User manual

STM32F7 Series safety manual

Introduction

This document must be read along with the technical documentation such as reference manual(s) and datasheets for the STM32F7 Series microcontroller devices, available on www.st.com.

It describes how to use the devices 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. It also pertains to the X-CUBE-STL software product.

It provides the essential information pertaining to the applicable functional safety standards, which allows system designers to avoid going into unnecessary details.

The document is written in compliance with IEC 61508, and it provides information relative to other functional safety standards.

The safety analysis in this manual takes into account the device variation in terms of memory size, available peripherals, and package.

1 About this document

1.1 Purpose and scope

This document describes how to use Arm® Cortex®-M7 -based STM32F7 Series microcontroller unit (MCU) devices (further also referred to as Device(s)) in the context of a safety-related system, specifying the user's responsibilities for installation and operation, in order to reach the desired safety integrity level.

It is useful to system designers willing to evaluate the safety of their solution embedding one or more *Device(s)*.

For terms used, refer to the glossary at the end of the document.

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

arm

1.2 Normative references

This document is written in compliance with the IEC 61508 international norm for functional safety of electrical, electronic and programmable electronic safety-related systems, version IEC 61508:1-7 © IEC:2010.

The other functional safety standards considered in this manual are:

- ISO 13849-1:2015, ISO13849-2:2012
- IEC 62061:2005+AMD1:2012+AMD2:2015
- IEC 61800-5-2:2016

The following table maps the document content with respect to the IEC 61508-2 Annex D requirements.

Table 1. Document sections versus IEC 61508-2 Annex D safety requirements

Safety requirement	Section number
D2.1 a) a functional specification of the functions capable of being performed	3
D2.1 b) identification of the hardware and/or software configuration of the Compliant item	3.2
D2.1 c) constraints on the use of the *Compliant item* or assumptions on which analysis of the behavior or failure rates of the item are based	3.2
D2.2 a) the failure modes of the *Compliant item* due to random hardware failures, that result in a failure of the function and that are not detected by diagnostics internal to the *Compliant item*;	3.7
D2.2 b) for every failure mode in a), an estimated failure rate;	
D2.2 c) the failure modes of the *Compliant item* due to random hardware failures, that result in a failure of the function and that are detected by diagnostics internal to the *Compliant item*;	
D2.2 d) the failure modes of the diagnostics, internal to the *Compliant item* due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function;	
D2.2 e) for every failure mode in c) and d), the estimated failure rate;	
D2.2 f) for every failure mode in c) that is detected by diagnostics internal to the *Compliant item*, the diagnostic test interval;	3.2.2
D2.2 g) for every failure mode in c) the outputs of the *Compliant item* initiated by the internal diagnostics;	3.6
D2.2 h) any periodic proof test and/or maintenance requirements;	3.7
D2.2 i) for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information must be provided to facilitate the development of an external diagnostics capability.	
D2.2 j) the hardware fault tolerance;	3
D2.2 k) the classification as type A or type B of that part of the *Compliant item* that provides the function (see 7.4.4.1.2 and 7.4.4.1.3);	

1.3 Reference documents

[1] AN5137, Results of FMEA on STM32F7 Series microcontrollers.

[2] AN5132, Results of FMEDA on microcontrollers of the STM32F7 Series.

2 Device development process

STM32 series product development process (see Figure 1), compliant with the IATF 16949 standard, is a set of interrelated activities dedicated to transform customer specification and market or industry domain requirements into a semiconductor device and all its associated elements (package, module, sub-system, hardware, software, and documentation), qualified with ST internal procedures and fitting ST internal or subcontracted manufacturing technologies.

Figure 1. STMicroelectronics product development process

- Key characteristics and requirements related to future uses of the device
- Industry domain(s), specific customer requirements and definition of controls and tests needed for compliance
- Product target specification and strategy
- Project manager appointment to drive product development
- Evaluation of the technologies, design tools and IPs to be used
- Design objective specification and product validation strategy
- Design for quality techniques (DFD, DFT, DFR, DFM, …) definition
- Architecture and positioning to make sure the software and hardware system solutions meet the target specification
- Product approval strategy and project plan

- Semiconductor design development
- Hardware development
- Software development
- Analysis of new product specification to forecast reliability performance
- Reliability plan, reliability design rules, prediction of failure rates for operating life test using Arrhenius's law and other applicable models
- Use of tools and methodologies such as APQP, DFM, DFT, DFMEA
- Detection of potential reliability issues and solution to overcome them
- Assessment of Engineering Samples (ES) to identify the main potential failure mechanisms
- Statistical analysis of electrical parameter drifts for early warning in case of fast parametric degradation (such as retention tests)
- Failure analysis on failed parts to clarify failure modes and mechanisms and identify the root causes
- Physical destructive analysis on good parts after reliability tests when required
- Electrostatic discharge (ESD) and latch-up sensitivity measurement

- Successful completion of the product qualification plan
- Secure product deliveries on advanced technologies using stress methodologies to detect potential weak parts
- Successful completion of electrical characterization
- Global evaluation of new product performance to guarantee reliability of customer manufacturing process and final application of use (mission profile)
- Final disposition for product test, control and monitoring

3 Reference safety architecture

This section reports details of the STM32F7 Series safety architecture.

3.1 Safety architecture introduction

Device(s) analyzed in this document can be used as *Compliant item*(s) within different safety applications.

The aim of this section is to identify such *Compliant item*(s), that is, to define the context of the analysis with respect to a reference concept definition. The concept definition contains reference safety requirements, including design aspects external to the defined *Compliant item*.

As a consequence of *Compliant item* approach, the goal is to list the system-related information considered during the analysis, rather than to provide an exhaustive hazard and risk analysis of the system around the device. Such information includes, among others, application-related assumptions for danger factors, frequency of failures and diagnostic coverage already guaranteed by the application.

3.2 Compliant item

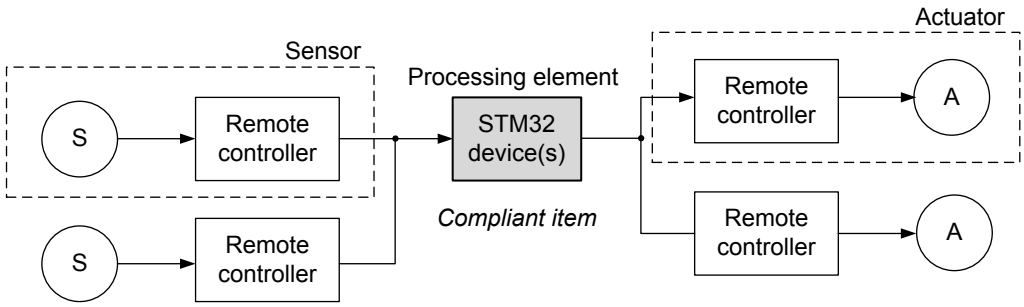
This section defines the *Compliant item* term and provides information on its usage in different safety architecture schemes.

3.2.1 Definition of Compliant item

According to IEC 61508:1 clause 8.2.12, *Compliant item* is any item (for example an element) on which a claim is being made with respect to the clauses of IEC 61508 series. Any mature *Compliant item* must be described in a safety manual available to End user.

In this document, *Compliant item* is defined as a system including one or two STM32 devices (see Figure 2). The communication bus is directly or indirectly connected to sensors and actuators.

Figure 2. STM32 as *Compliant item*



Other components might be related to the *Compliant item*, like the external HW components needed to guarantee either the functionality of the device (external memory, clock quartz and so on) or its safety (for example, the external watchdog or voltage supervisors).

A defined *Compliant item* can be classified as *element* according to IEC61508-4, 3.4.5.

3.2.2 Safety functions performed by Compliant item

In essence, *Compliant item* architecture encompasses the following processes performing the safety function or a part of it:

- input processing elements (PEi) reading safety related data from the remote controller connected to the sensor(s) and transferring them to the following computation elements
- computation processing elements (PEc) performing the algorithm required by the safety function and transferring the results to the following output elements
- output processing elements (PEo) transferring safety related data to the remote controller connected to the actuator

- in 1oo2 architecture, potentially a further voting processing element (PEv)
- the computation processing elements can be involved (to the extent depending to the target safety integrity) in the implementation of local software-based diagnostic functions; this is represented by the block PEd
- processes external to the *Compliant item* ensuring safety integrity, such as watchdog (WDTe) and voltage monitors (VMONe)

The role of the PEv process and WDTe and VMONe external processes is clarified in the sections where the conditions of use (CoU) (definition of safety mechanism) are detailed:

- WDTe: refer to *External watchdog* – CPU_SM_5 and *Control flow monitoring* in *Application software* – CPU_SM_1,
- VMONe: refer to *Supply voltage monitoring* – VSUP_SM_1 and *System-level power supply management* - VSUP_SM_5.

In summary, the devices support the implementation of *End user* safety functions consisting of three operations:

- safe acquisition of safety-related data from input peripheral(s)
- safe execution of application software program and safe computation of related data
- safe transfer of results or decisions to output peripheral(s)

Claims on the *Compliant item* and computation of safety metrics are done with respect to these three basic operations.

According to the definition for implemented safety functions, *Compliant item* (element) can be regarded as type B (as per IEC61508-2, 7.4.4.1.3 definition). Despite accurate, exhaustive and detailed failure analysis, *Device* has to be considered as intrinsically complex. This implies its type B classification.

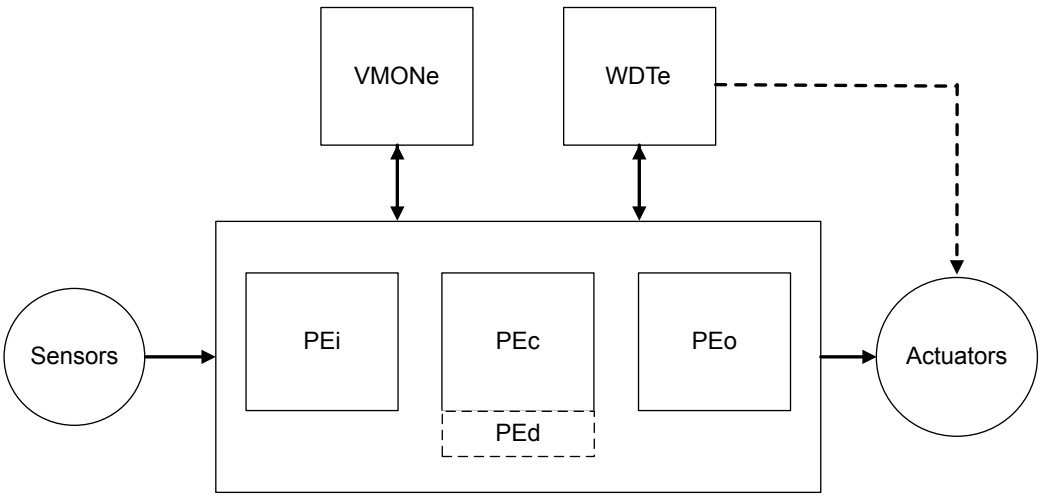
Two main safety architectures are identified: 1oo1 (using one device) and 1oo2 (using two devices).

3.2.3 Reference safety architectures - 1oo1

1oo1 reference architecture (Figure 3) ensures safety integrity of *Compliant item* through combining device internal processes (implemented safety mechanisms) with external processes WDTe and VMONe.

1oo1 reference architecture targets safety integrity level (SIL) *SIL2*.

Figure 3. 1oo1 reference architecture

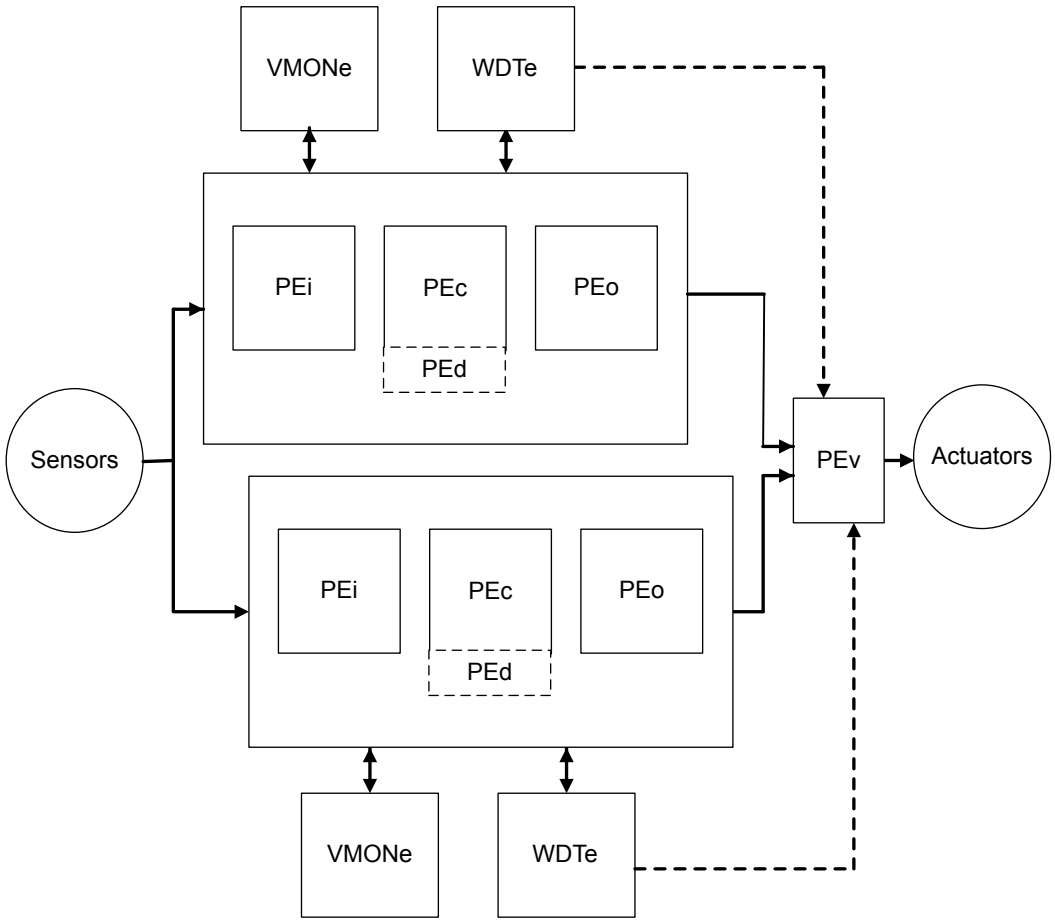


3.2.4 Reference safety architectures - 1oo2

1oo2 reference architecture (Figure 4) contains two separate channels, either implemented as 1oo1 reference architecture ensuring safety integrity of *Compliant item* through combining device internal processes (implemented safety mechanisms) with external processes WDTe and VMONe. The overall safety integrity is then ensured by the external voter PEv, which allows claiming hardware fault tolerance (HFT) equal to 1. Achievement of higher safety integrity levels as per IEC61508-2 Table 3 is therefore possible. Appropriate separation between the two channels (including power supply separation) should be implemented in order to avoid huge impact of common-cause failures (refer to Section 4.2 Analysis of dependent failures). However, β and βD parameters computation is required.

1oo2 reference architecture targets *SIL3*.

Figure 4. 1oo2 reference architecture



3.3 Safety analysis assumptions

This section collects all assumptions made during the safety analysis of the devices.

3.3.1 Safety requirement assumptions

The concept specification, the hazard and risk analysis, the overall safety requirement specification and the consequent allocation determine the requirements for *Compliant item* as further listed. *ASR* stands for assumed safety requirements.

Caution: It is the *End user*'s responsibility to check the compliance of the final application with these assumptions.

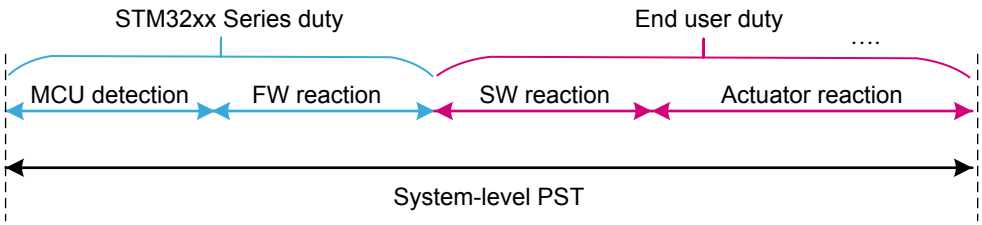
ASR1: *Compliant item* can be used to implement four kinds of safety function modes of operation according to part 4,3.5.16:

- a continuous mode (CM) or high-demand (HD) *SIL3* safety function (*CM3*), or
- a low-demand (LD) *SIL*3 safety function (*LD3*), or
- a *CM* or *HD SIL2* safety function (*CM2*), or
- a *LD SIL2* safety function (*LD2*).

ASR2: *Compliant item* is used to implement safety function(s) allowing a specific worst-case time budget (see note below) for the STM32 *MCU* to detect and react to a failure. That time corresponds to the portion of the process safety time (PST) allocated to the device (*STM32xx Series duty* in Figure 5) in error reaction chain at system level.

Note: The computation for time budget mainly depends on the execution speed for periodic tests implemented by software. Such duration might depends on the actual amount of hardware resources (RAM memory, Flash memory, peripherals) actually declared as safety-related. Further constraints and requirements from IEC61508-2, 7.4.5.3 must be considered.

Figure 5. Allocation and target for STM32 *PST*



ASR3: *Compliant item* is used to implement safety function(s) that can be continuously powered on for a period over eight hours. It is assumed to not require any proof test, and the lifetime of the product is considered to be no less than 10 years.

ASR4: It is assumed that only one safety function is performed or if many, all functions are classified with the same *SIL* and therefore they are not distinguishable in terms of their safety requirements.

ASR5: In case of multiple safety function implementations, it is assumed that *End user* is responsible to duly ensure their mutual independence.

ASR6: It is assumed that there are no *non-safety-related* functions implemented in application software, coexisting with safety functions.

ASR7: It is assumed that the implemented safety function(s) does (do) not depend on transition of the device to and from a low-power state.

ASR8: The local safe state of *Compliant item* is the one in which either:

- SS1: the application software is informed by the presence of a fault and a reaction by the application software itself is possible.
- SS2: the application software cannot be informed by the presence of a fault or the application software is not able to execute a reaction.

Note: End user must take into account that random hardware failures affecting the Device can compromise its operation (for example failure modes affecting the program counter prevent the correct execution of software).

The following table provides details on the SS1 and SS2 safe states.

Table 2. SS1 and SS2 safe state details

Safe state	Condition	*Compliant item* action	System transition to safe state – 1oo1 architecture	System transition to safe state – 1oo2 architecture
SS1	The application software is informed by the presence of a fault and a reaction by the application software itself is possible.	Fault reporting to application software	Application software drives the overall system in its safe state	Application software in one of the two channels drives the overall system in its safe state
SS2	The application software cannot be informed by the presence of a fault or the application software is not able to execute a reaction.	Reset signal issued by WDTe	WDTe drives the overall system in its safe state (“safe shut-down”) (1)	PEv drives the overall system in its safe state

1. *Safe state achievement intended here is compliant to Note on IEC 61508-2, 7.4.8.1*

ASR9: It is assumed that the safe state defined at system level by *End user* is compatible with the assumed local safe state (SS1, SS2) for *Compliant item*.

ASR10: *Compliant item* is assumed to be analyzed according to routes 1H and 1S of IEC 61508-2.

Note: Refer to Section 3.5 Systematic safety integrity and Section 3.6 Hardware and software diagnostics.

ASR11: *Compliant item* is assumed to be regarded as type B, as per IEC 61508:2, 7.4.4.1.2.

ASR12: It is assumed that dual-bank Flash memory mass erase and reprogramming features are used during maintenance state of the final system, and not for the implementation of the safety function.

3.4 Electrical specifications and environment limits

To ensure safety integrity, the user must operate the *Device*(s) within its (their) specified:

- absolute maximum rating
- capacity
- operating conditions

For electrical specifications and environmental limits of *Device*(s), refer to its (their) technical documentation such as datasheet(s) and reference manual(s) available on www.st.com.

3.5 Systematic safety integrity

According to the requirements of IEC 61508 -2, 7.4.2.2, the *Route 1S* is considered in the development of *Device*(s). As clearly authorized by IEC61508-2, 7.4.6.1, STM32 *MCU* products can be considered as standard, mass-produced electronic integrated devices, for which stringent development procedures, rigorous testing and extensive experience of use minimize the likelihood of design faults. However, ST internally assesses the compliance of the *Device* development flow, through techniques and measures suggested in the IEC 61508-2 Annex F. A *safety case database* (see Section 5 List of evidences) keeps evidences of the current compliance level to the norm.

3.6 Hardware and software diagnostics

This section lists all the safety mechanisms (hardware, software and application-level) considered in the device safety analysis. It is expected that users are familiar with the architecture of the device, and that this document is used in conjunction with the related device datasheet, user manual and reference information. To avoid inconsistency and redundancy, this document does not report device functional details. In the following descriptions, the words *safety mechanism*, *method*, and *requirement* are used as synonyms.

As the document provides information relative to the superset of peripherals available on the devices it covers (not all devices have all peripherals), users are supposed to disregard any recommendations not applicable to their *Device* part number of interest.

Information provided for a function or peripheral applies to all instances of such function or peripheral on *Device*. Refer to its reference manual or/and datasheet for related information.

The implementation guidelines reported in the following section are for reference only. The safety verification executed by ST during the device safety analysis and related diagnostic coverage figures reported in this manual (or related documents) are based on such guidelines. For clarity, safety mechanisms are grouped by *Device* function.

Information is organized in form of tables, one per safety mechanism, with the following fields:

SM CODE	Unique safety mechanism code/identifier used also in *FMEA* document. Identifiers use the scheme *mmm_SM_x* where *mmm* is a 3- or 4-letter module (function, peripheral) short name, and *x* is a number. It is possible that the numbering is not sequential (although usually incremental) and/or that the module short name is different from that used in other documents.
Description	Short mnemonic description
Ownership	ST : means that method is available on silicon. *End user*: method must be implemented by *End user* through *Application software* modification, hardware solutions, or both.
Detailed implementation	Detailed implementation sometimes including notes about the safety concept behind the introduction of the safety mechanism.
Error reporting	Describes how the fault detection is reported to application software.
Fault detection time	Time that the safety mechanism needs to detect the hardware failure.
Addressed fault model	Reports fault model(s) addressed by the diagnostic (permanent, transient, or both), and other information: • If ranked for *Fault avoidance*: method contributes to lower the probability of occurrence of a failure • If ranked for *Systematic*: method is conceived to mitigate systematic errors (bugs) in application software design
Dependency on *Device* configuration	Reports if safety mechanism implementation or characteristics change among different *Device* part numbers.
Initialization	Specific operation to be executed to activate the contribution of the safety mechanism
Periodicity	Continuous : safety mechanism is active in continuous mode. Periodic: safety mechanism is executed periodically(1). On-demand: safety mechanism is activated in correspondence to a specified event (for instance, reception of a data message). Startup: safety mechanism is supposed to be executed only at power-up or during off-line maintenance periods.
Test for the diagnostic	Reports specific procedure (if any and recommended) to allow on-line tests of safety mechanism efficiency.
Multiple-fault protection	Reports the safety mechanism(s) associated in order to correctly manage a multiple-fault scenario (refer to Section 4.1.3 Notes on multiple-fault scenario).
Recommendations and known limitations	Additional recommendations or limitations (if any) not reported in other fields.

1. *In CM systems, safety mechanism can be accounted for diagnostic coverage contribution only if it is executed at least once per PST. For LD and HD systems, constraints from IEC61508-2, 7.4.5.3 must be applied.*

3.6.1 Arm® Cortex®-M7 CPU

Table 3. CPU_SM_0

SM CODE	CPU_SM_0
Description	Periodical core self-test software for Arm® Cortex®-M7 *CPU*
Ownership	*End user* or ST
Detailed implementation	The software test is built around well-known techniques already addressed by IEC 61508:7, A.3.2 (Self-test by software: walking bit one-channel). To reach the required values of coverage, the self-test software is specified by means of a detailed analysis of all the *CPU* failure modes and related failure modes distribution
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	None
Periodicity	Periodic
Test for the diagnostic	Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen. The adoption of checksum protection on results variables and defensive programming are recommended.
Multiple-fault protection	CPU_SM_5: external watchdog
Recommendations and known limitations	This method is the main asset in STM32F7 Series safety concept. *CPU* integrity is a key factor because the defined diagnostics for *MCU* peripherals are to major part software-based. Startup execution of this safety mechanism is recommended for multiple fault mitigations - refer to Section 4.1.3 Notes on multiple-fault scenario for details.

Table 4. CPU_SM_1

SM CODE	CPU_SM_1
Description	Control flow monitoring in *Application software*
Ownership	*End user*
Detailed implementation	A significant part of the failure distribution of *CPU* core for permanent faults is related to failure modes directly related to program counter loss of control or hang-up. Due to their intrinsic nature, such failure modes are not addressed by a standard software test method like SM_CPU_0. Therefore it is necessary to implement a run-time control of the *Application software* flow, in order to monitor and detect deviation from the expected behavior due to such faults. Linking this mechanism to watchdog firing assures that severe loss of control (or, in the worst case, a program counter hang-up) is detected. The guidelines for the implementation of the method are the following: • Different internal states of the *Application software* are well documented and described (the use of a dynamic state transition graph is encouraged). • Monitoring of the correctness of each transition between different states of the *Application software* is implemented. • Transition through all expected states during the normal *Application software* program loop is checked. • A function in charge of triggering the system watchdog is implemented in order to constrain the triggering (preventing the issue of *CPU* reset by watchdog) also to the correct execution of the above-described method for program flow monitoring. The use of window feature available on internal window watchdog (WWDG) is recommended.

SM CODE	CPU_SM_1
	• The use of the independent watchdog (IWDG), or an external one, helps to implement a more robust control flow mechanism fed by a different clock source. In any case, safety metrics do not depend on the kind of watchdog in use (the adoption of independent or external watchdog contributes to the mitigation of dependent failures, see Section 4.2.2 Clock)
Error reporting	Depends on implementation
Fault detection time	Depends on implementation. Higher value is fixed by watchdog timeout interval.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	NA
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	-

Table 5. CPU_SM_2

SM CODE	CPU_SM_2
Description	Double computation in *Application software*
Ownership	*End user*
Detailed implementation	A timing redundancy for safety-related computation is considered to detect transient faults affecting the Arm® Cortex®-M7 *CPU* subparts devoted to mathematical computations and data access. The guidelines for the implementation of the method are the following: • The requirement needs be applied only to safety-relevant computation, which in case of wrong result could interfere with the system safety functions. Such computation must be therefore carefully identified in the original *Application software* source code • Both mathematical operation and comparison are intended as computation. • The redundant computation for mathematical computation is implemented by using copies of the original data for second computation, and by using an equivalent formula if possible
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	*End user* is responsible to carefully avoid that the intervention of optimization features of the used compiler removes timing redundancies introduced according to this condition of use.

Table 6. CPU_SM_3

SM CODE	CPU_SM_3
Description	Arm® Cortex®-M7 HardFault exceptions

SM CODE	CPU_SM_3
Ownership	ST
Detailed implementation	HardFault exception raise is an intrinsic safety mechanism implemented in Arm® Cortex®-M7 core, mainly dedicated to intercept systematic faults due to software limitations or error in software design (causing for example execution of undefined operations, unaligned address access). This safety mechanism is also able to detect hardware random faults inside the *CPU* bringing to such described abnormal operations.
Error reporting	High-priority interrupt event
Fault detection time	Depends on implementation. Refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	None
Periodicity	Continuous
Test for the diagnostic	It is possible to write a test procedure to verify the generation of the HardFault exception; anyway, given the expected minor contribution in terms of hardware random-failure detection, such implementation is not recommended.
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Enabling related interrupt generation on the detection of errors is highly recommended.

Table 7. CPU_SM_4

SM CODE	CPU_SM_4
Description	Stack hardening for *Application software*
Ownership	*End user*
Detailed implementation	The stack hardening method is required to address faults (mainly transient) affecting *CPU* register bank. This method is based on source code modification, introducing information redundancy in register-passed information to called functions. The guidelines for the implementation of the method are the following: • To pass also a redundant copy of the passed parameters values (possibly inverted) and to execute a coherence check in the function. • To pass also a redundant copy of the passed pointers and to execute a coherence check in the function. • For parameters that are not protected by redundancy, to implement defensive programming techniques (plausibility check of passed values). For example enumerated fields are to be checked for consistency.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	This method partially overlaps with defensive programming techniques required by IEC61508 for software development. Therefore in presence of *Application software* qualified for safety integrity greater or equal to SC2, optimizations are possible.

Table 8. CPU_SM_5

SM CODE	CPU_SM_5
Description	External watchdog
Ownership	*End user*
Detailed implementation	Using an external watchdog linked to control flow monitoring method (refer to CPU_SM_1) addresses failure mode of program counter or control structures of *CPU*. External watchdog can be designed to be able to generate the combination of signals needed on the final system to achieve the safe state. It is recommended to carefully check the assumed requirements about system safe state reported in Section 3.3.1 Safety requirement assumptions. It also contributes to dramatically reduce potential common cause failures, because the external watchdog is clocked and supplied independently of *Device*.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation (watchdog timeout interval)
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	To be defined at system level (outside the scope of *Compliant item* analysis)
Multiple-fault protection	CPU_SM_1: control flow monitoring in *Application software*
Recommendations and known limitations	In case of usage of windowed watchdog, *End user* must consider possible tolerance in *Application software* execution, to avoid false error reports (affecting system availability). It is worth to note that the use of an external watchdog could be needed anyway when the *Device* is used to trigger final elements, in order to comply at system level with requirements from IEC61508-2:2010 Table A.1/Table A.14.

Table 9. CPU_SM_6

SM CODE	CPU_SM_6
Description	Independent watchdog
Ownership	ST
Detailed implementation	Using the IDWG watchdog linked to control flow monitoring method (refer to CPU_SM_1) addresses failure mode of program counter or control structures of *CPU*.
Error reporting	Reset signal generation
Fault detection time	Depends on implementation (watchdog timeout interval)
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	IWDG activation. It is recommended to use *hardware watchdog* in Option byte settings (IWDG is automatically enabled after reset)
Periodicity	Continuous
Test for the diagnostic	WDG_SM_1: Software test for watchdog at startup
Multiple-fault protection	CPU_SM_1: control flow monitoring in *Application software* WDG_SM_0: periodical read-back of configuration registers
Recommendations and known limitations	The IWDG intervention is able to achieve a potentially “incomplete” local safe state because it can only guarantee that *CPU* is reset. No guarantee that *Application software* can be still executed to generate combinations of output signals that might be needed by the external system to achieve the final safe state. If this limitation turn out in a blocking point, *End user* must adopt CPU_SM_5

Table 10. CPU_SM_7

SM CODE	CPU_SM_7
Description	Memory protection unit (*MPU*)
Ownership	ST
Detailed implementation	The *CPU* memory protection unit is able to detect illegal access to protected memory areas, according to criteria set by *End user*.
Error reporting	Exception raise (MemManage)
Fault detection time	Refer to functional documentation
Addressed fault model	Systematic (software errors) Permanent and transient (only program counter and memory access failures)
Dependency on *Device* configuration	None
Initialization	*MPU* registers must be programmed at start-up
Periodicity	On line
Test for the diagnostic	Not needed
Multiple-fault protection	MPU_SM_0: Periodical read-back of configuration registers
Recommendations and known limitations	The use of memory partitioning and protection by *MPU* functions is highly recommended when multiple safety functions are implemented in *Application software*. The *MPU* can be indeed used to • enforce privilege rules • separate processes • enforce access rules Hardware random-failure detection capability for *MPU* is restricted to well-selected failure modes, mainly affecting program counter and memory access *CPU* functions. The associated diagnostic coverage is therefore not expected to be relevant for the safety concept of *Device*. Enabling related interrupt generation on the detection of errors is highly recommended.

Table 11. CPU_SM_9

SM CODE	CPU_SM_9
Description	Periodical self-test software for Arm® Cortex® -M7 caches
Ownership	*End user* or ST
Detailed implementation	The software test is built around well-known techniques already addressed by IEC61508:7, A.3.2 (Self-test by software: walking bit one-channel). The scope of the software test are failure modes affecting Arm® Cortex® -M7 L1 caches structures (including caches RAMs). Because failure modes of caches control logic and caches memory arrays are separated and different, this test could be implemented in a separate way for those two different structures. The achieved diagnostic coverage strongly depends on the complexity of the test implementation, and on the percentage of caches failure modes addressed.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	N/A
Multiple faults protection	CPU_SM_5 : external watchdog

SM CODE	CPU_SM_9
Recommendations and known limitations	End user waiver of cache features, disabling it by software, leads to following benefits in STM32F7 Series safety concept: • No need to implement this method (CPU_SM_9) • Decrease of Arm® Cortex® -M7 overall failure rate

Table 12. MPU_SM_0

SM CODE	MPU_SM_0
Description	Periodical read-back of *MPU* configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to *MPU* configuration registers (also unused by the *End user Application software*). Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

3.6.2 Embedded Flash memory

Table 13. FLASH_SM_0

SM CODE	FLASH_SM_0
Description	Periodical software test for Flash memory
Ownership	*End user* or ST
Detailed implementation	Permanent faults affecting the system Flash memory, memory cells and address decoder, are addressed through a dedicated software test that checks the memory cell contents versus the expected value, using signature-based techniques. According to IEC 61508:2 Table A.5, the effective diagnostic coverage of such techniques depends on the width of the signature in relation to the block length of the information to be protected - therefore the signature computation method is to be carefully selected. Note that the simple signature method (IEC 61508:7 - A.4.2 Modified checksum) is inadequate as it only achieves a low value of coverage. The information block does not need to be addressed with this test as it is not used during normal operation (no data nor program fetch).
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	Flash memory size changes according part number
Initialization	Memory signatures must be stored in Flash memory as well
Periodicity	Periodic

SM CODE	FLASH_SM_0
Test for the diagnostic	Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen
Multiple-fault protection	CPU_SM_1: control flow monitoring in application software CPU_SM_0: periodical core self-test software
Recommendations and known limitations	This test is expected to have a relevant time duration – test integration must therefore consider the impact on application software execution. The use of internal cyclic redundancy check (CRC) module is recommended. In principle direct memory access (DMA) feature for data transfer can be used. Unused Flash memory sections can be excluded from testing. Startup execution of this safety mechanism is recommended for multiple fault mitigations - refer to Section 4.1.3 Notes on multiple-fault scenario for details.

Table 14. FLASH_SM_1

SM CODE	FLASH_SM_1
Description	Control flow monitoring in application software
Ownership	*End user*
Detailed implementation	Permanent and transient faults affecting the system Flash memory, memory cells and address decoder, can interfere with the access operation by the *CPU*, leading to wrong data or instruction fetches. Such failures can be detected by control flow monitoring techniques implemented in the application software loaded from Flash memory. For more details on the implementation, refer to description CPU_SM_1.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation. Higher value is fixed by watchdog timeout interval.
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	NA
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	CPU_SM_1 correct implementation supersedes this requirement.

Table 15. FLASH_SM_2

SM CODE	FLASH_SM_2
Description	Arm® Cortex®-M7 HardFault exceptions
Ownership	ST
Detailed implementation	Hardware random faults (both permanent and transient) affecting system Flash memory (memory cells, address decoder) can lead to wrong instruction codes fetches, and eventually to the intervention of the Arm® Cortex®-M7 HardFault exceptions. Refer to CPU_SM_3 for detailed description.
Error reporting	Refer to CPU_SM_3
Fault detection time	Refer to CPU_SM_3
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None

SM CODE	FLASH_SM_2
Initialization	Refer to CPU_SM_3
Periodicity	Continuous
Test for the diagnostic	Refer to CPU_SM_3
Multiple-fault protection	Refer to CPU_SM_3
Recommendations and known limitations	Refer to CPU_SM_3

Table 16. FLASH_SM_3

SM CODE	FLASH_SM_3
Description	Option byte write protection
Ownership	ST
Detailed implementation	This safety mechanism prevents unintended writes on the option byte. The use of this method is encouraged to enhance end application robustness for systematic faults.
Error reporting	Write protection exception
Fault detection time	Not applicable
Addressed fault model	None (Systematic only)
Dependency on *Device* configuration	None
Initialization	Not needed (enabled by default)
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	This method addresses systematic faults in software application and it have zero efficiency in addressing hardware random faults affecting the option byte value during running time. No DC value is therefore associated.

Table 17. FLASH_SM_4

SM CODE	FLASH_SM_4
Description	Static data encapsulation
Ownership	*End user*
Detailed implementation	If static data are stored in Flash memory, encapsulation by a checksum field with encoding capability (such as *CRC*) must be implemented. Checksum validity is checked by application software before static data consuming.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	None

Table 18. **FLASH_SM_6**

SM CODE	FLASH_SM_6
Description	Flash memory unused area filling code
Ownership	*End user*
Detailed implementation	Used Flash memory area must be filled with deterministic data. This way in case that the program counter jumps outside the application program area due to a transient fault affecting *CPU*, the system evolves in a deterministic way.
Error reporting	NA
Fault detection time	NA
Addressed fault model	None (Fault avoidance)
Dependency on *Device* configuration	None
Initialization	NA
Periodicity	NA
Test for the diagnostic	NA
Multiple-fault protection	NA
Recommendations and known limitations	Filling code can be made of NOP instructions, or an illegal code that leads to a HardFault exception raise.

Table 19. **FLASH_SM_8**

SM CODE	FLASH_SM_8
Description	Read protection (RDP), Write protection (WRP), Proprietary code readout protection (PCROP)
Ownership	ST
Detailed implementation	Flash memory can be protected against illegal reads or erase/write by using these protection features. The combination of these techniques and the related different protection level allows *End user* to build an effective access protection policy.
Error reporting	Refer to functional documentation - in some cases an HardFault error is generated
Fault detection time	Refer to functional documentation
Addressed fault model	Systematic
Dependency on *Device* configuration	None
Initialization	Not needed
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	Not needed
Recommendations and known limitations	Hardware random-failure detection capability for Flash memory access policy is restricted to well-selected marginal failure modes, mainly affecting program counter and Flash memory interface functions. The associated diagnostic coverage is therefore expected to be not relevant in the framework of STM32F7 Series safety concept.

3.6.3 Embedded SRAM

Table 20. **RAM_SM_0**

SM CODE	RAM_SM_0
Description	Periodical software test for static random access memory (SRAM or RAM)
Ownership	End user or ST

SM CODE	RAM_SM_0
Detailed implementation	To enhance the coverage on SRAM data cells and to ensure adequate coverage for permanent faults affecting the address decoder it is required to execute a periodical software test on the system RAM memory. The selection of the algorithm must ensure the target SFF coverage for both the RAM cells and the address decoder. Evidences of the effectiveness of the coverage of the selected method must be also collected
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	RAM size can change according to the part number
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Usage of a March test C- is recommended. Because the nature of this test can be destructive, RAM contents restore must be implemented. Possible interferences with interrupt-serving routines fired during test execution must be also considered (such routines can access to RAM invalid contents). Note: unused RAM section can be excluded by the testing, under end user responsibility on actual RAM usage by final application software. Startup execution of this safety mechanism is recommended for multiple fault mitigations - refer to Section 4.1.3 Notes on multiple-fault scenario for details.

Table 21. RAM_SM_2

SM CODE	RAM_SM_2
Description	Stack hardening for application software
Ownership	End user
Detailed implementation	The stack hardening method is used to enhance the application software robustness to SRAM faults that affect the address decoder. The method is based on source code modification, introducing information redundancy in the stack-passed information to the called functions. Method contribution is relevant in case the combination between the final application software structure and the compiler settings requires a significant use of the stack for passing function parameters. Implementation is the same as method CPU_SM_4
Error reporting	Refer to CPU_SM_4
Fault detection time	Refer to CPU_SM_4
Addressed fault model	Refer to CPU_SM_4
Dependency on *Device* configuration	Refer to CPU_SM_4
Initialization	Refer to CPU_SM_4
Periodicity	Refer to CPU_SM_4
Test for the diagnostic	Refer to CPU_SM_4
Multiple-fault protection	Refer to CPU_SM_4
Recommendations and known limitations	Refer to CPU_SM_4

Table 22. RAM_SM_3

SM CODE	RAM_SM_3
Description	Information redundancy for safety-related variables in application software
Ownership	End user
Detailed implementation	To address transient faults affecting SRAM controller, it is required to implement information redundancy on the safety-related system variables stored in the RAM. The guidelines for the implementation of this method are the following: • The system variables that are safety-related (in the sense that a wrong value due to a failure in reading on the RAM affects the safety functions) are well-identified and documented. • The arithmetic computation or decision based on such variables are executed twice and the two final results are compared. • Safety-related variables are stored and updated in two redundant locations, and comparison is checked before consuming data. • Enumerated fields must use non-trivial values, checked for coherence at least one time per *PST* • Data vectors stored in SRAM must be protected by a encoding checksum (such as *CRC*)
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Implementation of this safety method shows a partial overlap with an already foreseen method for Arm® Cortex®-M7 (CPU_SM_1); optimizations in implementing both methods are therefore possible

Table 23. RAM_SM_4

SM CODE	RAM_SM_4
Description	Control flow monitoring in application software
Ownership	End user
Detailed implementation	In case the end user application software is executed from SRAM, permanent and transient faults affecting the memory (cells and address decoder) can interfere with the program execution. To address such failures it is needed to implement this method. For more details on the implementation, refer to description CPU_SM_1
Error reporting	Depends on implementation
Fault detection time	Depends on implementation. Higher value is fixed by watchdog timeout interval.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	NA

SM CODE	RAM_SM_4
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Needed just in case of application software execution from SRAM. CPU_SM_1 correct implementation supersedes this requirement

Table 24. RAM_SM_5

SM CODE	RAM_SM_5
Description	Periodical integrity test for application software in RAM
Ownership	End user
Detailed implementation	In case application software or diagnostic libraries are executed in RAM, it is needed to protect the integrity of the code itself against soft-error corruptions and related code mutations. This method must check the integrity of the stored code by checksum computation techniques, on a periodic basis (at least once per *PST*). For implementation details refer to similar method FLASH_SM_0
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen.
Multiple-fault protection	CPU_SM_0: periodical core self test software CPU_SM_1: control flow monitoring in application software
Recommendations and known limitations	This method must be implemented only in case of application software or diagnostic libraries are executed from RAM

Table 25. RAM_SM_6

SM CODE	RAM_SM_6
Description	Read protection (RDP), Write protection (WRP)
Ownership	ST
Detailed implementation	SRAM2 memory can be protected against illegal reads or erase/write by using these protection features. The combination of these techniques and the related different protection level allows End user to build an effective access protection policy
Error reporting	Refer to functional documentation - in some cases an HardFault error is generated
Fault detection time	Refer to functional documentation
Addressed fault model	Systematic
Dependency on *Device* configuration	SRAM2 size can vary depending on part number
Initialization	Not needed
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	Not needed

SM CODE	RAM_SM_6
Recommendations and known limitations	Hardware random-failure detection capability for SRAM2 access policy is restricted to well-selected marginal failure modes, mainly affecting program counter and SRAM2 interface functions. The associated diagnostic coverage is therefore expected to be irrelevant in the framework of STM32F7 Series safety concept.

3.6.4 System bus architecture/peripherals interconnect matrix

Table 26. BUS_SM_0

SM CODE	BUS_SM_0
Description	Periodical software test for interconnections
Ownership	*End user*
Detailed implementation	The intra-chip connection resources (Bus Matrix, AHB or APB bridges) needs to be periodically tested for permanent faults detection. Note that STM32F7 Series devices have no hardware safety mechanism to protect these structures. The test executes a connectivity test of these shared resources, including the testing of the arbitration mechanisms between peripherals. According to IEC 61508:2 Table A.8, A.7.4 the method is considered able to achieve high levels of coverage
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Implementation can be considered in large part as overlapping with the widely used *Periodical read-back of configuration registers* required for several peripherals

Table 27. BUS_SM_1

SM CODE	BUS_SM_1
Description	Information redundancy in intra-chip data exchanges
Ownership	*End user*
Detailed implementation	This method requires to add some kind of redundancy (for example a *CRC* checksum at packet level) to each data message exchanged inside *Device*. Message integrity is verified using the checksum by the application software, before consuming data.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software

SM CODE	BUS_SM_1
Recommendations and known limitations	Implementation can be in large part overlapping with other safety mechanisms requiring information redundancy on data messages for communication peripherals. Optimizations are therefore possible.

Table 28. LOCK_SM_0

SM CODE	LOCK_SM_0
Description	Lock mechanism for configuration options
Ownership	ST
Detailed implementation	The STM32F7 Series devices feature spread protection to prevent unintended configuration changes for some peripherals and system registers (for example PVD_LOCK, timers); the spread protection detects systematic faults in software application. The use of this method is encouraged to enhance the end application robustness to systematic faults.
Error reporting	Not generated (when locked, register overwrites are just ignored)
Fault detection time	NA
Addressed fault model	None (Systematic only)
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	Not needed
Recommendations and known limitations	No DC associated because this test addresses systematic faults

3.6.5 EXTI controller

Table 29. NVIC_SM_0

SM CODE	NVIC_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This test is implemented by executing a periodical check of the configuration registers for a system peripheral against its expected value. Expected values are previously stored in RAM and adequately updated after each configuration change. The method mainly addresses transient faults affecting the configuration registers, by detecting bit flips in the registers contents. It addresses also permanent faults on registers because it is executed at least one time within *PST* after a peripheral update. Method must be implemented to any configuration register whose contents are able to interfere with NVIC or EXTI behavior in case of incorrect settings. Check includes NVIC vector table. According to the state-of-the-art automotive safety standard ISO26262, this method can achieve high levels of diagnostic coverage (DC) (refer to ISO26262:5, Table D.4) An alternative valid implementation requiring less space in SRAM can be realized on the basis of signature concept: • Peripheral registers to be checked are read in a row, computing a *CRC* checksum (use of hardware *CRC* is encouraged) • Obtained signature is compared with the golden value (computed in the same way after each register update, and stored in SRAM) • Coherence between signatures is checked by the application software – signature mismatch is considered as failure detection
Error reporting	Depends on implementation

SM CODE	NVIC_SM_0
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Values of configuration registers must be read after the boot before executing the first check
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	This method addresses only failures affecting configuration registers, and not peripheral core logic or external interface. Attention must be paid to registers containing mixed combination of configuration and status bits. Mask must be used before saving register contents affecting signature, and related checks, to avoid false positive detections.

Table 30. NVIC_SM_1

SM CODE	NVIC_SM_1
Description	Expected and unexpected interrupt check
Ownership	*End user*
Detailed implementation	According to IEC 61508:2 Table A.1 recommendations, a diagnostic measure for continuous, absence or cross-over of interrupt must be implemented. The method of expected and unexpected interrupt check is implemented at application software level. The guidelines for the implementation of the method are the following: • The interrupts implemented on the *MCU* are well documented, also reporting, when possible, the expected frequency of each request (for example, the interrupts related to ADC conversion completion that come on a regular basis). • Individual counters are maintained for each interrupt request served, in order to detect in a given time frame the cases of a) no interrupt at all b) too many interrupt requests (“babbling idiot” interrupt source). The control of the time frame duration must be regulated according to the individual interrupt expected frequency. • Interrupt vectors related to unused interrupt source point to a default handler that reports, in case of triggering, a faulty condition (unexpected interrupt). • In case an interrupt service routine is shared between different sources, a plausibility check on the caller identity is implemented. • Interrupt requests related to non-safety-related peripherals are handled with the same method here described, despite their originator safety classification
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	In order to decrease the complexity of method implementation, it is suggested to use polling technique (when possible) instead of interrupt for end system implementation

3.6.6 Direct memory access controller (DMA/ DMAMUX)

Table 31. DMA_SM_0

SM CODE	DMA_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to *DMA* configuration register and channel addresses register as well. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 32. DMA_SM_1

SM CODE	DMA_SM_1
Description	Information redundancy on data packet transferred via *DMA*
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by *DMA* a redundancy check (such as *CRC* check, or similar one) with encoding capability. Full data packet redundancy would be overkilling. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet Consistency of data packet must be checked by the application software before consuming data
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	To give an example about checksum encoding capability, using just a bit-by-bit addition is unappropriated

Table 33. DMA_SM_2

SM CODE	DMA_SM_2
Description	Information redundancy by including sender or receiver identifier on data packet transferred via *DMA*
Ownership	*End user*
Detailed implementation	This method helps to identify inside the MCU the source and the originator of the message exchanged by *DMA*. Implementation is realized by adding an additional field to protected message, with a coding convention for message type identification fixed at *Device* level. Guidelines for the identification fields are: • Identification field value must be different for each possible couple of sender or receiver on *DMA* transactions • Values chosen must be enumerated and non-trivial • Coherence between the identification field value and the message type is checked by application software before consuming data. This method, when implemented in combination with DMA_SM_4, makes available a kind of “virtual channel” between source and destinations entities.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	None

Table 34. DMA_SM_3

SM CODE	DMA_SM_3
Description	Periodical software test for *DMA*
Ownership	*End user*
Detailed implementation	This method requires the periodical testing of the DMA basic functionality, implemented through a deterministic transfer of a data packet from one source to another (for example from memory to memory) and the checking of the correct transfer of the message on the target. Data packets are composed by non-trivial patterns (avoid the use of 0x0000, 0xFFFF values) and organized in order to allow the detection during the check of the following failures: • incomplete packed transfer • errors in single transferred word • wrong order in packed transmitted data
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software

SM CODE	DMA_SM_3
Recommendations and known limitations	None

Table 35. DMA_SM_4

SM CODE	DMA_SM_4
Description	*DMA* transaction awareness
Ownership	*End user*
Detailed implementation	DMA transactions are non-deterministic by nature, because typically driven by external events like communication messages reception. Anyway, well-designed safety systems should keep much control as possible of events – refer for instance to IEC61508:3 Table 2 item 13 requirements for software architecture. This method is based on system knowledge of frequency and type of expected *DMA* transaction. For instance, an externally connected sensor supposed to send periodically some messages to a STM32 peripheral. Monitoring *DMA* transaction by a dedicated state machine allows to detect missing or unexpected *DMA* activities.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Because *DMA* transaction termination is often linked to an interrupt generation, implementation of this method can be merged with the safety mechanism NVIC_SM_1: expected and unexpected interrupt check.

3.6.7 Controller area network (bxCAN)

Table 36. CAN_SM_0

SM CODE	CAN_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to CAN configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 37. **CAN_SM_1**

SM CODE	CAN_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	CAN communication module embeds protocol error checks (like error counters) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself. Error signals connected to these checkers are normally handled in a standard communication software, so the overhead is reduced
Error reporting	Several error condition are reported by flag bits in related CAN registers.
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	NA
Multiple faults protection	CAN_SM_2: Information redundancy techniques on messages, including end-to-end protection
Recommendations and known limitations	Enabling related interrupt generation on the detection of errors is highly recommended.

Table 38. **CAN_SM_2**

SM CODE	CAN_SM_2
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*
Detailed implementation	This method aims to protect the communication between a peripheral and his external counterpart establishing a kind of “protected” channel. The aim is to specifically address communication failure modes as reported in IEC61508:2, 7.4.11.1. Implementation guidelines are the following: • Data packet must be protected (encapsulated) by an information redundancy check, like for instance a CRC checksum computed over the packet and added to payload. Checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. • Additional field added in payload reporting an unique identification of sender or receiver and an unique increasing sequence packet number • Timing monitoring of the message exchange (for example check the message arrival within the expected time window), detecting therefore missed message arrival conditions • Application software must verify before consuming data packet its consistency (CRC check), its legitimacy (sender or receiver) and the sequence correctness (sequence number check, no packets lost)
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Important note: it is assumed that the remote CAN counterpart has an equivalent capability of performing the checks described. A major overlap between the requirements of this method and the implementation of complex communication software protocols can exists. Due to large adoption of these protocols in industrial applications, optimizations can be possible

3.6.8 Universal synchronous/asynchronous and low-power universal asynchronous receiver/ transmitter (USART and LPUART)

Table 39. **UART_SM_0**

SM CODE	UART_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to UART configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0

SM CODE	UART_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 40. UART_SM_1

SM CODE	UART_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	USART communication module embeds protocol error checks (like additional parity bit check, overrun, frame error) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself. Error signals connected to these checkers are normally handled in a standard communication software, so the overhead is reduced.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not required
Multiple-fault protection	UART_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	USART communication module is fitted by several different configurations – the actual composition of communication error checks depends on selected configuration. Enabling related interrupt generation on the detection of errors is highly recommended.

Table 41. UART_SM_2

SM CODE	UART_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by UART a redundancy check (like a *CRC* check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation

SM CODE	UART_SM_2
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	It is assumed that the remote UART counterpart has an equivalent capability of performing the check described. Transmission full redundancy (message repetition) should not be used because its detection capability is limited to a subset of communication unit failure modes. To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated.

Table 42. UART_SM_3

SM CODE	UART_SM_3
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*
Detailed implementation	This method aims to protect the communication between a peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information.
Error reporting	Refer to CAN_SM_2
Fault detection time	Refer to CAN_SM_2
Addressed fault model	Refer to CAN_SM_2
Dependency on *Device* configuration	Refer to CAN_SM_2
Initialization	Refer to CAN_SM_2
Periodicity	Refer to CAN_SM_2
Test for the diagnostic	Refer to CAN_SM_2
Multiple-fault protection	Refer to CAN_SM_2
Recommendations and known limitations	Important note: it is assumed that the remote UART counterpart has an equivalent capability of performing the checks described. Refer to CAN_SM_2 for further notice.

3.6.9 Inter-integrated circuit (I2C)

Table 43. IIC_SM_0

SM CODE	IIC_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to I2C configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0

SM CODE	IIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 44. IIC_SM_1

SM CODE	IIC_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	I2C communication module embeds protocol error checks (like overrun, underrun, packet error etc.) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	IIC_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	Adoption of SMBus option grants the activation of more efficient protocol-level hardware checks such as CRC-8 packet protection. Enabling related interrupt generation on the detection of errors is highly recommended.

Table 45. IIC_SM_2

SM CODE	IIC_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by I2C a redundancy check (such as a *CRC* check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed

SM CODE	IIC_SM_2
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	It is assumed that the remote I2C counterpart has an equivalent capability of performing the check described. Transmission full redundancy (message repetition) should not be used because its detection capability is limited to a subset of communication unit failure modes. To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated. This method is overlapped with IIC_SM_3 if hardware handled *CRC* insertion is possible.

Table 46. IIC_SM_3

SM CODE	IIC_SM_3
Description	*CRC* packet-level
Ownership	ST
Detailed implementation	I2C communication module allows to activate for specific mode of operation (SMBus) the automatic insertion (and check) of *CRC* checksums to packet data.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	IIC_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	This method can be part of the implementation for IIC_SM_2 Enabling related interrupt generation on the detection of errors is highly recommended.

Table 47. IIC_SM_4

SM CODE	IIC_SM_4
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*
Detailed implementation	This method aims to protect the communication between a I2C peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information.
Error reporting	Refer to CAN_SM_2
Fault detection time	Refer to CAN_SM_2
Addressed fault model	Refer to CAN_SM_2
Dependency on *Device* configuration	Refer to CAN_SM_2
Initialization	Refer to CAN_SM_2
Periodicity	Refer to CAN_SM_2
Test for the diagnostic	Refer to CAN_SM_2
Multiple-fault protection	Refer to CAN_SM_2

SM CODE	IIC_SM_4
Recommendations and known limitations	Important note: it is assumed that the remote I2C counterpart has an equivalent capability of performing the checks described. Refer to CAN_SM_2 for further notice.

3.6.10 Serial peripheral interface (SPI)

Table 48. SPI_SM_0

SM CODE	SPI_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to SPI configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 49. SPI_SM_1

SM CODE	SPI_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	SPI communication module embeds protocol error checks (like overrun, underrun, timeout and so on) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself.
Error reporting	Error flag raise and optional interrupt event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	NA
Multiple-fault protection	SPI_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	Enabling related interrupt generation on the detection of errors is highly recommended.

Table 50. **SPI_SM_2**

SM CODE	SPI_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by SPI a redundancy check (such as a *CRC* check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	It is assumed that the remote SPI counterpart has an equivalent capability of performing the check described. Transmission full redundancy (message repetition) should not be used because its detection capability is limited to a subset of communication unit failure modes. To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated. This method is overlapped with SSP_SM_3 if hardware handled *CRC* insertion is possible.

Table 51. **SPI_SM_3**

SM CODE	SPI_SM_3
Description	*CRC* packet-level
Ownership	ST
Detailed implementation	SPI communication module allows to activate automatic insertion (and check) of CRC-8 or CRC-18 checksums to packet data.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	SPI_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	This method can be part of the implementation for SPI_SM_2 Enabling related interrupt generation on the detection of errors is highly recommended.

Table 52. **SPI_SM_4**

SM CODE	SPI_SM_4
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*
Detailed implementation	This method aims to protect the communication between SPI peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information.
Error reporting	Refer to CAN_SM_2
Fault detection time	Refer to CAN_SM_2
Addressed fault model	Refer to CAN_SM_2
Dependency on *Device* configuration	Refer to CAN_SM_2
Initialization	Refer to CAN_SM_2
Periodicity	Refer to CAN_SM_2
Test for the diagnostic	Refer to CAN_SM_2
Multiple-fault protection	Refer to CAN_SM_2
Recommendations and known limitations	Important note: it is assumed that the remote SPI counterpart has an equivalent capability of performing the checks described. Refer to CAN_SM_2 for further notice.

3.6.11 USB on-the-go full-speed (OTG_FS)

Table 53. **USB_SM_0**

SM CODE	USB_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to USB configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 54. USB_SM_1

SM CODE	USB_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	USB communication module embeds protocol error checks (like overrun, underrun, NRZI, bit stuffing etc.) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	USB_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	Enabling related interrupt generation on the detection of errors is highly recommended.

Table 55. USB_SM_2

SM CODE	USB_SM_2
Description	Information redundancy techniques on messages
Ownership	ST or *End user*
Detailed implementation	The implementation of required information redundancy on messages, USB communication module is fitted by hardware capability. It basically allows to activate the automatic insertion (and check) of CRC checksums to packet data.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Error reporting configuration, if interrupt events are planned
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	USB_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	None

Table 56. **USB_SM_3**

SM CODE	USB_SM_3
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*
Detailed implementation	This method aims to protect the communication between an USB peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information
Error reporting	Refer to CAN_SM_2
Fault detection time	Refer to CAN_SM_2
Addressed fault model	Refer to CAN_SM_2
Dependency on *Device* configuration	Refer to CAN_SM_2
Initialization	Refer to CAN_SM_2
Periodicity	Refer to CAN_SM_2
Test for the diagnostic	Refer to CAN_SM_2
Multiple faults protection	Refer to CAN_SM_2
Recommendations and known limitations	This method apply in case USB bulk or isochronous transfers are used. For other transfers modes the USB hardware protocol already implements several features of this requirement. Refer to CAN_SM_2 for further notice

3.6.12 Analog-to-digital converters (ADC)

Table 57. **ADC_SM_0**

SM CODE	ADC_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to ADC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 58. **ADC_SM_1**

SM CODE	ADC_SM_1
Description	Multiple acquisition by application software
Ownership	*End user*
Detailed implementation	This method implements a timing information redundancy by executing multiple acquisitions on the same input signal. Multiple acquisition data are then combined by a filter algorithm to determine the signal correct value
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	It is highly probable that this recommendation is satisfied by design by the end user application software. Usage of multiple acquisitions followed by average operations is a common technique in industrial applications where it is needed to survive with spurious EMI disturbs on sensor lines

Table 59. **ADC_SM_2**

SM CODE	ADC_SM_2
Description	Range check by application software
Ownership	*End user*
Detailed implementation	The guidelines for the implementation of the method are the following: • The expected range of the data to be acquired are investigated and adequately documented. Note that in a well-designed application it is improbable that during normal operation an input signal has a very near or over the upper and lower rail limit (saturation in signal acquisition). • If the application software is aware of the state of the system, this information is to be used in the range check implementation. For example, if the ADC value is the measurement of a current through a power load, reading an abnormal value such as a current flowing in opposite direction versus the load supply may indicate a fault in the acquisition module. • As the ADC module is shared between different possible external sources, the combination of plausibility checks on the different signals acquired can help to cover the whole input range in a very efficient way
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	The implementation (and the related diagnostic efficiency) of this safety mechanism are strongly application-dependent

Table 60. **ADC_SM_3**

SM CODE	ADC_SM_3
Description	Periodical software test for ADC
Ownership	*End user*
Detailed implementation	The method is implemented acquiring multiple signals and comparing the read value with the expected one, supposed to be know. Method can be implemented with different level of complexity: • Basic complexity: acquisition and check of upper or lower rails (VDD or VSS) and internal reference voltage • High complexity: in addition to basic complexity tests, acquisition of a DAC output connected to ADC input and checking all voltage excursion and linearity
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Combination of two different complexity method can be used to better optimize test frequency in high demand safety functions

Table 61. **ADC_SM_4**

SM CODE	ADC_SM_4
Description	1oo2 scheme for ADC inputs
Ownership	*End user*
Detailed implementation	This safety mechanism is implemented using two different SAR ADC channels belonging to separate ADC modules to acquire the same input signal. The application software checks the coherence between the two readings.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	ADC_SM_0: Periodical read-back of ADC configuration registers
Recommendations and known limitations	This method can be used in conjunction with ADC_SM_0/ ADC_SM_2/ ADC_SM_3 to achieve highest level of ADC module diagnostic coverage

3.6.13 Digital-to-analog converter (DAC)

Table 62. **DAC_SM_0**

SM CODE	DAC_SM_0
Description	Periodical read-back of configuration registers

SM CODE	DAC_SM_0
Ownership	*End user*
Detailed implementation	This method must be applied to DAC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 63. DAC_SM_1

SM CODE	DAC_SM_1
Description	DAC output loopback on ADC channel
Ownership	*End user*
Detailed implementation	Implementation is realized by routing the active DAC output to one ADC channel, and by checking the output current value with his expected one.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous or on demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Efficiency versus transient failures is linked to final application characteristics. We define as Tm the minimum duration of DAC wrong signal permanence required to violate the related safety function(s). Efficiency is maximized when execution test frequency is higher than 1/Tm.

3.6.14 Basic timers TIM 6/7

Table 64. GTIM_SM_0

SM CODE	GTIM_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to basic counter timer TIM6 or TIM7 configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 65. GTIM_SM_1

SM CODE	GTIM_SM_1
Description	1oo2 for counting timers
Ownership	*End user*
Detailed implementation	This method implements via software a 1oo2 scheme between two counting resources. The guidelines for the implementation of the method are the following: • Two timers are programmed with same time base or frequency. • In case of timer use as a time base: use in the application software one of the timer as time base source, and the other one just for check. Coherence check for the 1oo2 is done at application level, comparing two counters values each time the timer value is used to affect safety function. • In case of interrupt generation usage: use the first timer as main interrupt source for the service routines, and use the second timer as a “reference” to be checked at the initial of interrupt routine
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Tolerance implementation in timer checks is recommended to avoid false positive outcomes of the diagnostic

3.6.15 Advanced, general and low-power timers TIM1/2/3/4/5/8/9/10/11/12/13/14 LPTIM1

Note: As the timers are equipped with many different channels, each independent from the others, and possibly programmed to realize different features, the safety mechanism is selected individually for each channel.

Table 66. ATIM_SM_0

SM CODE	ATIM_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to advanced, general and low-power timers TIM1/2/3/4/5/8/9/10/11/12/13/14 LPTIM1 configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 67. **ATIM_SM_1**

SM CODE	ATIM_SM_1
Description	1oo2 for counting timers
Ownership	*End user*
Detailed implementation	This method implements via software a 1oo2 scheme between two counting resources. The guidelines for the implementation of the method are the following: • Two timers are programmed with same time base or frequency. • In case of timer use as a time base: use in the application software one of the timer as time base source, and the other one just for check. Coherence check for the 1oo2 is done at application level, comparing two counters values each time the timer value is used to affect safety function. • In case of interrupt generation usage: use the first timer as main interrupt source for the service routines, and use the second timer as a “reference” to be checked at the initial of interrupt routine
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Tolerance implementation in timer checks is recommended to avoid false positive outcomes of the diagnostic. This method apply to timer channels merely used as elapsed time counters

Table 68. **ATIM_SM_2**

SM CODE	ATIM_SM_2
Description	1oo2 for input capture timers
Ownership	*End user*
Detailed implementation	This method is conceived to protect timers used for external signal acquisition and measurement, like “input capture” and “encoder reading”. Implementation requires to connect the external signals also to a redundant timer, and to perform a coherence check on the measured data at application level. Coherence check between timers is executed each time the reading is used by the application software
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	To reduce the potential effect of common cause failures, it is suggested to use for redundant check a channel belonging to a different timer module and mapped to non-adjacent pin on the device package

Table 69. **ATIM_SM_3**

SM CODE	ATIM_SM_3
Description	Loop-back scheme for PWM outputs
Ownership	*End user*
Detailed implementation	This method is implemented by connecting the PWM to a separate timer channel to acquire the generated waveform characteristics. The guidelines are the following: • Both PWM frequency and duty cycle are measured and checked versus the expected value. • To reduce the potential effect of common cause failure, it is suggested to use for the loopback check a channel belonging to a different timer module and mapped to non-adjacent pins on the device package. This measure can be replaced under the end-user responsibility by different loopback schemes already in place in the final application and rated as equivalent. For example if the PWM is used to drive an external power load, the reading of the on-line current value can be used instead of the PWM duty cycle measurement.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	Efficiency versus transient failures is linked to final application characteristics. We define as Tm the minimum duration of PWM wrong signal permanence (wrong frequency, wrong duty, or both) required to violate the related safety function(s). Efficiency is maximized when execution test frequency is higher than 1/Tm

Table 70. **ATIM_SM_4**

SM CODE	ATIM_SM_4
Description	Lock bit protection for timers
Ownership	ST
Detailed implementation	This safety mechanism allows the end user to lock down specified configuration options, avoiding unintended modifications by application software. It addresses therefore software development systematic faults
Error reporting	NA
Fault detection time	NA
Addressed fault model	None (Fault avoidance)
Dependency on *Device* configuration	None
Initialization	Lock protection must be enabled using LOCK bits in the TIMx_BDTR register
Periodicity	Continuous
Test for the diagnostic	NA
Multiple faults protection	NA
Recommendations and known limitations	This method does not addresses timer configuration changes due to soft-errors

Note: IRTIM is not individually mentioned here, being mainly implemented by TIM16 and TIM17 functions. Refer therefore to related prescriptions.

3.6.16 General-purpose input/output (GPIO) - port A/B/C/D/E/F/G

Table 71. GPIO_SM_0

SM CODE	GPIO_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to GPIO configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	GPIO availability can differ according to part number
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 72. GPIO_SM_1

SM CODE	GPIO_SM_1
Description	1oo2 for input GPIO lines
Ownership	*End user*
Detailed implementation	This method addresses GPIO lines used as inputs. Implementation is done by connecting the external safety-related signal to two independent GPIO lines. Comparison between the two GPIO values is executed by application software each time the signal is used to affect application software behavior.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	To reduce the potential impact of common cause failure, it is recommended to use GPIO lines: • belonging to different I/O ports (for instance port A and B) • with different bit port number (for instance PA1 and PB5) • mapped to non-adjacent pins on the device package

Table 73. GPIO_SM_2

SM CODE	GPIO_SM_2
Description	Loopback scheme for output GPIO lines

SM CODE	GPIO_SM_2
Ownership	*End user*
Detailed implementation	This method addresses GPIO lines used as outputs. Implementation is done by a loopback scheme, connecting the output to a different GPIO line programmed as input and by using the input line to check the expected value on output port. Comparison is executed by application software periodically and each time output is updated.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	To reduce the potential impact of common cause failure, it is recommended to use GPIO lines: • belonging to different I/O ports (for instance port A and B) • with different bit port number (for instance PA1 and PB5) • mapped to non-adjacent pins on the device package Efficiency versus transient failures is linked to final application characteristics. We define as Tm the minimum duration of GPIO output wrong signal permanence required to violate the related safety function(s). Efficiency is maximized when execution test frequency is higher than 1/Tm.

Table 74. GPIO_SM_3

SM CODE	GPIO_SM_3
Description	GPIO port configuration lock register
Ownership	ST
Detailed implementation	This safety mechanism prevents configuration changes for GPIO registers; it addresses therefore systematic faults in software application. The use of this method is encouraged to enhance the end-application robustness for systematic faults.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	None (Systematic only)
Dependency on *Device* configuration	None
Initialization	*Application software* must apply a correct write sequence to LCKK bit (bit 16 of the GPIOx_LCKR register) after writing the final GPIO configuration.
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	Not needed
Recommendations and known limitations	This method does not address transient faults (soft errors) that can possibly cause bit-flips on GPIO registers at running time.

3.6.17 Real-time clock module (RTC)

Table 75. RTC_SM_0

SM CODE	RTC_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to RTC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 76. RTC_SM_1

SM CODE	RTC_SM_1
Description	Application check of running RTC
Ownership	*End user*
Detailed implementation	The application software implements some plausibility check on RTC calendar or timing data, mainly after a power-up and further date reading by RTC. The guidelines for the implementation of the method are the following: • RTC backup registers are used to store coded information in order to detect the absence of VBAT during power-off period. • RTC backup registers are used to periodically store compressed information on current date or time • The application software executes minimal consistence checks for date reading after power-on (detecting “past” date or time retrieve). • Application software periodically checks that RTC is actually running, by reading RTC timestamp progress and comparing with an elapsed time measurement based on STM32 internal clock or timers.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodical
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software

SM CODE	RTC_SM_1
Recommendations and known limitations	This method provides a limited diagnostic coverage for RTC failure modes. In case of *End user* application where RTC timestamps accuracy can affect in severe way the safety function (for example, medical data storage devices), it is strongly recommended to adopt more efficient system-level measures.

Table 77. RTC_SM_2

SM CODE	RTC_SM_2
Description	Information redundancy on backup registers
Ownership	End user
Detailed implementation	Data stored in RTC backup registers must be protected by a checksum with encoding capability (for instance, CRC). Checksum must be checked by application software before consuming stored data. This method guarantees data versus erases due to backup battery failures
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	None

Table 78. RTC_SM_3

SM CODE	RTC_SM_3
Description	Application-level measures to detect failures in timestamps/event capture
Ownership	*End user*
Detailed implementation	This method must detect failures affecting the RTC capability to correct execute the timestamps/event capture functions. Due to the nature strictly application-dependent of this solution, no detailed guidelines for its implementation are given here.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic / On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: Periodical core self-test software
Recommendations and known limitations	This method must be used only if the timestamps/event capture function is used in the safety function implementation. It is worth noting that the use of timestamp / event capture in safety-related applications with the *MCU* in Sleep or Stop mode is prevented by the assumed requirement ASR7 (refer to Section 3.3.1 Safety requirement assumptions).

3.6.18 Power controller (PWR)

Table 79. VSUP_SM_0

SM CODE	VSUP_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 80. VSUP_SM_1

SM CODE	VSUP_SM_1
Description	Supply voltage internal monitoring (PVD)
Ownership	ST
Detailed implementation	The device features an embedded programmable voltage detector (PVD) that monitors the VDD power supply and compares it to the VPVD threshold. An interrupt can be generated when VDD drops below the VPVD threshold or when VDD is higher than the VPVD threshold
Error reporting	Interrupt Event generation
Fault detection time	Depends on threshold programming, refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Protection enable by PVDE bit and threshold programming in Power control register (PWR_CR)
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	DIAG_SM_0: Periodical read-back of hardware diagnostics configuration registers
Recommendations and known limitations	Internal monitoring PVD has limited capability to address failures affecting STM32F7 Series internal voltage regulator. Refer to device FMEA for details Enabling related interrupt generation on the detection of errors is highly recommended.

Table 81. **VSUP_SM_2**

SM CODE	VSUP_SM_2
Description	Independent watchdog
Ownership	ST
Detailed implementation	Failures in the power supplies for digital logic (core or peripherals) may lead to alteration of the application software timing, which can be detected by IWDG as safety mechanism introduced to monitor the application software control flow. Refer to CPU_SM_1 and CPU_SM_6 for further information.
Error reporting	Reset signal generation
Fault detection time	Depends on implementation (watchdog timeout interval)
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	IWDG activation. It is recommended to use the “Hardware watchdog” in Option byte settings (IWDG is automatically enabled after reset)
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_1: control flow monitoring in application software
Recommendations and known limitations	In specific part numbers IWDG can be fed by a power supply independent from the one used for CPU core and main peripherals. Such diversity helps to increase the protection guaranteed by IWDG from main power supply anomalies. The adoption of an external watchdog (refer to CPU_SM_5) adds further diversity.

Table 82. **VSUP_SM_3**

SM CODE	VSUP_SM_3
Description	Internal temperature sensor check
Ownership	*End user*
Detailed implementation	The internal temperature sensor must be periodically tested in order to detect abnormal increase of the die temperature – hardware faults in supply voltage system may cause excessive power consumption and consequent temperature rise
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	None
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	This method also mitigates the eventuality of common-cause affecting the MCU and due to too high temperature. Refer to the device datasheet to set the threshold temperature

Table 83. **VSUP_SM_5**

SM CODE	VSUP_SM_5
Description	System-level power supply management
Ownership	*End user*
Detailed implementation	This method is implemented at system level in order to guarantee the stability of power supply value over time. It can include a combination of different overlapped solutions, some listed here below (but not limited to): • Additional voltage monitoring by external components • Passive electronics devices able to mitigate overvoltage • Specific design of power regulator in order to avoid power supply perturbation in presence of a single failure
Fault detection time	Depends on implementation
Addressed fault model	Fault avoidance
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	N/A
Recommendations and known limitations	Usually this method is already required/implemented to guarantee the stability of each component of the final electronic board

3.6.19 Reset and clock controller (RCC)

Table 84. **CLK_SM_0**

SM CODE	CLK_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to configuration registers for clock and reset system (refer to RCC register map). Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 85. **CLK_SM_1**

SM CODE	CLK_SM_1
Description	Clock security system (CSS)

SM CODE	CLK_SM_1
Ownership	ST
Detailed implementation	The clock security system (CSS) detects the loss of high-speed external (HSE) oscillator clock activity and executes the corresponding recovery action, such as: • Switch-off HSE • Commutation on the HSI • Generation of related NMI
Error reporting	NMI
Fault detection time	Depends on implementation (clock frequency value).
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	CSS protection must be enabled through Clock interrupt register (RCC_CIR) after boot stabilization.
Periodicity	Continuous
Test for the diagnostic	CLK_SM_0: periodical read-back of configuration registers
Multiple-fault protection	CPU_SM_5: external watchdog
Recommendations and known limitations	It is recommended to carefully read reference manual instruction on NMI generation, in order to correctly managing the faulty situation by *Application software*.

Table 86. CLK_SM_2

SM CODE	CLK_SM_2
Description	Independent watchdog
Ownership	ST
Detailed implementation	The independent watchdog IWDG is able to detect failures in internal main *MCU* clock (lower frequency).
Error reporting	Reset signal generation
Fault detection time	Depends on implementation (watchdog timeout interval).
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	IWDG activation. It is recommended to use the *hardware watchdog* in Option byte settings (IWDG is automatically enabled after reset).
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_1: control flow monitoring in application software
Recommendations and known limitations	If IWDG window option is used, *End user* must consider possible tolerance in application software execution, to avoid false error reports (affecting system availability).

Table 87. CLK_SM_3

SM CODE	CLK_SM_3
Description	Internal clock cross-measure
Ownership	*End user*
Detailed implementation	This method is implemented using TIM14 capabilities to be fed by the 32 KHz RTC clock or an external clock source (if available). TIM14 counter progresses are compared with another counter (fed by internal clock). Abnormal values of oscillator frequency can therefore be detected.

SM CODE	CLK_SM_3
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_1: control flow monitoring in application software CPU_SM_5: external watchdog
Recommendations and known limitations	Efficiency versus transient faults is negligible. It provides only medium efficiency in permanent clock-related failure mode coverage.

3.6.20 Independent and system window watchdogs (IWDG and WWDG)

Table 88. WDG_SM_0

SM CODE	WDG_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to IWDG/WWDG configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 89. WDG_SM_1

SM CODE	WDG_SM_1
Description	Software test for watchdog at startup
Ownership	*End user*
Detailed implementation	This safety mechanism ensures the right functionality of the internal watchdogs in use. At startup, the software test programs the watchdog with the required expiration timeout, stores a specific non-trivial code in SRAM and waits for the reset signal. After the watchdog reset, the software understands that the watchdog has correctly triggered, and does not execute the procedure again.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent

SM CODE	WDG_SM_1
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Startup (see below)
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	In a typical *End user* application, this test can be executed only at startup and during maintenance or offline periods. It could be associated to IEC61508 concept of “proof test” and so it cannot be accounted for a diagnostic coverage contribution during operating time.

3.6.21 Clock recovery system (CRS)

No safety mechanisms are defined for CRS because of the consequences of CoU_8 (refer to Table 142). CRS disactivation is guaranteed by Section 3.6.41 .

3.6.22 Debug support (DBG)

Table 90. DBG_SM_0

SM CODE	DBG_SM_0
Description	Independent watchdog
Ownership	ST
Detailed implementation	The debug unintentional activation due to hardware random fault results in the massive disturbance of *CPU* operations, leading to intervention of the independent watchdog or alternately, the other system watchdog WWGDG or an external one.
Error reporting	Reset signal generation
Fault detection time	Depends on implementation (watchdog timeout interval).
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_1: control flow monitoring in application software
Recommendations and known limitations	None

3.6.23 Cyclic redundancy-check module (CRC)

Table 91. CRC_SM_0

SM CODE	CRC_SM_0
Description	CRC self-coverage
Ownership	ST
Detailed implementation	The CRC algorithm implemented in this module (CRC-32 Ethernet polynomial: 0x4C11DB7) offers excellent features in terms of error detection in the message. Therefore permanent and transient faults affecting CRC computations are easily detected by any operations using the module to recompute an expected signature
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	None

3.6.24 System configuration controller (SYSCFG)

Table 92. SYSCFG_SM_0

SM CODE	SYSCFG_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to System Configuration controller configuration registers. This method is strongly recommended to protect registers related to hardware diagnostics activation and error reporting chain related features. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	This method is mainly overlapped by several other “configuration register read-backs” required for other *MCU* peripherals. It is reported here for the sake of completeness.

Table 93. **DIAG_SM_0**

SM CODE	DIAG_SM_0
Description	Periodical read-back of hardware diagnostics configuration registers
Ownership	*End user*
Detailed implementation	In STM32F7 Series several hardware-based safety mechanisms are available (they are reported in this manual with the wording Ownership=ST). This method must be applied to any configuration register related to diagnostic measure operations, including error reporting. *End user* must therefore individuate configuration registers related to: • Hardware diagnostic enable • Interrupt/NMI enable (if used for diagnostic error management)
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

3.6.25 SD/SDIO/MMC card host interface (SDMMC)

Table 94. **SDIO_SM_0**

SM CODE	SDIO_SM_0
Description	Periodical read-back of SDIO/SMMC configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to SDIO/SMMC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 95. **SDIO_SM_1**

SM CODE	SDIO_SM_1
Description	Protocol error signals including hardware CRC
Ownership	ST

SM CODE	SDIO_SM_1
Detailed implementation	SDIO/SMMC communication module embeds protocol error checks (like overrun, underrun, timeout etc.) and CRC-packet checks as well, conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a percentage of hardware random failures affecting the module itself
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), please refer to functional documentation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	SDIO_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	-

Table 96. SDIO_SM_2

SM CODE	SDIO_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by SDIO/SMMC a redundancy check (like a CRC check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated. This safety mechanism can overlap with information redundancy techniques implemented at system level to address failure of physical device connected to SDIO/SMMMC port

Note: The safety mechanisms mentioned above are addressing the SDIO/SMMC interface included in STM32 MCUs. No claims are done in this Safety Manual about the mitigation of hardware random faults affecting the external memory connected to SDIO/SMMC port.

3.6.26 Flexible static memory controller (FSMC)

Table 97. FSMC_SM_0

SM CODE	FSMC_SM_0
Description	Control flow monitoring in application software
Ownership	*End user*
Detailed implementation	If FSMC is used to connect an external memory containing software code to be executed by the CPU, permanent and transient faults affecting the FSMC memory controller are able to interfere with the access operation by the CPU, leading to wrong data or instruction fetches. A strong control flow mechanism linked to a system watchdog is able to detect such failures, in case they interfere with the expected flow of the application software. The implementation of this method is identical to the one reported for CPU_SM_1, refer there for details
Error reporting	Depends on implementation
Fault detection time	Depends on implementation. Higher value is fixed by watchdog timeout interval
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	FSMC interface is available only on selected part numbers
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	This mechanism must be used just if FSMC external memory is used to store executable programs

Table 98. FSMC_SM_1

SM CODE	FSMC_SM_1
Description	Information redundancy on external memory connected to FSMC
Ownership	*End user*
Detailed implementation	If FSMC interface is used to connect an external memory where safety-relevant data are stored, information redundancy techniques for stored data are able to address faults affecting the FSMC interface. The possible techniques are: To use redundant copies of safety relevant data and perform coherence check before consuming. To organize data in arrays and compute the checksum field to be checked before use
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	FSMC interface is available only on selected part numbers
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	This mechanism must be used just if FSMC external memory is used to store safety-related data. This safety mechanism can overlap with information redundancy techniques implemented at system level to address failure of physical device connected to FSMC port

Table 99. **FSMC_SM_2**

SM CODE	FSMC_SM_2
Description	Periodical read-back of FSMC configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to FSMC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	FSMC interface is available only on selected part numbers
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 100. **FSMC_SM_3**

SM CODE	FSMC_SM_3
Description	ECC engine on NAND interface in FSMC module
Ownership	ST
Detailed implementation	The FMC NAND Card controller includes two error correction code computation hardware blocks, one per memory bank. They reduce the host CPU workload when processing the ECC by software. ECC mechanism protects data integrity on the external memory connected to NAND port
Error reporting	Refer to functional documentation
Fault detection time	ECC bits are checked during a memory reading
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	FSMC interface is available only on selected part numbers
Initialization	None
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	FSMC_SM_2: Periodical read-back of FSMC configuration registers
Recommendations and known limitations	This method has negligible efficiency in detecting hardware random failures affecting the FSMC interface. It can be part of End user safety concept because addressing memories outside STM32F7 Series MCU

3.6.27 Quad-SPI interface (QUADSPI)

Table 101. QSPI_SM_0

SM CODE	QSPI_SM_0
Description	Periodical read-back of QUADSPI configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to QUADSPI configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 102. QSPI_SM_1

SM CODE	QSPI_SM_1
Description	Protocol error signals including hardware CRC
Ownership	ST
Detailed implementation	QUADSPI communication module embeds protocol error checks (like overrun, underrun, timeout etc.), conceived to detect communication-related abnormal conditions. These mechanisms are able anyway to detect a percentage of hardware random failures affecting the module itself.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for example baud rate), please refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	QSPI_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	Enabling related interrupt generation on the detection of errors is highly recommended.

Table 103. **QSPI_SM_2**

SM CODE	QSPI_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets (not commands) transferred by QSPI interface a redundancy check (like a CRC check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated. This safety mechanism can overlap with information redundancy techniques implemented at system level to address failure of physical device connected to QSPI port

3.6.28 Serial audio interface (SAI)

Table 104. **SAI_SM_0**

SM CODE	SAI_SM_0
Description	Periodical read-back of SAI configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to SAI configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 105. **SAI_SM_1**

SM CODE	SAI_SM_1
Description	SAI output loopback scheme
Ownership	*End user*
Detailed implementation	This method uses a loopback scheme to detect permanent and transient faults on the output channel used for serial audio frame generation. It is implemented by connecting the second serial audio interface as input for primary output generation. The application software is able therefore to identify wrong or missing audio frame generation
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous/ On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	Efficiency versus transient failures is linked to final application characteristics. We define as Tm the minimum duration of serial audio wrong signal permanence required to violate the related safety function(s). Efficiency is maximized when execution test frequency is higher than 1/Tm. Method to be used when SAI interface safety-related use is “audio stream generation”

Table 106. **SAI_SM_2**

SM CODE	SAI_SM_2
Description	1oo2 scheme for SAI module
Ownership	*End user*
Detailed implementation	This safety mechanism is implemented using the two SAI interfaces to decode/receive the same input stream audio. The application software checks the coherence between the received data
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	The MCU performance overload and the implementation complexity associated to this method can be relevant. Method to be used when SAI interface safety-related use is “audio stream receive”

3.6.29 DSI Host (DSIHOST)

Table 107. **DSI_SM_0**

SM CODE	DSI_SM_0
Description	Periodical read-back of DSI Host configuration registers

SM CODE	DSI_SM_0
Ownership	*End user*
Detailed implementation	This method must be applied to DSI Host configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 108. DSI_SM_1

SM CODE	DSI_SM_1
Description	Protocol error signals and information redundancy including hardware checksums
Ownership	ST
Detailed implementation	DSI communication/command protocol is based on a packet handling concept, including (where applicable) ECC and checksum capabilities. This mechanism, mainly implemented to manage on field communication disturbance, is able to achieve a relevant diagnostic coverage on several DSI module failure modes
Error reporting	Error conditions are reported by flag bits in related registers
Fault detection time	Depends on peripheral configuration and the type of violation detected, please refer to functional documentation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	DSI_SM_0: Periodical read-back of DSI Host configuration registers
Recommendations and known limitations	-

Note: The above-described safety mechanisms addresses the DSI interface included in STM32 MCUs, including PHY. Because actual capability of correct physical signal generation to drive the connected monitor is not addressed by these safety mechanisms, in case such feature is considered safety relevant the End user is warned to evaluate the adoption of adequate system-level measures.

3.6.30 Ethernet (ETH): media access control (MAC) with DMA controller

Table 109. ETH_SM_0

SM CODE	ETH_SM_0
Description	Periodical read-back of Ethernet configuration registers
Ownership	*End user*

SM CODE	ETH_SM_0
Detailed implementation	This method must be applied to Ethernet configuration registers (including those relate to unused module features). Detailed information on the implementation of this method can be found in EXTI controller .
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 110. ETH_SM_1

SM CODE	ETH_SM_1
Description	Protocol error signals including hardware CRC
Ownership	ST
Detailed implementation	Ethernet communication module embeds protocol error checks (like overrun, underrun, timeout, packet composition violation etc.) and CRC-packet checks as well, conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a percentage of hardware random failures affecting the module itself.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (e.g. baud rate), refer to functional documentation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	ETH_SM_2 information redundancy techniques on messages, including end-to-end operation
Recommendations and known limitations	-

Table 111. ETH_SM_2

SM CODE	ETH_SM_2
Description	Information redundancy techniques on messages, including End to End safing
Ownership	*End user*
Detailed implementation	This method aim to protect the communication between a peripheral and its external counterpart. It is used in Ethernet local safety concept to address failures not detected by ETH_SM_1 and to increase its associated diagnostic coverage. Refer to CAN_SM_2 description for detailed information.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient

SM CODE	ETH_SM_2
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self test software
Recommendations and known limitations	The implementation on the application software of complex Ethernet-based communication stacks (like TCP/IP) is able to satisfy the requirements of this method.

Note: The use of the DMA feature inside Ethernet module brings to adopt the same set of safety mechanism defined for the system DMA (refer to Direct memory access controller (DMA)).

3.6.31 JPEG codec (JPEG)

Table 112. JPEG_SM_0

SM CODE	JPEG_SM_0
Description	Periodical read-back of JPEG codec configuration registers.
Ownership	*End user*
Detailed implementation	This method must be applied to JPEG codec configuration registers. Detailed information on the implementation of this method can be found in EXTI controller .
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 113. JPEG_SM_1

SM CODE	JPEG_SM_1
Description	Periodic test for JPEG encoding/decoding functions
Ownership	*End user*
Detailed implementation	JPEG encoding/decoding functions performed by JPEG codec are tested by comparison, executing the functions over a set of reference images stored in the Flash memory and checking the correctness of output images. The method diagnostic coverage depends on the quantity and composition of image set used for the checks. The comparison of output image with expected result can be executed bit-by-bit or even by faster methods like CRC-seed (computed via DMA transactions) checks.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None

SM CODE	JPEG_SM_1
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	N/A
Multiple faults protection	CPU_SM_0: periodical core self test software
Recommendations and known limitations	If only one kind of function between encoding and decoding is used by application software, the method can be simplified restricting the test to the used function only.

Table 114. JPEG_SM_2

SM CODE	JPEG_SM_2
Description	Application-level detection of failures affecting JPEG coding/encoding
Ownership	*End user*
Detailed implementation	Several application-level methods can be used to detect failures affecting JPEG coding/encoding; being no possible to give detailed information for its implementation, only high level guidelines/hints are provided: • Permanent and transient failures: application software checks on expected output image characteristics (e.g. after the processing by image recognition algorithms) • – Transient faults: application software checks on images redundancy (in case of sequence coming from video stream) possibly discarding wrongly-processed frames. This rationale could be also used to derate part of transient failure rate as “no effect”.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic/on demand
Test for the diagnostic	N/A
Multiple faults protection	CPU_SM_0: periodical core self test software
Recommendations and known limitations	These methods are strictly application-dependent; therefore, their implementation and any related claims in terms of failure mitigations are end user’s responsibility

Note: The use of the DMA feature inside Ethernet module brings to adopt the same set of safety mechanism defined for the system DMA (refer to Direct memory access controller (DMA)).

3.6.32 HDMI-CEC controller (CEC)

Table 115. HDMI_SM_0

SM CODE	HDMI_SM_0
Description	Periodical read-back of configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to CEC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0

SM CODE	HDMI_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 116. HDMI_SM_1

SM CODE	HDMI_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	CEC communication module embeds protocol error checks (such as additional parity bit check, overrun, frame error) conceived to detect network-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself. Error signals connected to these checkers are normally handled in a standard communication software, so the overhead is reduced.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration (for instance baud rate), refer to functional documentation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation.
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple-fault protection	HDMI_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	None

Table 117. HDMI_SM_2

SM CODE	HDMI_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data packets transferred by CEC a redundancy check (such as *CRC* check, or similar one) with encoding capability. The checksum encoding capability must be robust enough to guarantee at least 90% probability of detection for a single bit flip in the data packet. Consistency of data packet must be checked by the application software before consuming data.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None

SM CODE	HDMI_SM_2
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple-fault protection	CPU_SM_0: periodical core self-test software
Recommendations and known limitations	It is assumed that the remote HDMI-CEC counterpart has an equivalent capability of performing the check described. Transmission full redundancy (message repetition) should not be used because its detection capability is limited to a subset of communication unit failure modes. To give an example on checksum encoding capability, using just a bit-by-bit addition is unappropriated.

3.6.33 Management data input/output (MDIOS)

Table 118. MDIO_SM_0

SM CODE	MDIO_SM_0
Description	Periodical read-back of MDIO slave configuration registers.
Ownership	*End user*
Detailed implementation	This method must be applied to MDIO slave configuration registers. Detailed information on the implementation of this method can be found in EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 119. MDIO_SM_1

SM CODE	MDIO_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	MDIO communication protocol is based on a packet handling concept, including preamble/start/stop correct conditions checks. This mechanism, mainly implemented to manage on field communication disturbance, is able to achieve a relevant diagnostic coverage on several MDIO module failure modes
Error reporting	Error conditions are reported by flag bits in related registers, and interrupt generation
Fault detection time	Depends on peripheral configuration and the type of violation detected, refer to functional documentation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation

SM CODE	MDIO_SM_1
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	DSI_SM_0: periodical read-back of MDIO Host configuration registers.
Recommendations and known limitations	-

Table 120. MDIO_SM_2

SM CODE	MDIO_SM_2
Description	Information redundancy techniques on MDIO registers contents, including register update awareness.
Ownership	*End user*
Detailed implementation	Information provided by external parties by MDIO communication must be protected by redundancy schemes (encoded data values and possibly the definition of a “checksum” register). The application software must be aware of any register value update executed by external parties, so it is needed the implementation of a “validate/unvalidate” mechanism to: • report to external party that updated data have been consumed • mark as “unvalidated” any data already consumed • allow external party to inform application software that new data are available
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self test software
Recommendations and known limitations	It is assumed that the external entity responsible to update/send data to application software by the MDIO communication link is able to contribute to the MDIO failure mitigation, by detecting missing or incomplete data consumption.

3.6.34 SPDIF receiver interface (SPDIFRX)

Table 121. SPDF_SM_0

SM CODE	SPDF_SM_0
Description	Periodical read-back of SPDIF configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to SPDIF configuration registers. Detailed information on the implementation of this method can be found in section NVIC_SM_0
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0

SM CODE	SPDF_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 122. SPDF_SM_1

SM CODE	SPDF_SM_1
Description	Protocol error signals
Ownership	ST
Detailed implementation	IEC60598 S/PDIF data frame specification used in SPDIF interface embeds protocol error checks (like overrun, underrun, bit timing violations, parity, etc.) conceived to detect transmission-related abnormal conditions. These mechanisms are able anyway to detect a marginal percentage of hardware random failures affecting the module itself.
Error reporting	Error flag raise and optional Interrupt Event generation
Fault detection time	Depends on peripheral configuration, refer to functional documentation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	SPDF_SM_0: periodical read-back of SPDIF configuration registers
Recommendations and known limitations	-

Table 123. SPDF_SM_2

SM CODE	SPDF_SM_2
Description	Information redundancy techniques on messages
Ownership	*End user*
Detailed implementation	This method is implemented adding to data S/PDIF data stream some form of information redundancy, possibly including information repetition, to address failure modes affecting the decoding section of the module.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: periodical core self test software
Recommendations and known limitations	This method could be replaced by application-level alternative measures checking the correctness of the audio stream received. One given example could be represented by a set of plausibility checks executed after post-elaboration by voice recognition algorithms.

3.6.35 True random number generator (RNG)

Table 124. RNG_SM_0

SM CODE	RNG_SM_0
Description	Periodical read-back of RNG configuration register RNG_CR
Ownership	*End user*
Detailed implementation	This method must be applied to RNG configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	RNG module available only on specific part numbers
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple-fault protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 125. RNG_SM_1

SM CODE	RNG_SM_1
Description	RNG module entropy on-line tests
Ownership	ST and *End user*
Detailed implementation	RNG module include an internal diagnostic for the analog source entropy that can be used to detect failures on the module itself. Furthermore, the required test on generated random number difference between the previous one (as required by FIPS PUB 140-2) can be exploited as well. Implementation: • Check for RNG error conditions. • Check the difference between generated random number and the previous one.
Error reporting	CEIS, SEIS error bits in RNG status register (RNG_SR) Application software error for FIPS PUB 140-2 test fail
Fault detection time	Depends on implementation.
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	RNG module available only on specific part numbers
Initialization	Depends on implementation.
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple-fault protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	-

3.6.36 Cryptographic processor (CRYP)

Table 126. AES_SM_0

SM CODE	AES_SM_0
Description	Periodical read-back of CRYP configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to CRYP configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	CRYP module available only on specific part numbers
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 127. AES_SM_1

SM CODE	AES_SM_1
Description	Encryption/decryption collateral detection
Ownership	ST
Detailed implementation	Encryption and decryption operations performed by CRYP module are composed by several data manipulations and checks, with different level of complexity according to the selected chaining algorithm. A major part of the hardware random failures affecting CRYP module leads to algorithm violations/errors. Leading to decoding errors on the receiver side.
Error reporting	Several error conditions can happen, check functional documentation.
Fault detection time	Depends on peripheral configuration
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	CRYP module available only on specific part numbers
Initialization	Depends on implementation.
Periodicity	Continuous
Test for the diagnostic	*NA*
Multiple faults protection	AES_SM_2: Information redundancy techniques on messages
Recommendations and known limitations	-

Table 128. AES_SM_2

SM CODE	AES_SM_2
Description	Information redundancy techniques on messages, including end-to-end protection.
Ownership	*End user*

SM CODE	AES_SM_2
Detailed implementation	This method aim to protect the communication between a peripheral and his external counterpart. It is used in AES local safety concept to address failures not detected by the encryption/decryption features. Refer to CAN_SM_2 description for detailed information.
Error reporting	Refer to CAN_SM_2
Fault detection time	Refer to CAN_SM_2
Addressed fault model	Refer to CAN_SM_2
Dependency on *Device* configuration	CRYP module available only on specific part numbers
Initialization	Refer to CAN_SM_2
Periodicity	Refer to CAN_SM_2
Test for the diagnostic	Refer to CAN_SM_2
Multiple-fault protection	Refer to CAN_SM_2
Recommendations and known limitations	Important note: it is assumed that the remote counterpart has an equivalent capability of performing the checks described. Refer to CAN_SM_2 for further notice.

*Note: Hardware random failure consequences on potential security feature violations are **not** detailed in this manual.*

3.6.37 HASH processor (HASH)

Table 129. HASH_SM_0

SM CODE	HASH_SM_0
Description	Periodical read-back of HASH configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to HASH configuration registers. Detailed information on the implementation of this method can be found in EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	HASH module available only on specific part numbers
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 130. HASH_SM_1

SM CODE	HASH_SM_1
Description	HASH processing collateral detection
Ownership	ST
Detailed implementation	Message digest computation performed by HASH module is composed by several data manipulations and checks. A major part of the hardware random failures affecting HASH module will lead to algorithm violations/errors, and so to decoding errors on the receiver side

SM CODE	HASH_SM_1
Error reporting	Several error condition can happens, check functional documentation
Fault detection time	Depends on peripheral configuration
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	HASH module available only on specific part numbers
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	HASH_SM_0: periodical read-back of HASH configuration registers CPU_SM_0: periodical core self-test software
Recommendations and known limitations	-

*Note: Hardware random failures consequences on potential security features violations are **not** analyzed in this manual.*

3.6.38 Digital filter for sigma delta modulators (DFSDM)

Table 131. DFS_SM_0

SM CODE	DFS_SM_0
Description	Periodical read-back of DFSDM configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to DFSDM configuration registers. Detailed information on the implementation of this method can be found in EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 132. DFS_SM_1

SM CODE	DFS_SM_1
Description	Multiple acquisition by application software
Ownership	*End user*
Detailed implementation	This method implements a timing information redundancy by executing multiple acquisitions on the same input signal. Multiple acquisition data are then combined by a filter algorithm to determine the signal correct value.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Transient

SM CODE	DFS_SM_1
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	It is highly probable that this recommendation is satisfied by design by the end user application software. Usage of multiple acquisitions followed by average operations is a common technique in industrial applications where it is needed to survive with spurious EMI disturbs on sensor lines

Table 133. DFS_SM_2

SM CODE	DFS_SM_2
Description	Range check by application software
Ownership	*End user*
Detailed implementation	This method is implemented as described in ADC_SM_2: Range check by application software, refer to such safety mechanism for details.
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	The implementation of this safety mechanism is strongly application-dependent

Table 134. DFS_SM_3

SM CODE	DFS_SM_3
Description	1oo2 scheme for DFSM inputs
Ownership	*End user*
Detailed implementation	This safety mechanism is implemented using two different DFSM modules to acquire the same input signal. The application software checks the coherence between the two readings
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent and Transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	On demand
Test for the diagnostic	Not needed
Multiple faults protection	DSF_SM_0: Periodical read-back of DFSDM configuration registers
Recommendations and known limitations	This method can be used in conjunction with DFS_SM_0 to achieve highest level of DFSM module diagnostic coverage (in alternative to DFS_SM1 and DFS_SM_2)

3.6.39 Digital camera interface (DCMI)

Table 135. DCMI_SM_0

SM CODE	DCMI_SM_0
Description	Periodical read-back of DCMI configuration registers
Ownership	*End user*
Detailed implementation	This method must be applied to DCMI configuration registers. Detailed information on the implementation of this method can be found in EXTI controller .
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	DCMI interface is available only on selected part numbers
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 136. DCMI_SM_1

SM CODE	DCMI_SM_1
Description	DCMI video input data synchronization
Ownership	ST
Detailed implementation	According to the nature of video data stream received, DCMI module implements synchronization controls, from the simplest one (hardware synchronization) to the most complex (e.g. embedded data synchronization mode). DCMI internal failures leading to the incapability of correcting synchronizing the data stream can be therefore detected
Error reporting	No explicit error signal/message generation is provided (*)
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	DCMI interface is available only on selected part numbers
Initialization	Depends on implementation
Periodicity	Continuous
Test for the diagnostic	N/A
Multiple faults protection	DCMI_SM_0: Periodical read-back of DCMI configuration registers
Recommendations and known limitations	(*) For its nature, the detection of an actual hardware failure by this safety mechanism can be confused with functional-related scenarios (e.g. camera device disconnected or powered-off). It is responsibility of the application software to discriminate, as far as it is technically possible, among different events

3.6.40 LCD-TFT display controller (LTDC)

Table 137. LCD_SM_0

SM CODE	LCD_SM_0
Description	Periodical read-back of LTDC configuration registers and buffer memory.

SM CODE	LCD_SM_0
Ownership	*End user*
Detailed implementation	This method must be applied to LTDC configuration registers and to the buffer memory as well. Detailed information on the implementation of this method can be found in EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

Table 138. LCD_SM_1

SM CODE	LCD_SM_1
Description	LTDC acquisition by ADC channel
Ownership	*End user*
Detailed implementation	Correct generation of LTDC driving signals is checked by ADC reading versus expected values
Error reporting	Depends on implementation
Fault detection time	Depends on implementation
Addressed fault model	Permanent
Dependency on *Device* configuration	None
Initialization	None
Periodicity	Periodic
Test for the diagnostic	Not needed
Multiple faults protection	CPU_SM_0: Periodical core self test software
Recommendations and known limitations	This method is conceived to mainly detect permanent failures affecting analog parts and therefore the execution on periodic way is acceptable. Diagnostic coverage achievable depends on the quantity of LTDC signals checked

Note: The above-described safety mechanism addresses the LTDC interface included in STM32 MCUs. Because actual capability of correct image generation on LTDC is not addressed by this safety mechanism, in case such feature is considered safety relevant the End user is warned to evaluate the adoption of adequate system-level measures.

3.6.41 Disable and periodic cross-check of unintentional activation of unused peripherals

This section reports the safety mechanism that addresses peripherals not used by the safety application, or not used at all.

Table 139. FFI_SM_0

SM CODE	FFI_SM_0
Description	Unused peripherals disable
Ownership	*End user*

SM CODE	FFI_SM_0
Detailed implementation	This method contributes to the reduction of the probability of cross-interferences caused by peripherals not used by the software application, in case a hardware failure causes an unintentional activation. After the system boot, the application software must disable all unused peripherals with this procedure: • Enable reset flag on AHB and APB peripheral reset register • Disable clock distribution on AHB and APB peripheral clock enable register
Error reporting	NA
Fault detection time	NA
Addressed fault model	NA
Dependency on *Device* configuration	None
Initialization	NA
Periodicity	Startup
Test for the diagnostic	Not needed
Multiple faults protection	FFI_SM_1: Periodical read-back of interference avoidance registers
Recommendations and known limitations	None

Table 140. FFI_SM_1

SM CODE	FFI_SM_1
Description	Periodical read-back of interference avoidance registers
Ownership	*End user*
Detailed implementation	This method contributes to the reduction of the probability of cross-interferences between peripherals that can potentially conflict on the same input/output pins, including for instance unused peripherals. This diagnostic measure must be applied to following registers: • clock enable and disable registers • alternate function programming registers Detailed information on the implementation of this method can be found in Section 3.6.5 EXTI controller.
Error reporting	Refer to NVIC_SM_0
Fault detection time	Refer to NVIC_SM_0
Addressed fault model	Refer to NVIC_SM_0
Dependency on *Device* configuration	Refer to NVIC_SM_0
Initialization	Refer to NVIC_SM_0
Periodicity	Refer to NVIC_SM_0
Test for the diagnostic	Refer to NVIC_SM_0
Multiple faults protection	Refer to NVIC_SM_0
Recommendations and known limitations	Refer to NVIC_SM_0

3.6.42 System

Table 141. **DUAL_SM_0**

SM CODE	DUAL_SM_0
Description	Cross-check between two STM32 MCUs
Ownership	*End user*
Detailed implementation	This method is implemented in the spirit of technique described in IEC61508-7, A.3.5 “Reciprocal comparison by software”, which is rated in IEC61508-2 Table A.4 as capable to achieve high level of diagnostic coverage. The two processing units exchange data reciprocally, and a fail in the comparison is considered as a detection of a failure in one of the two unit. The guidelines for the implementation are the following: • Data exchanged include output results, intermediate results(1) and the results of each software-implemented safety mechanisms executed on periodical basis on both MCUs (for example CPU_SM_0) • Software routines devoted to data exchange/comparison must be logically separated from the software implementing the safety function(s). • Systematic capability of data exchange/comparison software must be equal or above the one of the software implementing the safety function(s). • Independency and lack of interference between the software implementing the data exchange/comparison and the one implementing the safety function(s) must be proven. • Frequency of data exchange/comparison is imposed by the system PST (refer to (1) related timing constraints for “periodic” safety mechanisms), except for output results which needs to be exchanged/compared at the same rate they are potentially updated.
Fault detection time	Depends on implementation
Addressed fault model	Permanent and transient
Dependency on *Device* configuration	None
Initialization	Depends on implementation
Periodicity	Periodic
Test for the diagnostic	N/A
Multiple faults protection	CPU_SM_0: periodical core self-test software (individually executed on both processing units)
Recommendations and known limitations	This method is usually rated as “optional” because it is not strictly needed in the framework of 1oo2 architecture described in Section 3.2.4 ; anyway, it is included here only for its use in such an architecture. This method can provide additional safety margin for systems needing further protection against fault accumulation. Because this method could be a potential source of common cause failure between the two 1oo2 channels (in case of incorrect implementation), End User is recommended to carefully follow above the reported guidelines (box “Detailed Implementation”).

1. *It is defined here “intermediate result” the value of each variable able to directly influence the final individual channel output. To give some examples:*
   - if final output is a value resulting from some computation (for example a PWM rate), “intermediate results” are the values of each variable included in such computation.
   - if final output if the result of a decision (for example GPIO value decided on the basis of the comparison between values), “intermediate results” are the values of each variable involved in such decision.

3.7 Conditions of use

The table below provides a summary of the safety concept recommendations reported in Section 3.6: Description of hardware and software diagnostics. The conditions of use to be applied to STM32F7 Series devices are reported in form of safety mechanism requirements. Exception is represented by some conditions of use introduced by FMEA analysis in order to correctly address specific failure modes. These conditions of use are reported at the end of the table presented in this section.

Rank column reports how related safety mechanism has been considered during the analysis, with following meaning:

- M = this safety mechanism is always operating during normal operations – no end user activity can deactivate it.
- ++ = Highly recommended being a common practice and considered in this safety manual for the computation of the safety metrics to achieve *SIL*2 on a single *MCU*.
- + = Recommended as additional safety measure, but not considered in this Safety Manual for the computation of safety metrics. STM32F7 Series users can skip the implementation in case it is in contradiction with functional requirements or overlapped by another mechanism marked as “++”.
- o = optional, not needed or related to specific *MCU* configuration

The “X” marker in the *Perm* and *Trans* columns in the table below, indicates that the related safety mechanism is effective for such fault model.

Table 142. List of safety mechanisms

STM32F7 Series function	Diagnostic	Description	Rank	Perm	Trans
Arm® Cortex®-M7 CPU	CPU_SM_0	Periodical software test addressing permanent faults in Arm® Cortex®-M7 CPU core	++	X	-
	CPU_SM_1	Control flow monitoring in application software	++	X	X
	CPU_SM_2	Double computation in application software	++	-	X
	CPU_SM_3	Arm® Cortex®-M7 HardFault exceptions	M	X	X
	CPU_SM_4	Stack hardening for application software	+	X	X
	CPU_SM_5	External watchdog	++ (1)	X	X
	CPU_SM_6	Independent watchdog	++(1)	X	X
	CPU_SM_7	MPU – Memory protection unit	++(2)	X	X
	CPU_SM_9	Periodical self-test software for Arm® Cortex®-M7 caches	++(3)	X	-
	MPU_SM_0	Periodical read-back of MPU configuration registers	++(2)	X	X
Embedded Flash memory	FLASH_SM_0	Periodical software test for Flash memory	++	X	-
	FLASH_SM_1	Control flow monitoring in application software	++	X	X
	FLASH_SM_2	Arm® Cortex®-M4 HardFault exceptions	M	X	X
	FLASH_SM_3	Option byte write protection	M	-	-
	FLASH_SM_4	Static data encapsulation	+	X	X
	FLASH_SM_6	Flash unused area filling code	+	-	-
	FLASH_SM_8	Read/Write/Proprietary code protection	+	-	-
Embedded SRAM	RAM_SM_0	Periodical software test for SRAM memory	++	X	-
	RAM_SM_2	Stack hardening for application software	+	X	X
	RAM_SM_3	Information redundancy for system variables in application software	++	X	X
	RAM_SM_4	Control flow monitoring in application software	o(4)	X	X
	RAM_SM_5	Periodical integrity test for application software in RAM	o(4)	X	X
	RAM_SM_6	Read protection (RDP), Write protection (WRP)	+	-	-
System architecture	BUS_SM_0	Periodical software test for interconnections	++	X	-
	BUS_SM_1	Information redundancy in intra-chip data exchanges	++	X	X
EXTI controller	NVIC_SM_0	Periodical read-back of configuration registers	++	X	X

STM32F7 Series function	Diagnostic	Description	Rank	Perm	Trans
EXTI controller	NVIC_SM_1	Expected and unexpected interrupt check by application software	++	X	X
DMA	DMA_SM_0	Periodical read-back of configuration registers	++	X	X
	DMA_SM_1	Information redundancy on data packet transferred via DMA	++	X	X
	DMA_SM_2	Information redundancy including sender or receiver identifier on data packet transferred via DMA	++	X	X
	DMA_SM_3	Periodical software test for DMA	++	X	-
	DMA_SM_4	DMA transaction awareness	++	X	X
bxCAN	CAN_SM_0	Periodical read-back of configuration registers	++	X	X
	CAN_SM_1	Protocol error signals	++	X	X
	CAN_SM_2	Information redundancy techniques on messages, including end-to-end protection	++	X	X
USART	UART_SM_0	Periodical read-back of configuration registers	++	X	X
	UART_SM_1	Protocol error signals	++	X	X
	UART_SM_2	Information redundancy techniques on messages	++	X	X
	UART_SM_3	Information redundancy techniques on messages, including end-to-end protection	++	X	X
I2C	IIC_SM_0	Periodical read-back of configuration registers	++	X	X
	IIC_SM_1	Protocol error signals	++	X	X
	IIC_SM_2	Information redundancy techniques on messages	++	X	X
	IIC_SM_3	CRC packet-level	+	X	X
	IIC_SM_4	Information redundancy techniques on messages, including end-to-end protection	+	X	X
SPI	SPI_SM_0	Periodical read-back of configuration registers	++	X	X
	SPI_SM_1	Protocol error signals	++	X	X
	SPI_SM_2	Information redundancy techniques on messages	++	X	X
	SPI_SM_3	CRC packet-level	+	X	X
	SPI_SM_4	Information redundancy techniques on messages, including end-to-end protection	+	X	X
USB OTG	USB_SM_0	Periodical read-back of configuration registers	++	X	X
	USB_SM_1	Protocol error signals	++	X	X
	USB_SM_2	Information redundancy techniques on messages	++	X	X
	USB_SM_3	Information redundancy techniques on messages, including end-to-end protection	+	X	X
ADC	ADC_SM_0	Periodical read-back of configuration registers	++	X	X
	ADC_SM_1	Multiple acquisition by application software	++	-	X
	ADC_SM_2	Range check by application software	++	X	X
	ADC_SM_3	Periodical software test for ADC	++	X	-
	ADC_SM_4	1oo2 scheme for ADC inputs	+	X	X
DAC	DAC_SM_0	Periodical read-back of configuration registers	++	X	X
	DAC_SM_1	DAC output loopback on ADC channel	++	X	X
Basic timers TIM6/7	GTIM_SM_0	Periodical read-back of configuration registers	++	X	X

STM32F7 Series function	Diagnostic	Description	Rank	Perm	Trans
Basic timers TIM6/7	GTIM_SM_1	1oo2 for counting timers	++	X	X
Advanced, general and low-power timers TIM1/2/3/4/5/8/9/10/11/12/13/14 LPTIM1	ATIM_SM_0	Periodical read-back of configuration registers	++	X	X
	ATIM_SM_1	1oo2 for counting timers	++	X	X
	ATIM_SM_2	1oo2 for input capture timers	++	X	X
	ATIM_SM_3	Loopback scheme for PWM outputs	++	X	X
	ATIM_SM_4	Lock bit protection for timers	+	-	-
CRC	CRC_SM_0	CRC self-coverage	++	X	X
GPIO	GPIO_SM_0	Periodical read-back of configuration registers	++	X	X
	GPIO_SM_1	1oo2 for input GPIO lines	++	X	X
	GPIO_SM_2	Loopback scheme for output GPIO lines	++	X	X
	GPIO_SM_3	GPIO port configuration lock register	+	-	-
RTC	RTC_SM_0	Periodical read-back of configuration registers	++	X	X
	RTC_SM_1	Application check of running RTC	++	X	X
	RTC_SM_2	Information redundancy on backup registers	+	X	X
	RTC_SM_3	Application-level measures to detect failures in timestamps or event capture	o	X	X
Power control	VSUP_SM_0	Periodical read-back of configuration registers	++	X	X
	VSUP_SM_1	Supply voltage monitoring	++	X	-
	VSUP_SM_2	Independent Watchdog	++	X	-
	VSUP_SM_3	Internal temperature sensor check	o	-	-
	VSUP_SM_5	System-level power supply management	+	-	-
Clock and Reset	CLK_SM_0	Periodical read-back of configuration registers	++	X	X
	CLK_SM_1	CSS Clock Security System	++	X	-
	CLK_SM_2	Independent Watchdog	++	X	-
	CLK_SM_3	Internal clock cross-measure	+	X	-
IWDG/WWDG	WDG_SM_0	Periodical read-back of configuration registers	++	X	X
	WDG_SM_1	Software test for watchdog at startup	o	X	-
Debug	DBG_SM_0	Independent watchdog	++	X	X
System or peripheral control	LOCK_SM_0	Lock mechanism for configuration options	+	-	-
	SYSCFG_SM_0	Periodical read-back of configuration registers	++	X	X
	DIAG_SM_0	Periodical read-back of hardware diagnostics configuration registers	++	X	X
SDMMC	SDIO_SM_0	Periodical read-back of SDIO/SMMC configuration registers.	++	X	X
	SDIO_SM_1	Protocol error signals including hardware CRC	++	X	X
	SDIO_SM_2	Information redundancy techniques on messages	++	X	X
Flexible static memory controller (FSMC)	FSMC_SM_0	Control flow monitoring in application software	++(5)	X	X
	FSMC_SM_1	Information redundancy on external memory connected to FSMC	++(5)	X	X
	FSMC_SM_2	Periodical read-back of FSMC configuration registers.	++	X	X
	FSMC_SM_3	ECC engine on NAND interface in FSMC module	o	X	X

STM32F7 Series function	Diagnostic	Description	Rank	Perm	Trans
QUADSPI	QSPI_SM_0	Periodical read-back of QUADSPI configuration registers.	++	X	X
	QSPI_SM_1	Protocol error signals including hardware CRC	++	X	X
	QSPI_SM_2	Information redundancy techniques on messages	++	X	X
SAI	SAI_SM_0	Periodical read-back of SAI configuration registers.	++	X	X
	SAI_SM_1	SAI output loopback scheme	++	X	X
	SAI_SM_2	1oo2 scheme for SAI module	++	X	X
DSI Host (DSIHOST)	DSI_SM_0	Periodical read-back of DSI Host configuration registers.	++	X	X
	DSI_SM_1	Protocol error signals and information redundancy including hardware checksums	++	X	X
Ethernet (ETH): media access control (MAC) with DMA controller	ETH_SM_0	Periodical read-back of Ethernet configuration registers.	++	X	X
	ETH_SM_1	Protocol error signals including hardware CRC	++	X	X
	ETH_SM_2	Information redundancy techniques on messages, including End to End safing	++	X	X
JPEG codec	JPEG_SM_0	Periodical read-back of JPEG codec configuration registers.	++	X	X
	JPEG_SM_1	Periodic test for JPEG encoding/decodin functions	++	X	-
	JPEG_SM_2	Application-level detection of failures affecting JPEG coding/encoding	++	X	X
HDMI CEC	HDMI_SM_0	Periodical read-back of HDMI CEC configuration registers	++	X	X
	HDMI_SM_1	Protocol error signals	++	X	X
	HDMI_SM_2	Information redundancy techniques on messages	++	X	X
MDIOS	MDIO_SM_0	Periodical read-back of MDIO slave configuration registers.	++	X	X
	MDIO_SM_1	Protocol error signals	++	X	X
	MDIO_SM_2	Information redundancy techniques on MDIO registers contents, including register update awareness.	++	X	X
SPDIFRX	SPDF_SM_0	Periodical read-back of SPDIF configuration registers	++	X	X
	SPDF_SM_1	Protocol error signals	++	X	X
	SPDF_SM_2	Information redundancy techniques on messages	++	X	X
RNG	RNG_SM_0	Periodical read-back of RNG configuration register RNG_CR.	++	X	X
	RNG_SM_1	RNG module entropy on-line tests	++	X	-
CRYP	AES_SM_0	Periodical read-back of AES configuration registers	++	X	X
	AES_SM_1	Encryption/decryption collateral detection	++	X	X
	AES_SM_2	Information redundancy techniques on messages, including end-to-end safing	++	X	X
HASH	HASH_SM_0	Periodical read-back of HASH configuration registers	++	X	X
	HASH_SM_1	HASH processing collateral detection	++	X	X

STM32F7 Series function	Diagnostic	Description	Rank	Perm	Trans
DFSDM	DFS_SM_0	Periodical read-back of DFSDM configuration registers	++	X	X
	DFS_SM_1	Multiple acquisition by application software	++	-	X
	DFS_SM_2	Range check by application software	++	X	X
	DFS_SM_3	1oo2 scheme for DFSM inputs	+	X	X
DCMI	DCMI_SM_0	Periodical read-back of DCMI configuration registers	++	X	X
	DCMI_SM_1	DCMI video input data synchronization	++	X	X
LCD	LCD_SM_0	Periodical read-back of LCD configuration registers and buffer memory.	++	X	X
	LCD_SM_1	LCD acquisition by ADC channel	++	X	-
Part separation (no interference)	FFI_SM_0	Unused peripherals disable	++	-	-
	FFI_SM_1	Periodical read-back of interference avoidance registers	++	-	-
Arm® Cortex®-M7 CPU	CoU_1	The reset condition of Arm® Cortex®-M7 CPU must be compatible as valid safe state at system level	++	-	-
Debug	CoU_2	STM32F7 Series debug features must not be used in safety function(s) implementation	++	-	-
Arm® Cortex®-M7 / Supply system	CoU_3	Low power mode state must not be used in safety function(s) implementation	++	-	-
STM32F7 Series peripherals	CoU_4	End user must implement the required combination of safety mechanism/CoUs for each STM32 peripherals used in safety function(s) implementation	++	X	X
Flash subsystem	CoU_5	During Flash bank mass erase and reprogramming there must not be safety functions(s) executed by STM32F7 Series MCU.	++	-	-
Flash subsystem	CoU_6	On-field application software live update by dual-Flash system must include the execution of code/ data integrity check by methods like FLASH_SM_0	++	X	X
CPU subsystem	CoU_7	In case of multiple safety functions implementations, methods to guarantee their mutual independence must include MPU use.	++	-	-
Device	DUAL_SM_0	Cross-check between two STM32 MCUs	o	X	X

1. *To achieve on the single MCU local safety metrics compatible with SIL2 target , method CPU_SM_6 could be sufficient. Anyway, to understand the rationale behind "++" classification for both methods, refer to the "Recommendations" row of related description in Section 3.6 for more details.*
2. *Can be considered ranked as "+" if only one safety function is implemented and the presence of non-safety related software is excluded.*
3. *In case of L1 cache disable in end user final application, this method must be not implemented (not needed to achieve any safety integrity level).*
4. *Must be considered ranked as "++" if the application software is executed on RAM.*
5. *Can be considered ranked as "o" depending on the intended use of external memory connected to FSMC.*

The above-described safety mechanism or conditions of use are conceived with different levels of abstraction depending on their nature: the more a safety mechanism is implemented as application-independent, the wider is its possible use on a large range of end-user applications.

The safety analysis highlights two major partitions inside the *MCU*:

- System-critical *MCU* modules. Every *End user* application is affected, from safety point of view, by a failure on these modules. Because they are used by every end user application, related methods or safety mechanism are mainly conceived to be application-independent. The system-critical modules on the *Device* are: CPU, RCC, PWR, bus matrix and interconnect, and Flash memory and RAM (including their interfaces).
- Peripheral modules. Such modules could be not used by the end-user application, or they could be used for non-safety related tasks. Related safety methods are therefore implemented mainly at application level, as *Application software* solutions or architectural solutions.

4 Safety results

This section reports the results of the safety analysis of the STM32F7 Series devices, according to IEC 61508 and to ST methodology flow, related to the hardware random and dependent failures.

4.1 Random hardware failure safety results

The analysis for random hardware failures of STM32F7 Series devices reported in this safety manual is executed according to STMicroelectronics methodology flow for safety analysis of semiconductor devices in compliance with IEC61508. The accuracy of results obtained are guaranteed by three factors:

- STMicroelectronics methodology flow strict adherence to IEC61508 requirements and prescriptions
- the use, during the analysis, of detailed and reliable information on microcontroller design
- the use of state-of-the-art fault injection methods and tools for safety metrics verification

The device safety analysis explored the overall and exhaustive list of device failure modes, to individuate for each of them an adequate mitigation measure (safety mechanism). The overall list of device failure modes is maintained in related *FMEA* document, provided on demand by local STMicroelectronics sales office.

In summary, with the adoption of the safety mechanisms and conditions of use reported in Section 3.7 Conditions of use, it is possible to achieve the integrity levels summarized in the following table.

Table 143. Overall achievable safety integrity levels

Number of devices used	Safety architecture	Target	Safety analysis result
1	1oo1/1oo1D	*SIL2 LD*	Achievable
		SIL2 HD/CM	Achievable with potential performance impact (1)
2	1oo2	*SIL3 LD*	Achievable
		SIL3 HD/CM	Achievable with potential performance impact

1. *Note that the potential performance impact related to some above-reported target achievements is mainly related to the need of execution of periodical software-based diagnostics (refer to safety mechanism description for details). The impact is therefore strictly related to how much "aggressive" the system level PST is (see Section 3.3.1 Safety requirement assumptions).*

The resulting relative safety metrics (diagnostic coverage (DC) and safe failure fraction (SFF)) and absolute safety metrics (probability of failure per hour (PFH), probability of dangerous failure on demand (PFD)) are not reported in this section but in the failure mode effect diagnostic analysis (FMEDA) snapshot, due to:

- a large number of different STM32F7 Series parts,
- a possibility to declare non-safety-relevant unused peripherals, and
- a possibility to enable or not the different available safety mechanisms.

The *FMEDA* snapshot is a static document reporting the safety metrics computed at different detail levels (at microcontroller level and for microcontroller basic functions) for a given combination of safety mechanisms and for a given part number. If *FMEDA* computation sheet is needed, early contact the local STMicroelectronics sales representative, in order to receive information on expected delivery dates for specific device target part number.

Note: Safety metrics computations are restricted to STM32F7 Series boundary, hence they do not include the WDTe, PEv, and VMONe processes described in Section 3.3.1 Safety requirement assumptions).

4.1.1 Safety analysis result customization

The safety analysis executed for STM32F7 Series devices documented in this safety manual considers all microcontroller modules to be safety-related, thus able to interfere with the safety function, with no exclusion. This is in line with the conservative approach to be followed during the analysis of a general-purpose microcontroller, in order to be agnostic versus the final application. This means that no microcontroller module has been declared *safe* as per IEC61508-4, 3.6.8. Therefore, all microcontroller modules are included in *SFF* computations.

In actual *End user* applications, not all the STM32F7 Series parts or modules implement a safety function. That happens if:

- The part is not used at all (disabled), or
- The part implements functions that are not safety-related (for example, a GPIO line driving a *power-on* signaling light on an electronic board).

Implementing safety mechanisms on such parts would be a useless effort for *End user*. The safety analysis results can therefore be customized.

End user can define a STM32F7 Series part as *non-safety-related* based on:

- Collecting rationales and evidences that the part does not contribute to safety function.
- Collecting rationales and evidences that the part does not interfere with the safety function during normal operation, due to final system design decisions.
- Fulfilling the general condition for the mitigation of intra-*MCU* interferences (see Table 1).

For a *non-safety-related* part, *End user* is allowed to:

- Exclude the part from computing metrics to report in *FMEDA*, and
- Not implement safety mechanisms as listed in Table 142. List of safety mechanisms.

With regard to *SFF* computation, this section complies with the *no part / no effect* definition as per IEC 61508-4, 3.6.13 / 3.6.14.

4.1.2 General requirements for freedom from interferences (FFI)

A dedicated analysis has highlighted a list of general requirements to be followed in order to mitigate potential interferences between *Device* internal modules in case of internal failures (freedom from interferences, FFI). These precautions are integral part of the *Device* safety concept and they can play a relevant role when multiple microcontroller modules are declared as *non-safety-related* by *End user* as per Section 4.1.1 Safety analysis result customization.

End user must implement the safety mechanisms listed in Table 144 (implementation details in Section 3.6 Hardware and software diagnostics) regardless any evaluation of their contribution to safety metrics.

Table 144. List of general requirements for FFI

Diagnostic	Description
FFI_SM_0	Unused peripheral disable
FFI_SM_1	Periodical read-back of interference avoidance registers
BUS_SM_0	Periodical software test for interconnections
NVIC_SM_0	Periodical read-back of configuration registers
NVIC_SM_1	Expected and unexpected interrupt check by application software
DMA_SM_0	Periodical read-back of configuration registers
DMA_SM_2	Information redundancy including sender or receiver identifier on data packet transferred via *DMA* (1)
DMA_SM_4	*DMA* transactions awareness(1)
GPIO_SM_0	Periodical read-back of configuration registers

1. *To be implemented only if DMA is actually used*

4.1.3 Notes on multiple-fault scenario

According to the requirements of IEC61508, the safety analysis for STM32F7 Series devices considered multiple-fault scenarios. Furthermore, following the spirit of ISO26262 (the reference and state-of-the-art standard norm for integrated circuit safety analysis), the analysis investigated possible causes preventing the implemented safety mechanisms from being effective, in order to determine appropriate counter-measures. In the *Multiple-fault protection* field, the tables in Section 3.6 Hardware and software diagnostics report the safety mechanisms required to properly manage a multiple-fault scenario, including mitigation measures against failures making safety mechanisms ineffective.

It is strongly recommended that the safety concept includes such mitigation measures, and in particular for systems operating during long periods, as they tend to accumulate errors.

Indeed, fault accumulation issue has been taken into account during STM32F7 Series devices safety analysis.

Another potential source of multiple error condition is the accumulation of permanent failures during power-off periods. Indeed, if the end system is not powered, no safety mechanism are active and so able to early detect the insurgence of such failures. To mitigate this potential issue, it is strongly recommended to execute all periodic safety mechanism at each system power-up; this measure guarantees a fresh system start with a fault-free hardware. This recommendation is given for periodic safety mechanisms rated as "++" (highly recommended) in the Device safety concept, and mainly for the most relevant ones in term of failure distribution: CPU_SM_0, FLASH_SM_0, RAM_SM_0. This startup execution is strongly recommended regardless the safety functions mode of operations and/or the value of PST.

4.2 Analysis of dependent failures

The analysis of dependent failures is important for microcontroller and microprocessor devices. The main subclasses of dependent failures are *CCFs*. Their analysis is ruled by the IEC 61508:2 annex E that lists the design requirements to be verified to allow the use of on-chip redundancy for integrated circuits with one common semiconductor substrate.

As there is no on-chip redundancy on STM32F7 Series devices, the *CCF* quantification through the βIC computation method - as required by Annex E.1, item i - is not required. Note that, in the case of 1oo2 safety architecture implementation, *End user* is required to evaluate the β and βD parameters (used in *PFH* computation) that reflect the common cause factors between the two channels.

The *Device* architecture and structures can be potential sources of dependent failures. These are analyzed in the following sections. The referred safety mechanisms are described in Section 3.6 Hardware and software diagnostics.

4.2.1 Power supply

Power supply is a potential source of dependent failures, because any alteration can simultaneously affect many modules, leading to not-independent failures. The following safety mechanisms address and mitigate those dependent failures:

- VSUP_SM_1: detection of abnormal value of supply voltage;
- VSUP_SM_2: the independent watchdog is different from the digital core of the *MCU*, and this diversity helps to mitigate dependent failures related to the main supply alterations. As reported in VSUP_SM_2 description, separate power supply for IWDG or/and the adoption of an external watchdog (CPU_SM_5) increase such diversity.

The adoption of such safety mechanisms is therefore highly recommended despite their minor contribution to the safety metrics to reach the required safety integrity level. Refer to Section 3.6.18 Power controller (PWR) for the detailed safety mechanism descriptions.

4.2.2 Clock

System clocks are a potential source of dependent failures, because alterations in the clock characteristics (frequency, jitter) can affect many parts, leading to not-independent failures. The following safety mechanisms address and mitigate such dependent failures:

- CLK_SM_1: the clock security system is able to detect hard alterations (stop) of system clock and activate the adequate recovery actions.
- CLK_SM_2: the independent watchdog has a dedicated clock source. The frequency alteration of the system clock leads to the watchdog window violations by the triggering routine on the application software, leading to the *MCU* reset by watchdog.

The adoption of such safety mechanism is therefore highly recommended despite their minor contribution to the safety metrics to reach the required safety integrity level. Refer to Section 3.6.19 Reset and clock controller (RCC) for detailed safety mechanisms description.

4.2.3 DMA

The *DMA* function can be involved in data transfers operated by most of the peripherals. Failures of *DMA* can interfere with the behavior of the system peripherals or application software, leading to dependent failures. The adoption of the following safety mechanisms is therefore highly recommended (refer to Section 3.6.6 Direct memory access controller (DMA/ DMAMUX) for description):

- DMA_SM_0
- DMA_SM_1
- DMA_SM_2

Note: Only DMA_SM_0 must be implemented if DMA is not used for data transfer.

4.2.4 Internal temperature

The abnormal increase of the internal temperature is a potential source of dependent failures, as it can affect many *MCU* parts. The following safety mechanism mitigates this potential effect (refer to Section 3.6.18 Power controller (PWR) for description):

VSUP_SM_3: the internal temperature read and check allows the user to quickly detect potential risky conditions before they lead to a series of internal failures.

5 List of evidences

A *safety case database* stores all the information related to the safety analysis performed to derive the results and conclusions reported in this safety manual.

The safety case database is composed of the following:

- safety case with the full list of all safety-analysis-related documents
- STMicroelectronics' internal *FMEDA* tool database for the computation of safety metrics, including estimated and measured values
- safety report, a document that describes in detail the safety analysis executed on STM32F7 Series devices and the clause-by-clause compliance to IEC 61508
- STMicroelectronics' internal fault injection campaign database including tool configuration and settings, fault injection logs and results

As these materials contain STMicroelectronics' confidential information, they are only available for the purpose of audit and inspection by authorized bodies, without being published, which conforms to Note 2 of IEC 61508:2, 7.4.9.7.

6 Change impact analysis for other safety standards

The safety analysis reported in this safety manual is executed according to the IEC 61508 safety norm. This section 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 62061:2005+AMD1:2012+AMD2:2015 – *Safety of machinery and Functional safety of safety-related electrical, electronic and programmable electronic control systems*,
- IEC 61800-5-2:2016 –*Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

6.1 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.

6.1.1 ISO 13849 architectural categories

ISO 13849-1:2015 reports in section 4.4, Figure 4 a typical safety function diagrammatic presentation. Under the assumption that the compliant item as defined in section is used to implement the *b* (logic), the equivalence of the ISO 13849 representation with the one in Section 3.2.1 is evident. The mapping of ISO 13849 architectures with the one described in Section 3 is possible.

ISO 13849-1:2015 in section §6 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 this manual in Section 3 . 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 Section 6.1.2 for details on computations).

Table 145. 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 *MTTFd* and DC_{avg} are given for category B, anyway it is recommended to follow safety manual recommendation.
1	6.2.4	Not recommended	Category not recommended because of the NOTE1 in IEC13849-1, section §6.2.4.
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 *MTTFd* can be satisfied but computations are needed(1). Constraints on *CCF* are satisfied(2).
3	6.2.6	Possible with 1oo2 architecture + DUAL_SM_0	Constraints on DC_{avg} and *MTTFd* can be satisfied but computations are needed(1) Constraints on *CCF* are satisfied(2).
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 *MTTFd* can be satisfied but computations are needed(1) Constraints on *CCF* are satisfied(2).

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 – refer to Section 6.1.2 for the correct interpretation of Device data in such a computation.*
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 this manual. It is worth to note that the complete safety analysis resulting as output of the IEC61508 compliance activity (this manual) helps to claim the score for item #4 in Table F.1.*

6.1.2 ISO 13849 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 this 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* << 1 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 this 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. The 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 this safety manual.

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

6.2 IEC 62061:2005+AMD1:2012+AMD2:2015

This standard is applicable in the specification, design and verification or validation of safety-related electrical control systems (SRECS) of machines. *SRECS* is the electrical or electronics control system of the machine which failure could lead to reduction or loss of safety. *SRECS* implements a safety-related control function (SRCF) to prevent any increase of the risk.

Because STM32xx has been classified as Type B according IEC61508 (refer to Section 3.2.2), it must be considered as a “complex component” in IEC62061 definition.

6.2.1 IEC 62061 architectural categories

IEC 62061 defines a set of basic system architectures to be used for the design of safety-related electrical control systems (safety-related electrical control systems (SRECS)) implementing their *SRCF*s. The following table lists for each system architecture the possible implementation/mapping by/to one of the IEC 61508 compliant architectures described in this manual in Section 3 .

Safety metrics related to STM32xx *MCU* can be reused from IEC61508 analysis (refer to device FMEDA), while their combination with the ones related to other devices included in the system is full responsibility of *End user*.

Table 146. IEC 62061 architectural categories

IEC 62061		Link to IEC61508-compliant safety architectures	Notes/constraints
Architecture	Clause		
A	6.7.8.2.2	Equivalent of 1oo1, with *HFT* = 0, no diagnostic function(s) implemented.	-
B	6.7.8.2.3	Equivalent to 1oo2 with *HFT* = 1, a single failure does not lead to the loss of *SRCF*. No diagnostic function(s) implemented.	-
C	6.7.8.2.4	Equivalent of 1oo1 architecture.	All requirements related to 1oo1 architecture must be implemented.
D	6.7.8.2.5	Equivalent of 1oo2 architecture.	All requirements related to 1oo2 architecture must be implemented.

6.2.2 IEC 62061 safety metrics computation

The failure rate (λ) in T is the smaller proof test interval or the life time of the subsystem.

As seen in ISO 13849, the approximation §6.7.8.2.1 NOTE2 is still considered valid, hence

λ = 1 / *MTTFd*, where it is assumed that 1 >> λ x T.

So, as $PFH_D = \lambda_D$ x 1h, so *PFD* = 1 / *MTTFd*.

Safety analysis executed for STM32F7 Series devices according to IEC 61508 is more and more accurate for the definition of dangerous failure identifications that can be re-mapped in IEC 62061 domain. Thus, values of λ, *PFH* and *SFF* that are reported in the *FMEDA* (refer to Section 4 Safety results), are still valid and can be reused.

For evaluation of *CCF* in basic architectures with *HFT* = 1, *End user* can rely to what reported in Section 4.2 Analysis of dependent failures, and to the guidelines included in IEC 61508:2010-6 Annex D.

Alternatively, *End user* can apply the simplified approach from the standard (refer to Annex F) to calculate the β factor value to be used in formulas for *PFD*.

6.3 IEC 61800-5-2:2016

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

6.3.1 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 Section 3.2.2 .

6.3.2 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 this safety manual (and related *FMEA* and *FMEDA*) can be re-mapped in IEC 61800 domain.

Revision history

Table 147. **Document revision history**

Date	Revision	Changes
24-Nov-2017	1	Initial release.
28-Nov-2017	2	Updated *List of safety mechanisms FLASH_SM_0 rank from '+' to '++'* table.
19-Apr-2018	3	Updated introduction. Updated title of Section 6.2 IEC 62061:2005+AMD1:2012+AMD2:2015. Updated *SIL classification versus HFT* table. Updated Section 4.2 Analysis of dependent failures. Updated *SRECS high-level diagram* figure. Updated Section 6.2.2 IEC 62061 safety metrics computation. Removed Section A.4: IEC 60730-1:2010. Updated Section 1.2 Normative references.
12-Nov-2018	4	Updated *Terms and abbreviations* table. Updated Table 146. IEC 62061 architectural categories.
13-Jan-2020	5	Updated functional safety documentation framework. Added Section 1.3 Reference documents. Added Section 3.6.21 Clock recovery system (CRS) Updated: • Section Introduction. • Section 1.2 Normative references. • Section 2 Device development process. • Section 3.2.2 Safety functions performed by Compliant item. • Section 3.2.4 Reference safety architectures - 1oo2. • Section 3.3.1 Safety requirement assumptions all Devices functions. • Section 3.6.2 Embedded Flash memory. • Section 3.6.18 Power controller (PWR) adding VSUP_SM_5. • Section 3.7 Conditions of use. • Section 4.1.3 Notes on multiple-fault scenario adding paragraph on fault accumulation issue. • Section 4.2 Analysis of dependent failures. • Section 6 Change impact analysis for other safety standards. • Section 6.1.1 ISO 13849 architectural categories. • Section 6.1.2 ISO 13849 safety metrics computation. • Section 6.2 IEC 62061:2005+AMD1:2012+AMD2:2015. • Section 6.2.1 IEC 62061 architectural categories. • Section 6.2.2 IEC 62061 safety metrics computation. • Section 6.3 IEC 61800-5-2:2016. • Section 6.3.1 IEC 61800 architectural categories. • Section 6.3.2 IEC 61800 safety metrics computation. Changed appendix in paragraphs. Removed: • ISO 13849 work products from Section 6.1 ISO 13849-1:2015, ISO 13849-2:2012. • ISO 62061 work products from Section 6.2 IEC 62061:2005+AMD1:2012+AMD2:2015. • IEC 61800 work products from Section 6.3 IEC 61800-5-2:2016.

Glossary

Application software within the software executed by *Device*, the part that ensures functionality of *End user*'s application and integrates safety functions

CCF common cause failure

CM continuous mode

Compliant item any item subject to claim with respect to the clauses of IEC 61508 series of standards

COTS commercial off-the-shelf

CoU conditions of use

CPU central processing unit

CRC cyclic redundancy check

DC diagnostic coverage

Device depending on context, any single or all of the STM32F7 Series silicon products

DMA direct memory access

DTI diagnostic test interval

ECM engine control module

ECU electronic control unit

End user individual person or company who integrates *Device* in their application, such as an electronic control board

EUC equipment under control

FIT failure in time

FMEA failure mode effect analysis

FMEDA failure mode effect diagnostic analysis

HD high-demand

HFT hardware fault tolerance

HW hardware

ITRS international technology roadmap for semiconductors

LD low-demand

MCU microcontroller unit

MPU memory protection unit

MTBF mean time between failures

MTTFd mean time to dangerous failure

NA not applicable/available

PDS(SR) safety-related power drive system

PEc programmable electronics - core

PEd programmable electronics - diagnostic

PFD probability of dangerous failure on demand

PFH probability of failure per hour

PL performance level

PST process safety time

SFF safe failure fraction

SIL safety integrity level

SILCL safety integrity level claim limit

SRCF safety-related control function

SRECS safety-related electrical control systems

SRP/CS safety-related parts of machinery control systems

Contents

List of tables

List of figures

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics International NV and its affiliates (“ST”) reserve the right to make changes corrections, enhancements, modifications, and improvements to ST products and/or to this document any time without notice.

This document is provided solely for the purpose of obtaining general information relating to an ST product. Accordingly, you hereby agree to make use of this document solely for the purpose of obtaining general information relating to the ST product. You further acknowledge and agree that this document may not be used in or in connection with any legal or administrative proceeding in any court, arbitration, agency, commission or other tribunal or in connection with any action, cause of action, litigation, claim, allegation, demand or dispute of any kind. You further acknowledge and agree that this document shall not be construed as an admission, acknowledgment or evidence of any kind, including, without limitation, as to the liability, fault or responsibility whatsoever of ST or any of its affiliates, or as to the accuracy or validity of the information contained herein, or concerning any alleged product issue, failure, or defect. ST does not promise that this document is accurate or error free and specifically disclaims all warranties, express or implied, as to the accuracy of the information contained herein. Accordingly, you agree that in no event will ST or its affiliates be liable to you for any direct, indirect, consequential, exemplary, incidental, punitive, or other damages, including lost profits, arising from or relating to your reliance upon or use of this document.

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 acknowledgment, including, without limitation, the warranty provisions thereunder.

In that respect please note that ST products are not designed for use in some specific applications or environments described in above mentioned terms and conditions.

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.

Information furnished is believed to be accurate and reliable. However, ST assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. 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. 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.