Introduction

This document describes how to use the microcontrollers of the STM32F3 Series in the context of a safety-related system, specifying the user's responsibilities for installation and operation in order to reach the targeted safety integrity level.

This manual applies to the microcontrollers of the STM32F3 Series and to X-CUBE-STL part number.

System designers can avoid going into the details of the functional safety standards application of the STM32F3 Series by following the indications reported in this manual.

This manual is written in compliance with IEC 61508. It indicates how to use the STM32F3 Series microcontrollers in the context of other functional safety standards such as safety machine directives ISO 13849.

The safety analysis summarized in this manual takes into account the variation in terms of memory size, internal peripheral number and package among the different part numbers of the Arm® Cortex®-M4 based STM32F3 Series microcontrollers.

This manual has to be read along with the technical documentation for the related part numbers (such as reference manuals and datasheets) available on www.st.com.
1 About this document

1.1 Purpose and scope

This document describes how to use the Arm® Cortex®-M4 based STM32F3 Series 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.

This document is useful to system designers willing to evaluate the safety of their solution embedding one or more STM32F3 Series microcontroller(s).

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

1.2 Terms and abbreviations

Abbreviations related to STM32F3 Series hardware modules (such as DMA or GPIO) are the same than the ones used in STM32F3 Series technical documentation. See the following table for a list of acronyms used in this document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCF</td>
<td>Common cause failure</td>
</tr>
<tr>
<td>CM</td>
<td>Continuous mode</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off-the-shelf</td>
</tr>
<tr>
<td>CoU</td>
<td>Conditions of use</td>
</tr>
<tr>
<td>CPU</td>
<td>Central processing unit</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic redundancy check</td>
</tr>
<tr>
<td>DC</td>
<td>Diagnostic coverage</td>
</tr>
<tr>
<td>DMA</td>
<td>Direct memory access</td>
</tr>
<tr>
<td>DTI</td>
<td>Diagnostic test interval</td>
</tr>
<tr>
<td>ECM</td>
<td>Engine control module</td>
</tr>
<tr>
<td>ECU</td>
<td>Electronic control unit</td>
</tr>
<tr>
<td>EUC</td>
<td>Equipment under control</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure in time</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure mode effect analysis</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure mode effect diagnostic analysis</td>
</tr>
<tr>
<td>HD</td>
<td>High demand</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware fault tolerance</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>ITRS</td>
<td>International technology roadmap for semiconductors</td>
</tr>
<tr>
<td>LD</td>
<td>Low demand</td>
</tr>
<tr>
<td>MCU</td>
<td>Microcontroller unit</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between failure</td>
</tr>
<tr>
<td>MTTFd</td>
<td>Mean time to failure</td>
</tr>
<tr>
<td>NA</td>
<td>Not available</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>PDS(SR)</td>
<td>Power drive system (safety related)</td>
</tr>
<tr>
<td>PEc</td>
<td>Programmable electronics - core</td>
</tr>
<tr>
<td>PEd</td>
<td>Programmable electronics - diagnostic</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of dangerous failure on demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of failure per hour</td>
</tr>
<tr>
<td>PL</td>
<td>Performance level</td>
</tr>
<tr>
<td>PST</td>
<td>Process safety time</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe failure fraction</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety integrity level</td>
</tr>
<tr>
<td>SRCF</td>
<td>Safety-related control function</td>
</tr>
<tr>
<td>SRECS</td>
<td>Safety-related electrical control systems</td>
</tr>
<tr>
<td>SRP/CS</td>
<td>Safety-related parts of control systems</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
</tbody>
</table>

Read also the following definitions used within this manual:
- **End user**: the STM32F3 Series final user in charge of integrating the MCU in a real application (for example an electronic control board).
- **Application software**: the actual software running on the STM32F3 Series MCUs and implementing the safety function.

### 1.3 Reference normative

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

The version used as reference is IEC 61508:1-7 © IEC:2010.

The other functional safety standards considered in this manual are the following:
- IEC 62061:2012-11, ed. 1.1
- IEC 61800-5-2:2007, ed.1.0

The following table reports the mapping of this document content with respect to the requirements listed in the IEC 61508-2 Annex D.

<table>
<thead>
<tr>
<th>IEC 61508 requirement (part 2 annex D)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>D2.1 a) a functional specification of the functions capable of being performed</td>
<td>Section 3</td>
</tr>
<tr>
<td>D2.1 b) identification of the hardware and/or software configuration of the compliant item</td>
<td>Section 3.2</td>
</tr>
<tr>
<td>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</td>
<td>Section 3.2</td>
</tr>
</tbody>
</table>
The safe failure fraction reported in this manual has been computed under the assumptions described in this document and especially according to the conditions of use described in Section 3.7. Conditions of use.
2 STM32F3 Series microcontroller development process

The development process of a microelectronic device that is used in safety critical application takes into account the adequate management to reduce the probability of systematic faults introduced during the design phase. IEC 61508:2 in Annex F (Techniques and measures for ASICs - avoidance of systematic failures) act as a guidance in tailoring the microcontroller standard design and manufacturer process to the compliance of the IEC 61508 requirements. The checklist reported in the named Annex F helps to collect all related evidences of a given real process.

2.1 STMicroelectronics standard development process

STMicroelectronics (ST) serves four industry domains:

- Standard products.
- Automotive products: ST automotive products are AEC-Q100 compliant. They are subject to specific stress testing and processing instructions in order to achieve the required quality levels and product stability.
- Automotive safety: a subset of the automotive domain. ST uses as a reference the ISO 26262 Road vehicles Functional safety standard. ST supports customer inquiries regarding product failure rates and FMEDA to support hardware system compliance to established safety goals. ST provides products that are safe in their intended use, working in cooperation with customers to understand the mission profile, adopt common methods and define countermeasures for residual risks.
- Medical products: ST complies with applicable regulations for medical products and applies due diligence in the development and validation of these products.

STMicroelectronics product development process, compliant with the ISO/TS 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, application, hardware, software and documentation), qualified respecting ST internal procedures and able to be manufactured using ST internal or subcontracted technologies.

Figure 1 presents a summary of the STMicroelectronics product-development process.
Figure 1. STMicerelectronics 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 and application 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, FMKM
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 the details of the STM32F3 Series safety architecture.

3.1 Safety architecture introduction

The STM32F3 Series microcontroller analyzed in this document can be used as a compliant item within different safety applications.

The aim of this section is to identify such compliant item and therefore to define the context of the analysis in terms of assumptions with respect to a reference concept definition. This concept definition includes therefore reference safety requirements as also assumptions on the design external to the defined compliant item.

As a consequence of compliant item approach, the goal is not to provide an exhaustive hazard and risk analysis of the system around the microcontroller, but rather to list the system-related information considered during the analysis. Such information include - among others - application related assumptions for dangerousness factors, frequency of failures and diagnostic coverage already guaranteed by the application.

3.2 Compliant item

This section includes all the information related to the definition of the compliant item, including its usage in different safety architecture schemes.

3.2.1 Definition of the compliant item

According to IEC 61508:1 clause 8.2.12, a 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. With respect to its user, at the end of its development the compliant item must be described by a safety manual.

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

Figure 2. Definition of the compliant item

Other components might be related to the compliant item, like the external HW components needed to guarantee either the functionality of the STM32F3 Series (external memory, clock quartz etc) or its safety (for example the external watchdog, voltage supervisors).

Defined compliant item can be classified as "element" according IEC61508-4, 3.4.5.

3.2.2 Safety functions performed by the compliant item

In essence, the compliant item architecture can be represented as composed by the following processes performing the safety function or 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 the case of the 1oo2 architecture, a further voting processing element (PEv) can be present;
• Processes external to the compliant item are considered to guarantee safety integrity, such as a watchdog (WDTe) and voltage monitors (VMONe).

The role of the PEv and of the external processes WDTe and VMONe is clarified in the sections where the CoU (definition of safety mechanism) are detailed:
• WDTe: refer to Independent watchdog – VSUP_SM_2, Control flow monitoring in application software – CPU_SM_1,
• VMONe: refer to Supply Voltage Monitoring – VSUP_SM_1.

In summary, STM32F3 Series microcontrollers support the implementation of end user safety functions composed by 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 above reported definition for implemented safety functions, the compliant item i.e. the element can be regarded as type B (as per IEC61508-2, 7.4.4.1.2 definition). Despite accurate, exhaustive and detailed failure analysis has been done for STM32F3 Series, this device has to be considered intrinsically complex and therefore type B classification is appropriate.

Two main safety architecture are therefore identified: 1oo1 (using one MCU) and 1oo2 (using two MCUs).

3.2.3 Reference safety architectures - 1oo1

In 1oo1 reference architecture (shown in below Figure 3) the safety integrity of the compliant item is guaranteed by the combination of STM32F3 Series internal processes (implemented safety mechanisms) and external processes WDTe and VMONe.

Target for 1oo1 reference architecture is SIL2.

Figure 3. 1oo1 reference architecture
3.2.4 Reference safety architectures - 1oo2

1oo2 reference architecture (shown in below Figure 4) is composed by two separate channels, each of them implemented in the same way of 1oo1 reference architecture. Safety integrity of each channel is guaranteed by the combination of STM32F3 Series internal processes (implemented safety mechanisms) and external processes WDTe and VMONe. Safety integrity of overall compliant item is guaranteed by the external voter PEv allowing to claim HFT=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 Dependent failures analysis). $\beta_D$ computation is anyway required.

Target for 1oo2 reference architecture is SIL3.

Figure 4. 1oo2 reference architecture
3.3 Assumed requirements

This section collects all assumptions done during the safety analysis of STM32F3 Series microcontrollers.

3.3.1 Assumed safety requirements

The concept specification, the hazard and risk analysis, the overall safety requirement specification and the consequent allocation has determined the requirements for the compliant item (ASR: assumed safety requirements) listed here below.

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

**ASR1:** The compliant item can be used for four kinds of safety functions mode of operations according part 4, 3.5.16:
- A continuous mode or high-demand SIL3 safety function (CM3), or
- A low-demand SIL3 safety function (LD3), or
- A continuous mode or high-demand SIL2 safety function (CM2), or
- A low-demand SIL2 safety function (LD2).

**ASR2:** The compliant item is used to implement a safety function allowing a time budget of 10 ms (worst case) for the STM32 MCU to detect and react to a failure. That time corresponds to the portion of the Process Safety Time allocated to STM32F3 Series MCUs (“STM32xx Series duty” in the figure below) in error reaction chain at system level.

**ASR3:** The compliant item is used in a safety function that can be continuously powered-on for a time higher than 8 hours. It is assumed to not require any proof test and the lifetime of the product is considered to be not 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 functions implementations, it is assumed that end user is responsible to guarantee their needed mutual independence.

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

**ASR7:** It is assumed that the implemented safety function(s) is not depending on STM32F3 Series MCU transition to and from a low-power state.

**ASR8:** The local safe state of the 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

1. The end user must take into account that random hardware failures affecting the STM32 can compromise the MCU capability of operating properly (for example failure modes affecting the program counter prevent the correct execution of software).

Details on safe states SS1 and SS2 are provided in the following table:
Table 3. SS1 and SS2 safe state details

<table>
<thead>
<tr>
<th>Safe state</th>
<th>Condition</th>
<th>Compliant item action</th>
<th>System Transition to Safe state – 1oo1 architecture</th>
<th>System Transition to Safe state – 1oo2 architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS1</td>
<td>The application software is informed by the presence of a fault and a reaction by the application software itself is possible.</td>
<td>Fault reporting to application software</td>
<td>Application software drives the overall system in his safe state</td>
<td>Application software in one of the two channels drives the overall system in his safe state</td>
</tr>
<tr>
<td>SS2</td>
<td>The application software cannot be informed by the presence of a fault or the application software is not able to execute a reaction.</td>
<td>Reset signal issued by WDTe</td>
<td>WDTe drives the overall system in his safe state (&quot;safe shut-down&quot;) (1)</td>
<td>PEv drives the overall system in his safe state</td>
</tr>
</tbody>
</table>

1. Safe state achievement intended here is compliant to Note on IEC61508-2, 7.4.8.1

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

ASR10: The 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 Description of hardware and software diagnostics.

ASR11: The compliant item is assumed to be regarded as type B as per IEC61508:2, 7.4.4.1.2.

ASR12: It is assumed that dual-Flash banks mass erase and reprogramming features can be used only during end system’s maintenance state, and not during safety function implementation.

3.4 Electrical specifications and environment limits

The user must not exceed the electrical specification and the environmental limits defined in the below list as reported in the STM32F3 Series user manual in order to guarantee the STM32F3 Series safety integrity:

- Absolute maximum rating,
- Capacity,
- Operating conditions.

Due to the large number of STM32F3 Series part numbers, the related user manuals and datasheets are not listed in this document; users are responsible to carefully check the above reported limits in the technical documentation on the related part number available on .

3.5 Systematic safety integrity

According to the requirements of IEC 61508 -2, 7.4.2.2, the Route 1S has been considered in the STM32F3 Series development. As clearly authorized by IEC61508-2, 7.4.6.1, STM32 MCU series can be considered a standard, mass-produced electronic integrated device – for which stringent development procedures, rigorous testing and extensive experience of use minimizes the likelihood of design faults. Anyway, an internal assessment against the compliance of STM32 MCU development flow with the techniques and measures suggested in IEC 61508-2 Annex F has been executed. The Safety Case Database (Section 5 List of evidences) maintains the evidences of the compliance to the norm.

3.6 Description of hardware and software diagnostics

This section lists all the safety mechanisms (hardware, software and application level) considered in the safety analysis of the microcontrollers of the STM32F3 Series. It is expected that users are familiar with the STM32F3 Series architecture, and that this document is used in conjunction with the related device datasheet, user manual and reference information. Therefore, to avoid the eventuality of mistakes and reduce the amount of information to be shown, minimum functional details are included in this document. In following descriptions the words “safety mechanism”, “method” or “requirement” are used as synonym.

Note that each part number of the STM32F3 Series owns different combinations of peripherals (for instance, some of them are not equipped with USB peripheral). To reduce the number of documents and avoid informationless repetitions, the current Safety Manual (and therefore this section) addresses the overall possible peripherals
available in the targeted part numbers. Users have to select which peripherals are really available on their devices, and discard the meaningless recommendations accordingly.

The implementation guidelines reported in the following section are for reference only. The safety verification executed by ST during STM32F3 Series safety analysis and related diagnostic coverage figures reported in this manual (or its Annexes) are based on such guidelines. For the sake of clarity, safety mechanism are grouped for MCU basic functions.

Information are organized in form of tables (one for each safety mechanism). Table 4 below presents the explanation of each field:

### Table 4: Safety mechanism field explanation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM CODE</td>
<td>Unique safety mechanism code/identifier used also in FMEA document. Identifiers use the scheme <code>mmm_SM_x</code> where <code>mmm</code> is a 3 or 4 letter module acronym, and “x” is an incremental number. Please note that module acronym and numbering could be not sequential and/or different from module’s actual name being derived by legacy documents.</td>
</tr>
<tr>
<td>Description</td>
<td>Short mnemonic description</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST : means that method is available on silicon</td>
</tr>
<tr>
<td></td>
<td>End user: method must be implemented by the end user by application software modification, hardware solutions, or both.</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>Detailed implementation sometimes including notes about the safety concept behind the introduction of the safety mechanism.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Describes how the fault detection is reported to application software</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Time that the safety mechanism needs to detect the hardware failure</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>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</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Reports if safety mechanism implementation or characteristics change among different part numbers belonging to STM32F3 Series</td>
</tr>
<tr>
<td>Initialization</td>
<td>Specific operation to be executed to activate the contribution of the safety mechanism</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous : safety mechanism is active in continuous mode</td>
</tr>
<tr>
<td></td>
<td>Periodic: safety mechanism is executed periodically. Note that safety mechanism can be accounted for diagnostic coverage contribution only if it is executed at least one per PST On Demand: safety mechanism is activated in correspondence of 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</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Reports specific procedure (if any and recommended) to allow on-line tests of safety mechanism efficiency</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Reports the safety mechanism(s) associated in order to correctly manage a multi-fault scenario (refer to Section 4.1.3 Notes on multiple faults scenario)</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Additional recommendations or limitations (if any) not reported in other fields</td>
</tr>
</tbody>
</table>
3.6.1 Arm® Cortex®-M4 CPU

Table 5. CPU_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
<th>CPU_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Periodical core self-test software for Arm® Cortex®-M4 CPU</td>
<td></td>
</tr>
<tr>
<td>Ownership</td>
<td>End user or ST</td>
<td></td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depending on implementation</td>
<td></td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depending on implementation</td>
<td></td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Initialization</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Periodicity</td>
<td>Periodic</td>
<td></td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Self-diagnostic capabilities can be embedded in the software, according to the test implementation design strategy chosen. The adoption of checksum protection on results variables and defensive programming are recommended</td>
<td></td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_5 : external watchdog</td>
<td></td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>This method is the main asset in STM32F3 Series safety concept. CPU integrity is a key factor, given that the major part of defined diagnostics for MCU peripherals are software-based</td>
<td></td>
</tr>
</tbody>
</table>

Table 6. CPU_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
<th>CPU_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Control flow monitoring in application software</td>
<td></td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
<td></td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The different internal states of the application software is well documented and described (the use of a dynamic state transition graph is encouraged).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The monitoring of the correctness of each transition between different states of the application software is implemented.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The transition through all expected states during the normal application software program loop is checked.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The use of the window feature of the independent watchdog (IWDG) (or an external one) helps to implement a more robust control flow mechanism fed by a different clock source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
<td></td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation. Higher value is fixed by watchdog timeout interval.</td>
<td></td>
</tr>
<tr>
<td>SM CODE</td>
<td>CPU_SM_1</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
<td></td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
<td></td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
<td></td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
<td></td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

**Table 7. CPU_SM_2**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CPU_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Double computation in application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| Detailed implementation | A timing redundancy for safety-related computation is considered to detect transient faults affecting the Arm® Cortex®-M4 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 MCU 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 | 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 8. CPU_SM_3**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CPU_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Arm® Cortex®-M4 HardFault exceptions</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>HardFault exception raise is an intrinsic safety mechanism implemented in Arm® Cortex®-M4 core, mainly devoted 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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>High-priority interrupt event</td>
</tr>
</tbody>
</table>
### Table 9. CPU_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CPU_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Stack hardening for application software</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>On demand</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>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</td>
</tr>
</tbody>
</table>

### Table 10. CPU_SM_5

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CPU_SM_5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>External watchdog</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
</tbody>
</table>
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 Assumed safety requirements.

It also contributes to reduce potential common cause failures, because the external watchdog is clocked and supplied independently from the STM32F3 Series.

Error reporting
- Depends on implementation

Fault detection time
- Depends on implementation (watchdog timeout interval)

Addressed fault model
- Permanent and Transient

Dependency on MCU 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 faults 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).

---

### Table 11. CPU_SM_6

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_SM_6</td>
<td>Independent watchdog</td>
</tr>
</tbody>
</table>

| Ownership | ST                                               |

<table>
<thead>
<tr>
<th>Detailed implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset signal generation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fault detection time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depends on implementation (watchdog timeout interval)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Addressed fault model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dependency on MCU configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initialization</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWDG activation. It is recommended to use the “Hardware watchdog” in Option byte settings (IWDG is automatically enabled after reset)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Periodicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test for the diagnostic</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDG_SM_1: Software test for watchdog at startup</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiple faults protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_SM_1: control flow monitoring in application software</td>
</tr>
<tr>
<td>WDG_SM_0: periodical read-back of configuration registers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendations and known limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

---

### Table 12. CPU_SM_7

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_SM_7</td>
<td>MPU - Memory protection Unit</td>
</tr>
</tbody>
</table>

| Ownership | ST                                               |

---

Table 11. CPU_SM_6

Table 12. CPU_SM_7
### Detailed implementation

The CPU Memory Protection Unit is able to detect illegal access to protected memory areas, according to End user programmed criteria.

### 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 MCU configuration

MPU available only on specific part numbers

### Initialization

MPU registers shall be programmed at start-up

### Periodicity

On line

### Test for the diagnostic

Not needed

### Multiple faults 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 expected to be not relevant in the framework of STM32F3 Series safety concept.

### Table 13. MPU_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>MPU_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of MPU configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>MPU available only on specific part numbers</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>
3.6.2 Embedded FLASH memory

Table 14. FLASH_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical software test for Flash memory</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user or ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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)</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Flash size changes according part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Memory signatures must be stored in Flash as well</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Periodic</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen</td>
</tr>
</tbody>
</table>
| Multiple faults 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 CRC module is recommended. In principle DMA feature for data transfer can be used.  
Unused Flash sections can be excluded from testing |

Table 15. FLASH_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Control flow monitoring in application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 MCU configuration | None |
| Initialization | Depends on implementation |
### Table 16. FLASH_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Arm® Cortex®-M4 HardFault exceptions</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>Hardware random faults (both permanent and transient) affecting system Flash (memory cells, address decoder) can lead to wrong instruction codes fetches, and eventually to the intervention of the Arm® Cortex®-M4 HardFault exceptions. Refer to CPU_SM_3 for detailed description</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CPU_SM_3</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CPU_SM_3</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CPU_SM_3</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CPU_SM_3</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CPU_SM_3</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

### Table 17. FLASH_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Option byte write protection</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Write protection exception</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>None (Systematic only)</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Not needed (enabled by default)</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
### Table 18. FLASH_SM_4

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

### Table 19. FLASH_SM_5

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Option byte redundancy with load verification</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>During option byte loading after each power-on reset, the bit-wise complementarity of the option byte and its corresponding complemented option byte is verified. Mismatches are reported as error</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Option byte error (OPTERR) generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>None (always enabled)</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Startup</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

### Table 20. FLASH_SM_6

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Flash unused area filling code</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>Used Flash 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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>NA</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>NA</td>
</tr>
<tr>
<td>SM CODE</td>
<td>FLASH_SM_6</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>None (Fault avoidance)</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>NA</td>
</tr>
<tr>
<td>Periodicity</td>
<td>NA</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>NA</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Filling code can be made of NOP instructions, or an illegal code that leads to a HardFault exception raise</td>
</tr>
</tbody>
</table>

**Table 21. FLASH_SM_8**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FLASH_SM_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Read protection (RDP), Write protection (WRP)</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to functional documentation - in some cases an HardFault error is generated</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Systematic</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Not needed</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Not needed</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Hardware random-failure detection capability for Flash access policy is restricted to well-selected marginal failure modes, mainly affecting program counter and Flash interface functions. The associated diagnostic coverage is therefore expected to be not relevant in the framework of STM32F3 Series safety concept</td>
</tr>
</tbody>
</table>
### Embedded SRAM

Table 22. RAM_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical software test for SRAM memory</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user or ST</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>RAM size can change according to the part number</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Periodic</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Self-diagnostic capabilities can be embedded in the software, according the test implementation design strategy chosen</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>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</td>
</tr>
</tbody>
</table>

Table 23. RAM_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Parity on SRAM</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>ST</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>Internal SRAM is protected by additional parity bits (1 bit per byte). The parity bits are computed and stored when writing into the SRAM</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Error bit flag set SYSCFG_CFGR2 NMI raise</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Parity bits are checked during a reading.</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>Parity protection available only on specific part numbers.</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>The end user shall enable the parity check using the option bit SYSCFG_CFGR2, after the boot</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>DIAG_SM_0: Periodical read-back of hardware diagnostics configuration registers</td>
</tr>
</tbody>
</table>
Recommendations and known limitations

It is advised to initialize by software the whole SRAM memory at application software startup, to avoid getting parity errors when reading non-initialized locations.

Being parity protection restricted to SRAM, End user is encouraged to store all safety-related data in SRAM (if possible), in order to get benefit of such additional hardware-based fast diagnostic.

Table 24. RAM_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Stack hardening for application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CPU_SM_4</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to CPU_SM_4</td>
</tr>
</tbody>
</table>

Table 25. RAM_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy for safety-related variables in application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 (like CRC) |
| Error reporting | Depends on implementation |
| Fault detection time | Depends on implementation |
| Addressed fault model | Permanent and Transient |
| Dependency on MCU configuration | None |
### Table 26. RAM_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Control flow monitoring in application software</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation. Higher value is fixed by watchdog timeout interval.</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>NA</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Needed just in case of application software execution from SRAM. CPU_SM_1 correct implementation supersedes this requirement</td>
</tr>
</tbody>
</table>

### Table 27. RAM_SM_5

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RAM_SM_5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical integrity test for application software in RAM</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Periodic</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Self-diagnostic capabilities can be embedded in the software, according to the test implementation design strategy chosen.</td>
</tr>
</tbody>
</table>
### Multiple faults 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
### 3.6.4 System bus architecture

#### Table 28. BUS_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>BUS_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical software test for interconnections</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>The intra-chip connection resources (Bus Matrix, AHB or APB bridges) needs to be periodically tested for permanent faults detection. Note that STM32F3 Series MCUs 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, the method is considered able to achieve high levels of coverage</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Periodic</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Implementation can be considered in large part overlapping with the widely used “Periodical readback of configuration registers” required for several peripherals</td>
</tr>
</tbody>
</table>

#### Table 29. BUS_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>BUS_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Information redundancy in intra-chip data exchanges</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>This method requires to add some kind of redundancy (e.g. a CRC checksum at packet level) to each data message exchanged inside the MCU. Message integrity is verified using the checksum by the application software, before consuming data.</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>On demand</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Implementation can be in large part overlapping with other safety mechanisms requiring information redundancy on data messages for communication peripherals. Optimizations are therefore possible</td>
</tr>
</tbody>
</table>
### Table 30. LOCK_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>LOCK_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lock mechanism for configuration options</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>The STM32F3 Series MCUs 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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Not generated (when locked, register overwrites are just ignored)</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>NA</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>None (Systematic only)</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Not needed</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>No DC associated because this test addresses systematic faults</td>
</tr>
</tbody>
</table>
3.6.5 EXTI controller

Table 31. NVIC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>NVIC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>

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 the state of the art automotive safety standard ISO26262, this method can achieve high levels of Diagnostic Coverage (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

Fault detection time

Depends on implementation

Addressed fault model

Permanent and Transient

Dependency on MCU 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 faults 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 32. NVIC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>NVIC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Expected and unexpected interrupt check</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
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 list of the implemented interrupt for the MCU are well documented, reporting also the expected frequency of each request when possible (for example the interrupts related to ADC conversion completion, therefore coming on a deterministic way).
- 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.

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>NVIC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed implementation</td>
<td>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:</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
3.6.6 Direct memory access controller (DMA)

Table 33. DMA_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DMA_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 34. DMA_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DMA_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy on data packet transferred via DMA</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method is implemented adding to data packets transferred by DMA a redundancy check (like a 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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>To give an example about checksum encoding capability, using just a bit-by-bit addition is unappropriate</td>
</tr>
</tbody>
</table>

Table 35. DMA_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DMA_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy including sender or receiver identifier on data packet transferred via DMA</td>
</tr>
</tbody>
</table>
### Table 36. DMA_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DMA_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical software test for DMA</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Incomplete packed transfer</td>
</tr>
<tr>
<td></td>
<td>• Errors in single transferred word</td>
</tr>
<tr>
<td></td>
<td>• Wrong order in packed transmitted data</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Periodic</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>None</td>
</tr>
</tbody>
</table>
## Table 37. DMA_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DMA_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>DMA transaction awareness</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>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</td>
</tr>
</tbody>
</table>
3.6.7 Controller area network (CAN)

Table 38. CAN_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CAN_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 39. CAN_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CAN_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Protocol error signals</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Several error condition are reported by flag bits in related CAN registers.</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CAN_SM_2: Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 40. CAN_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CAN_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
This method aims to protect the communication between a peripheral and its 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)

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CAN_SM_2</th>
</tr>
</thead>
</table>
| Detailed implementation | This method aims to protect the communication between a peripheral and its 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 MCU 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 receiver/transmitter (USART) 1/2/3/4/5

**Table 41. UART_SM_0**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>UART_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>USART availability depends on part number</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

**Table 42. UART_SM_1**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>UART_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Protocol error signals</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>ST</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>USART availability depends on part number</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not required</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>UART_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>USART communication module is fitted by several different configurations – the actual composition of communication error checks depends on selected configuration</td>
</tr>
</tbody>
</table>

**Table 43. UART_SM_2**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>UART_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Information redundancy techniques on messages</td>
</tr>
</tbody>
</table>


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 MCU configuration: USART availability depends on part number

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 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 44. UART_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>UART_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method aims to protect the communication between a peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>USART availability depends on part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
3.6.9 Inter-integrated circuit (I2C) 1/2

Table 45. IIC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>IIC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 46. IIC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>IIC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Protocol error signals</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>IIC_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Adoption of SMBus option grants the activation of more efficient protocol-level hardware checks like CRC-8 packet protection</td>
</tr>
</tbody>
</table>

Table 47. IIC_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>IIC_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
This method is implemented adding to data packets transferred by I2C 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 MCU 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 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 superseded by IIC_SM_3 if hardware handled CRC insertion is possible.

Table 48. IIC_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>IIC_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>CRC packet-level</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>I2C communication module allows to activate for specific mode of operation (SMBus) the automatic insertion (and check) of CRC checksums to packet data.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>IIC_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 49. IIC_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>IIC_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method aims to protect the communication between a I2C peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information.</td>
</tr>
<tr>
<td>SM CODE</td>
<td>IIC_SM_4</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
### 3.6.10 Serial peripheral interface (SPI) 1/2/3/4

#### Table 50. SPI_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SPI_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 51. SPI_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SPI_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Protocol error signals</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>SPI communication module embeds protocol error checks (like overrun, underrun, timeout 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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>SPI_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Table 52. SPI_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SPI_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
This method is implemented adding to data packets transferred by SPI 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 MCU 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 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 superseded by SSP_SM_3 if hardware handled CRC insertion is possible.

### Table 53. SPI_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SPI_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>CRC packet-level</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>SPI communication module allows to activate automatic insertion (and check) of CRC-8 or CRC-18 checksums to packet data</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>SPI_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

### Table 54. SPI_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SPI_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method aims to protect the communication between SPI peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information.</td>
</tr>
<tr>
<td>SM CODE</td>
<td>SPI_SM_4</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
3.6.11 USB on-the-go full-speed (OTG_FS)

Table 55. USB_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Periodical read-back of configuration registers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>End user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Detailed implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Error reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Fault detection time</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Addressed fault model</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Dependency on MCU configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Initialization</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Periodicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Test for the diagnostic</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Not needed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Multiple faults protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>USB_SM_2: Information redundancy techniques on messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Recommendations and known limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_0</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 56. USB_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Protocol error signals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>ST</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Detailed implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Error reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Fault detection time</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Depends on peripheral configuration (e.g. baud rate), refer to functional documentation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Addressed fault model</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Permanent and Transient</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Dependency on MCU configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Initialization</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Depends on implementation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Periodicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Test for the diagnostic</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>Not needed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Multiple faults protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>USB_SM_2: Information redundancy techniques on messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Recommendations and known limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_1</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 57. USB_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_2</td>
<td>Information redundancy techniques on messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_2</td>
<td>ST or end user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Detailed implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB_SM_2</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 MCU 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 58. USB_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>USB_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method aims to protect the communication between an USB peripheral and his external counterpart. Refer to CAN_SM_2 description for detailed information</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to CAN_SM_2</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
3.6.12 Touch sensing controller (TSC)

Table 59. TSC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>TSC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to TSC configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 60. TSC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>TSC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Multiple acquisition by application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method implements a timing information redundancy by executing multiple acquisitions on TSC input data. Multiple acquisition data are then used to determine the acquisition correct state. This method overlaps on the native features of the TSC module of counting events in order to ensure a stable acquisition against external noise</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 61. TSC_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>TSC_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Application-level detection of permanent failures of TSC acquisition</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must detect TSC module permanent failure leading to wrong or missing acquisition of touch sensing events.</td>
</tr>
<tr>
<td>SM CODE</td>
<td>TSC_SM_2</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Periodic</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: Periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Due to the nature strictly application-dependent of this solution, no detailed guidelines for its implementation are given here. Being not possible a solution fully based on microcontroller resources, leveraging on the contribution from other components of the final system is necessary</td>
</tr>
</tbody>
</table>
3.6.13 Analog-to-digital converters (ADC)

Table 62. ADC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ADC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 63. ADC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ADC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Multiple acquisition by application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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 disturbson sensor lines</td>
</tr>
</tbody>
</table>

Table 64. ADC_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ADC_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Range check by application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
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.

### Table 65. ADC_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ADC_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical software test for ADC</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>The method is implemented acquiring multiple signals and comparing the read value with the expected one, supposed to be known. Method can be implemented with different level of complexity:</td>
</tr>
<tr>
<td></td>
<td>• Basic complexity: acquisition and check of upper or lower rails (VDD or VSS) and internal reference voltage</td>
</tr>
<tr>
<td></td>
<td>• High complexity: in addition to basic complexity tests, acquisition of a DAC output connected to ADC input and checking all voltage excursion and linearity</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Periodic</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Combination of two different complexity method can be used to better optimize test frequency in high demand safety functions</td>
</tr>
</tbody>
</table>
Table 66. ADC_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ADC_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1oo2 scheme for ADC inputs</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This safety mechanism is implemented using two different SAR ADC channels to acquire the same input signal. The application software checks the coherence between the two readings. It is recommended to use two different ADC modules belonging to different ADC modules</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU config</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>ADC_SM_0: Periodical read-back of ADC configuration registers</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
### 3.6.14 Digital-to-analog converter (DAC)

#### Table 67. DAC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DAC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 68. DAC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DAC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>DAC output loopback on ADC channel</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>Implementation is realized by routing the active DAC output to one ADC channel, and by checking the output current value with his expected one</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous or on demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>
### 3.6.15 Comparator (COMP)

**Table 69. COMP_SM_0**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>COMP_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to COMP configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

**Table 70. COMP_SM_1**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>COMP_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1oo2 scheme for comparator</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This safety mechanism is implemented using the two internal comparators to take the same decision. It requires that the comparator voting is handled accordingly</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>This method is not compatible with “window” comparator feature</td>
</tr>
</tbody>
</table>

**Table 71. COMP_SM_2**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>COMP_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Plausibility check on inputs</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method is used to redundantly acquire on dedicated ADC channels the analog inputs that are subjected to comparator function, and to periodically check the coherence of the comparator output on the measured values</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
</tbody>
</table>
Table 72. COMP_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>COMP_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Multiple acquisition by application software</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method requires that application software takes a decision not on the basis of a comparator single-shot transition, but after multiple events or after the permanence of comparator trigger conditions for a certain amount of time</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>It is highly probable that this recommendation is satisfied by design on end user application - multiple acquisition is a common technique in industrial applications where it is needed to survive with spurious EMI disturbs on sensor lines</td>
</tr>
</tbody>
</table>

Table 73. COMP_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>COMP_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Comparator Lock mechanism</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This safety mechanism prevents configuration changes for comparator control and status registers; it addresses therefore systematic faults in the software application</td>
</tr>
<tr>
<td>Error reporting</td>
<td>NA</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>NA</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>None (Fault avoidance)</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Lock protection must be enabled using COMPxLOCKbits in COMP_CSR register</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>NA</td>
</tr>
</tbody>
</table>
Recommendations and known limitations

This method does not address comparator configuration changes due to soft-errors.

### 3.6.16 Basic timers TIM 6/7

#### Table 74. GTIM_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>GTIM_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>This method must be applied to general purpose counter timer TIM6 or TIM7 configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 75. GTIM_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>GTIM_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>1oo2 for counting timers</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
</tbody>
</table>
| **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 MCU 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 |
3.6.17 Advanced, general and low-power timers TIM1/2/3/4/5/8/12/13/14/15/16/17/18/19/20

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 76. ATIM_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to advanced, general and low-power timers TIM1/2/3/4/5/8/9/10/11/12/13/14 configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Timers availability differs according to specific part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

### Table 77. ATIM_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1oo2 for counting timers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 |
<p>| Error reporting | Depends on implementation |
| Fault detection time | Depends on implementation |
| Addressed fault model | Permanent and Transient |
| Dependency on MCU configuration | Timers availability differs according to specific part number |
| Initialization | Depends on implementation |
| Periodicity | On demand |
| Test for the diagnostic | Not needed |</p>
<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>

**Table 78. ATIM_SM_2**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1oo2 for input capture timers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Timers availability differs according to specific part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>

**Table 79. ATIM_SM_3**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Loopback scheme for PWM outputs</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 MCU configuration | Timers availability differs according to specific part number |
## ATIM_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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</td>
</tr>
</tbody>
</table>

## ATIM_SM_4

Table 80. ATIM_SM_4

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>ATIM_SM_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Lock bit protection for timers</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>NA</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>NA</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>None (Fault avoidance)</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Timers availability differs according to specific part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Lock protection must be enabled using LOCK bits in the TIMx_BDTR register</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>NA</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>This method does not addresses timer configuration changes due to soft-errors</td>
</tr>
</tbody>
</table>
3.6.18 General-purpose input/output (GPIO) - port A/B/C/D/E/F/G/H

Table 81. GPIO_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>GPIO_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>GPIO availability can differ according to part number</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 82. GPIO_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>GPIO_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1oo2 for input GPIO lines</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
</tbody>
</table>
| 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 PORTA.1 and PORTB.5)  
• Mapped to non-adjacent pins on the device package |

Table 83. GPIO_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>GPIO_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Loopback scheme for output GPIO lines</td>
</tr>
</tbody>
</table>
**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 MCU configuration** | None
**Initialization** | Depends on implementation
**Perodicity** | Continuous
**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 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 number (for instance PORTA.1 and PORTB.5)
- 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

---

**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 MCU configuration** | None
**Initialization**
The correct write sequence must be applied to bit 16 (LCKK) of GPIOx_LCKR after the final GPIO configuration has been written by the application software.

**Perodicity** | Continuous
**Test for the diagnostic** | Not needed
**Multiple faults 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

---

**Table 84. GPIO_SM_3**
### 3.6.19 Real-time clock module (RTC)

#### Table 85. RTC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RTC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 86. RTC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RTC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Application check of running RTC</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 retrieval).  
  • 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 MCU configuration | None |
| Initialization | Depends on implementation |
| Periodicity | Periodical |
| Test for the diagnostic | Not needed |
| Multiple faults protection | CPU_SM_0: periodical core self-test software |
| 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 (e.g. medical data storage devices), it is strongly recommended to adopt more efficient system-level measures |
### Table 87. RTC_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RTC_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy on backup registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Implementation of this safety method shows a partial overlap with an already foreseen method for Cortex®-M4 (CPU_SM_1); optimizations in implementing both methods are therefore possible</td>
</tr>
</tbody>
</table>

### Table 88. RTC_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>RTC_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Application-level measures to detect failures in timestamps/event capture</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Periodic/On demand</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: Periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>This method must be used only if the timestamps/event capture function is used in the safety function implementation. It is worth to note that the use of timestamp/event capture in safety related applications where the MCU is in sleep or stop mode is prevented by the assumed requirement ASR7 (refer to Section 3.3.1 Assumed safety requirements)</td>
</tr>
</tbody>
</table>
### 3.6.20 Power control

#### Table 89. VSUP_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>VSUP_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>This method must be applied to configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 90. VSUP_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>VSUP_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Supply voltage internal monitoring (PVD)</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>ST</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Interrupt Event generation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on threshold programming, refer to functional documentation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Protection enable by PVDE bit and threshold programming in Power control register (PWR_CR)</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>VSUP_SM_0: periodical read-back of configuration registers</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_5: external watchdog</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>Internal monitoring PVD has limited capability to address failures related to wrong VDD values. It can be integrated by VSUP_SM_4 (PVM) in case specific power schemes are implemented (i.e. some independent supplies directly connected to VDD, allowing to use PVD and PVM to control high and low thresholds for VDD). Internal monitoring PVD has limited capability to address failures affecting STM32F3 Series internal voltage regulator. Refer to device FMEA for details</td>
</tr>
</tbody>
</table>

#### Table 91. VSUP_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>VSUP_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Independent watchdog</td>
</tr>
</tbody>
</table>
### SM CODE VSUP_SM_2

<table>
<thead>
<tr>
<th>Ownership</th>
<th>ST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>The independent watchdog is fed directly by VDD; therefore, major failures in the power supplies for digital logic (core or peripherals) does not affect its behavior but may lead to a violation of the IDWG timeout</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Reset signal generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation (watchdog timeout interval)</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>IWDG activation. It is recommended to use the &quot;Hardware watchdog&quot; in Option byte settings (IWDG is automatically enabled after reset)</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_1: control flow monitoring in application software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>An external watchdog (refer to CPU_SM_5) can guarantee the same level of protection</td>
</tr>
</tbody>
</table>

### 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 MCU configuration | None |
| Initialization | None |
| Periodicity | Periodic |
| Test for the diagnostic | Not needed |
| Multiple faults protection | VSUP_SM_3: Supply voltage internal monitoring (PVD) |
| 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 92. VSUP_SM_3**
### 3.6.21  Reset and clock control (RCC) subsystem

#### Table 93. CLK_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK_SM_0</td>
<td>Periodical read-back of configuration registers</td>
</tr>
</tbody>
</table>

#### 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

#### 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 MCU 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 94. CLK_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK_SM_1</td>
<td>Clock security system (CSS)</td>
</tr>
</tbody>
</table>

#### Ownership

ST

#### Detailed implementation

The clock security system (CSS) detects the loss of HSE clock activity and executes the corresponding recovery action, such as:

- Switch-off HSE
- Commutation on the HIS
- Generation of related NMI

#### Error reporting

NMI

#### Fault detection time

Depends on implementation (clock frequency value)

#### Addressed fault model

Permanent and Transient

#### Dependency on MCU configuration

None

#### Initialization

CSS protection must be enabled on Clock interrupt register (RCC_CIR) after boot stabilization

#### Periodicity

Continuous

#### Test for the diagnostic

CLK_SM_0: periodical read-back of configuration registers

#### Multiple faults 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 correct managing the faulty situation by application software features

#### Table 95. CLK_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK_SM_2</td>
<td>Independent watchdog</td>
</tr>
</tbody>
</table>
### SM CODE CLK_SM_2

<table>
<thead>
<tr>
<th>Ownership</th>
<th>ST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed implementation</td>
<td>The independent watchdog IWDG is able to detect failures in internal main MCU clock (lower frequency)</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Reset signal generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation (watchdog timeout interval)</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>IWDG activation. It is recommended to use the “Hardware watchdog” in Option byte settings (IWDG is automatically enabled after reset)</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_1: control flow monitoring in application software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>In case of usage of IWDG window option, end user must consider possible tolerance in application software execution, to avoid false error reports (affecting system availability)</td>
</tr>
</tbody>
</table>

### SM CODE CLK_SM_3

<table>
<thead>
<tr>
<th>Description</th>
<th>Internal clock cross-measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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 be therefore detected.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Periodic</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_1: control flow monitoring in application software CPU_SM_5: external watchdog</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Efficiency versus transient faults is negligible. It provides only medium efficiency in permanent clock-related failure mode coverage</td>
</tr>
</tbody>
</table>
### 3.6.22 Independent watchdog (IWDG), system window watchdog (WWDG)

#### Table 97. WDG_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>WDG_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to WDG or WDG configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 98. WDG_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>WDG_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Software test for watchdog at startup</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Startup (see below)</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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.</td>
</tr>
</tbody>
</table>
3.6.23 Debug

Table 99. DBG_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DBG_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Independent watchdog</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Reset signal generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation (watchdog timeout interval)</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_1: control flow monitoring in application software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>
### 3.6.24 Cyclic redundancy-check module (CRC)

Table 100. **CRC_SM_0**

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>CRC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>CRC self-coverage</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>CPU_SM_0: periodical core self-test software</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>
### 3.6.25 System configuration controller (SYSCFG)

#### Table 101. SYSCFG_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>SYSCFG_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>This method is mainly overlapped by several other “configuration register read-back” required for other MCU peripherals. It is reported here for the sake of completeness</td>
</tr>
</tbody>
</table>

#### Table 102. DIAG_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DIAG_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of hardware diagnostics configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>In STM32F3 Series several hardware-based efficient safety mechanisms (e.g. ECC on Flash) are available. This method shall be applied to any configuration register related to diagnostic measure operations, including error reporting. End user shall therefore individuate configuration registers related to: • Hardware diagnostic enable • Interrupt/NMI enable (if used for diagnostic error management)</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>
### Flexible static memory controller (FSMC)

#### Table 103. FSMC_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FSMC_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Control flow monitoring in application software</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation. Higher value is fixed by watchdog timeout interval</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>FSMC interface is available only on selected part numbers</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>Continuous</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: Periodical core self test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>This mechanism must be used just if FSMC external memory is used to store executable programs</td>
</tr>
</tbody>
</table>

#### Table 104. FSMC_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FSMC_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Information redundancy on external memory connected to FSMC</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>End user</td>
</tr>
<tr>
<td><strong>Detailed implementation</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Error reporting</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Fault detection time</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Addressed fault model</strong></td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td><strong>Dependency on MCU configuration</strong></td>
<td>FSMC interface is available only on selected part numbers</td>
</tr>
<tr>
<td><strong>Initialization</strong></td>
<td>Depends on implementation</td>
</tr>
<tr>
<td><strong>Periodicity</strong></td>
<td>On demand</td>
</tr>
<tr>
<td><strong>Test for the diagnostic</strong></td>
<td>Not needed</td>
</tr>
<tr>
<td><strong>Multiple faults protection</strong></td>
<td>CPU_SM_0: Periodical core self test software</td>
</tr>
<tr>
<td><strong>Recommendations and known limitations</strong></td>
<td>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</td>
</tr>
</tbody>
</table>
### Table 105. FSMC_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FSMC_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of FSMC configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>FSMC interface is available only on selected part numbers</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

### Table 106. FSMC_SM_3

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FSMC_SM_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>ECC engine on NAND interface in FSMC module</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to functional documentation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>ECC bits are checked during a memory reading</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and Transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>FSMC interface is available only on selected part numbers</td>
</tr>
<tr>
<td>Initialization</td>
<td>None</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>FSMC_SM_2: Periodical read-back of FSMC configuration registers</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>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 STM32F3 Series MCU</td>
</tr>
</tbody>
</table>
### 3.6.27 High-definition multimedia interface (HDMI-CEC)

#### Table 107. HDMI_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>HDMI_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to HDMI CEC configuration registers. Detailed information on the implementation of this method can be found in section NVIC_SM_0.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

#### Table 108. HDMI_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>HDMI_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Protocol error signals</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>The HDMI 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.</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Error flag raise and optional Interrupt Event generation</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on peripheral configuration (for instance baud rate), refer to functional documentation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent and transient</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>None</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Not needed</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>HDMI_SM_2: Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Table 109. HDMI_SM_2

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>HDMI_SM_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information redundancy techniques on messages</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
### Detailed implementation

This method is implemented adding to data packets transferred by HDMI or CEC 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 MCU 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 remote HDMI or 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.
### Operational amplifiers (OPAMP)

Table 110. AMP_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>AMP_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of OPAMP configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to OPAMP configuration registers.</td>
</tr>
<tr>
<td></td>
<td>Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU config</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

**Note:** Because OPAMP modules are expected to be used in signal conditioning/amplification, their use in safety-related functions lead to an application level scenario. End user is therefore responsible for the mitigation of failure modes affecting the analog section of used OPAMP module(s).
3.6.29 Digital camera interface (DCMI)

Table 111. DCMI_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DCMI_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of DCMI configuration registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>This method must be applied to DCMI configuration registers. Detailed information on the implementation of this method can be found in Section 3.6.5</td>
</tr>
<tr>
<td>Error reporting</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>DCMI interface is available only on selected part numbers</td>
</tr>
<tr>
<td>Initialization</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>Refer to NVIC_SM_0</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>Refer to NVIC_SM_0</td>
</tr>
</tbody>
</table>

Table 112. DCMI_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>DCMI_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>DCMI video input data synchronization</td>
</tr>
<tr>
<td>Ownership</td>
<td>ST</td>
</tr>
<tr>
<td>Detailed implementation</td>
<td>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</td>
</tr>
<tr>
<td>Error reporting</td>
<td>No explicit error signal/message generation is provided (*)</td>
</tr>
<tr>
<td>Fault detection time</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Addressed fault model</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dependency on MCU configuration</td>
<td>DCMI interface is available only on selected part numbers</td>
</tr>
<tr>
<td>Initialization</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Periodicity</td>
<td>Continuous</td>
</tr>
<tr>
<td>Test for the diagnostic</td>
<td>N/A</td>
</tr>
<tr>
<td>Multiple faults protection</td>
<td>DCMI_SM_0: Periodical read-back of DCMI configuration registers</td>
</tr>
<tr>
<td>Recommendations and known limitations</td>
<td>(*) 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</td>
</tr>
</tbody>
</table>
3.6.30  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 113. FFI_SM_0

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FFI_SM_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Unused peripherals disable</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 MCU 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 114. FFI_SM_1

<table>
<thead>
<tr>
<th>SM CODE</th>
<th>FFI_SM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Periodical read-back of interference avoidance registers</td>
</tr>
<tr>
<td>Ownership</td>
<td>End user</td>
</tr>
</tbody>
</table>
| 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 functions programming registers  
Detailed information on the implementation of this method can be found in Section 3.6.5 |
| 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 MCU 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 |
3.7 Conditions of use

Table 115 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 STM32F3 Series MCUs 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 Table 115.

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 SIL2 on a single MCU.
- **+** = Recommended as additional safety measure, but not considered in this Safety Manual for the computation of safety metrics. STM32F3 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 Table 115, indicates that the related safety mechanism is effective for such fault model.

### Table 115. List of safety mechanisms

<table>
<thead>
<tr>
<th>STM32F3 Series function</th>
<th>Diagnostic</th>
<th>Description</th>
<th>Rank</th>
<th>Perm</th>
<th>Trans</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Arm® Cortex®-M4 CPU</strong></td>
<td>CPU_SM_0</td>
<td>Periodical software test addressing permanent faults in Arm® Cortex®-M4 CPU core</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_1</td>
<td>Control flow monitoring in application software</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_2</td>
<td>Double computation in application software</td>
<td>++</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_3</td>
<td>Arm® Cortex®-M4 HardFault exceptions</td>
<td>M</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_4</td>
<td>Stack hardening for application software</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_5</td>
<td>External watchdog</td>
<td>+ (1)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_6</td>
<td>Independent watchdog</td>
<td>++(1)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CPU_SM_7</td>
<td>MPU – Memory protection unit</td>
<td>++ (2)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MPU_SM_0</td>
<td>Periodical read-back of MPU configuration registers</td>
<td>++(2)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Embedded Flash memory</strong></td>
<td>FLASH_SM_0</td>
<td>Periodical software test for Flash memory</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_1</td>
<td>Control flow monitoring in application software</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_2</td>
<td>Arm® Cortex®-M4 HardFault exceptions</td>
<td>M</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_3</td>
<td>Option byte write protection</td>
<td>M</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_4</td>
<td>Static data encapsulation</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_5</td>
<td>Option byte redundancy with load verification</td>
<td>M</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_6</td>
<td>Flash unused area filling code</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FLASH_SM_8</td>
<td>Read/Write/Proprietary code protection</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>STM32F3 Series function</td>
<td>Diagnostic</td>
<td>Description</td>
<td>Rank</td>
<td>Perm</td>
<td>Trans</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Embedded SRAM</strong></td>
<td>RAM_SM_0</td>
<td>Periodical software test for SRAM memory</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>RAM_SM_1</td>
<td>Parity bit check</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RAM_SM_2</td>
<td>Stack hardening for application software</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RAM_SM_3</td>
<td>Information redundancy for system variables in application software</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RAM_SM_4</td>
<td>Control flow monitoring in application software</td>
<td>o</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RAM_SM_5</td>
<td>Periodical integrity test for application software in RAM</td>
<td>o</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>System architecture</strong></td>
<td>BUS_SM_0</td>
<td>Periodical software test for interconnections</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>BUS_SM_1</td>
<td>Information redundancy in intra-chip data exchanges</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>EXTI controller</strong></td>
<td>NVIC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>NVIC_SM_1</td>
<td>Expected and unexpected interrupt check by application software</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>DMA</strong></td>
<td>DMA_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>DMA_SM_1</td>
<td>Information redundancy on data packet transferred via DMA</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>DMA_SM_2</td>
<td>Information redundancy including sender or receiver identifier on data packet transferred via DMA</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>DMA_SM_3</td>
<td>Periodical software test for DMA</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>DMA_SM_4</td>
<td>DMA transaction awareness</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>bxCAN</strong></td>
<td>CAN_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CAN_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CAN_SM_2</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>USART</strong></td>
<td>UART_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>UART_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>UART_SM_2</td>
<td>Information redundancy techniques on messages</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>UART_SM_3</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>I2C</strong></td>
<td>IIC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>IIC_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>IIC_SM_2</td>
<td>Information redundancy techniques on messages</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>IIC_SM_3</td>
<td>CRC packet-level</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>IIC_SM_4</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>STM32F3 Series function</td>
<td>Diagnostic</td>
<td>Description</td>
<td>Rank</td>
<td>Perm</td>
<td>Trans</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>SPI</td>
<td>SPI_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>SPI_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>SPI_SM_2</td>
<td>Information redundancy techniques on messages</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>SPI_SM_3</td>
<td>CRC packet-level</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>SPI_SM_4</td>
<td>Information redundancy techniques on messages, including end-to-end Safing</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>USB OTG</td>
<td>USB_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>USB_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>USB_SM_2</td>
<td>Information redundancy techniques on messages</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>USB_SM_3</td>
<td>Information redundancy techniques on messages, including end-to-end safing</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>TSC</td>
<td>TSC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>TSC_SM_1</td>
<td>Multiple acquisition by application software</td>
<td>++</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>TSC_SM_2</td>
<td>Application-level detection of permanent failures of TSC acquisition</td>
<td>+</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>ADC</td>
<td>ADC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ADC_SM_1</td>
<td>Multiple acquisition by application software</td>
<td>++</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ADC_SM_2</td>
<td>Range check by application software</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ADC_SM_3</td>
<td>Periodical software test for ADC</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>ADC_SM_4</td>
<td>1oo2 scheme for ADC inputs</td>
<td>+</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>DAC</td>
<td>DAC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>DAC_SM_1</td>
<td>DAC output loopback on ADC channel</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>COMP</td>
<td>COMP_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>COMP_SM_1</td>
<td>1oo2 scheme for comparator</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>COMP_SM_2</td>
<td>Plausibility check on inputs</td>
<td>+</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>COMP_SM_3</td>
<td>Multiple acquisition by application software</td>
<td>+</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>COMP_SM_4</td>
<td>Comparator LOCK mechanism</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Basic timers TIM6/7</td>
<td>GTIM_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>GTIM_SM_1</td>
<td>1oo2 for counting timers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Advanced, general and low-power timers TIM1/2/3/4/5/8/12/13/14/15/16/17/18/19/20</td>
<td>ATIM_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ATIM_SM_1</td>
<td>1oo2 for counting timers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ATIM_SM_2</td>
<td>1oo2 for input capture timers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ATIM_SM_3</td>
<td>Loopback scheme for PWM outputs</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>ATIM_SM_4</td>
<td>Lock bit protection for timers</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CRC</td>
<td>CRC_SM_0</td>
<td>CRC self-coverage</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>STM32F3 Series function</td>
<td>Diagnostic</td>
<td>Description</td>
<td>Rank</td>
<td>Perm</td>
<td>Trans</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>GPIO</td>
<td>GPIO_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>GPIO_SM_1</td>
<td>1oo2 for input GPIO lines</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>GPIO_SM_2</td>
<td>Loopback scheme for output GPIO lines</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>GPIO_SM_3</td>
<td>GPIO port configuration lock register</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RTC</td>
<td>RTC_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RTC_SM_1</td>
<td>Application check of running RTC</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RTC_SM_2</td>
<td>Information redundancy on backup registers</td>
<td>+</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>RTC_SM_3</td>
<td>Application-level measures to detect failures in timestamps or event capture</td>
<td>o</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Power control</td>
<td>VSUP_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>VSUP_SM_1</td>
<td>Supply voltage monitoring</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>VSUP_SM_2</td>
<td>Independent Watchdog</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>VSUP_SM_3</td>
<td>Internal temperature sensor check</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Clock and Reset</td>
<td>CLK_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CLK_SM_1</td>
<td>CSS Clock Security System</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>CLK_SM_2</td>
<td>Independent Watchdog</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>CLK_SM_3</td>
<td>Internal clock cross-measure</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IWDG/WWDG</td>
<td>WDG_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>WDG_SM_1</td>
<td>Software test for watchdog at startup</td>
<td>o</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Debug</td>
<td>DBG_SM_0</td>
<td>Independent watchdog</td>
<td>++</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>System or peripheral control</td>
<td>LOCK_SM_0</td>
<td>Lock mechanism for configuration options</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>SYSCFG_SM_0</td>
<td>Periodical read-back of configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>DIAG_SM_0</td>
<td>Periodical read-back of hardware diagnostics configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Flexible static memory controller (FSMC)</td>
<td>FSMC_SM_0</td>
<td>Control flow monitoring in application software</td>
<td>++ (5)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FSMC_SM_1</td>
<td>Information redundancy on external memory connected to FSMC</td>
<td>++(5)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FSMC_SM_2</td>
<td>Periodical read-back of FSMC configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FSMC_SM_3</td>
<td>ECC engine on NAND interface in FSMC module</td>
<td>o</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>HDMI CEC</td>
<td>HDMI_SM_0</td>
<td>Periodical read-back of HDMI CEC configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>HDMI_SM_1</td>
<td>Protocol error signals</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>HDMI_SM_2</td>
<td>Information redundancy techniques on messages</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>OPAMP</td>
<td>AMP_SM_0</td>
<td>Periodical read-back of OPAMP configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>STM32F3 Series function</td>
<td>Diagnostic</td>
<td>Description</td>
<td>Rank</td>
<td>Perm</td>
<td>Trans</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>DCMI</td>
<td>DCMI_SM_0</td>
<td>Periodical read-back of DCMI configuration registers</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DCMI</td>
<td>DCMI_SM_1</td>
<td>DCMI video input data synchronization</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Part separation (no interference)</td>
<td>FFI_SM_0</td>
<td>Unused peripherals disable</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>FFI_SM_1</td>
<td>Periodical read-back of interference avoidance registers</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Arm® Cortex®-M4 CPU</td>
<td>CoU_1</td>
<td>The reset condition of Arm® Cortex®-M4 CPU must be compatible as valid safe state at system level</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Debug</td>
<td>CoU_2</td>
<td>STM32F3 Series debug features must not be used in safety function(s) implementation</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Arm® Cortex®-M4 / Supply system</td>
<td>CoU_3</td>
<td>Low power mode state must not be used in safety function(s) implementation</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>STM32F3 Series peripherals</td>
<td>CoU_4</td>
<td>End user must implement the required combination of safety mechanism/CoUs for each STM32 peripherals used in safety function(s) implementation</td>
<td>++</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Flash subsystem</td>
<td>CoU_5</td>
<td>During Flash bank mass erase and reprogramming there must not be safety functions(s) executed by STM32F3 Series MCU.</td>
<td>++</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CPU subsystem</td>
<td>CoU_7</td>
<td>In case of multiple safety functions implementations, methods to guarantee their mutual independence must include MPU use.</td>
<td>++(6)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

1. To achieve SIL2 on a single MCU, method CPU_SM_5 is rated as “+”. Anyway, in case of specific definition for system-level safe state, it can be necessary to rate CPU_SM_5 as ++; in that case CPU_SM_6 can be rated as “+”. Refer to the “Recommendations” row of Table 7 for more details.

2. Can be considered ranked as “+” if no multiple safety functions are implemented.

3. For STM32F3 Series part number not implementing parity on SRAM, this method is not necessary

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.

6. This Condition of Use implicitly excludes multiple safety functions implementation by STM32F3 Series part numbers not including MPU feature.

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 a safety point of view by a failure on these modules. Because these modules are used by every end user application, related methods or safety mechanism are mainly conceived to be application-independent. For STM32F3 Series microcontroller system critical modules are: CPU, Reset, Power, Clocks, Busmatrixs and Interconnect, Flash and RAM memories (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 STM32F3 Series MCUs, 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 STM32F3 Series devices reported in this Safety Manual is executed according to ST methodology flow for safety analysis of semiconductor devices according IEC61508. The accuracy of results obtained are guaranteed by three factors:

- ST 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 injections methods and tools for safety metrics verification

The STM32F3 Series safety analysis has been therefore able to explore the overall and exhaustive list of MCU failure modes, and to individuate for each of them an adequate mitigation measure (safety mechanism). The overall list of STM32F3 Series failure modes is maintained in related FMEA document. STM32F3 Series FMEA document can be provided on demand, refer to your local ST sales contact.

In summary, with the adoptions 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>
<thead>
<tr>
<th>MCUs used</th>
<th>Safety architecture</th>
<th>Target</th>
<th>Safety analysis result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1oo1/1oo1D</td>
<td>SIL2 LD</td>
<td>Achievable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIL2 HD/CM</td>
<td>Achievable with potential performance impact (1)</td>
</tr>
<tr>
<td>2</td>
<td>1oo2</td>
<td>SIL3 LD</td>
<td>Achievable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIL3 HD/CM</td>
<td>Achievable with potential performance impact</td>
</tr>
</tbody>
</table>

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 Assumed safety requirements).

The resulting relative safety metrics (DC and SFF) and absolute safety metrics (PFH, PFD) are not reported in this section but in the FMEDA snapshot, due to:

- The large number of STM32F3 Series part numbers,
- The possibility to declare non-safety-relevant unused peripherals, and
- The 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 MCU target part number.

Note: Safety metrics computations are restricted to STM32F3 Series boundary, therefore not including the WDTe, PEv and VMONE (they are described in Assumed safety requirements).

4.1.1 Safety analysis results customization

The safety analysis executed for STM32F3 Series devices and contained in this Safety Manual considers all microcontroller modules to be safety related, and so 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 as “safe” as per IEC61508-4, 3.6.8, and therefore all microcontroller modules are included in SFF computations.
In actual end-user applications, not all the STM32F3 Series parts or modules are used for the implementation of the safety function. That can happen under two possible alternative conditions:

- The part is not used at all (disabled).
- The part is used for the implementation of a function that is non-safety related (for example a GPIO line driving a "power-on" signaling led on an electronic board).

Requiring the implementation of the respective safety mechanism for those unused parts could result in an overkill. The safety analysis results can therefore be customized.

The end user can define the selected STM32F3 Series parts as “non-safety related” under the following conditions (end user responsibility):

- Collect rationales and evidences that the parts play no role in safety function implementation.
- Collect rationales and evidences that the parts do not interfere with the safety function during normal operation due to final system design decisions.
- Fulfill the below-reported general condition for the mitigation of the intra-MCU interferences (Table 117. List of general requirements for FFI).

The end user is therefore allowed for “non-safety related” parts to do the following:

- Discard the part contribution from metrics computations in FMEDA;
- Do not implement the related safety mechanisms listed in section Conditions of use.

With regard to SFF computation, this procedure is equivalent to declare "no part/no effect" as per IEC61508-4, 3.6.13 or 14 definition any failure of discarded modules.

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 STM32F3 Series internal modules in case of internal failures (freedom from interferences, FFI). These precautions are integral part of the STM32F3 Series safety concept and they can play a relevant role when multiple microcontroller modules are declared as “non-safety related” by the end user as per Section 4.1.1 Safety analysis results customization.

The requirement for the end user is to implement the safety mechanism listed in Table 117. List of general requirements for FFI (implementation details can be found in Description of hardware and software diagnostics) despite any evaluation about their contribution for the safety metrics computations.

### Table 117. List of general requirements for FFI

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

1. To be implemented only if DMA is actually used

4.1.3 Notes on multiple faults scenario

In principle, IEC61508 requires to analyze multiple faults scenarios, therefore restrictions to one fault at time conditions could be not acceptable. Accordingly, the safety analysis for STM32F3 Series took into consideration also multiple faults scenarios. Furthermore, following the spirit of ISO26262 (the reference and state-of-art standard norm for integrated circuit safety analysis) the analysis investigated faults able to "disable" each safety mechanism, in order to individuate mitigation measure for such condition. Section 3.6 tables report on the
“Multiple faults protection” field the associated safety mechanisms needed to correctly manage a multi-fault scenario, including mitigation measures against safety mechanism disable.

It is strongly recommended to include into the safety concept the implementation of such mitigation measures. This is more relevant for long-term operating systems, where error accumulation issues must be considered.

4.2 Dependent failures analysis

The analysis of dependent failures is important for microcontrollers. The main sub-classes of dependent failures are the Common Cause Failures (CCF). 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 ICs with one common semiconductor substrate. However, annexes E.1 and E.2 apply for HFT=1 while the Annex E.3 must be applied to every on-chip redundancy, intended also in terms of diagnostic implemented on the same silicon.

As there are no on-chip redundancy on STM32F3 Series devices, the CCF quantification through the BetaIC computation method is not required. Note that in the case of 1oo2 safety architecture implementation, the end user is required to evaluate the parameter βD, which is the measure of the common-cause between the two channels used in PFH computation.

The STM32F3 Series 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 detail in Section 3.6 Description of hardware and software diagnostics.

4.2.1 Power supply

Power supply is a potential source of dependent failures, because any alteration of the power the supply can affect many parts, 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 has a different supply source from the digital core of the MCU, and this diversity helps to mitigate dependent failures related to the main supply alterations.

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 3.6.20 Power control 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 those 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 3.6.21 Reset and clock control (RCC) subsystem for detailed safety mechanisms description.

4.2.3 DMA

DMA is a widely shared resource involved in data transfers operated mainly by all peripherals. Failures of DMA can interfere with the behavior of the system peripherals or application software, leading to non independent failures. The safety mechanisms addressing such dependent failures are the following:

- DMA_SM_0.
- DMA_SM_1.
- DMA_SM_2.

The adoption of such safety mechanisms is therefore highly recommended. It is worth to note that if DMA is not used for data transfer, then only DMA_SM_0 must be implemented. Refer to Section 3.6.6 Direct memory access controller (DMA) for detailed safety mechanisms description.
4.2.4 **Internal temperature**

The abnormal increase of the internal temperature is a potential source of dependent failures, because it can affect many MCU parts and therefore lead to not-independent failures. The safety mechanism to be used to mitigate this potential effect is the following:

- VSUP_SM_3: the internal temperature read and check allow the user to quickly detect potential risky conditions before they lead to a series of internal failures. Refer to Section 3.6.20 Power control for the detailed safety mechanism descriptions.
The Safety Case Database stores all the informations related to the safety analysis performed to derive the results and conclusions reported in this Safety Manual.

In detail, the Safety Case Database is composed of the following:

- Safety Case with the full list of all safety analysis related documents
- ST internal FMEDA tool database for the computation of the safety metrics, including the estimated and measured values
- Safety Report, the document that describes in detail the safety analysis executed on STM32F3 Series devices and the clause-by-clause compliance to IEC 61508
- ST internal fault injection campaign database including tools configuration and settings, fault injection logs and results

Due to presence of ST confidential information, above-described contents are not publicly available and are available for possible competent bodies audit and inspections. This is in line with the clarification of Note 2 on IEC61508:2, 7.4.9.7 requirement.
Appendix A  Change impact analysis for other safety standards

The safety analysis reported in this Safety Manual is executed according to IEC 61508 safety norm. This appendix reports the outcomes of a change impact analysis with respect to different safety standards. The following topics are considered for each addressed new safety standard:

• 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 STM32F3 Series devices according to the new standard.
• Work products required by the new safety norms, and how to remap or rework (if needed) the existing work products resulting as output of the IEC 61508 compliance activity.

The safety standards examined within this change impact analysis are the followings:

• ISO 13849-1:2006, ISO 13849-2:2010 – Safety of machinery and Safety-related parts of control systems,
• IEC 62061:2012-11, ed. 1.1 – Safety of machinery and Functional safety of safety-related electrical, electronic and programmable electronic control systems,
• IEC 61800-5-2:2007, ed.1.0 – Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional

A.1 ISO 13849-1 / ISO 13849-2

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

A.1.1 ISO 13849 architectural categories

The section §6.2 of ISO 13849 identifies five categories for the basic parameters, DC, MTTFd and CCF, reflecting the expected resistance to faults of SRP or CS under design and needed for achieving the required PLr. For each category, the standard suggests a typical architecture that meets the related requirements.

Considering ISO 13849 architectural categories defined in §6.2 and focusing on microcontrollers, Table 118 presents a summary for end users willing to develop Logic Solver units suitable for safety critical channels and performing a defined safety function.

The assumptions are listed hereafter:

1. The safety function is realized by combining in series the elements (SRP or CS) input system, signal processing unit, output system.
2. The SRP or CSs elements may be assigned to one or different categories and different PLs.
3. The safety function is completely in the scope of the end user application.
4. The STM32F3 Series MCUs with the adoption of safety mechanism described in this Safety Manual as single compliant item is by itself suitable for CM application up to PLd (equivalent to SIL2).

The ISO 13849 architectural categories for Logic Solver are shown in the following table.
### Table 118. ISO 13849 architectural categories

<table>
<thead>
<tr>
<th>Cat.</th>
<th>Ref. §</th>
<th>Summary</th>
<th>Designated architecture of Logic</th>
<th>Block diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>6.2.3</td>
<td>The main category; occurrence of one fault can lead to the loss of the safety function. No need of DC and CCF (usually single channel), MTTFd is low or medium. Highest achievable is PL = b.</td>
<td>Single channel architecture, one MCU in 1oo1 Refer to Section 3 Compliant item’s MTTFd = high</td>
<td>Figure 6</td>
</tr>
<tr>
<td>1</td>
<td>6.2.4</td>
<td>Enforcing category B requirements by adopting solutions based on “well tried components” for safety critical application and “well tried” safety principles. A microprocessor is not classified as a “well tried” component. No need of DC and CCF (usually single channel), MTTFd is high. Highest achievable is PL = c.</td>
<td>Single channel architecture, one MCU in 1oo1 Refer to Section 3 Compliant item’s MTTFd = high</td>
<td>Figure 6</td>
</tr>
<tr>
<td>2</td>
<td>6.2.5</td>
<td>With respect to category 1, it is expected to include in the architecture a test equipment performing checks on the safety function and reporting its loss. Overall DC is low, CCF must be evaluated, MTTFd can range from low to high allowing up to PL = d.</td>
<td>Single channel architecture, one MCU in 1oo1d Refer to Section 3 Compliant item’s MTTFd = high TE is in charge of end user, PL = d</td>
<td>Figure 7</td>
</tr>
<tr>
<td>3</td>
<td>6.2.6</td>
<td>With respect to category 1, it is expected to have fault detection mechanisms and any single fault occurrence does not lead the loss of the safety function. Overall DC is low, CCF must be evaluated for the channels, MTTFd can range from low to high allowing up to PL = d.</td>
<td>Double channel architecture, two identical MCUs in 1oo2 Refer to Section 3 Continuous testing or monitoring Compliant item’s MTTFd = high</td>
<td>Figure 8</td>
</tr>
<tr>
<td>4</td>
<td>6.2.7</td>
<td>With respect to category 1, it is expected to have fault detection mechanisms and any single fault occurrence does not lead the loss of the safety function. Overall DC is high, CCF must be evaluated for the channels, MTTFd is high allowing PL = e.</td>
<td>Double channel architecture, two identical MCUs in 1oo2 Refer to Section 3 Continuous testing or monitoring Compliant item’s MTTFd = high PLe achievable</td>
<td>Figure 8</td>
</tr>
</tbody>
</table>

**Figure 6. Block diagram for ISO 13849 Cat. B and Cat. 1**

```
I  _______________  i m
|               |      |
|               |      |
|               |      |
|               |      |
|               |      |
|               |      |
|               |      |
L  _______________  i m
|               |      |
|               |      |
|               |      |
|               |      |
|               |      |
|               |      |
O
```

i m  interconnecting means
i    input device, e.g. sensor
L    logic
O    output device, e.g. main contactor
Figure 7. Block diagram for ISO 13849 Cat. 2

<table>
<thead>
<tr>
<th>I</th>
<th>L</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>m</td>
<td>i</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TE</th>
<th>OTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>m</td>
</tr>
</tbody>
</table>

- i: interconnecting means
- I: input device, e.g. sensor
- L: logic
- O: output device, e.g. main contactor
- m: monitoring
- TE: test equipment
- OTE: output of TE

Figure 8. Block diagram for ISO 13849 Cat. 3 and Cat. 4

<table>
<thead>
<tr>
<th>I1</th>
<th>L1</th>
<th>O1</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>m</td>
<td>i</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I2</th>
<th>L2</th>
<th>O2</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>m</td>
<td>i</td>
</tr>
</tbody>
</table>

- i: interconnecting means
- c: cross monitoring
- I1, I2: input device, e.g. sensor
- L1, L2: logic
- m: monitoring
- O1, O2: output device, e.g. main contactor

A.1.2 ISO 13849 safety metrics computation

Appendix C of ISO 13849 presents tables of standardized 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 we can assume that MTTFd = 1 / PFH [years].

From the reliability theory, MTTF (the inverse of λ and PFH) is a metric applicable only to not reparable systems. Nowadays it is a common practice to use MTBF also for not repairable systems where MTBF has to be
understood as the average time for the first (and only) failure of the equipment; in this case MTBF is equal to MTTF.

In ISO 13849-1 the DC for each single component has the same meaning of the IEC 61508 metric; results of this Safety Manual can therefore be reused. However, this standard defines the concept of DC_{avg} applicable to the whole SRP or 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 MTTF of the various subsystems of the channel. The standard denies any possibility of fault exclusion while calculating DC_{avg} (ISO13849-2 Tab.D.21 no exclusion allowed) and this is the same assumption done in STM32F3 Series analysis in this Safety Manual.

It is necessary to calculate the DC_{avg} only for subsystem made of a 2 MCUs architecture by applying the formula:

\[
DC_{avg} = \frac{DC_{MCU1}}{MTTF_{MCU1}} + \frac{DC_{MCU2}}{MTTF_{MCU2}}
\]

For two identical MCUs having the same DC and MTTF, DC_{avg} = DC.

Note: An evaluation of the possible common failure modes is required for any architectural solution implemented with two channels. ISO 13849 defines a simplified approach with respect to IEC 61508 approach.

Table 7 of the ISO 13849 standard provides a simplified procedure for PL evaluation of SRP or CS based on category, DC_{avg} and MTTFd. It is worth to note that each architectural solution analyzed in this Safety Manual results in PFH-values producing high values of MTTF.

A.1.3 ISO 13849 work products

The following table lists the work products required by the ISO 13849, and how to map these into available work products from IEC 61508 compliance activity:

<table>
<thead>
<tr>
<th>ISO 13849-1 Information to be provided</th>
<th>ISO 13849-1 Part-Clause</th>
<th>STM32F3 Series IEC 61508 document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety functions provided by the SRP or CS</td>
<td>10 Technical documentation</td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Characteristics of each safety function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exact points at which the safety-related part(s) start and end</td>
<td>10 Technical documentation</td>
<td>STM32F3 Series Safety Manual and FMEA</td>
</tr>
<tr>
<td>Environmental conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance level (PL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category or categories selected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters relevant to the reliability (MTTFd, DC, CCF and mission time)</td>
<td>10 Technical documentation</td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Measures against systematic failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology or technologies used;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All safety-relevant faults considered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification for fault exclusions (see ISO 13849-2)</td>
<td>10 Technical documentation</td>
<td></td>
</tr>
<tr>
<td>ISO 13849-1 Information to be provided</td>
<td>ISO 13849-1 Part-Clause</td>
<td>STM32F3 Series IEC 61508 document</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Design rationale (e.g. faults considered, faults excluded)</td>
<td>10 Technical documentation</td>
<td></td>
</tr>
<tr>
<td>Measures against reasonably foreseeable misuse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dated reference to this part of ISO 13849 (that is “ISO 13849-1:2006”);</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category (B, 1, 2, 3, or 4)</td>
<td>11 Information for use</td>
<td>STM32F3 Series Safety Manual</td>
</tr>
<tr>
<td>Performance level (a, b, c, d, or e)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of de-energization (see ISO 13849-2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, under voltage</td>
<td>G.2 Measures for the control of systematic failures</td>
<td></td>
</tr>
<tr>
<td>Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program sequence monitoring must be used with SRP or CS containing software to detect defective program sequences</td>
<td>G.2 Measures for the control of systematic failures</td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2000, 7.4.8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure detection by automatic tests</td>
<td>G.2 Measures for the control of systematic failures</td>
<td>STM32F3 Series Safety Manual</td>
</tr>
<tr>
<td>Computer-aided design tools capable of simulation or analysis</td>
<td>G.3 Measures for avoidance of systematic failures</td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Simulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety-related specification for machine control</td>
<td>App. J, tab.J.1 (SW)</td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Definition of the control architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(End user responsibility because in charge of implementing software-based diagnostics)</td>
</tr>
<tr>
<td>Function block modeling</td>
<td>App. J, tab.J.1 (SW)</td>
<td>SW requirements specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(End user responsibility because in charge of implementing software-based diagnostics)</td>
</tr>
<tr>
<td>Encoding comments in the code</td>
<td>App. J, tab.J.1 (SW)</td>
<td>Code inspection results</td>
</tr>
<tr>
<td>Encoding re-reading sheets</td>
<td>App. J, tab.J.1 (SW)</td>
<td>(End user responsibility because in charge of implementing software-based diagnostics)</td>
</tr>
<tr>
<td>Correspondence matrix</td>
<td>App. J, tab.J.1 (SW)</td>
<td>Software module test specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software system integration test specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Programmable electronic hardware and software integration tests specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(End user responsibility because in charge of implementing software-based diagnostics)</td>
</tr>
</tbody>
</table>

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.

With respect of the safety lifecycle, the scope of this standard is limited from safety requirements allocation to safety validation.

IEC 62061 is the special standard for the machine domain within the framework of the more generic IEC 61508:2010. Since it is just an application standard, IEC 62061 is not strict with respect to the technical solutions. Moreover it is focused on electrical, electronic and programmable electronic parts of safety-related control systems.

Note that §3.2.26 and §3.2.27 in IEC 62061 apply only to SRECS in HD or CM, suitable for the machines domain. LD equipment are still ruled by IEC 61508 requirements.

The close relationship with IEC 61508:2010 is synthesized by the main assumption that the design of complex electronic components as subsystems or elements of subsystems has to be compliant with requirements of IEC 61508:2010 part 2, Route 1H, ref. to §7.4.4.2. Coming from the IEC 62061 definition §3.2.8, natively a microprocessor has to be considered as a complex component.

For this reason, the results reported in this Safety Manual for the STM32F3 Series item (refer to Section 4 Safety results), in the scope of IEC 61508 are still applicable also in the machines context ruled by IEC 62061.

End-users can effectively adopt the STM32F3 Series compliant item to design SRECS suitable for the achievement of SIL2 or SIL3 (by adopting two STM32F3 Series MCUs) machines control loops.

Concerning the integrity levels achievable for subsystems, the standard suggests a classification based on HFT and SFF as shown in Table 120.

Table 120. SIL classification versus HFT

<table>
<thead>
<tr>
<th>SFF</th>
<th>HFT 0</th>
<th>HFT 1</th>
<th>HFT 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>Not allowed</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60% - &lt;90%</td>
<td>SIL1</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90% - &lt;99%</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL3</td>
</tr>
<tr>
<td>≥99%</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

SIL 3 is the highest requirement for SRCF in this context. SIL 4 is out of scope since the final outcome of the development is a control system for one machine only.

For the designer, the SIL values listed in the table has to be seen as the SILCL for the subsystem where SILCL is the maximum SIL claimable for a SRECS subsystem, as defined in IEC 62061, §3.2.24.
A.2.1 IEC 62061 architectural categories

The standard in §6.7.8.2 defines a set of basic system architectures to be used for the design of SRECS implementing their SRCFs. A key point is the definition of "subsystem", refer to §3.2.5, as the level of parts for a system architecture where a dangerous failure could lead to the loss of the safety function.

Focusing on the microcontrollers, IEC 62061 proposed architectures are here quickly summarized for supporting end users in the development of their Logic Solver units usable as subsystems for the implementation of a SRCF. The assumptions for the correct understanding of the architectures are listed hereafter:

1. The SRCF is completely in the scope of the end user.
2. The STM32F3 Series device with the adoption of safety mechanism described in this Safety Manual as single compliant item is by itself suitable for applications up to SILCL 2.
3. Two identical STM32F3 Series devices with the adoption of safety mechanism described in this Manual must be used for achieving HFT ≠ 0, when required by basic architectures.
4. For a microcontroller, the parameter T1, mentioned in the standard as the minimum between service life or proof test, is intended as the lifetime (mission time) assumed equal to 10 years, as per Section 3.3.1 Assumed safety requirements of this Manual.

<table>
<thead>
<tr>
<th>Cat.</th>
<th>Ref. §</th>
<th>Summary</th>
<th>Basic architecture of Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>6.7.8.2.2</td>
<td>Equivalent of 1oo1, with HFT = 0, no diagnostic function(s). Overall PFH_{DSSA} is the probability of dangerous failure of MCU</td>
<td>Single channel architecture, one MCU in 1oo1, n=1 PFH_{DSSA} = \lambda_{De1} \frac{1}{Hour's}</td>
</tr>
</tbody>
</table>
|      |        |         | • SILCL = 1 if SFF < 90%  
|      |        |         | • SILCL = 2 if 90% ≤ SFF < 99%  
|      |        |         | • SILCL = 3 if SFF ≥ 99%  |
| 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). | Dual channel architecture with two identical MCUs  
|      |        |         | • SILCL = 1 if SFF < 60%  
|      |        |         | • SILCL = 2 if 60% ≤ SFF < 90%  
|      |        |         | • SILCL = 3 if SFF ≥ 90%  |
|      |        |         | In this case:  
|      |        |         | \lambda_{DSSB} = (1 - \beta)^2 \times \lambda_{De}^2 \times T_1 + \beta \times \lambda_{De}  
|      |        |         | For \beta factor see Section 4.2 |
| C    | 6.7.8.2.4 | It is the equivalent of 1oo1d with a diagnostic function that initiates a reaction function as a dangerous failure happens on SRCF. NOTE: diagnostic function provides the Logic Solver with a diagnosis of an external subsystem, e.g. the actuator | Single channel architecture, one MCU in 1oo1, n=1  
|      |        |         | Diagnostic function is in charge of the end user  
|      |        |         | • SILCL = 1 if SFF < 90%  
|      |        |         | • SILCL = 2 if 90% < SFF < 99%  
|      |        |         | • SILCL = 3 if SFF ≥ 99%  
|      |        |         | \lambda_{DSSC} = \lambda_{De}(1-DC_1)  
|      |        |         | DC (Diagnostic Coverage) as resulting from FMEDA  |
|      |        |         | PFH_{DSSC} = \lambda_{DSSC} \frac{1}{Hour's} |
Based on IEC 62061 §6, Figure 9 shows how to proceed with the development of SRECS implementing the generic control architecture depicted in figure B.1 of the standard where the microprocessor here presented is an STM32F3 Series device with the adoption of the safety mechanisms as defined in Section 3.7 Conditions of use.

**Figure 9. SRECS high-level diagram**

Allocated functions and integrity requirements

---

**A.2.2 IEC 62061 safety metrics computation**

The failure rate ($\lambda$) 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 $\lambda = 1/\text{MTTF}$, where it is assumed that $1 > \lambda x T$.

So, as $\text{PFH}_D = \lambda D x 1h$, so $\text{PFHD} = 1/\text{MTTF}$.

Safety analysis executed for STM32F3 Series according IEC61508 is more and more accurate for the definition of dangerous failure identifications that can be re-mapped in IEC 62061 domain. Thus, values of $\lambda$ and PFH that are reported in the FMEDA (refer to Section 4 Safety results), are still valid and can be used into formulas of the previous paragraph.

There is no need for re-computation for the SFF of a microcontroller. The end-user uses the same value resulting from this Safety Manual.

As previously discussed in Section 4.2 Dependent failures analysis, in evaluating CCF for those basic architectures with an HFT = 1, the end-user uses the same result, if available, as achieved by the IEC 61508 approach (refer to IEC 61508:2010-6 Annex D). Alternatively, the end-user can apply the simplified approach from the standard (refer to Annex F) to calculate the $\beta$ factor value to be used in formulas for PFHD.
A.2.3 IEC 62061 work products

The following table lists the work products required by the IEC 62061 standard and their mapping with the work products from IEC 61508 compliance activity:

<table>
<thead>
<tr>
<th>Information to be provided</th>
<th>IEC 62061-1.1 Clause</th>
<th>STM32F3 Series Safety Manual</th>
<th>IEC 61508 document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional safety plan</td>
<td>4.2.1</td>
<td></td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Specification of requirements for SRCFs</td>
<td>5.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional safety requirements specification for SRCFs</td>
<td>5.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety integrity requirements specification for SRCFs</td>
<td>5.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRECS design</td>
<td>6.2.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structured design process</td>
<td>6.6.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRECS design documentation</td>
<td>6.6.1.8</td>
<td></td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Structure of function blocks</td>
<td>6.6.2.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRECS architecture</td>
<td>6.6.2.1.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem safety requirements specification</td>
<td>6.6.2.1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem realization</td>
<td>6.7.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem architecture (elements &amp; their interrelationships)</td>
<td>6.7.4.3.1.2</td>
<td></td>
<td>STM32F3 Series Safety Manual</td>
</tr>
<tr>
<td>Fault exclusions claimed when estimating fault tolerance or SFF</td>
<td>6.7.8.1c / 6.7.7.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software safety requirements specification</td>
<td>6.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software based parameterization</td>
<td>6.11.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software configuration management items</td>
<td>6.11.3.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suitability of software development tools</td>
<td>6.11.3.4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation of the application program</td>
<td>6.11.3.4.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Results of application software module testing</td>
<td>6.11.3.7.4</td>
<td></td>
<td>End user responsibility</td>
</tr>
<tr>
<td>Results of application software integration testing</td>
<td>6.11.3.8.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation of SRECS integration testing</td>
<td>6.12.1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation of SRECS installation</td>
<td>6.13.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation for installation, use and maintenance</td>
<td>7.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation of SRECS validation testing</td>
<td>8.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation for SRECS configuration management</td>
<td>9.3.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A.3 IEC 61800-5-2:2007

The scope of this standard is the functional safety of adjustable speed electric drive systems. Part 5.2 of the IEC 61800 defines the requirements for the design, development, integration and validation of the safety related parts for power drive speed applications, PDS(SR), within the framework of IEC 61508 first edition. More precisely, this part of IEC 61800 just limits its application to those PSD(RS) operating in HD or CM, referring to §3.10 NOTE1, implementing safety functions with a target integrity up to SIL 3.

Form the architectural point of view, this limitation is reflected in two tables, §6.2.2.3 Tab. 3 and Tab. 4, for the two different types of classified devices. The CPU or the whole microcontroller, since these are complex electronics parts, is classified as Type B. Also the concept of HFT is derived from IEC 61508 as it is.
A.3.1 IEC 61800 architectural categories
From the architectural point of view, IEC 61800 application is reflected in two tables, §6.2.2.3 Tab. 3 and Tab. 4, for the two different types of classified devices. The CPU or the whole microcontroller, considered as complex electronics parts, are classified as Type B. Also the concept of HFT is derived from IEC 61508 as it is. Architectural remapping on IEC61508 is therefore straightforward.

A.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, ref. to §6.2.1, and SFF, ref. to §6.2.3. So, results of this Safety Manual (and related FMEA or FMEDA) can be remapped in IEC61800 domain.

A.3.3 IEC 61800 work products
The following table lists the work products required by the IEC 61800-5-2 standard and their mapping with the work products from IEC 61508 compliance activity.

<table>
<thead>
<tr>
<th>IEC 618000 5.2</th>
<th>STM32F3 Series Safety Manual and FMEDA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information to be provided</strong></td>
<td><strong>IEC 61800-5.2 Part-Clause</strong></td>
</tr>
<tr>
<td>Safety requirements specification (SRS) for PDS(SR) including safety function requirements and safety integrity requirements</td>
<td>5.4</td>
</tr>
<tr>
<td>Verification of PDS(SR) safety requirements specification</td>
<td>8.2</td>
</tr>
<tr>
<td>Hardware design on an architectural level</td>
<td>6</td>
</tr>
<tr>
<td>Software design on an architectural level</td>
<td>IEC 61508-3</td>
</tr>
<tr>
<td>Estimation of the probability of failure of safety functions due to random hardware failures on a level of functional block diagrams</td>
<td>IEC 61508-2</td>
</tr>
<tr>
<td>Reviews of system design</td>
<td>8.2</td>
</tr>
<tr>
<td>Detailed planning of the validation of safety related PDS(SR).</td>
<td>8.3</td>
</tr>
<tr>
<td>Hardware design</td>
<td>6</td>
</tr>
<tr>
<td>Software design</td>
<td></td>
</tr>
<tr>
<td>Reliability Prediction</td>
<td>6</td>
</tr>
<tr>
<td>Information to be provided</td>
<td>IEC 61800-5.2 Part-Clause</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Reviews of the system design</td>
<td>8.2</td>
</tr>
<tr>
<td>Functional tests on module level</td>
<td></td>
</tr>
<tr>
<td>Integration and test of the safety related PDS(SR).</td>
<td>6.5</td>
</tr>
<tr>
<td>Review of HW or SW integration test results and documentation</td>
<td>8.2</td>
</tr>
<tr>
<td>Develop user documentation describing PDS(SR) installation, commissioning, operation and maintenance.</td>
<td>7</td>
</tr>
<tr>
<td>Complete software and appropriate documentation</td>
<td></td>
</tr>
<tr>
<td>Documentation of the results of the validation tests</td>
<td>8.3</td>
</tr>
<tr>
<td>Validation tests and procedures according to the validation plan</td>
<td></td>
</tr>
<tr>
<td>Documentation of the results of the validation tests</td>
<td></td>
</tr>
<tr>
<td>Subsystem testing plan</td>
<td></td>
</tr>
<tr>
<td>Integration testing plan</td>
<td>6.2.4.1.4</td>
</tr>
<tr>
<td>Validation testing plan</td>
<td></td>
</tr>
<tr>
<td>Configuration testing plan</td>
<td></td>
</tr>
<tr>
<td>Detailed results of each test</td>
<td>9.2.g)</td>
</tr>
<tr>
<td>Any discrepancy between expected and actual results</td>
<td>9.2.h)</td>
</tr>
<tr>
<td>Conclusion of the test: either it has been passed or the reasons for failure</td>
<td>9.2.i)</td>
</tr>
</tbody>
</table>
## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-Jan-2015</td>
<td>1</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
| 30-Jan-2015| 2        | Updated:  
- Figure 1. STMicroelectronics product development process,  
- Block diagram for IEC-62061 Cat B figure  
- Block diagram for IEC-62061 Cat D figure |
| 30-Nov-2017| 3        | Added!  
- Section 3.2.3 Reference safety architectures - 1oo1  
- Section 3.2.4 Reference safety architectures - 1oo2  
- Figure 3. 1oo1 reference architecture  
- Figure 4. 1oo2 reference architecture  
- Section 3.6.25 System configuration controller (SYSCFG)  
- Section 4.1.3 Notes on multiple faults scenario  
- Table 5. CPU_SM_0 to Table 114. FFI_SM_1 for description of hardware and software diagnostics.  
Removed:  
- Section: Yogitech fRMethodology process,  
- Section: Dual MCU architecture,  
- Section: Latent fault detection,  
- Appendix A: overview of fRMethodology,  
- Appendix B: Examples of safety architecture.  
Updated:  
- Section 3.3.1 Assumed safety requirements  
- Section A.4.1: Architectural categories,  
- Table 1. Terms and abbreviations  
- Section Appendix A: Change impact analysis for other safety standards |
| 19-Apr-2018| 4        | Updated introduction.  
Updated Table 120. SIL classification versus HFT.  
Updated Section 4.2 Dependent failures analysis.  
Updated Figure 9. SRECS high-level diagram.  
Updated Section A.2.2 IEC 62061 safety metrics computation.  
Updated Section 1.3 Reference normative. |
| 04-Oct-2018| 5        | Updated Table 1. Terms and abbreviations.  
Updated Section 1.3 Reference normative.  
Updated Table 121. IEC 62061 architectural categories. |
Removed ISO 26262:2010 section.  
Updated Section 1.3 Reference normative  
Updated Section Appendix A: Change impact analysis for other safety standards |

Table 124. Document revision history
1 About this document .............................................................. 2
  1.1 Purpose and scope ............................................................. 2
  1.2 Terms and abbreviations ........................................................ 2
  1.3 Reference normative ........................................................... 3
2 STM32L1 Series microcontroller development process ............................. 5
  2.1 STMicroelectronics standard development process ............................... 5
3 Reference safety architecture ...................................................... 7
  3.1 Safety architecture introduction................................................... 7
  3.2 Compliant item ................................................................. 7
    3.2.1 Definition of the compliant item .............................................. 7
    3.2.2 Safety functions performed by the compliant item .............................. 7
    3.2.3 Reference safety architectures - 1oo1 ......................................... 8
    3.2.4 Reference safety architectures - 1oo2 ......................................... 9
  3.3 Assumed requirements ......................................................... 10
    3.3.1 Assumed safety requirements .............................................. 10
  3.4 Electrical specifications and environment limits .................................... 11
  3.5 Systematic safety integrity ...................................................... 11
  3.6 Description of hardware and software diagnostics ............................... 11
    3.6.1 Arm® Cortex®-M4 CPU ................................................... 13
    3.6.2 Embedded FLASH memory ............................................... 18
    3.6.3 Embedded SRAM ....................................................... 22
    3.6.4 System bus architecture .................................................. 26
    3.6.5 EXTI controller ......................................................... 28
    3.6.6 Direct memory access controller (DMA) ..................................... 30
    3.6.7 Controller area network (CAN) ........................................... 33
    3.6.8 Universal synchronous/asynchronous receiver/transmitter (USART) 1/2/3/4/5 ......... 35
    3.6.9 Inter-integrated circuit (I2C) 1/2. ........................................ 37
    3.6.10 Serial peripheral interface (SPI) 1/2/3/4....................................... 40
    3.6.11 USB on-the-go full-speed (OTG_FS) ........................................ 43
    3.6.12 Touch sensing controller (TSC) ......................................... 45
| A.1.1 | ISO 13849 architectural categories | 86 |
| A.1.2 | ISO 13849 safety metrics computation | 88 |
| A.1.3 | ISO 13849 work products | 89 |
| A.2 | IEC 62061:2005/AMD1:2012 | 91 |
| A.2.1 | IEC 62061 architectural categories | 92 |
| A.2.2 | IEC 62061 safety metrics computation | 93 |
| A.2.3 | IEC 62061 work products | 94 |
| A.3 | IEC 61800-5-2:2007 | 94 |
| A.3.1 | IEC 61800 architectural categories | 95 |
| A.3.2 | IEC 61800 safety metrics computation | 95 |
| A.3.3 | IEC 61800 work products | 95 |

**Revision history** | 97
# List of tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Terms and abbreviations</td>
<td>2</td>
</tr>
<tr>
<td>Table 2</td>
<td>Mapping between this document content and IEC 61508-2 Annex D requirements</td>
<td>3</td>
</tr>
<tr>
<td>Table 3</td>
<td>SS1 and SS2 safe state details</td>
<td>11</td>
</tr>
<tr>
<td>Table 4</td>
<td>Safety mechanism field explanation</td>
<td>12</td>
</tr>
<tr>
<td>Table 5</td>
<td>CPU_SM_0</td>
<td>13</td>
</tr>
<tr>
<td>Table 6</td>
<td>CPU_SM_1</td>
<td>13</td>
</tr>
<tr>
<td>Table 7</td>
<td>CPU_SM_2</td>
<td>14</td>
</tr>
<tr>
<td>Table 8</td>
<td>CPU_SM_3</td>
<td>14</td>
</tr>
<tr>
<td>Table 9</td>
<td>CPU_SM_4</td>
<td>15</td>
</tr>
<tr>
<td>Table 10</td>
<td>CPU_SM_5</td>
<td>15</td>
</tr>
<tr>
<td>Table 11</td>
<td>CPU_SM_6</td>
<td>16</td>
</tr>
<tr>
<td>Table 12</td>
<td>CPU_SM_7</td>
<td>16</td>
</tr>
<tr>
<td>Table 13</td>
<td>MPU_SM_0</td>
<td>17</td>
</tr>
<tr>
<td>Table 14</td>
<td>FLASH_SM_0</td>
<td>18</td>
</tr>
<tr>
<td>Table 15</td>
<td>FLASH_SM_1</td>
<td>18</td>
</tr>
<tr>
<td>Table 16</td>
<td>FLASH_SM_2</td>
<td>19</td>
</tr>
<tr>
<td>Table 17</td>
<td>FLASH_SM_3</td>
<td>19</td>
</tr>
<tr>
<td>Table 18</td>
<td>FLASH_SM_4</td>
<td>20</td>
</tr>
<tr>
<td>Table 19</td>
<td>FLASH_SM_5</td>
<td>20</td>
</tr>
<tr>
<td>Table 20</td>
<td>FLASH_SM_6</td>
<td>20</td>
</tr>
<tr>
<td>Table 21</td>
<td>FLASH_SM_8</td>
<td>21</td>
</tr>
<tr>
<td>Table 22</td>
<td>RAM_SM_0</td>
<td>22</td>
</tr>
<tr>
<td>Table 23</td>
<td>RAM_SM_1</td>
<td>22</td>
</tr>
<tr>
<td>Table 24</td>
<td>RAM_SM_2</td>
<td>23</td>
</tr>
<tr>
<td>Table 25</td>
<td>RAM_SM_3</td>
<td>23</td>
</tr>
<tr>
<td>Table 26</td>
<td>RAM_SM_4</td>
<td>24</td>
</tr>
<tr>
<td>Table 27</td>
<td>RAM_SM_5</td>
<td>24</td>
</tr>
<tr>
<td>Table 28</td>
<td>BUS_SM_0</td>
<td>26</td>
</tr>
<tr>
<td>Table 29</td>
<td>BUS_SM_1</td>
<td>26</td>
</tr>
<tr>
<td>Table 30</td>
<td>LOCK_SM_0</td>
<td>27</td>
</tr>
<tr>
<td>Table 31</td>
<td>NVIC_SM_0</td>
<td>28</td>
</tr>
<tr>
<td>Table 32</td>
<td>NVIC_SM_1</td>
<td>28</td>
</tr>
<tr>
<td>Table 33</td>
<td>DMA_SM_0</td>
<td>30</td>
</tr>
<tr>
<td>Table 34</td>
<td>DMA_SM_1</td>
<td>30</td>
</tr>
<tr>
<td>Table 35</td>
<td>DMA_SM_2</td>
<td>30</td>
</tr>
<tr>
<td>Table 36</td>
<td>DMA_SM_3</td>
<td>31</td>
</tr>
<tr>
<td>Table 37</td>
<td>DMA_SM_4</td>
<td>32</td>
</tr>
<tr>
<td>Table 38</td>
<td>CAN_SM_0</td>
<td>33</td>
</tr>
<tr>
<td>Table 39</td>
<td>CAN_SM_1</td>
<td>33</td>
</tr>
<tr>
<td>Table 40</td>
<td>CAN_SM_2</td>
<td>33</td>
</tr>
<tr>
<td>Table 41</td>
<td>UART_SM_0</td>
<td>35</td>
</tr>
<tr>
<td>Table 42</td>
<td>UART_SM_1</td>
<td>35</td>
</tr>
<tr>
<td>Table 43</td>
<td>UART_SM_2</td>
<td>35</td>
</tr>
<tr>
<td>Table 44</td>
<td>UART_SM_3</td>
<td>36</td>
</tr>
<tr>
<td>Table 45</td>
<td>IIC_SM_0</td>
<td>37</td>
</tr>
<tr>
<td>Table 46</td>
<td>IIC_SM_1</td>
<td>37</td>
</tr>
<tr>
<td>Table 47</td>
<td>IIC_SM_2</td>
<td>37</td>
</tr>
<tr>
<td>Table 48</td>
<td>IIC_SM_3</td>
<td>38</td>
</tr>
<tr>
<td>Table 49</td>
<td>IIC_SM_4</td>
<td>38</td>
</tr>
<tr>
<td>Table 50</td>
<td>SPI_SM_0</td>
<td>40</td>
</tr>
<tr>
<td>Table 51</td>
<td>SPI_SM_1</td>
<td>40</td>
</tr>
<tr>
<td>Table 52</td>
<td>SPI_SM_2</td>
<td>40</td>
</tr>
<tr>
<td>Table 53.</td>
<td>SPI_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 54.</td>
<td>SPI_SM_4</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 55.</td>
<td>USB_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 56.</td>
<td>USB_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 57.</td>
<td>USB_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 58.</td>
<td>USB_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 59.</td>
<td>TSC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 60.</td>
<td>TSC_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 61.</td>
<td>TSC_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 62.</td>
<td>ADC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 63.</td>
<td>ADC_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 64.</td>
<td>ADC_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 65.</td>
<td>ADC_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 66.</td>
<td>ADC_SM_4</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 67.</td>
<td>DAC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 68.</td>
<td>DAC_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 69.</td>
<td>COMP_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 70.</td>
<td>COMP_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 71.</td>
<td>COMP_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 72.</td>
<td>COMP_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 73.</td>
<td>COMP_SM_4</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 74.</td>
<td>GTIM_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 75.</td>
<td>GTIM_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 76.</td>
<td>ATIM_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 77.</td>
<td>ATIM_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 78.</td>
<td>ATIM_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 79.</td>
<td>ATIM_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 80.</td>
<td>ATIM_SM_4</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 81.</td>
<td>GPIO_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 82.</td>
<td>GPIO_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 83.</td>
<td>GPIO_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 84.</td>
<td>GPIO_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 85.</td>
<td>RTC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 86.</td>
<td>RTC_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 87.</td>
<td>RTC_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 88.</td>
<td>RTC_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 89.</td>
<td>VSUP_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 90.</td>
<td>VSUP_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 91.</td>
<td>VSUP_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 92.</td>
<td>VSUP_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 93.</td>
<td>CLK_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 94.</td>
<td>CLK_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 95.</td>
<td>CLK_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 96.</td>
<td>CLK_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 97.</td>
<td>WDG_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 98.</td>
<td>WDG_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 99.</td>
<td>DBG_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 100.</td>
<td>CRC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 101.</td>
<td>SYSCFG_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 102.</td>
<td>DIAG_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 103.</td>
<td>FSMC_SM_0</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 104.</td>
<td>FSMC_SM_1</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 105.</td>
<td>FSMC_SM_2</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table 106.</td>
<td>FSMC_SM_3</td>
<td>.................................................................</td>
</tr>
<tr>
<td>Table No.</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>107</td>
<td>HDMI_SM_0</td>
<td>71</td>
</tr>
<tr>
<td>108</td>
<td>HDMI_SM_1</td>
<td>71</td>
</tr>
<tr>
<td>109</td>
<td>HDMI_SM_2</td>
<td>71</td>
</tr>
<tr>
<td>110</td>
<td>AMP_SM_0</td>
<td>73</td>
</tr>
<tr>
<td>111</td>
<td>DCMI_SM_0</td>
<td>74</td>
</tr>
<tr>
<td>112</td>
<td>DCMI_SM_1</td>
<td>74</td>
</tr>
<tr>
<td>113</td>
<td>FFI_SM_0</td>
<td>75</td>
</tr>
<tr>
<td>114</td>
<td>FFI_SM_1</td>
<td>75</td>
</tr>
<tr>
<td>115</td>
<td>List of safety mechanisms</td>
<td>76</td>
</tr>
<tr>
<td>116</td>
<td>Overall achievable safety integrity levels</td>
<td>81</td>
</tr>
<tr>
<td>117</td>
<td>List of general requirements for FFI</td>
<td>82</td>
</tr>
<tr>
<td>118</td>
<td>ISO 13849 architectural categories</td>
<td>87</td>
</tr>
<tr>
<td>119</td>
<td>ISO 13849 work product grid</td>
<td>89</td>
</tr>
<tr>
<td>120</td>
<td>SIL classification versus HFT</td>
<td>91</td>
</tr>
<tr>
<td>121</td>
<td>IEC 62061 architectural categories</td>
<td>92</td>
</tr>
<tr>
<td>122</td>
<td>IEC 62061 work product grid</td>
<td>94</td>
</tr>
<tr>
<td>123</td>
<td>IEC 61800 work product grid</td>
<td>95</td>
</tr>
<tr>
<td>124</td>
<td>Document revision history</td>
<td>97</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Figure 1.</td>
<td>STMicroelectronics product development process</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2.</td>
<td>Definition of the compliant item</td>
<td>7</td>
</tr>
<tr>
<td>Figure 3.</td>
<td>1oo1 reference architecture</td>
<td>8</td>
</tr>
<tr>
<td>Figure 4.</td>
<td>1oo2 reference architecture</td>
<td>9</td>
</tr>
<tr>
<td>Figure 5.</td>
<td>Allocation and target for STM32 PST.</td>
<td>10</td>
</tr>
<tr>
<td>Figure 6.</td>
<td>Block diagram for ISO 13849 Cat. B and Cat. 1</td>
<td>87</td>
</tr>
<tr>
<td>Figure 7.</td>
<td>Block diagram for ISO 13849 Cat. 2</td>
<td>88</td>
</tr>
<tr>
<td>Figure 8.</td>
<td>Block diagram for ISO 13849 Cat. 3 and Cat. 4</td>
<td>88</td>
</tr>
<tr>
<td>Figure 9.</td>
<td>SRECS high-level diagram</td>
<td>93</td>
</tr>
</tbody>
</table>
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.

© 2019 STMicroelectronics – All rights reserved