, this standard defines the concept of  $DC_{avg}$  applicable to the whole SRP/CS in the form of the equation defined in Annex E, formula E.1, where the contribution of each part of the control system is weighted with respect to MTTFd of the various subsystems of the channel. End user is therefore responsible for the computations of the overall  $DC_{avg}$ .

The standard denies any possibility of fault exclusion while calculating  $DC_{avg}$  (ISO13849-2 Tab.D.21 no exclusion allowed), which is also the assumption of Device analysis documented in MCU safety manual..

*Note: Each architectural solution analyzed in STM32 MCU safety manual results in PFH values producing high MTTFd.*

---

## 3 IEC 61800-5-2:2016

---

The scope of this standard is the functional safety of adjustable speed electric drive systems.

### 3.1 IEC 61800 architectural categories

Because IEC 61800 definitions for HFT and for architectures are equivalent to the ones of IEC61508, the remapping is straightforward.

The STM32xx MCU is considered as Type B for the consideration reported in the MCU Safety Manual (refer to the section related to Assumptions).

### 3.2 IEC 61800 safety metrics computation

The PFH of a safety function performed by PDS(SR) is evaluated by the application of IEC 61508-2. The strong link with the norm IEC 61508 is reflected also by the adoption in IEC 61800-5-2 of the same relevant metrics PFH, and SFF. So, results of the MCU safety manual (and related FMEA and FMEDA) can be re-mapped in IEC 61800 domain.

## Revision history

**Table 3. Document revision history**

Date	Version	Changes
12-Oct-2021	1	Initial release.

## Contents

<b>1</b>	<b>About this document</b>	<b>2</b>
1.1	Purpose and scope	2
1.2	Terms and abbreviations	2
1.3	Reference safety standards	2
<b>2</b>	<b>ISO 13849-1:2015, ISO 13849-2:2012</b>	<b>3</b>
2.1	ISO 13849 architectural categories	3
2.2	ISO13849 safety metrics computation	4
<b>3</b>	<b>IEC 61800-5-2:2016</b>	<b>5</b>
3.1	IEC 61800 architectural categories	5
3.2	IEC 61800 safety metrics computation	5
	<b>Revision history</b>	<b>6</b>
	<b>Contents</b>	<b>7</b>
	<b>List of tables</b>	<b>8</b>

## List of tables

<b>Table 1.</b>	Terms and abbreviations . . . . .	2
<b>Table 2.</b>	ISO 13849 architectural categories . . . . .	3
<b>Table 3.</b>	Document revision history . . . . .	6



**IMPORTANT NOTICE – PLEASE READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to [www.st.com/trademarks](http://www.st.com/trademarks). All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2021 STMicroelectronics – All rights reserved