FS26

Safety System Basis Chip with Low Power

REV 1.0 May 2020

Safety manual

COMPANY CONFIDENTIAL

Document information

Info	FS26 Functional Safety Manual
Author	Mathieu GONDON
Author Role	System and Application Engineer
Abstract	This document discusses the safety requirements for the use of an NXP product in functional safety relevant applications requiring high functional safety integrity levels. It is intended to support system and software engineers using the available features, as well as achieving additional diagnostic coverage by software measures for FS26.

Revision History

Revision	Date	Description	Author
0.1	2020/03/15	Initial draft version	Mathieu GONDON
1.0	2020/05/15	Initial release	Mathieu GONDON

1 Document purpose & scope

1.1 Purpose

The functional safety manual describes how to use the FS26 System Basis Chip in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level.

It is intended to support system and software engineers using the FS26 available features, as well as achieving additional diagnostic coverage by software measures.

1.2 Scope

The Safety Manual provides a minimum set of requirements and practices for safe operation of the safety element considered in a given context of use. This functional safety manual provides necessary assumptions of FS26 use, i.e. details of the assumed functional safety (ASIL capability, safe states, FTTI, technical safety requirements, etc.), assumed use case(s).

The contents of functional safety manual are driven and defined by the following:

- Safety context and Safety concept established during the development of FS26 IC
- Safety analysis results and information about failures of the element, their distribution, calculation of the failure rate, etc., and the diagnostic coverage offered by the safety mechanisms implemented in the element
- Appropriate use of the safety mechanisms implemented within FS26 IC to ensure safe operation
- Safety measures to be implemented by the integrator to ensure safe operation

1.3 Content

This Safety Manual includes the following:

- Description of ISO 26262 lifecycle tailored for this integrated circuit development mentioning which parts and work products were done.
- Description of Assumptions of Use of the integrated circuit with respect to its intended use, including: assumption on the IC safe state; assumptions on fault tolerant time interval, assumptions on use of functional safety features or FS26 from a potential integrator (interfacing MCU),
- Description of the IC safety concept and safety architecture with an abstract description of IC functionalities and description of safety requirements and mechanisms,
- Reference to the other safety relevant documentation which is not covered in the Safety Manual document.
- Summary table for system integrator usage.

1.4 Component Safety Analysis

In distributed development, user(s) integrating the NXP component into their applications/systems need to perform safety analysis at application/system level. Under the customer application/system those results will be aggregated with others from other components or sub/system to perform the customer application/system safety analysis under the safety architecture considered by the customers.

The customer level application/system safety analysis is under the responsibility of the customer and the customer is solely responsible for the safety metric values.

The FS26 is developed as a “Safety-related Element Out of Context”, thus the system requirements are NOT available in detail. Therefore, some assumptions are made regarding the “context of use” of the FS26.

1.5 General information

The FS26 is an automotive functionally safe multi-output power supply integrated circuit, with focus on Body, Gateway, car electrification and chassis applications. It includes multiple switch mode and linear voltage regulators.

The FS26 includes enhanced safety features, with one or two fail-safe output(s), becoming a full part of a safety-oriented system partitioning, covering both ASIL B and ASIL D safety integrity level. It is developed in compliance with ISO26262 standard.

Several device versions are available, offering choice in number of output rails, output voltage setting, operating frequency and power up sequencing, to address multiple applications.

2 Description of ISO 26262 lifecycle used for the component development.

1.6 Brief description of NXP safety life cycle

Within NXP an organizational level approved product creation process with safety extension is defined with several gates and milestones, where in the objectives, input and deliverables are defined and checked. The product creation process is used as a guideline document for any project execution.

Within a development project, several gates/milestones are defined based on the governing product creation process, which divide the project up into manageable project phases. Within these project phases activities will be planned to generate several deliveries. Each of these deliveries will have their own maturity. It is related to the type of delivery, i.e. document, design, hardware, software, etc. based on the maturity model is applied. The longer implementation phase is further sub divided into different phases with defined milestones based on product maturity expectations. At the end of each planned phases, formal reviews and audits are conducted to make sure that the expected process compliance and product level maturity are in place.

The section below describes a basic overview and the project gates.

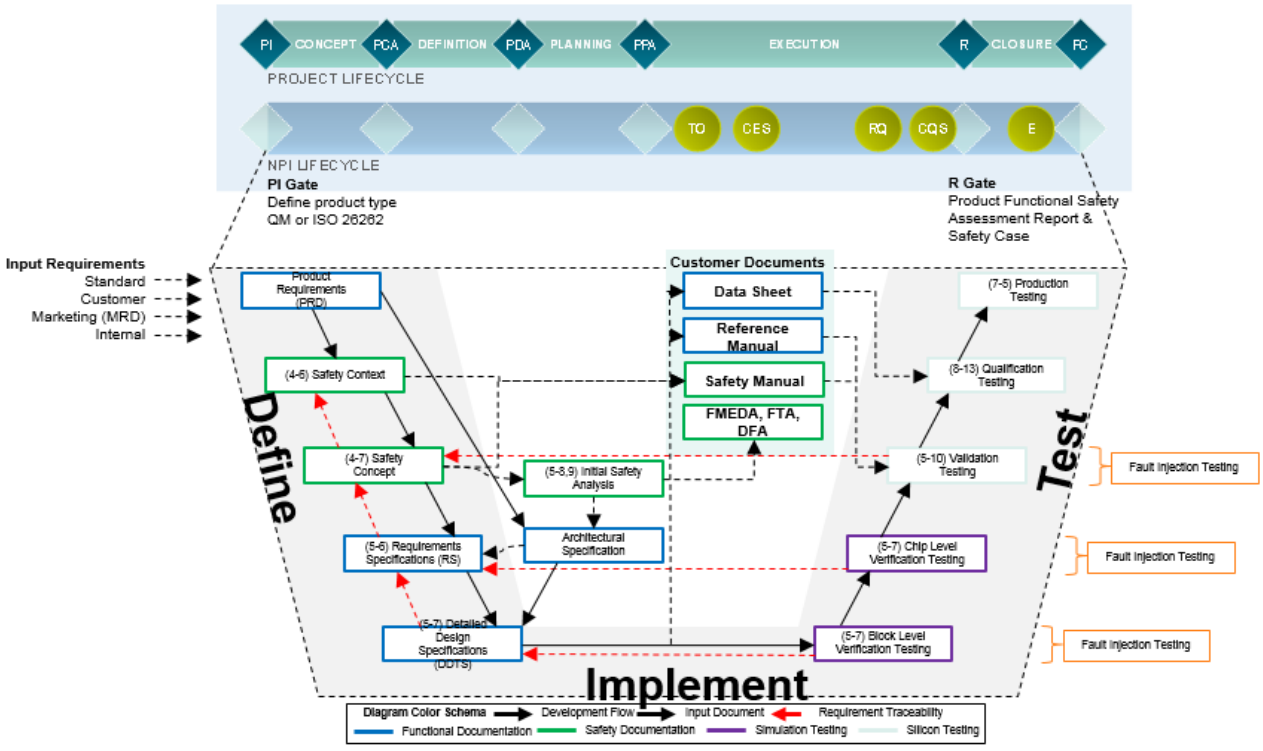

Figure 1 - Functional safety life cycle

Table 1 - Major safety deliverables and gates

Gate and objectives	Key (safety) inputs	Key (safety)deliverables	Critical reviews
Project initiation (PI)	Capture market requirements including functional safety requirements Functional safety manager and architect allocated to project		
Concept phase (PCA): evaluate concept for technical and commercial viability	From project initiation	ASIL target Initial structure and content for the following. • Safety context and safety concept • Safety plan • DIA • Safety case • Safety requirements • Resource requirements	Verification review of safety concept
Definition phase (PDA). Complete requirement specifications, architectural specifications and qualification strategy	PCA deliverables	Safety concept, Safety requirements, safety architecture, Base FIT calculations, Initial safety analysis (FMEA, FMEDA, FTA, DFA) TCL (initial)	Verification Review of Safety Concept, safety requirements in the Requirements Specification, Safety Analysis (FMEDA, FTA, DFA, SW FMEA)
Planning phase (PPA) Build and baseline Project Management Plan(s) Commitment for funding and people	PDA deliverables	• Technical specification (detailed) with safety features, • Updated safety plan and safety assessment plan. • Initial TCL reports • V&V, qualification plan, production test plan	Confirmation review of safety plan
Execution phase (R) Develop and qualify the product and associated product collateral Release product configurations to production and supply	PPA deliverables	All Major Milestone Requirements met including safety Updated safety case report	All major verification reviews (Design reports, V&V reports, safety manual, safety analysis) Confirmation review of safety analysis, TCL, safety case, qualification reports Safety assessments and audit (if applicable)

2.1 Tailored ISO26262 life cycle applied at component level

Table 2 - ISO26262 applicability

ISO26262 part	ISO26262 section	Topic of the part	Applicability	Justification or exceptions
1	All sections	Vocabulary	Applicable	–
2	All sections	Management of functional safety	Applicable	–
3	All sections	Concept phase	NOT applicable	Under customer responsibility,
4	All sections	Product development at system level	Partially applicable	Sections 6.5.1, 6.5.2, 7.5.5, 10.5.1, and 11.5.1 are considered in the development of the product. It is the customer's responsibility to verify that the assumptions made at system level are applicable to their target application.
5	All sections	Product development at Hardware level	Applicable	–
6	All sections	Product development at Software level	Not Applicable	Under customer responsibility
7	All sections	Production and operation	Applicable	No maintenance, no reparation and no decommissioning planned at product level. The maintenance and reparation can be done only at system or vehicle level.
8	All sections	Supporting processes	Applicable	Exception to the software part since the element contains none.
9	All sections	ASIL-oriented and safety-oriented analysis	Applicable	There is no ASIL considered in IC development
10	All sections	Guideline on ISO 26262	Not Applicable	Informative part only

2.2 Customer specific actions required

In a context of customer applications, this is a list of required customer tasks under their responsibility. The list is delivered as an example and is not exhaustive. In case of questions, the customer should contact their local NXP representative.

- Use the latest FS26 documentation revision (datasheet, safety manual, FMEDA, application notes, errata, etc.). Other or additional safety requirements might have to be considered depending of the target application and required standard (e.g. IEC 61508, IEC 61784, etc.)
- Verify the application mission profile is well covered by the FS26
- Compare system requirements versus FS26 requirements and make sure there are no deviations
- Establish validity of the system level assumptions described in **Chapter 4**
- Verify the FS26 FTTI is under the system FTTI requirement for all faults
- Verify the safe states described in **Chapter 4.7** are compatible with the system requirements
- Verify that the Functional Safety Requirements described in **Chapter 4.6.1** are compatible with the system requirements
- Perform safety analysis at the system level, considering the safety analysis provided for the FS26. Consider assumptions like typical mission profile and failure rate data book (IEC 62380)
- Perform calculation and verify the safety metrics
- Validate FS26 outputs behave as expected in the application, including error conditions
- Consider and verify single point failures and latent failures at system level.
- Verify the effectiveness of diagnostics at the system level (including **SMAx**)
- Perform fault injection tests and validate safety mechanisms at the system level.
- Consider all Safety Assumptions identified as **[SA_xx]**
- Consider all safety System Integration Requirements identified as **[SIR_xx]**

The installation of the device at the module level is the responsibility of the system integrator. However, NXP gives recommendations on NXP SOIC packages during printed circuit board (PCB) assembly. This document serves only as a guideline to help users develop a specific solution. Actual experience and development efforts are still required to optimize the assembly process and application design per individual device requirements, industry standards, such as IPC and JEDEC, and prevalent practices in the user's assembly environment.

In case of questions, the customer should contact their local NXP Semiconductor representative.

3 List of supporting documents

3.1 Integration related documents

The system integrator should consider the following referenced documents for the safe integration of the FS26.

Table 3 - Integration related documentation

Document Number	Document	Title	Description	Reference
TBA (to be assigned)	Data Sheet (rev 0.93)	Safety System Basis Chip with Low Power	Draft FS26 data sheet	[1]
FS26_Dynamic _FMEDA.xls	FMEDA (rev 0.2)	FS26_Dynamic_FMEDA	FS26 Failure Mode Effects and Diagnostic Analysis Document	[2]
TBA	Not yet released	FS26_OTP_Mapping	OTP configuration file	[3]
TBA	Errata	TBA	FS26 customer errata	[4]
TBA	PPAP	TBA	Report summarizing data gathered during qualification of the FS26 following AECQ100-RevH requirements	[5]
TBA	Report	Safety Analysis Report	safety analysis (FTA, FMEA, DFA, FMEDA) summary report	[6]

3.2 Reference documents

The additional following referenced documents were used during the development of the FS26. Some of the documents are available during audit only.

Table 4 - Reference documents

Document Number	Document	Title	Description	Reference
ISO 26262	Standard	ISO 26262	ISO 26262 Road vehicles - Functional safety, November 2011	[7]
doc_FS8500_IEC_TR_62380_customer_communication.docx	Report	Failure Rate Evaluation Report	FIT rate calculated based on IEC-TR62380 standard	[8]
TBA	Report	Fault Tree Analysis	Visible during audit only	[9]
TBA	Report	Dependent Failure Analysis	Visible during audit only	[10]
TBA	Report	Fault Injection Test Report	Visible during audit only	[11]

3.3 Vocabulary

For the purposes of this document, the vocabulary defined in ISO 26262-1 apply to this document. Specifically, the following terms apply.

- **System:** functional safety-related system implementing the required functional safety goals necessary to achieve or maintain a safe state$_{system}$ for the equipment under control (control system). The system is intended to achieve on its own or with other electrical/electronic/programmable electronic functional safety-related systems, the necessary functional safety integrity for the required safety functions.
- **System integrator:** the person responsible for the system integration.
- **Element:** part of a subsystem comprising of a single component or any group of components (for example, hardware, software, hardware parts, software units) performing one or more element safety functions (functional safety requirements).
- **Trip time:** the maximum time of operation of the SBC without switching to a power down state.

4 Assumptions on Use

The part numbers supported by this safety manual are listed in the FS26 data sheet document.

In this safety manual, **[SA_xx]** tags indicate Safety Assumptions listed in the FS26 Safety Context.

4.1 Targeted application

The FS26 features and safety requirements are derived from an automotive power rain application (Battery Management System, Electrical Power Steering, …). The FS26 is a safety System Basis Chip. It generates the power supply of the MCU and sensors for the application. It monitors all the power supplies, the MCU with Watchdog and FCCU. It manages the MCU power on reset and/or reset pins, as well as the application safe state in redundancy with the MCU. Figure 2 illustrates the FS26 generic safety application used for the safety analysis.

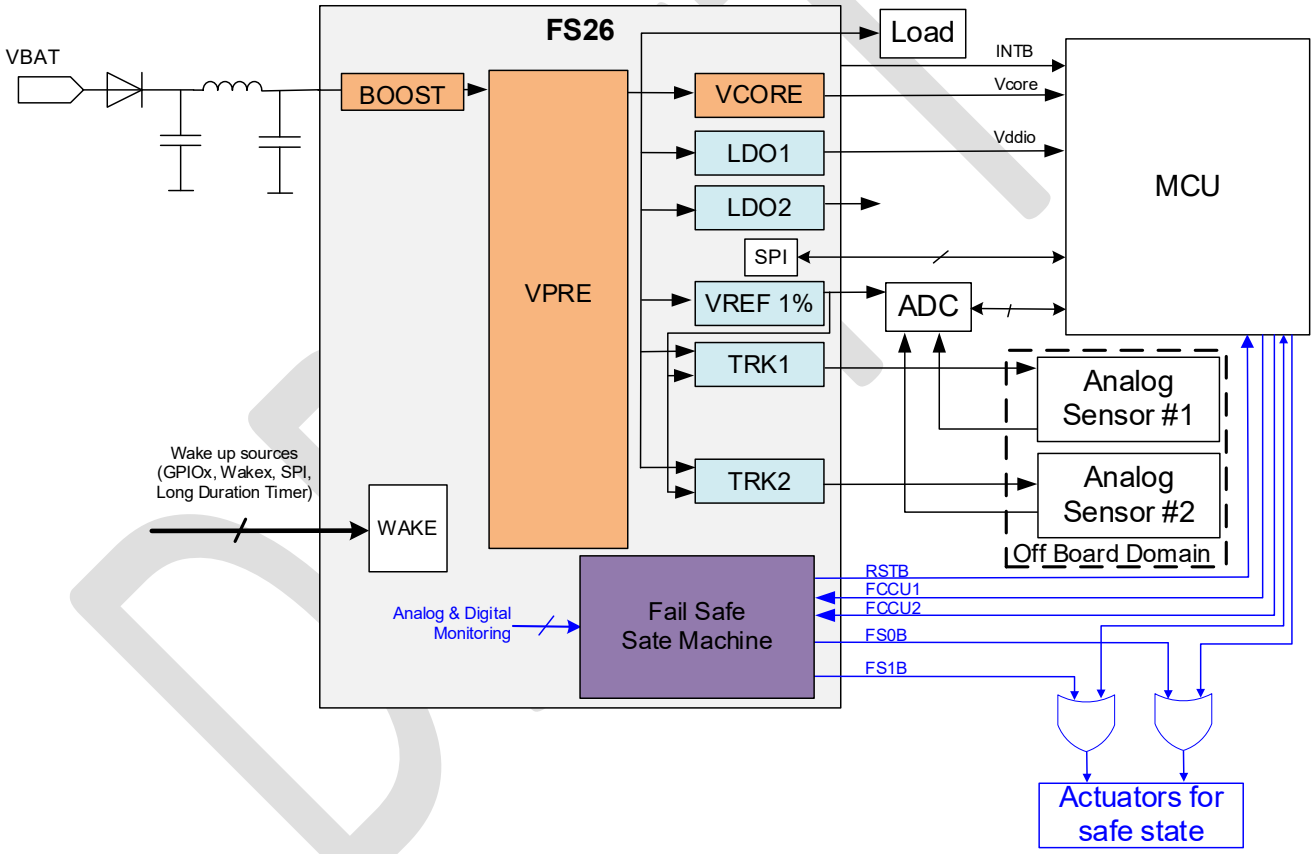

Figure 2 - FS26 generic safety application

List of the safety related functions and the hardware connection used for the safety analysis (FMEDA):

- Analog & Digital Monitoring: Internal connection to monitor all the voltages generated by the power management
- FCCU1/2 = FCCU input monitoring with bi-stable protocol, default polarity
- ERRMON = External IC (radar sensor) error monitoring
- RSTB = Active low Reset bidirectional output

- FS0B = Active low Fail-safe output
- FS1B = secondary active low Fail-safe output
- SPI: communication interface between MCU and FS26 used for configuration, diagnostic, and Watchdog monitoring

The external components required around the FS26 device are available in the datasheet.

4.2 Applicable ASIL

The FS26xyD is developed to target the Automotive Safety Integrity Level D and the FS26xyB is developed to target the Automotive Safety Integrity Level B when applying the corresponding recommendations and applicability of the system assumptions mentioned in this safety manual.

- ASIL B vs ASIL D safety features the safety features available for the FS26xyD and the FS26xyB.

Table 5 - ASIL B vs ASIL D safety features

Safety Features	ASIL B (FS26xyD)	ASIL D (FS26xyB)
RSTB output pin	Yes	Yes
FS0B output pin	Yes	Yes
FS1B output pin	Yes	Yes
VPRE voltage monitoring	Yes	Yes
VCORE voltage monitoring	Yes	Yes
VLDO1 voltage monitoring	Yes	Yes
VLDO2 voltage monitoring	Yes	Yes
VTRK1 voltage monitoring	Yes	Yes
VTRK2 voltage monitoring	Yes	Yes
VREF voltage monitoring	Yes	Yes
VMONEXT voltage monitoring	Yes	Yes
Watchdog monitoring	Simple WD	Challenger WD
FCCU monitoring	No	Yes
MCU Fault Recovery Strategy	No	Yes
External IC monitoring (ERRMON)	No	Yes
Analog BIST (ABIST)	Yes	Yes
Logical BIST (LBIST)	No	Yes

4.3 Requirements and measures at system level

4.3.1 System level assumptions

The system level assumptions for the FS26 are:

[SA_02]: It is assumed that the FS26 product family is used in application for which the battery voltage never exceeds the defined maximum ratings (e.g., 40 V).

[SA_03]: It is assumed the normal operating of the FS26 product family is fulfilled by the compliance to the datasheet.

[SA_04]: It is assumed the FS26 product family shall meet all the datasheet specification after qualification tests.

[SA_05]: It is assumed that the FS26 is used in combination with other devices in the application (e.g. MCU, DDR, other analog IC).

[SA_06]: It is assumed that FS26 product family can be designed in systems that request highest Automotive Safety Integrity Level ASIL D and lower.

[SA_07]: It is assumed that the FS26 is used in application for witch the fault tolerant time interval (FTTI) is ≥ of the FS26 fault detection time plus the FS26 fault reaction time (max 10 ms).

[SA_08]: It is assumed that the multiple point fault interval is ≤ 12 hours then the "Driving Cycle" is assumed to be ≤ 12 hours.

[SA_09]: It is assumed that the number of FS26 pin disconnection, at the same time (i.e. Pin lift on the PCB), is restricted to 1.

[SA_10]: It is assumed the thermal connection of the exposed-pad to the PCB is always ensured thanks to its large size.

[SA_11]: Short circuit between PCB track is not considered in the FS26 (i.e diagnostic, countermeasures).

[SA_12]: External component disconnection is not considered (i.e. diagnostic, countermeasures).

[SA_13]: It is assumed that a power source is always available on the supply pin of the FS26.

[SA_14]: It is assumed the safety signals used to transition the system in safe state is delivered by the MCU and the FS26, to propose redundant and independent safety paths at system level.

[SA_16]: It is assumed that the BMS application safe states is the following: - contactors opened (battery cells isolated from power source)

[SA_17]: It is assumed that one or several contactors (relays) are available to isolate the battery cells for BMS. On different application, a CAN physical layer can be de-activated to isolate the ECU in fault.

4.4 Restrictions in use

4.4.1 Electrical specification limits

The FS26 operating range is described in the datasheet **Supply voltage operating range** chapter. Operating outside of the range of functionality may reduce device lifetime, cause fault conditions, etc. and thereby compromise meeting safety goals.

4.4.2 Operational limits

The FS26 max rating range is described in the datasheet **Maximum ratings** chapter. Exceeding the ratings in that table may cause malfunction or permanent damage to the FS26 and the inability to meet its safety requirements. The system integrator must ensure that the system operates within those constraints. It is assumed that the automotive system provides over voltage protection if excessive voltages are possible.

4.4.3 Mission profile

[SA_01]: It is assumed that the FS26 product family is used in "12 V Automotive" application where a Fail-safe reaction is expected.

[SA_23]: ***It is assumed that the FS26 product family is used in application for which the mission profile is the following (or less aggressive)***

- ***Operation lifetime : 7495 Hours***
- ***Junction Temperature : -40C ≤ Tj ≤ 150°C***
- ***Non-operational lifetime : 15 years - 12000H at an average temperature of 35°C***

Table 6 - Assumed FS26 mission profile

Junction temperature [°C]	Operating time [%]	Operating time [hours]	Cumulated time [hours]
6	0.04	3	3
26	0.61	45	48
46	1.12	83	131
66	1.66	123	254
86	6.86	507	761
106	47.3	3598	4359
126	40.5	2995	7354
146	1.91	141	7495

Thermal cycling considered:

- 335 operating days with four-day light starts with temperature increase of 62 °C.
- 335 operating days with two night starts with temperature increase of 72 °C.
- 30 days non-operating with temp increase of 10 °C.

If the application mission profile at customer if more aggressive than SA_15 assumption above, please contact your local NXP representative to re-calculate the base FIT rate according to IEC/TR62380.

4.5 Assumed system safety goals

As FS26 is developed as a “Safety-related Element Out of Context”, the following system safety goals are assumed:

System Safety Goal (SA1_1): An element shall be available that monitors MCU and other peripherals supply voltage to transition the system into safe state ➔ **ASIL D required.**

System Safety Goal (SA2_1): A safe state control mechanism shall be available to open or close (instantaneously or after a specified delay) relays and isolate the battery cells from the power domain in case of system failure ➔ **ASIL D required.**

System Safety Goal (SA1_2): MCU shall be monitored by an error monitor in case of MCU HW failure (i.e. FCCU) ➔ **ASIL D required.**

System Safety Goal (SA1_3): MCU shall be monitored by a watchdog ➔ **ASIL D required.**

4.5.1 Functional Safety Requirements

To satisfy the assumed system safety goals, described in the **Chapter 4.5**, the Functional Safety Requirements in normal operating mode (FS0B released) are:

Component Safety Requirement (CSR001): All output voltages of the voltage regulators (VPRE, VCORE, LDO1, LDO2, TRK1, TRK2, VREF) must remain within the programmed voltage ranges when reset output FS0B and/or FS1B are not asserted.

Component Safety Requirement (CSR002): The FS26 shall provide an independent WD monitoring to the MCU. Fault reaction time could be different based on WD window period configuration and counter strategy. Fault reaction time < 9.5ms

Component Safety Requirement (CSR003): The FS26 shall provide an independent monitoring of the MCU HW failure pins (i.e. FCCU). Fault reaction time shall be <250us

4.6 Safe states

The assumed FS26 safe states are listed below:

- Explicitly indicating an error: Fail-safe output(s) FS0B (and FS1B) asserted low (FS0B < 0.5V; FS1B < 0.5 V)
- Completely unpowered: VSUP_PWR=VSUP=0V

It is assumed that an external switch, controlled by the MCU and by the FS26, is available to unpower the application, or de-activate various functions in the ECU (e.g. enable pin).

It is assumed the system safe state from an automotive power train application (Battery Management System, Electrical Power Steering, …) is when the communication protocol to the master ECU is disabled (e.g. CAN). The fail-safe output signal(s) from the FS26 (FS0B or FS1B) disables the transceiver when asserted.

4.6.1 Faults reaction on safety outputs

In normal operation when FS0B and RSTB are released, the table 7 below list all the faults and their impact on RSTB and FS0B pins according to the device configuration. In Orange, the reaction in not configurable. In Green, the reaction is configurable by SPI for RSTB and FS0B during *Init FS* state.

System Integration Requirement: [SIR_01] it is the system integrator's responsibility to make sure the MCU checks the FS_GRL_FLAGS and FS_STATES registers after each RSTB or FS0B assertion

Rationale: To allow the MCU to diagnose why RSTB or FS0B was asserted and take appropriate action

Table 7 Application related Fail-safe fault list and reaction

Apps related Fail-safe Faults	Fault error counter update	FS0B assertion	RSTB assertion	§
VPRE power rail overvoltage	+1	VMON_PRE_OV_FS_REACTION [0]	VMON_PRE_OV_FS_REACTION [1]	5.2.3
VCORE power rail overvoltage	+1	VMON_CORE_OV_FS_REACTION [0]	VMON_CORE_OV_FS_REACTION [1]	5.2.4
VLDO1 power rail overvoltage	+1	VMON_LDO1_OV_FS_REACTION [0]	VMON_LDO1_OV_FS_REACTION [1]	5.2.5
VLDO2 power rail overvoltage	+1	VMON_LDO2_OV_FS_REACTION [0]	VMON_LDO2_OV_FS_REACTION [1]	5.2.6
VTRK1 power rail overvoltage	+1	VMON_TRK1_OV_FS_REACTION [0]	VMON_TRK1_OV_FS_REACTION [1]	5.2.7
VTRK2 power rail overvoltage	+1	VMON_TRK2_OV_FS_REACTION [0]	VMON_TRK2_OV_FS_REACTION [1]	5.2.8
VREF power rail overvoltage	+1	VMON_VREF_OV_FS_REACTION [0]	VMON_VREF_OV_FS_REACTION [1]	5.2.9
Over voltage on the analog input Monitoring	+1	VMON_EXT_OV_FS_REACTION [0]	VMON_EXT_OV_FS_REACTION [1]	5.2.10
VPRE power rail undervoltage	+1	VMON_PRE_UV_FS_REACTION [0]	VMON_PRE_UV_FS_REACTION [1]	5.2.3
VCORE power rail undervoltage	+1	VMON_CORE_UV_FS_REACTION [0]	VMON_CORE_UV_FS_REACTION [1]	5.2.4
VLDO1 power rail undervoltage	+1	VMON_LDO1_UV_FS_REACTION [0]	VMON_LDO1_UV_FS_REACTION [1]	5.2.5
VLDO2 power rail undervoltage	+1	VMON_LDO2_UV_FS_REACTION [0]	VMON_LDO2_UV_FS_REACTION [1]	5.2.6
VTRK1 power rail undervoltage	+1	VMON_TRK1_UV_FS_REACTION [0]	VMON_TRK1_UV_FS_REACTION [1]	5.2.7
VTRK2 power rail undervoltage	+1	VMON_TRK2_UV_FS_REACTION [0]	VMON_TRK2_UV_FS_REACTION [1]	5.2.8
VREF power rail undervoltage	+1	VMON_VREF_UV_FS_REACTION [0]	VMON_VREF_UV_FS_REACTION [1]	5.2.9
Undervoltage on the analog input Monitoring	+1	VMON_EXT_UV_FS_REACTION [0]	VMON_EXT_UV_FS_REACTION [1]	5.2.10
An error is sent by the MCU on FCCU1 and FCCU2 pins (dual wire protocol)	+1	FCCU12_FS_REACTION [0]	FCCU12_FS_REACTION [1]	5.2.12
An error is sent by the MCU on FCCU1 pin (single wire protocol)	+1	FCCU1_FS_REACTION [0]	FCCU1_FS_REACTION [1]	5.2.12
An error is sent by the MCU on FCCU2 pin (single wire protocol)	+1	FCCU2_FS_REACTION [0]	FCCU2_FS_REACTION [1]	5.2.12
An external IC is driving to the error state the signal connected on ERRMON pin	+1	ERRMON_ FS_REACTION [0]	ERRMON_ FS_REACTION [1]	5.2.8
Watchdog error counter reaches its maximum value (WD_ERR_CNT = WD_ERR_LIMIT)	+1	WD_FS_REACTION [0]	WD_FS_REACTION [1]	5.2.11
The Fault Error counter reaches its intermediate value: (WD_ERR_LIMIT)/2	none	FLT_ERR_REACTION [0]	FLT_ERR_REACTION [1]	5.2.18
Wrong WD refresh in INIT_FS state	+1	Yes	Yes	5.2.11
No WD refresh in INIT_FS	+1	Yes	Yes	5.2.11
RESET pin asserted externally	+1	No	Yes (low externally)	5.2.16
RSTB pulse request by MCU	No	No	Yes	5.2.16
RSTB Short to high	+1	Yes	No (high externally)	5.2.16
FS0B Short to high	+1	No (high externally)	BACKUP_SAFETY_PATH_FS0B [0]	5.2.17
FS0B request by the MCU	No	Yes	No	5.2.17
FS1B Short to high	+1	No (high externally)	BACKUP_SAFETY_PATH_FS1B [0]	5.2.17
FS1B request by the MCU	No	Yes	No	5.2.18

REG_CORRUPT = 1	+1	Yes	No	5.2.1
OTP_CORRUPT = 1	+1	Yes	No	5.1.2

4.6.2 Release from safe state

When the fail-safe output(s) FS0B (and FS1B) is (are) asserted low by the device due to a fault, the exit conditions must be validated before allowing these pins to be released. These conditions are:

- Fault is removed
- LBIST_OK
- ABIST_OK
- Fault Error Counter = 0
- SPI write to RELEASE_FS0B_FS1B [15:0] register:
  - Bits 15, 14 and 13 will select the safety(s) output(s) to release
  - Bits 12 to 0 filled with ongoing FS_WD_TOKEN reversed and complemented

Below is depicted the procedure to compute the RELEASE_FS0B_FS1B [15:0] value to release the safety outputs. **Table 8** illustrate all these steps with an example:

1. The first step to get the FS_WD_TOKEN value.
2. The second step is to swap MSB/LSB of the value get in step #1.
3. The second step is to invert all computed bits at step #2.
4. The fourth step is to write bits 12 to 0 computed in step #3 into RELEASE_FS0B_FS1B [12:0] register. Bits 15 to 13 are used to select the safety output(s) to release as shown in table 9.

Table 8 Example of Procedure to release FS0B and FS1B

Step #1	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	B0
Read FS_WD_TOKEN [15:0]	1	1	1	0	0	1	0	0	1	1	1	1	0	0	0	0

Step #2	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	B0
Reverse LSB/MSB	0	0	0	0	1	1	1	1	0	0	1	0	0	1	1	1

Step #3	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	B0
Complement bits	1	1	1	1	0	0	0	0	1	1	0	1	1	0	0	0

Step #4	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	B0
Write to RELEASE_FS0B_FS1B [12:0]	**1**	**0**	**1**	1	0	0	0	0	1	1	0	1	1	0	0	0

Table 9 Bits 15 to 13 RELEASE_FS0B_FS1B register bit description

Bit	Symbol	Description
15 to 13	RELEASE_FS0B_FS1B	**Bits to select the desired safety output to release**
		011 Release FS0B only
		110 Release FS1B only
		101 Release FS0B and FS1B

4.7 Single-point fault tolerant time interval and process safety time

The single-point fault tolerant time interval (FTTI)/process safety time (PST) is the time span between a failure having the potential to cause a hazardous event, and the time by which counteraction must be completed to prevent the hazardous event from occurring. It is used to define the sum of the worst-case fault indication time and the time for execution of corresponding countermeasures (reaction). **Figure 3** shows the FTTI for a single-point fault occurring in the SBC (a) with an appropriate functional safety mechanism to handle the fault (b). Without any suitable functional safety mechanism, a hazard may appear after the FTTI elapsed (c).

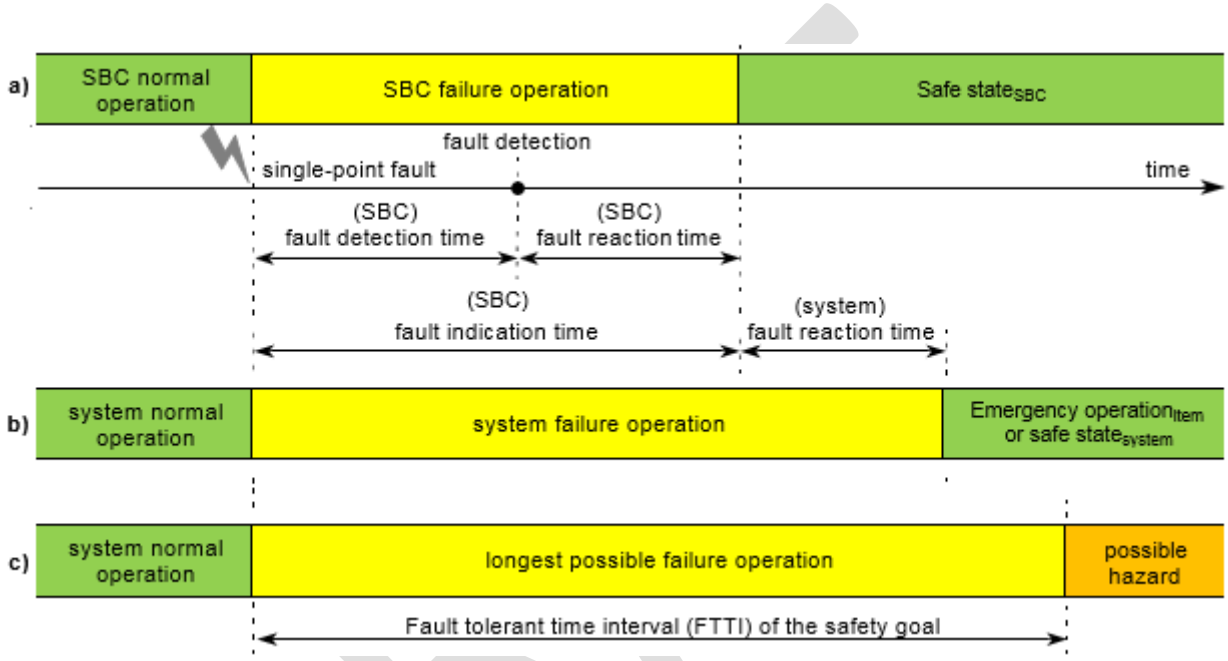

Figure 3 Fault tolerant time interval for single-point faults

Fault indication time is the time it takes from the occurrence of a fault to assert FS0B. **Fault indication time** of the SBC consists of **Fault detection time + Fault reaction time (Internal processing time + External indication time)**

The maximum **Fault indication time** is the sum of:

- The maximum **Fault detection time** of all involved functional safety mechanisms
- The maximum **Fault reaction time** of the reaction time of all involved functional safety mechanisms consisting of internal processing time and external indication time

The maximum **Internal processing time** for all internal safety mechanism is 1us except V1p6D_FS overvoltage which is 5us.

The External indication time to notify an observer about the failure external to the SBC is the time needed to activate Fail-safe output when the internal command is sent from digital and activates the analog drivers.

- The maximum **External indication time** is 12us for FS0B with 5.1KΩ pull up to VDDIO and 10nF pull down to GND.
- The maximum **External indication time** is 12us for FS1B with 5.1KΩ pull up to VDDIO and 10nF pull down to GND.
- The maximum **External indication time** is 4us for RSTB with 5.1KΩ pull up to VDDIO and 1nF pull down to GND.

The sum of the SBC fault indication time and system fault reaction time must be less than the FTTI of the system safety goal.

4.8 Faults and Failures definition

Failures are the main impairment to functional safety:

- A **systematic failure** is manifested in a deterministic way to a certain cause (systematic fault), which can only be eliminated by a change of the design process, manufacturing process, operational procedures, documentation, or other relevant factors. Thus, measures against systematic faults are reductions of systematic faults, for example, implementing and following adequate processes.
- A **random hardware failure** can occur unpredictably during the lifetime of a hardware element and follows a probability distribution. Thus, measures reducing the likelihood of random hardware faults are either the detection and control of the faults during the lifetime, or reduction of failure rates. A random hardware failure is caused by either a permanent fault (for example, physical damage), an intermittent fault, or a transient fault. Permanent faults are unrecoverable. Intermittent faults are for example, faults linked to specific operating conditions or noise. Transient faults are for example, EMI-radiation. An affected configuration register can be recovered by setting the desired value or by a power cycle. Due to a transient fault, an element may be switched into a self-destructive state (for example, single event latch-up), and therefore may cause permanent destruction.

4.8.1 Faults

The following random faults may generate failures, which may lead to the violation of a functional safety goal. Citations are according to ISO 26262-1. Random hardware faults occur at a random time, which results from one or more of the possible degradation mechanisms in the hardware.

- **Single-point fault (SPF):** A Single Point Fault is ‘a fault in an element not covered by a safety mechanism and results to a single-point failure ‘which leads directly to the violation of a safety goal’. **Figure 4a** shows an SPF inside an element generating a wrong output.
- **Latent fault (LF):** A Latent Fault is a ‘multiple-point fault whose presence is not detected by a safety mechanism nor perceived by the driver’. A Latent Fault is a fault which does not violate the functional safety goal(s) itself but leads in combination with at least one additional independent fault to a dual- or multiple-point failure, which then leads directly to the violation of a functional safety goal. **Figure 4b** shows a Latent Fault inside an element, which still generates a correct output.
- **Residual fault (RF):** An RF is a ‘portion of a fault which by itself leads to the violation of a safety goal’, ‘where the portion of the fault is not covered by a functional safety mechanism’. **Figure 4c** shows a Residual Fault inside an element, which - although a functional safety mechanism is set in place - generates a wrong output, as this particular fault is not covered by the functional safety mechanism.

- **Dual-point fault (DPF):** A Dual Point Fault is an 'individual fault which, in combination with another independent fault, leads to a dual-point failure', which leads directly to the violation to a goal. **Figure 4d** shows two Latent Faults inside an element generating a wrong output.
- **Multiple-point fault (MPF):** A Multiple Point Fault is an 'individual fault which, in combination with other independent faults, leads to a multiple-point failure', which leads directly to the violation of a functional safety goal. Multiple-point faults are not covered in functional safety concept of the FS26.
- **Safe Fault (SF):** An SF is a 'fault whose occurrence does not significantly increase the probability of violation of a safety goal'. Safe faults are not covered in this document. Single-point faults, residual faults, or dual-point faults are not safe faults.

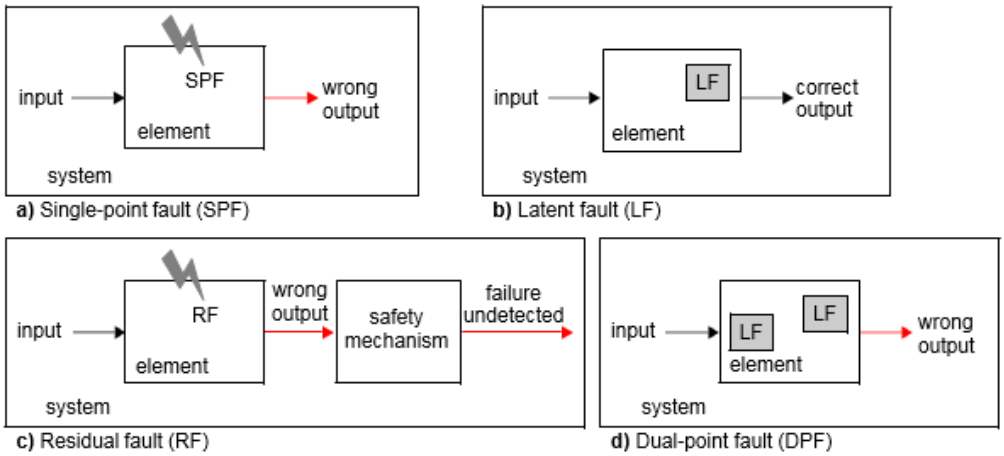

Figure 4 Faults types

Single Point Faults must be detected within the Fault Tolerant Time Interval. Latent Faults (dual-point faults) must be detected within the Multiple Point Fault Detection Interval. In automotive applications, Multiple Point Fault Detection Interval is generally accepted to be once per typical automotive trip time (t_{TRIP}) by test routines (for example, Built In Self Tests after power-up). This reduces the accumulation time of latent faults from the lifetime of the product t_{LIFE} to t_{TRIP}.

If an application requires to have a Multiple Point Fault Detection Interval shorter than the trip time, it's possible to check all voltages monitoring by SPI request in normal state.

4.8.2 Failures

- **Common cause failure (CCF):** Common Cause Failure is a coincidence of random failure states of two or more elements in separate channels of a redundancy element, leading to the defined element failing to perform its intended safety function, resulting from a single event or root cause (chance cause, non-assignable cause, noise, natural pattern, …). Common cause failure causes the probability of multiple channels (N) having a failure rate to be larger than $\lambda_{\text{single channel}}^{N}$ ($\lambda_{\text{redundant element}} > \lambda_{\text{single channel}}^{N}$)

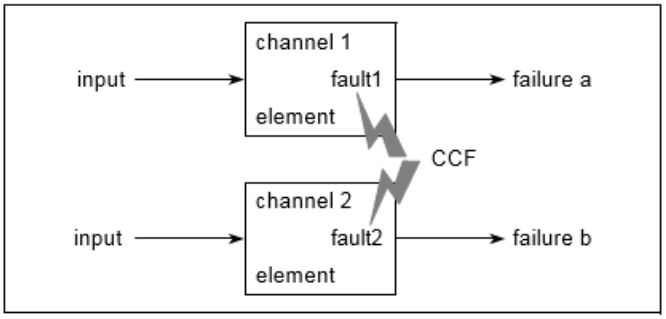

Figure 5 Common cause failures

- **Common mode failure (CMF):** Common Mode Failure is a subset of Common Cause Failure. A single root cause leads to similar coincidental erroneous behavior (with respect to the safety function) of two or more (not necessarily identical) elements in redundant channels, resulting in the inability to detect the failures. **Figure 6** shows three elements within two redundant channels. One single root cause (CMF A or CMF B) leads to undetected failures in the primary channel and in one of the elements of the redundant channel.

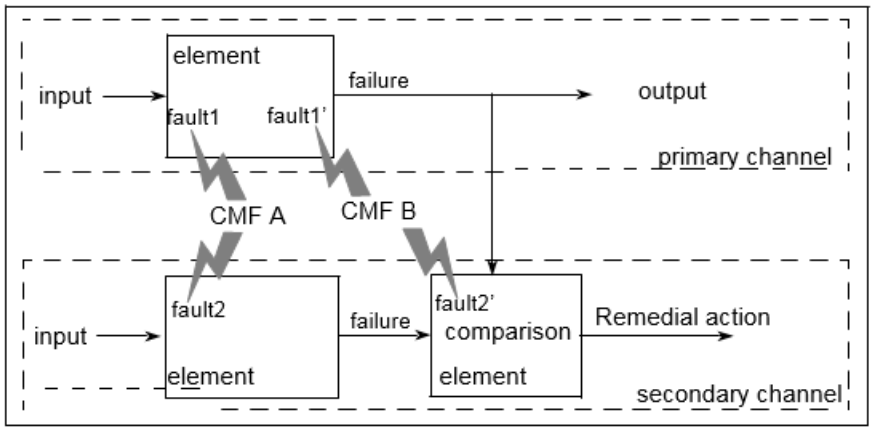

Figure 6 Common mode failures

- **Cascaded failure (CF):** Cascaded Failures occur when local faults of an element in a system ripple through interconnected elements causing another element or elements of the same system and within the same channel to fail. Cascading failures are dependent failures, not common cause failures. **Figure 7** shows two elements within a single channel, to which a single root cause leads to a fault (fault 1) in one element resulting in a failure (failure a), and causing a second fault (fault 2) within the second element (failure b).

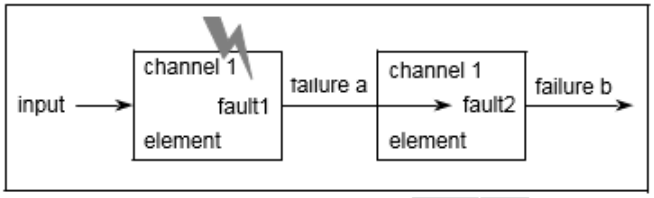

Figure 7 Common cause failures

4.8.3 Failure handling

Failure handling can be split into two categories:

- Failure handling before enabling the system level safety function (for example, during/following the MCU initialization). These errors are required to be handled before the system enables the safety function, or in a time shorter than the respective FTTI after enabling the safety function.
- Failure handling during runtime with repetitive supervision while the safety function is enabled. These errors have to be handled in a time shorter than the respective FTTI.

[SA_19]: It is assumed single-point and latent fault diagnostic measures complete operations (including fault reaction) in a time shorter than the respective FTTI when the safety function is enabled.

Recommendation: It is recommended to identify startup failures before enabling system level safety functions.

A typical failure reaction regarding power-up/start-up diagnostic measures is not to initialize and start the safety function, but instead to provide failure indication to the operator/user.

4.8.4 Failure rates

The FS26 failure rate data is derived from the IEC/TR 62380, to quantify the hardware architectural metrics for the evaluation of the effectiveness of the design architecture against the requirements for random hardware failures handling.

The random hardware failures addressed by these metrics are limited to some of the item's safety-related electrical and electronic hardware parts, namely those which can significantly contribute to the violation or the achievement of the safety goal, and to the single-point, residual, and latent faults for those parts. Only the electrical failure modes and failure rates are considered for the FS26.

The IEC/TR 62380 considers the failure rate model for permanent faults in a semiconductor device to be the sum of three subcomponents:

- the **Die** predictive failure rate (8.756 FIT), which depends mainly on
  - silicon parameters like the technology and its maturity, the number of transistors
  - and application parameters like the mission profile, the power dissipation and the junction to ambient thermal resistance

- the **Package** predictive failure rate (33.3 FIT), which depends mainly on
  - package parameters like the number of pins, the pitch
  - and application parameters like the mission profile, the temperature cycles, the board material
- the **Interface electrical overstress** predictive failure rate (7 FIT), which depends mainly on
  - application parameters like cable length attached to global pins (three meters considered)

with a total device failure rate of **49.0 FIT.**

The transient faults are not considered for FS26 developed in 0.13 mm technology without SRAM. The only potential concern for soft errors would be in logic latches and flops. Logic soft error upsets are simply not a significant risk at this size nodes, due to higher voltage and capacitance, making it very difficult to cause an upset by radiation. However, advanced digital architecture mechanisms have been implemented into the FS26 device to detect permanent faults, and some can also mitigate transient fault. Those technics are the redundancy of the state machine, the oscillator, filtering glitches, Hamming, and ECC technics.

The method used to evaluate and to quantify the hardware architectural metrics is based on the FMEDA, which details the determination of error causes and their impact on the system. The hardware architectural metrics are dependent upon the context of use of the FS26:

- Mission profile of the application in which the FS26 are operating
- Selection/usage of the functions and functional safety mechanisms implemented in the application

4.8.5 FMEDA overview

The FS26 is developed according to the ISO26262 standard, then a functional safety failure analysis on the hardware design was performed to identify failure causes and their effects with quantitative safety metric values. FMEDA inductive analysis as the method was applied. This FMEDA is based on Microsoft Excel sheets with the capability to enable safety analysis of the FS26 features implemented for a specific application.

The FS26 FMEDA sheet is an example only, based on the result of the safety analysis performed for the context of use of the FS26, using the mission profile described in **4.4.3**. This quantitative analysis is done considering all System Integration Requirements identified as **[SIR_xx]** and all Safety Assumptions **[SA_xx]** mentioned in this safety manual.

System Integration Requirement: [SIR_02] FMEDA safety metrics are achieved with all internal Safety Mechanism implemented (SMx) and all external Safety Mechanism at Application level implemented (SMAx). **Table 12** to **Table 15** are listing all integrated safety mechanisms into the FS36 and all external safety mechanism that are needed at application level.

In a context of customer applications, the FMEDA example provided by NXP must be customized to fit for the application requirements. The final customized FMEDA is under the responsibility of the customer, and then solely responsible for the safety metric values.

The FS26 FMEDA document associated with the FS26 failure rate estimation document is available upon request, when covered by NXP Semiconductors NDA (contact your local NXP representative).

5 Safety concept and Safety architecture

5.1 Safety architecture

The FS26 is designed to be used in automotive applications which are needed to fulfill functional safety requirements, as defined by functional safety integrity levels (ASIL B for FS26xyB and ASIL D for FS26xyD).It's assumed that digital pins buffers are supplied (through VDDIO pin) by a voltage generated and monitored by the FS26 (LDO1 is used into the FEDA. **Figure 8** shows the safety architecture example using the FS2633D high end version of the family with all features enabled.

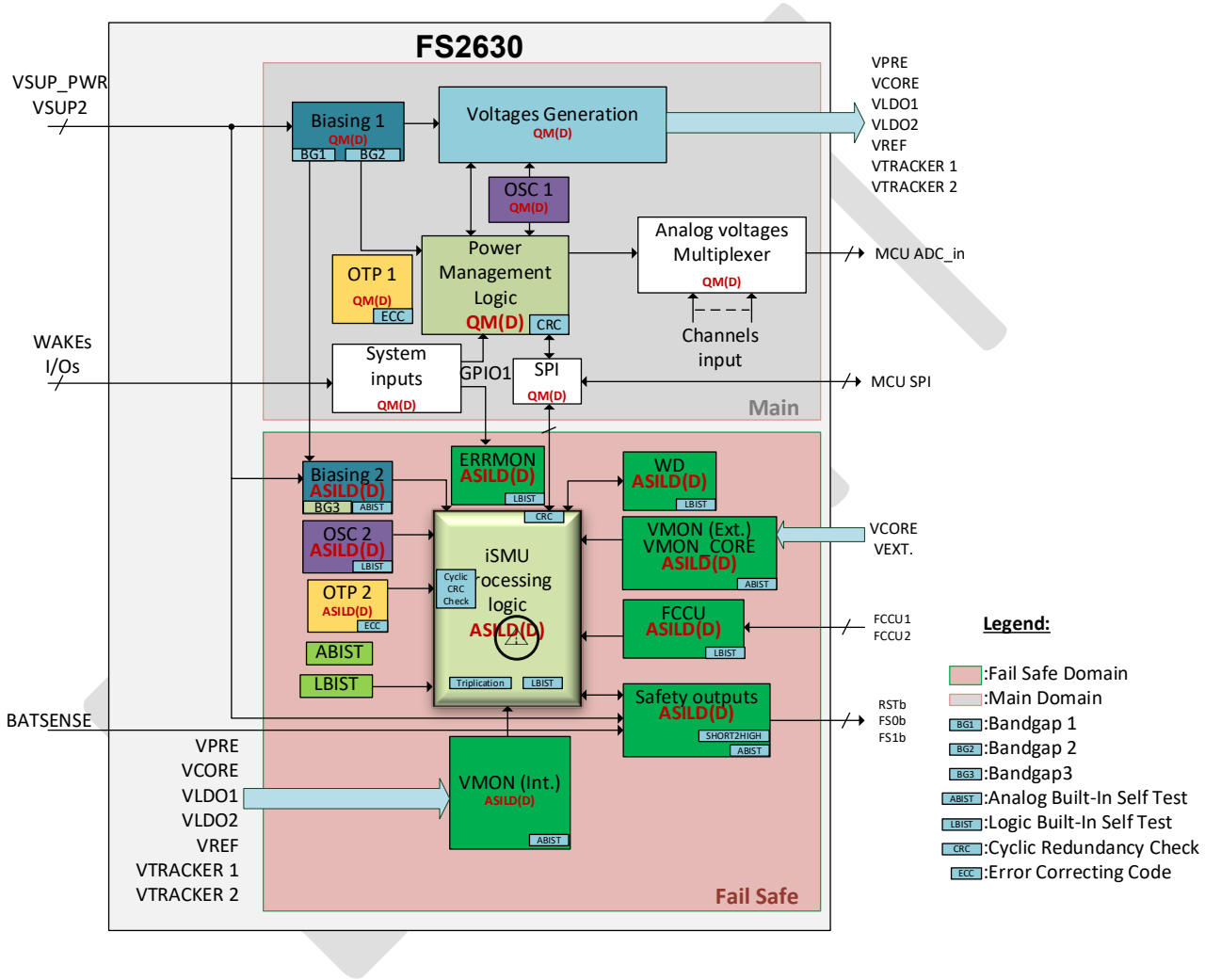

Figure 8 Safety Architecture

The FS26 is composed of two domains called the Main domain and the Fail-Safe domain. The Fail-Safe circuitries are electrically independents and physically isolated from the main circuitries. The Fail-Safe domain is described as a safety island where all the monitoring plus additional safety functions are implemented. The safety diagnostic and mitigation paths are performed by a dedicated state machine (Fail Safe State Machine). The Fail-Safe state machine is powered by dedicated and independent protected Analog and Digital reference blocks. The FS26 has redundant grounds and supply pins.

5.1.1 Safety domain description

The FS26 safety mechanisms, combined with the system MCU's monitoring and fault management, keep the application in one of the specified safe states.

The MCU can read the status of the FS26 safety related features by reading SPI status registers. Such information must be used for diagnostics and servicing failures.

The FS26 is defined in a context of safety and provides the following set of mechanisms to achieve the safety goals in such context.

- Redundant supplies with VSUP and VSUP_PWR pins
- Redundant grounds with GND and GNDFS pins and the exposed pad
- Physical isolation using multiple deep trenches mosfets
- Independent Fail-Safe State Machine
    - With an independent oscillator to generate the clock of the Fail-safe digital
    - With a monitoring of the main clock
    - With an independent power supply of the Fail-safe digital
- Independent Voltage Supervisor in charge of monitoring safety related regulators and internal reference voltages
    - With an independent reference voltage used for the OV/UV comparators
    - With an independent power supply of the UV/OV comparators
- Challenger watchdog function (FS26xyD – ASIL D) in charge of monitoring the MCU
- Simple watchdog function (FS26xyB – ASIL B) in charge of monitoring the MCU
- FCCU function (FS26xyD – ASIL D) in charge of monitoring the MCU HW error outputs
- Fault Recovery Strategy (FS26xyD – ASIL D) in combination with NXP S32x MCU family
- ERRMON function in charge of monitoring an External IC error output (not the MCU)
- RSTB output to reset the MCU (software reset)
- FS0B safety output to transition the system in safe state
- FS1B secondary safety output to transition the system in safe state
- SPI interface with CRC to configure, diagnose and refresh the Watchdog
- Integrated Analog and Logical Built In Self-test to detect latent failures

The FS26xyD and the FS26xyB are sharing the same independent safety architecture represented in **Figure 9**. The safety related functions not used in the FS26xyB, listed in **Chapter 4.2** are disabled by OTP.

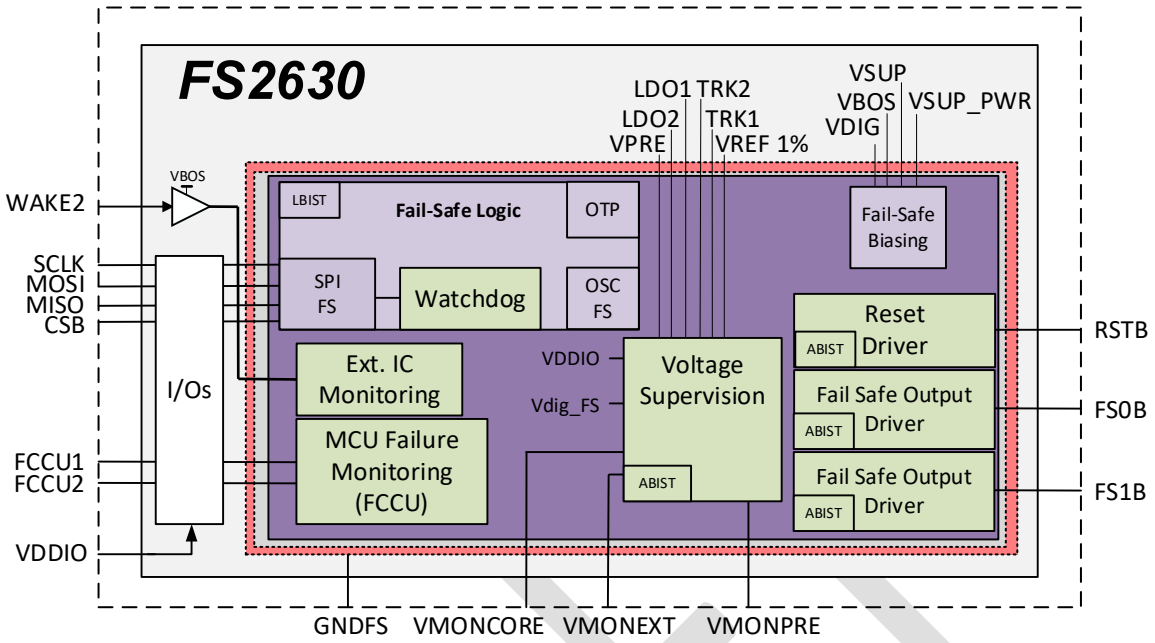

Figure 9 Fail Safe Block diagram

5.1.2 OTP configuration of the safety domain

Some safety features of the FS26xyD and FS26xyB safety domain are configurable by OTP. The exhaustive list of OTP configuration is given in the **Table 10** below.

Table 10 – OTP register map for functional safety settings

ADDRESS	Register Name	Default	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
0F	CFG_OVUV_1_OTP	0010_1100	SPARE0_OTP	SPARE3_OTP	VPRE_V_OTP[5:0] 0x3F: 6.35V | 0x20: 4.80 V |0x00: 3.20 V					
10	CFG_OVUV_2_OTP	0100_0110	VCORE_V_OTP[7:0] 0xFF: 3.35V | 0x80: 2.08 V |0x00: 0.80 V							
11	CFG_OVUV_3_OTP	0111_1111	SPARE1_OTP	TRK2_V_OTP[1:0] 0x03: 5.0 V |0x02: 3.3 V 0x01: 1.8 V |0x00: 1.2 V		TRK1_V_OTP[1:0] 0x03: 5.0 V |0x02: 3.3 V 0x01: 1.8 V |0x00: 1.2 V		LDO1_V_OTP 0x01: 5.0 V |0x00: 3.3 V	LDO2_V_OTP 0x01: 5.0 V |0x00: 3.3 V	VREF_V_OTP 0x01: 5.0 V |0x00: 3.3 V
12	CFG_OVUV_4_OTP	0000_0000	VMON_PRE_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_PRE_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
13	CFG_OVUV_5_OTP	0000_0000	VMON_CORE_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_CORE_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
14	CFG_OVUV_6_OTP	0000_0000	VMON_LDO1_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_LDO1_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
15	CFG_OVUV_7_OTP	0000_0000	VMON_LDO2_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_LDO2_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
16	CFG_OVUV_8_OTP	0000_0001	VMON_TRK1_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_TRK1_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
17	CFG_OVUV_9_OTP	0000_0000	VMON_TRK2_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_TRK2_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
18	CFG_OVUV_10_OTP	0000_0000	VMON_VREF_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_VREF_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
19	CFG_OVUV_11_OTP	0000_0000	VMON_EXT_UVTH_OTP[3:0] 0x0F: 112.0 % | 0x08: 108.5 % |0x00: 104.5 %				VMON_EXT_OVTH_OTP[3:0] 0x0F: 88 % | 0x08: 91.5 % |0x00: 95.5 %			
1A	CFG_OV_DGLT_OTP	1111_1111	VMON_EXT_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_REF_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_TRK2_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_TRK1_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_LDO2_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_LDO1_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_PRE_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs	VMON_CORE_OVDGLT_OTP 0x01: 45 µs | 0x00: 45 µs
1B	CFG_UV_DGLT1_OTP	1111_1111	VMON_LDO2_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_LDO1_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_PRE_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_CORE_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs	
1C	CFG_UV_DGLT2_OTP	1111_1111	VMON_EXT_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_REF_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_TRK2_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs		VMON_TRK1_UVDGLT_OTP[1:0] 0x03: 40 µs | 0x02: 25 µs | 0x01: 15 µs | 0x00: 5 µs	
1D	CFG_ABIST1_OTP	0000_0001	ABIST1_EXT_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_VREF_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_TRK2_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_TRK1_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_LDO2_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_LDO1_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_VCORE_EN_OTP 0x01: Enabled | 0x00: Disasbled	ABIST1_VPRE_EN_OTP 0x01: Enabled | 0x00: Disasbled
1E	CFG_MODE_OTP	0010_0000	WD_INIT_TIMEOUT_OTP[1:0] 0x00: 256 ms 0x01: 1024 ms 0X02: 32.5 s 0x03: 67.0 s		WD_DIS_OTP 0x00: WD timer enabled 0x01: WD timer disabled	DIS8S_DIS_OTP 0x00: 8 second timer enabled 0x01: 8 second timer disabled	PRE_RSTB_DLY_EN_OTP 0x01: 100 µs | 0x00: 0 µs	FS1B_FSOB_EN_OTP 0x00: Delayed assertion enabled 0x01: Delayed assertion disabled	FAULT_DFS_EN_OTP 0x01:Go to DFS when FSOB or RSTB asserted 0x00: Go to DFS when FLT_ERR_CNT = max	WAKE2_LP_EN_OTP 0x01: Enabled | 0x00: Disasbled
1F	CFG_LBIST_STDBY_OTP	0000_0000	LBIST_STDBY_OTP[7:0] 0xC9: Bypass LBIST from standby| 0x00: Always perform LBIST							

System Integration Requirement: [SIR_03] it is the system integrator's responsibility to define the OTP configuration desired for its safety application using the latest revision of the GUI to define its desired configuration.

Rational: To align the safety performance of the device with the system integrator's safety concept.

OTP programming by the system integrator is not allowed in production. NXP must do the OTP programming for parts in production. OTP programming by the system integrator is allowed only for engineering purpose during development (for OTP configuration validation for example).

Multiple safety features are depending on OTP. In order to ensure a robust safety configuration, the Fail-safe OTP settings are protected by a Cyclic Redundancy Check (CRC). The CRC signature is verified every 5ms as soon as the OTP configuration is loaded in the digital mirror registers used to configure the device. In case of bit flip, the failure is detected and reported thru the OTP_CORRUPT bit in FS_STATES register. The FS0B pin is asserted.

5.1.3 Fail-safe domain Voltage monitoring

The Fail-safe voltage supervision is using the independent reference voltage BG3 for all its UV/OV comparators. It monitors the internal supplies used for the Fail-Safe state machine and all the voltage regulators generated by the FS26 or external system supplies thru VMONEXT.

Two internal power rails are used to supply the analog (named VANA_FS) and digital (named VDIG_FS) of the Fail-Safe domain in this device. VANA_FS and VDIG_FS are both generated from the V5_FS supply.

V5_FS supply is generated from the VBOS supply from the main. In order to protect the whole fail-safe circuitry, a voltage clamp is implemented on the V5_FS supply (SMEAS4: V5_FS_CLAMP). V5FS_clamp works up to VSUP max rating voltage and does not requires overvoltage detection.

Then this protected supply (V5_FS) is used to generate both VANA_FS and VDIG_FS. In ordered to make sure that both analog and digital power rails are in a good range, a power on reset mechanism is implemented for both VANA_FS and VDIG_FS (SM29 and SM6). In addition, an overvoltage protection is implemented to monitor the digital supply VDIG_FS.

VDIG_FS overvoltage detection (SM24) will assert RSTB, FS0B and FS1B pins and the diagnostics may be available in the FS_DIGREF_OV bit in FS_DIAG_SAFETY1 register if the digital block is not damaged by the overvoltage.

In case of fail-safe logic circuitry failure (logic failure or biasing failure) a signal from the Logical Built In Self-Test checker is used to assert safety output. This safety mechanism is called Backup safety path (FS0b) in case of FS biasing or logic failure (SM18).

To ensure that safety outputs can be driven low at any time, various supplies are used to bias each gate drivers of RSTB, FS0B and FS1B open drains. This safety mechanism is called redundant RSTB, FSxB Driver supply available (SM21).

5.1.4 Main domain Voltage monitoring

The Main voltage supervision is using the reference voltage BG1 for all its UV/OV comparators. It monitors the internal V1P6D_Main and V1P6A_Main supplies used for the Main state machine and some voltage regulators (VSUP, VBOS, VPRE, VBOOST) generated by the FS26 to manage the state machine transitions, guarantee its functionality and protect the power management domain of the device.

V1P6D_Main and V1P6A_Main are two internal regulators used to supply the digital and analog of the Main domain of the device. V1P6D_Main undervoltage and V1P6A_Main undervoltage (SM27) corresponds to power on reset state of the Main domain of the device where RSTB, FS0B and FS1B pins are asserted low by the redundant analog path from VSUP.

VBOS regulator manages the best of supply from VSUP and VPRE to efficiently generate a 5V output to supply the internal biasing of the device. VBOS undervoltage (SM67) may not guarantee the full functionality of the device. Consequently, VBOS undervoltage detection power down the device and assert RSTB, FS0B and FS1B pins thru the redundant analog path to VSUP, and finally thru the integrated pull-down resistors if the device is completely unpowered.

5.1.5 Fail-safe clock monitoring (SM 48)

The independent Fail-safe oscillator, running at 20Mhz, is monitored against frequency drift more than +/-50% and stuck at fault. An oscillator failure condition will be detected within 2ms and reported thru the FS_OSC_DRIFT bit in FS_DIAG_SAFETY1 register. FS0B and FS1B pins are asserted. This feature can be disabled with the bit CLK_MON_DIS in F_I_FSSM register. However, disabling this feature may induce the inability to guaranty the FS26 safe state activation within the FFTI time.

5.2 Safety interoperation with MCU

This section describes safety interoperation between the FS26 and the MCU for applications requiring high functional safety integrity levels. Failure rates of external devices must be included in the system FMEDA by the system integrator.

5.2.1 Communication interface

The FS26 communicates with the MCU thru SPI. The communication is secured by an 8-bit CRC for each Write and Read command. Computation of a cyclic redundancy check is derived from the mathematics of polynomial division, modulo two. The CRC polynomial used is x^8+x^4+x^3+x^2+1. Refer to the datasheet **SPI Communication** chapter for more details.

5.2.1.1 Software diagnostic

Detailed SPI diagnostics are available reading FS_DIAG_SAFETY1 register:

- SPI_FS_CLK bit reports an error in the number of SPI clock cycles
- SPI_FS_REQ bit reports and Invalid Fail-Safe SPI access (Wrong Write or Read, Write to INIT registers in normal mode, wrong address)
- SPI_FS_CRC bit reports an error in the CRC

Generic Fail-Safe diagnostics are available reading FS_GRL_FLAGS register:

- FS_COM_G bit reports an error in the communication (SPI). If this bit is set, read the FS_DIAG_SAFETY1 register for a detailed diagnostic
- FS_WD_G bit reports an error on the Watchdog refresh. If this bit is set, read the FS_DIAG_SAFETY1 register for a detailed diagnostic
- FS_IO_G bit reports an error in one of the Fail Safe IOs. If this bit is set, read the FS_SAFE_IOS_1 register for a detailed diagnostic
- FS_REG_OVUV_G bit reports an error in one of the voltage monitoring (OV or UV). If this bit is set, read the FS_OVUVREG_STATUS register for a detailed diagnostic

System Integration Requirement: [SIR_04] it is the system integrator's responsibility to make sure the MCU checks the FS_GRL_FLAGS register after each Watchdog refresh

Rational: To ensure the safety diagnostic is available for the MCU in a timely manner

5.2.2 Initialization phase

After power up, wake up from Standby or RSTB assertion, the fail-safe state machine is moving through several states and wait in *Init_FS* state. In this state, the RSTB pin is released to high level and the MCU must configure FS_I_xxx registers and then perform a good watchdog refresh within 256 ms.

To secure the writing process during INIT_FS phase, in addition to CRC computation during SPI transfer, it is requested for the MCU to perform the following sequence for all FS_I_xxx registers:

1. Write the desired data in the FS_I_xxx register (DATA)
2. Write the opposite in the FS_I_NOT_xxx register (DATA_NOT)

When all FS_I_xxx and FS_I_NOT_xxx registers are written followed by a good watchdog refresh, the initialization phase is considered as closed and the state machine can move to *Safety Outputs not released* state. A real-time comparison process (XOR) is performed by the FS26 to ensure **DATA** FS_I_xxx = **DATA NOT** FS_I_NOT_xxx. If the comparison result is wrong, the REG_CORRUPT bit is set to '1' in FS_STATES register and FS0B pin is asserted.

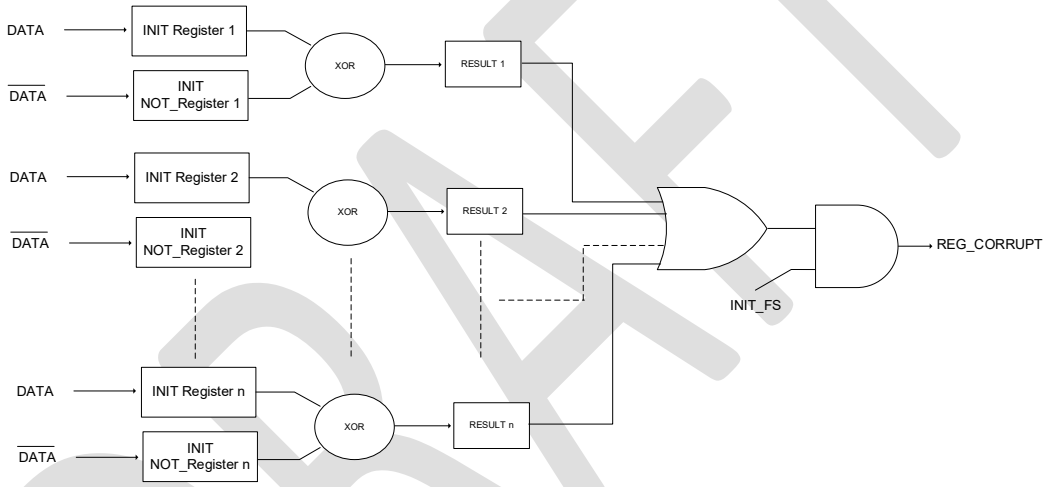

Figure 10 REG_CORRUPT logical diagram

As soon as the initialization phase is closed, the MCU must refresh the Watchdog periodically (see **5.2.11**).

The FS26 will go back to INIT_FS after the following two conditions:

- RSTB pin assertion (internal or external)
- SPI request by the MCU with the bit GOTO_INIT in FS_SAFE_IOS_1register

5.2.3 VPRE Monitoring (SM15 & SM16)

VMONPRE input pin is dedicated to monitor VPRE DCDC converter. Connection between VMONPRE pin and VPRE power rail need to be ensured by a PCB track.

5.2.3.1 OTP configuration

VPRE monitoring reference voltage must be equal to VPRE output voltage.

System Integration Requirement: [SIR_05] it is the system integrator's responsibility to verify that VPRE_OTP bits are identic to VPRE_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

VPRE monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_PRE_OVTH [3:0] OTP bits.

VPRE monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_PRE_UVTH [3:0] OTP bits.

VPRE monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_06] it is the system integrator's responsibility to configure the correct VPRE monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

VPRE monitoring overvoltage filtering time must be configured by OTP using VMON_PRE_OVDGLT_OTP bit.

VPRE monitoring undervoltage filtering time must be configured by OTP using VMON_PRE_UVDGLT_OTP [1:0] OTP bits. VPRE monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_07] it is the system integrator's responsibility to configure the correct VPRE monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the MCU according to its data sheet

The verification of VPRE monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_PRE_EN_OTP bit. If VPREMON is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If VPRE monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_08] it is recommended to assign VPRE monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VPRE monitoring to ABIST1.

Rational: To detect latent faults on VPRE monitoring OV/UV comparators

5.2.3.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VPRE monitoring, ABIST2_PRE need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_09] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VPRE monitoring OV/UV comparators when the application is running.

5.2.3.3 Hardware configuration

VPRE is intended to supply all regulators of the FS26. VMONPRE pin must be connected to VPRE regulator output.

System Integration Requirement: [SIR_10] it is the system integrator's responsibility to connect VMONPRE to VPRE regulator output.

Rational: In case of overvoltage detection on VPRE power rail, the VPRE will be disabled to protect all loads supplied by the FS26.

5.2.3.4 Software configuration and diagnostic

During initialization phase, the MCU configures the VPRE monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_PRE_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_PRE_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_11] It is the system integrator's responsibility to make sure the MCU configures the VPRE monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.3.5 Fault detection and reaction time

VPRE overvoltage detection time: VMON_PRE_OVDGLT_OTP (25 µs or 45us)

VPRE under voltage detection time: VMON_PRE_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.4 VCORE Monitoring (SM4 & SM5)

VMONCORE input pin is dedicated to monitor VCORE DCDC converter. Connection between VMONCORE pin and VCORE power rail need to be ensured by a PCB track.

5.2.4.1 OTP configuration

VCORE monitoring reference voltage must be equal to VCORE output voltage.

System Integration Requirement: [SIR_12] it is the system integrator's responsibility to verify that VCORE_OTP bits are identic to VCORE_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

VCORE monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_CORE_OVTH [3:0] OTP bits.

VCORE monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_CORE_UVTH [3:0] OTP bits.

VCORE monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_13] it is the system integrator's responsibility to configure the correct VCORE monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

VCORE monitoring overvoltage filtering time must be configured by OTP using VMON_CORE_OVDGLT_OTP bit.

VCORE monitoring undervoltage filtering time must be configured by OTP using VMON_CORE_UVDGLT_OTP [1:0] OTP bits. VCORE monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_14] it is the system integrator's responsibility to configure the correct VCORE monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the MCU according to its data sheet

The verification of VCORE monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_CORE_EN_OTP bit. If VCORE monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If VCORE monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_15] it is recommended to assign VCORE monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VCORE monitoring to ABIST1.

Rational: To detect latent faults on VCORE monitoring OV/UV comparators

5.2.4.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VCORE monitoring, ABIST2_CORE need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_16] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VCORE monitoring OV/UV comparators when the application is running.

5.2.4.3 Hardware configuration

VCORE is intended to supply all regulators of the FS26. VMONCORE pin must be connected to VCORE regulator output.

System Integration Requirement: [SIR_17] it is the system integrator's responsibility to connect VMONPE to VCORE regulator output.

Rational: In case of overvoltage detection on VCORE power rail, the VCORE will be disabled to protect all loads supplied by the FS26.

5.2.4.4 Software configuration and diagnostic

During initialization phase, the MCU configures the VCORE monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_CORE_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_CORE_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_18] It is the system integrator's responsibility to make sure the MCU configures the VCORE monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.4.5 Fault detection and reaction time

VCORE overvoltage detection time: VMON_CORE_OVDGLT_OTP (25 µs or 45us)

VCORE under voltage detection time: VMON_CORE_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.5 LDO1 Monitoring (SM3 & SM11)

In order to save pins and external connection, LDO1 output and its monitoring, LDO1 monitoring, are connected internally with a specific path from the DIE pad to the pin.

5.2.5.1 OTP configuration

LDO1 monitoring reference voltage must be equal to VLDO1 output voltage.

System Integration Requirement: [SIR_19] it is the system integrator's responsibility to verify that VLDO1_OTP bits are identic to VLDO1_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

LDO1 monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_LDO1_OVTH [3:0] OTP bits.

LDO1 monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_LDO1_UVTH [3:0] OTP bits.

LDO1 monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_20] it is the system integrator's responsibility to configure the correct LDO1 monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

LDO1 monitoring overvoltage filtering time must be configured by OTP using VMON_LDO1_OVDGLT_OTP bit.

LDO1 monitoring undervoltage filtering time must be configured by OTP using VMON_LDO1_UVDGLT_OTP [1:0] OTP bits. VLDO1 monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_21] it is the system integrator's responsibility to configure the correct LDO1 monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by LDO1 according to their data sheet.

The verification of LDO1 monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_LDO1_EN_OTP bit. If LDO1 monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If LDO1 monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_22] it is recommended to assign VLDO1 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VLDO1 monitoring to ABIST1.

Rational: To detect latent faults on VLDO1 monitoring OV/UV comparators

5.2.5.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VLDO1 monitoring, ABIST2_LDO1 need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_23] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VLDO1 monitoring OV/UV comparators when the application is running.

5.2.5.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VLDO1 monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_LDO1_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_LDO1_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_24] It is the system integrator's responsibility to make sure the MCU configures the VLDO1 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.5.4 Fault detection and reaction time

LDO1 overvoltage detection time: VMON_LDO1_OVDGLT_OTP (25 µs or 45us)

LDO1 under voltage detection time: VMON_LDO1_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.6 LDO2 Monitoring (SM13 & SM14)

In order to save pins and external connection, LDO2 output and its monitoring, LDO2 monitoring, are connected internally with a specific path from the DIE pad to the pin.

5.2.6.1 OTP configuration

LDO2 monitoring reference voltage must be equal to VLDO2 output voltage.

System Integration Requirement: [SIR_25] it is the system integrator's responsibility to verify that VLDO2_OTP bits are identic to VLDO2_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

LDO2 monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_LDO2_OVTH [3:0] OTP bits.

LDO2 monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_LDO2_UVTH [3:0] OTP bits.

LDO2 monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_26] it is the system integrator's responsibility to configure the correct LDO2 monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

LDO2 monitoring overvoltage filtering time must be configured by OTP using VMON_LDO2_OVDGLT_OTP bit.

LDO2 monitoring undervoltage filtering time must be configured by OTP using VMON_LDO2_UVDGLT_OTP [1:0] OTP bits. VLDO2 monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_27] it is the system integrator's responsibility to configure the correct LDO2 monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by LDO2 according to their data sheet.

The verification of LDO2 monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_LDO2_EN_OTP bit. If LDO2 monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If LDO2 monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_28] it is recommended to assign VLDO2 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VLDO2 monitoring to ABIST1.

Rational: To detect latent faults on VLDO2 monitoring OV/UV comparators

5.2.6.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VLDO2 monitoring, ABIST2_LDO2 need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_29] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VLDO2 monitoring OV/UV comparators when the application is running.

5.2.6.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VLDO2 monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_LDO2_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_LDO2_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_30] It is the system integrator's responsibility to make sure the MCU configures the VLDO2 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.6.4 Fault detection and reaction time

LDO2 overvoltage detection time: VMON_ LDO2 _OVDGLT_OTP (25 µs or 45us)

LDO2 under voltage detection time: VMON_ LDO2 _UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.7 TRK1 Monitoring (SM8 & SM9)

In order to save pins and external connection, TRK1 output and its monitoring, TRK1 monitoring, are connected internally with a specific path from the DIE pad to the pin.

5.2.7.1 OTP configuration

TRK1 monitoring reference voltage must be equal to VTRK1 output voltage.

System Integration Requirement: [SIR_31] it is the system integrator's responsibility to verify that VTRK1_OTP bits are identic to VTRK1_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

TRK1 monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_TRK1_OVTH [3:0] OTP bits.

TRK1 monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_TRK1_UVTH [3:0] OTP bits.

TRK1 monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_32] it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

TRK1 monitoring overvoltage filtering time must be configured by OTP using VMON_TRK1_OVDGLT_OTP bit.

TRK1 monitoring undervoltage filtering time must be configured by OTP using VMON_TRK1_UVDGLT_OTP [1:0] OTP bits. VTRK1 monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_33] it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by TRK1 according to their data sheet.

The verification of TRK1 monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_TRK1_EN_OTP bit. If TRK1 monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If TRK1 monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_34] it is recommended to assign VTRK1 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK1 monitoring to ABIST1.

Rational: To detect latent faults on VTRK1 monitoring OV/UV comparators

5.2.7.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VTRK1 monitoring, ABIST2_TRK1 need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_35] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VTRK1 monitoring OV/UV comparators when the application is running.

5.2.7.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VTRK1 monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_TRK1_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_TRK1_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_36] It is the system integrator's responsibility to make sure the MCU configures the VTRK1 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.7.4 Fault detection and reaction time

TRK1 overvoltage detection time: VMON_ TRK1_OVDGLT_OTP (25 µs or 45us)

TRK1under voltage detection time: VMON_ TRK1_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.8 TRK2 Monitoring (SM10 & SM12)

In order to save pins and external connection, TRK2 output and its monitoring, TRK2 monitoring, are connected internally with a specific path from the DIE pad to the pin.

5.2.8.1 OTP configuration

TRK2 monitoring reference voltage must be equal to VTRK2 output voltage.

System Integration Requirement: [SIR_37] it is the system integrator's responsibility to verify that VTRK2_OTP bits are equal to VTRK2_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

TRK2 monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_TRK2_OVTH [3:0] OTP bits.

TRK2 monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_TRK2_UVTH [3:0] OTP bits.

TRK2 monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_38] it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

TRK2 monitoring overvoltage filtering time must be configured by OTP using VMON_TRK2_OVDGLT_OTP bit.

TRK2 monitoring undervoltage filtering time must be configured by OTP using VMON_TRK2_UVDGLT_OTP [1:0] OTP bits. VTRK2 monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_39] it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by TRK2 according to their data sheet.

The verification of TRK2 monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_TRK2_EN_OTP bit. If TRK2 monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If TRK2 monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_40] it is recommended to assign VTRK2 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK2 monitoring to ABIST1.

Rational: To detect latent faults on VTRK2 monitoring OV/UV comparators

5.2.8.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VTRK2 monitoring, ABIST2_TRK2 need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_41] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VTRK2 monitoring OV/UV comparators when the application is running.

5.2.8.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VTRK2 monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_TRK2_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_TRK2_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_42] It is the system integrator's responsibility to make sure the MCU configures the VTRK2 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.8.4 Fault detection and reaction time

TRK2 overvoltage detection time: VMON_ TRK2_OVDGLT_OTP (25 µs or 45us)

TRK2under voltage detection time: VMON_ TRK2_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.9 VREF Monitoring (SM7 & SM47)

In order to save pins and external connection, VREF output and its monitoring, VREF monitoring, are connected internally with a specific path from the DIE pad to the pin.

5.2.9.1 OTP configuration

VREF monitoring reference voltage must be equal to VREF output voltage.

System Integration Requirement: [SIR_43] it is the system integrator's responsibility to verify that VREF_OTP bits are equal to VREF_V_OTP bits.

Rational: To ensure proper voltage monitoring and avoid unexpected OV/UV detection

VREF monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_VREF_OVTH [3:0] OTP bits.

VREF monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_VREF_UVTH [3:0] OTP bits.

VREF monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_44] it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the MCU according to its data sheet

VREF monitoring overvoltage filtering time must be configured by OTP using VMON_REF_OVDGLT_OTP bit.

VREF monitoring undervoltage filtering time must be configured by OTP using VMON_REF_UVDGLT_OTP [1:0] OTP bits. VREF monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_45] it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by VREF according to their data sheet.

The verification of VREF monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_VREF_EN_OTP bit. If VREF monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If VREF monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_46] it is recommended to assign VREF monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VREF monitoring to ABIST1.

Rational: To detect latent faults on VREF monitoring OV/UV comparators

5.2.9.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VREF monitoring, ABIST2_VREF need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_47] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VREF monitoring OV/UV comparators when the application is running.

5.2.9.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VREF monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_VREF_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_VREF_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_48] It is the system integrator's responsibility to make sure the MCU configures the VREF monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

5.2.9.4 Fault detection and reaction time

VREF overvoltage detection time: VMON_ VREF_OVDGLT_OTP (25 µs or 45us)

VREF voltage detection time: VMON_ VREF_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.10 Analog input Monitoring (SM69 & SM70)

Thanks to its extra monitoring pin, VMONEXT, the FS26 can monitor an additional voltage from the application. This extra voltage can be set as safety related at system level thanks to the monitoring proposed by the FS26.

5.2.10.1 OTP configuration

VMONEXT monitoring reference voltage must is 0.8 V fixed.

VMONEXT monitoring overvoltage thresholds must be configured by OTP, between +4.5% to +12% by step of +0.5% using VMON_EXT_OVTH [3:0] OTP bits.

VMONEXT monitoring undervoltage thresholds must be configured by OTP, between -4.5% to -12% by step of -0.5% using VMON_EXT_UVTH [3:0] OTP bits.

VMONEXT monitoring overvoltage and undervoltage configurations are independent and can be asymmetric.

System Integration Requirement: [SIR_49] it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage thresholds

Rational: To ensure overall operation of the device supplied by the power rail that VMONEXT is monitoring.

VMONEXT monitoring overvoltage filtering time must be configured by OTP using VMON_EXT_OVDGLT_OTP bit.

VMONEXT monitoring undervoltage filtering time must be configured by OTP using VMON_EXT_UVDGLT_OTP [1:0] OTP bits. VMONEXT monitoring overvoltage and undervoltage filtering times are independent and can be asymmetric.

System Integration Requirement: [SIR_50] it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage filtering times

Rational: To ensure overall operation of the safety related loads supplied by VMONEXT according to their data sheet.

The verification of VMONEXT monitoring overvoltage and undervoltage comparators must be configured by OTP using ABIST1_EXT_EN_OTP bit. If VMONEXT monitoring is "assigned" to ABIST1, overvoltage and undervoltage comparators will be verified during ABIST1 execution. If VMONEXT monitoring is "not assigned" to ABIST1, overvoltage and undervoltage comparators will not be verified during ABIST1 execution.

System Integration Requirement: [SIR_51] it is recommended to assign VMONEXT monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VMONEXT monitoring to ABIST1.

System Integration Requirement: [SIR_52] if VMONEXT is assign to ABIST1 self-test sequence, it's under the system integrator's responsibility to ensure that the voltage to be monitored on VMONEXT pin is available when ABIST1 sequence is ran by the FS26.

Rational: To avoid systematic latent fault detection during ABIST1.

5.2.10.2 ABIST on Demand

On top of the ABIST1, the MCU can check the integrity of the voltage comparators when the FS26 is in normal mode thanks to its ABIST on demand feature. To check comparators, the MCU need to request the ABIST on demand with FS_ABIST_ON_DEMAND SPI register. To check VMONEXT monitoring, ABIST2_EXT need to be set and LAUNCH_ABIST too. The FS26 will run self-test on comparators for the selected voltage monitoring. Self-test execution is indicated through ABIST2_DONE bit and the result is flagged in ABIST2_PASS bit, both bits are located into FS_DIAG_SAFETY1 register.

System Integration Requirement: [SIR_53] it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

Rational: To detect latent faults on VMONEXT monitoring OV/UV comparators when the application is running.

5.2.10.3 Software configuration and diagnostic

During initialization phase, the MCU configures the VMONEXT monitoring overvoltage and undervoltage impact on RSTB and FS0B with the FS_I_OVUV_SAFE_REACTION1 register:

- VMON_EXT_OV_FS_IMPACT[1:0] bits to configure the OV impact
- VMON_EXT_UV_FS_IMPACT[1:0] bits to configure the UV impact

Either FS0B only or RSTB and FS0B can be selected independently for OV and UV detection.

System Integration Requirement: [SIR_54] It is the system integrator's responsibility to make sure the MCU configures the VMONEXT monitoring OV and UV impact on RSTB and FS0B, FS1B during initialization phase after each RSTB release.

5.2.10.4 Fault detection and reaction time

VMONEXT overvoltage detection time: VMON_ EXT_OVDGLT_OTP (25 µs or 45us)

VMONEXT voltage detection time: VMON_ EXT_UVDGLT_OTP (5 µs or 15 µs or 25µs or 40us)

5.2.11 Watchdog monitoring (SM20 & SM20(bis))

The Watchdog is monitoring the software failures from the MCU by doing a periodical handshake with the FS26 thru SPI communication protocol.

5.2.11.1 OTP configuration

FS26xyD and FS26xyB watchdog monitoring must be enabled by OTP using WD_DIS OTP bit.

System Integration Requirement: [SIR_55] it is the system integrator's responsibility to enable the Watchdog monitoring for safety applications

Rational: To perform a periodic handshake (i.e. Watchdog) in order to confirm the correct behavior of the MCU software and bring the application in Fail-Safe state when needed

5.2.11.2 Software configuration and diagnostic

During initialization phase, the MCU configures the Watchdog monitoring with FS_I_WD_CFG register

- the Watchdog Error Counter Limit with WD_ERR_LIMIT[1:0] bits
- the Watchdog Refresh Counter Limit with WD_RFR_LIMIT[1:0] bits
- the Watchdog impact on RSTB and FS0B with WD_FS_REACTION [1:0] bits

By default, the Watchdog Window Period is set to 3ms and the Watchdog Window Duty Cycle is set to 50%. These settings can be changed during the initialization phase or during the Normal operation. The MCU configures these settings with the FS_WD_DURATION register

- the Watchdog Window Period with WDW_PERIOD[3:0] bits
- the Watchdog Window Duty Cycle with WDW_DC[2:0] bits

The Watchdog Window Period and the Watchdog Window Duty Cycle registers are triplicated, and a majority voter is implemented to avoid any unexpected change due to a bit flip. In case of a bit flip, the comparison is done with the two other registers and the bit in default is forced to be changed to the right value.

The Watchdog Window Period can be disabled during the initialization phase only. The watchdog disable is effective when the initialization phase is closed.

By default, the Watchdog Error Counter limit is 6. This counter is incremented by 2 after each bad Watchdog refresh. The Fault Error Counter is incremented by 1 and FS0B and RSTB will be asserted when this counter reaches its maximum value.

With default settings, after 3 consecutive bad Watchdog refreshes, both FS0B and RSTB will be asserted. In this case, the FS26 will react within 9ms, that is shorter than the FTTI time.

System Integration Requirement: [SIR_56] It is the system integrator's responsibility to make sure the MCU configures the Watchdog monitoring during the initialization phase after each RSTB release.

The first good Watchdog refresh closes the initialization phase. As soon as the initialization phase is closed, the MCU must refresh the Watchdog periodically in the middle of the OPEN window by writing the Watchdog answer in the FS_WD_ANSWER register. The Watchdog window is derived from the fail-safe oscillator with a +/-5% accuracy.

System Integration Requirement: [SIR_57] it is the system integrator's responsibility to make sure the MCU periodically refreshes the FS26xyD/ FS26xyB watchdog

		WD_Window	
		Closed	Opened
Watchdog Answer (from MCU)	Bad data	WD_failure	WD_failure
	Good data	WD_failure	WD_OK
	None	No issue	WD_failure

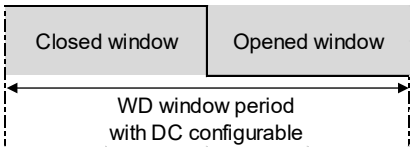

Figure 11 Watchdog refresh versus time window

For ASIL B applications, FS26xyB simple Watchdog is refreshed by a unique key. This key can be the default seed value read from FS_WD_TOKEN register which is always 0x5AB2, or the MCU can write its own seed in FS_WD_TOKEN register.

For ASIL C or D applications, FS26xyD challenger Watchdog is refreshed by a pseudo random key calculated from the Watchdog seed value read from FS_WD_TOKEN register. The seed is generated by a 16-bit linear feedback shift register implemented in the FS26xyD. The default seed value 0x5AB2 is available in the FS_WD_TOKEN register after power up or wake-up from Standby mode. During the initialization phase, the MCU can read the seed value to start its own calculation following the formula in Figure 13 below and write the watchdog answer in FS_WD_ANSWER register. The FS_WD_ANSWER register cannot be read.

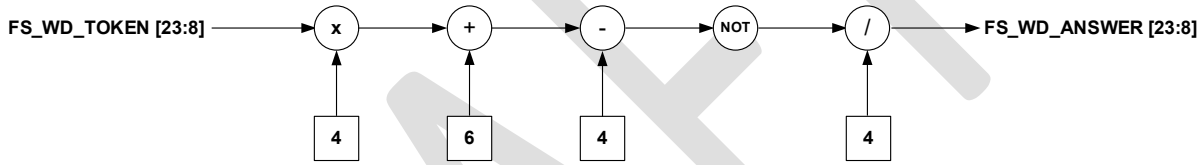

Figure 12 Challenger watchdog formula

System Integration Requirement: [SIR_58] it is the system integrator's responsibility to make sure the Watchdog answer calculation is correctly implemented in the MCU software

Rational: To ensure the maximum diagnostic coverage of the Watchdog safety mechanism avoiding software or calculation simplification.

The Watchdog Error Counter is triplicated, and a majority voter is implemented to avoid any unexpected change due to a bit flip. In case of a bit flip, the comparison is done with the two other registers and the bit in default is forced to be changed to the right value.

If the Watchdog Window Period or the Watchdog Window Duty Cycle is changed in normal operation:

- The new window period (except after disable) or the new window duty cycle is valid after the FS_WD_ANSWER register write command (good or bad WD) or when the previous WD window period is completed without any writing (WD timeout)
- The new WD window period after disable is valid after the FS_WDW_DURATION register write command
-

Some watchdog diagnostics are available reading FS_I_WD_CFG register:

- the Watchdog Error Counter value with WD_ERR_CNT[3:0] bits
- the Watchdog Refresh Counter value with WD_RFR_CNT[2:0] bits

Some watchdog diagnostics are available reading FS_DIAG_SAFETY1 register:

- WD_BAD_DATA bit reports a WD error due to a wrong calculation
- WD_BAD_TIMING bit reports a WD error due to an answer in the CLOSE window or a timeout error

5.2.11.3 Fault detection and reaction time

Watchdog detection time: WDW_PERIOD[3:0] (1 – 1024ms)

5.2.12 FCCU monitoring (SMLF5)

The FCCU input pins are monitoring the hardware failures from the MCU. The FCCU input pins can be configured by pair, or single independent inputs. The FCCU monitoring is active as soon as the initialization phase is closed.

5.2.12.1 OTP configuration

For FS26xyD FCCU monitoring is enabled. This monitoring is not available on FS26xyB.

System Integration Requirement: [SIR_59] it is the system integrator's responsibility to enable the FCCU monitoring for ASIL D safety applications

Rational: To listen to the error out signal of the MCU (i.e. FCCU) and bring the application in Fail-Safe state when needed.

If the FS26xyD is used in combination with NXP S32k3xx MCU and the FCCU monitoring is enabled, the FS26xyD Fault Recovery feature can be used for FS26xyD devices to benefit from the MCU Fault recovery strategy.

System Integration Requirement: [SIR_60] it is the system integrator's responsibility to select devices with Fault Recovery strategy of the FS26xyD if the Fault Recovery strategy of the MCU is used.

Rational: To ensure the Fault recovery operation of the MCU according to its data sheet

5.2.12.2 Hardware configuration by pair

It is recommended to use the FCCU configuration by pair with NXP MCU to benefit of the maximum diagnostic coverage for this safety mechanism.

When FCCU12 are used by pair, only the bi-stable protocol is supported. Refer to the respective NXP MCU data sheet to figure out how to select the bi-stable protocol.

System Integration Requirement: [SIR_61] it is the system integrator's responsibility to make sure the bi-stable protocol is configured in the NXP MCU for FCCU protocol

When FCCU12_FTL_POL = 0 (default), the internal pull up/down resistors can be used to provide passive error state if the MCU does not drive its FCCU output pins.

When FCCU12_FTL_POL = 1, external pull up/down resistors are required to provide passive error state if the MCU does not drive its FCCU output pins

System Integration Requirement: [SIR_62] it is the system integrator's responsibility to make sure the MCU configures the correct FCCU polarity during the initialization phase after each RSTB release.

The pull-down resistor must be at least 4 times bigger than the pull up resistor to detect FCCU1 short to FCCU2 failure mode, whatever the VDDIO voltage 3.3V or 5.0V.

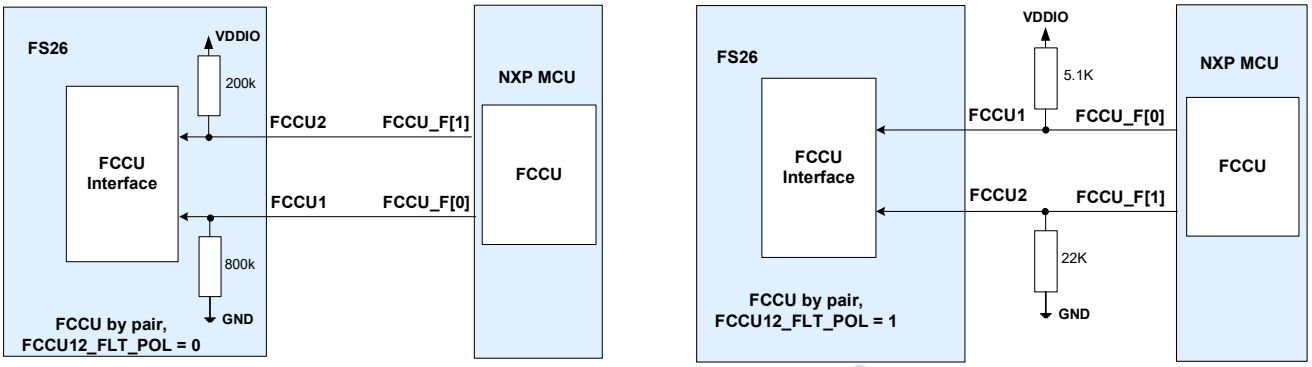

Figure 13 FCCU connection by pair

System Integration Requirement: [SIR_63] it is the system integrator's responsibility to make sure the correct pull up/down resistor values are properly connected to provide passive error state.

5.2.12.3 Hardware configuration as single independent input with static error level

In case the MCU has a single fault error output, it can be connected to one FS26xyD FCCU pin configured as single independent input.

When FCCUx_FTLT_POL = 0 (default), an external pull-down resistor provides passive error state if the MCU does not drive its fault error output pin.

When FCCUx_FTLT_POL = 1, an external pull-up resistor provides passive error state if the MCU does not drive its fault error output pin.

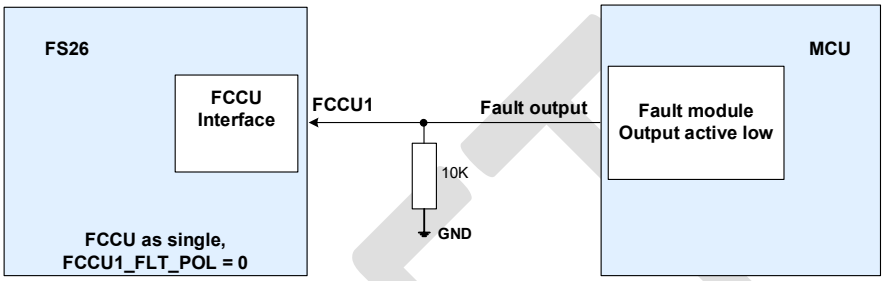

Figure 14 FCCU1 connection as a single independent input and FCCU1_FLT_POL = 0

System Integration Requirement: [SIR_64] It is the system integrator's responsibility to make sure the MCU fault error output is well connected to the FS26xyD FCCUx pin.

Rational: To detect FCCUx pin latent stuck at fault before releasing FS0B

Implementation hint: Toggle FCCUx pin and MCU check FCCUx_RT bit by SPI

5.2.12.4 Hardware configuration as single independent input with timing monitoring

In order to increase its compatibility with various MCU the FS26xyD is proposing to monitor both high and low levels timings to detect an error from the MCU. Some MCU in the market are using only one FCCU pin but the signal sent on this pin is a square waveform with a variable duty cycle.

When this timing monitoring is selected during the initialization phase with FCCU_CFG[2:0] = 110, high and low level timings are monitored on FCCU1 pin, level only is monitored on FCCU2 pin. When this timing monitoring is selected during the initialization phase with FCCU_CFG[2:0] = 111, high and low level timings are monitored on FCCU2 pin, level only is monitored on FCCU1 pin.

System Integration Requirement: [SIR_65] It is the system integrator's responsibility to make sure the MCU fault error output are capable to modulate high and low level timings and error timings are fitting FS26xyD high and low levels timings limits.

5.2.12.5 Software configuration and diagnostic

During INIT_FS, the MCU configures the FCCU monitoring with FS_I_SAFE_INPUTS register

- the FCCU configuration, by pair or single independent inputs with FCCU_CFG[2:0] bits
- if FCCU12 are used by pair:
  - the FCCU polarity with FCCU12_FLT_POL bit
  - the FCCU impact on RSTB and FS0B with FCCU12_FS_REACTION bit
- if FCCU1 is used as a single independent input:
  - the FCCU1 polarity with FCCU1_FLT_POL bit
  - the FCCU1 impact on RSTB and FS0B with FCCU1_FS_REACTION bit
- if FCCU2 is used as a single independent input:
  - the FCCU2 polarity with FCCU2_FLT_POL bit
  - the FCCU2 impact on RSTB and FS0B with FCCU2_FS_REACTION bit

System Integration Requirement: [SIR_66] It is the system integrator's responsibility to make sure the MCU configures the FCCU settings during INIT_FS after each RSTB release.

FCCU diagnostics are available reading FS_DIAG_SAFETY2 register:

- if FCCU12 are used by pair: FCCU12 bit reports an error detection
- if FCCU1 is used as a single independent input: FCCU1 bit reports an error detection
- if FCCU2 is used as a single independent input: FCCU2 bit reports an error detection

Whatever FCCU configuration, FCCU real-time pin state is available reading FS_DIAG_SAFETY2 register:

- FCCU1_RT and FCCU2_RT bits report the real-time pin state

5.2.12.6 Fault detection and reaction time

FCCU Fault detection time: t_{FCCU_ERR} (3 µs or 6us or 12 µs or 20µs) from datasheet

5.2.12.7 Fault Recovery Strategy

If the FS26 Fault Recovery feature is enabled by OTP, this function extends the watchdog window period to allow the MCU to perform a fault recovery strategy. The goal is to not reset the MCU while it is trying to recover the application after a failure event. When a fault is triggered by the MCU via its FCCU pins, the FS26xyD asserts FS0B pin and the watchdog window period becomes automatically an open window (no more duty cycle).

During INIT_FS, the MCU configures the Watchdog Window Recovery period when the device is in Fault Recovery Strategy with WDW_RECOVERY [3:0] bits in FS_WDW_DURATION register.

System Integration Requirement: [SIR_67] It is the system integrator's responsibility to make sure the MCU configures the Watchdog Window Recovery period during initialization phase after each RSTB release.

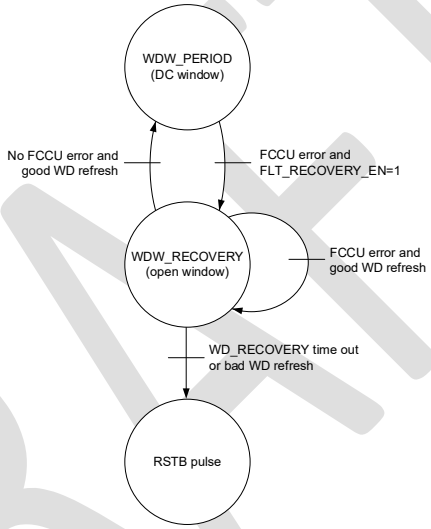

Figure 15 Fault recovery behaviour

The transition from WDW_PERIOD to WDW_RECOVERY happens when the FCCU pin indicates an error and FS0B is asserted. If the MCU send a good watchdog refresh before the end of the WDW_RECOVERY duration, the device switches back to the WDW_PERIOD duration and associated duty cycle if the FCCU pins does not indicate an error anymore. Otherwise, a new WDW_RECOVERY period is started. If the MCU does not send a good watchdog refresh before the end of the WDW_RECOVERY duration, then a reset pulse is generated, and the Fail-safe state machine moves back to initialization phase. Refer to data sheet chapter ***"Microcontroller fault recovery strategy"*** for more details.

5.2.13 ERRMON monitoring (SMLF6)

The WAKE 2 pin can be used to monitor an external IC on the application, neither the FS26, nor the MCU. This feature is available for FS26xyD part numbers. When this feature is available, WAKE 2 pin is no longer providing its wake up functionality. The ERRMON monitoring is active as soon as the initialization phase is closed.

System Integration Requirement: [SIR_68] it is the system integrator's responsibility to select part number with the ERRMON monitoring.

Rational: To listen to the error out signal of the external circuit (i.e. ERRMON) and bring the application in Fail-Safe state when needed.

5.2.13.1 Hardware configuration

The error output of the external IC to be monitored shall be connected to both the MCU and the FS26xyD WAKE2 input pin. A transition detected at ERRMON pin indicates an error from the external IC, seen by both the MCU and the FS26xyD. The FS26xyD waits the MCU acknowledgement by SPI before reaction.

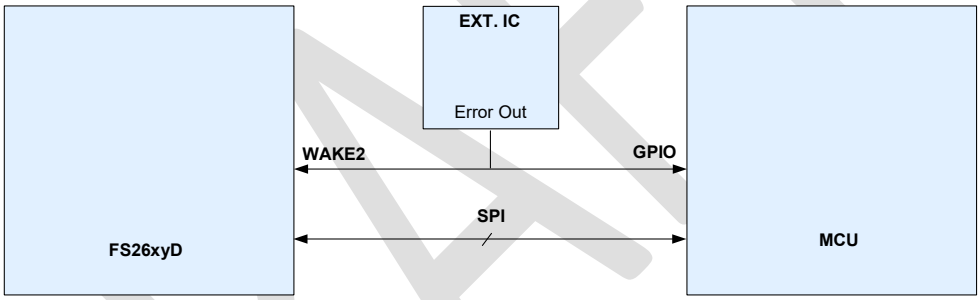

Figure 16 ERRMON connection

System Integration Requirement: [SIR_69] It is the system integrator's responsibility to make sure the error output signal from the external IC is well connected to the FS26 WAKE 2 pin and one MCU GPIO, to ensure the MCU can listen to the fault.

Rational: To detect WAKE2 pin latent short to high failure before releasing FS0B

Implementation hint: Toggle WAKE2 pin and MCU check ERRMON_STATUS bit by SPI

5.2.13.2 Software configuration and diagnostic

During the initialization phase, the MCU configures the ERRMON monitoring with FS_I_SAFE_INPUTS register

- the ERRMON polarity with ERRMON_FLT_POLARITY bit
- the ERRMON acknowledgement timing with ERRMON_ACK_TIME [1:0] bits
- the ERRMON impact on RSTB and FS0B with ERRMON_FS_REACTION bit

System Integration Requirement: [SIR_70] It is the system integrator's responsibility to make sure the MCU configures the ERRMON settings during the initialization phase after each RSTB release.

A transition detected at ERRMON pin indicates an error from the external IC. The acknowledgement timing is then started for the ERRMON_ACK_TIME configured and the FS26xyD is waiting for the MCU acknowledgement by SPI writing ERRMON_ACK = 1 in FS_DIAG_SAFETY2 register. If the MCU acknowledge the error detection before the ERRMON acknowledgement timing expires, the FS26xyD will do nothing. If the MCU acknowledge the error detection after the ERRMON acknowledgement timing expires, the FS26xyD will assert FS0B and/or RSTB depending on ERRMON_FS_REACTION configuration. By default, the ERRMON acknowledgement timing is set to 8ms what is shorter to the FFTI time.

ERRMON diagnostics are available reading FS_DIAG_SAFETY2 register:

- ERRMON bit reports an error detection
- ERRMON_PIN_STATUS bit reports real-time ERRMON pin state

5.2.13.3 Fault detection and reaction time

ERRMON Fault detection time: ERRMON_ACK_TIME[1:0] (1ms to 32ms)

5.2.14 Built-in Self-test (SMLF27 & SMLF34)

The FS26xyD has a Logical Built In Self-Test (LBIST) and an Analog Built In Self-Test (ABIST) strategy integrated. The FS26xyB has only an Analog BIST strategy integrated.

5.2.14.1 LBIST

The FS26xyD LBIST is performed after each power up or wake up from Standby or LPOFF. The LBIST verifies the correct functionality of the safety logic monitoring. In case of LBIST fail, RSTB is released but FS0B and FS1B remain stuck low and cannot be released. The maximum LBIST duration is 3ms.

5.2.14.2 ABIST

The ABIST1 is automatically executed after each power up or wake up from Standby. The ABIST coverage is described in the **Table 11** below where the voltage monitoring coverage (can be configured by OTP as described in detail in **5.2.3** to **5.2.10**).

At any time when the device can check voltages comparators that are monitoring all power rails. This can be done with FS_ABIST_ON_DEMAND SPI register (refer to “ABIST on Demand “ sub chapters from **5.2.3** to **5.2.10** sections).

Table 11 – Analog BIST coverage

Monitoring	Over voltage	Under voltage	Short to High	Low speed	High speed	ABIST1	ABIST On demand
VPRE	X	X				OTP	SPI request
VCORE	X	X				OTP	SPI request
TRK1	X	X				OTP	SPI request
TRK2	X	X				OTP	SPI request
LDO1	X	X				OTP	SPI request
LDO2	X	X				OTP	SPI request
VREF	X	X				OTP	SPI request
Analog input	X	X				OTP	SPI request
VANA_FS and VDIG_FS	X						
RSTB			X			X	
FS0B			X			X	
FS1B			X			X	
OSC				X	X		

Note: “X” means this monitoring is checked
“OTP” means can be disabled by OTP
“SPI request” means the self-test can be requested by SPI

It is recommended to verify latent faults on power rails’ monitoring that are safety related and used during the start up sequence.

In case of ABIST1 fail, RSTB is released but FS0B remains stuck low and cannot be released.

5.2.14.3 Software configuration and diagnosis

LBIST, ABIST1 and ABIST On Demand diagnostics are available reading FS_DIAG_SAFETY1 register

- LBIST_STATUS bit reports the LBIST result
- ABIST1_PASS bit reports the ABIST1 result
- ABIST2_PASS bit reports the ABIST On Demand result

System Integration Requirement: [SIR_71] It is the system integrator's responsibility to make sure the MCU checks that LBIST and ABIST1 are PASS after each power up or wake up from Standby.

If a regulator is not configured to be started in the power up sequence of the device, it's recommended to run the ABIST on demand just after the regulator is turned on through SPI request

System Integration Requirement: [SIR_72] It is the system integrator's responsibility to make sure the appropriate ABIST on demand is run for regulators' monitoring that are not part of the power up sequence.

5.2.15 RSTB input/output

FS26xyD/FS26xyB RSTB pin is intended to be connected to the MCU Software Reset input (RSTB). When RSTB is asserted low, FS0B is also asserted low.

5.2.15.1 Hardware configuration

RSTB is an open-drain output and requires an external pull up resistor to VDDIO and a filtering capacitor to GND for immunity. An integrated pull-down resistor guarantees a passive low level to maintain the Fail-safe sate even when the device is completely unpowered. A redundant analog path to VSUP will pull up RSTB low side gate to assert RSTB and maintain the Fail-safe sate in case of loss of the digital command.

RSTB is monitored internally and manages some Fail-safe state machine transitions. Consequently, the external pull up is mandatory.

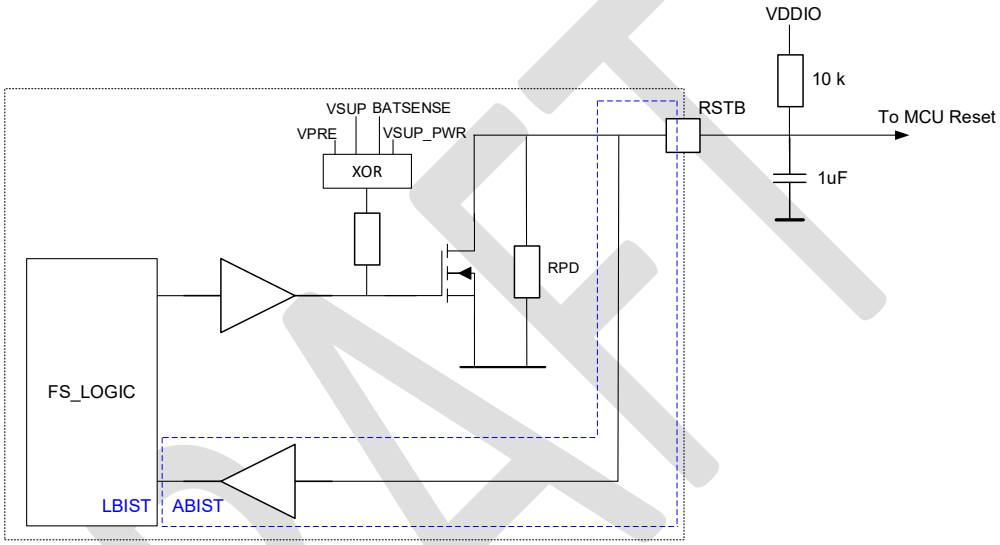

Figure 17 RSTB implementation

System Integration Requirement: [SIR_73] it is the system integrator's responsibility to make sure external components connected to RSTB are available to bring the safety critical outputs to known levels during operation

Rational: To bring the functional safety-critical outputs to a defined voltage level anytime

Implementation hint: RSTB path check with RSTB assertion request by MCU through SPI bus.

5.2.15.2 Software configuration and diagnosis

The fault source to activate RSTB is either hard coded or configurable by SPI during the initialization phase as described in **Chapter 5.2.2**.

RSTB pulse duration can be configured at 1ms or 10ms with the bit RSTB_DUR in FS_I_FSSM register. By default, RSTB pulse is configured at 10 ms.

RSTB assertion can be requested by SPI with the bit RSTB_REQ in FS_SAFE_IOS_1 register. The goal is to verify the hardware connection between the MCU reset pin and the FS26xyD or FS26xyB reset pin. This request comes from the MCU and is a software request. This action must be done before releasing FS0B and FS1B to high.

An internal sense path of the RSTB pin is implemented in the device. The function monitors the output of the pin and compares it with the digital command. If a difference between the digital command and the RSTB internal sense path is detected, the failure reported in RSTB_DIAG bit into FS_SAFE_IOS_1 register.

Diagnostic of RSTB pin/event is available reading FS_SAFE_IOS_1 register:

- RSTB_DIAG bit reports a RSTB short to high failure.
- RSTB_EVENT bit reports an activation of RSTB pin.
- RSTB_SNS bit reports real-time RSTB pin state.
- RSTB_DRV bit reports the real-time digital command to drive RSTB low side gate

The RSTB pin is bi-directional, so the FS26xyD or FS26xyB can bring the MCU under reset and the MCU can maintain the RSTB low externally even if the FS26xyD or FS26xyB is ready to release it. All the reset assertions by the FS26xyD or FS26xyB are incrementing the fault error counter.

By default, if RSTB pin is asserted low for a duration longer than eight seconds, the device goes to Deep Fail-Safe. This 8s timer can be disabled with the bit DIS8S in F_I_FSSM register.

5.2.16 FS0B output

FS26xyD or FS26xyB FS0B pin is intended to bring the system in safe state by disabling the CAN communication or de-activating various functions in the ECU or opening a contactor to unpower the application.

5.2.16.1 Hardware configuration

FS0B is an open-drain output and requires an external pull up resistor to VDDIO or VSUP and a filtering capacitor to GND for immunity. If FS0B is pulled up to VSUP, some current will be taken from VSUP thru the pull up resistor in Standby mode where FS0B is asserted low. FS0B pull up to VSUP shall be used only in applications where VSUP is switched ON/OFF.

When FS0B is used as a global pin (going outside the ECU), an additional serial resistor and capacitor are required. An integrated pull-down resistor guarantees a passive low level to maintain the Fail-safe sate even when the device is completely unpowered. A redundant analog path to VSUP will pull up FS0B low side gate to assert FS0B and maintain the Fail-safe sate in case of loss of the digital command.

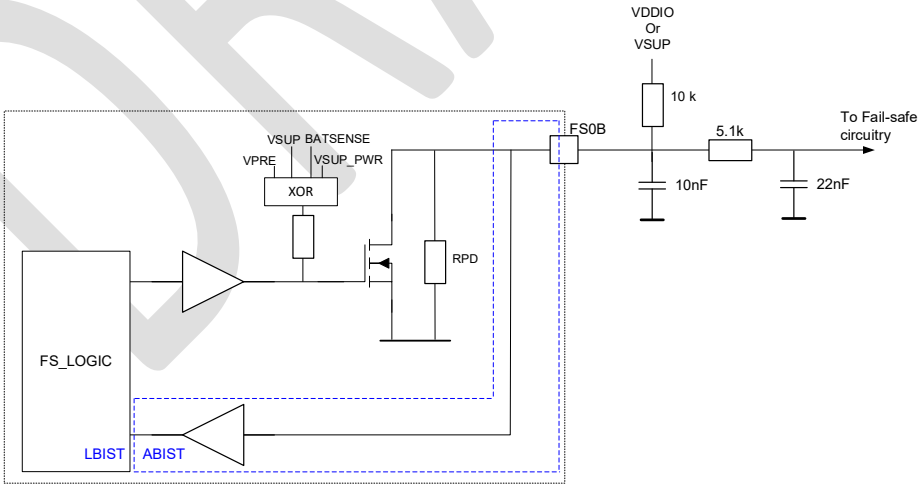

Figure 18 FS0B implementation

System Integration Requirement: [SIR_74] it is the system integrator's responsibility to make sure external components connected to FS0B are available to bring the safety critical outputs to known levels during operation

Rational: To bring the functional safety-critical outputs to a defined voltage level anytime

Implementation hint: FS0B safety path check with FS0B assertion request by MCU (SPI)

System Integration Requirement: [SIR_75] It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS0B only

Rational: To have a redundant path to cover an external FS0B short to high failure mode.

Implementation hint: A redundant signal coming from the MCU with a pull-down resistor to cover passive sate when the MCU is in reset

5.2.16.2 Software configuration and diagnosis

The fault source to activate FS0B is either hard coded or configurable by SPI during initialization phase as described in **Chapter 5.2.2**.

FS0B assertion can be requested by SPI with the bit FS0B_REQ in FS_SAFE_IOS_1 register. The goal is to verify the hardware connection between the FS0B pin of the SBC and the primary safety switch. This request comes from the MCU, which must monitor the good activation and release of the safety switch through a sense path from the safety switch to the MCU.

An internal sense path of the FS0B pin is implemented in the device. The function monitors the output of the pin and compares it with the digital command. If a difference between the digital command and the FS0B internal sense path is detected, the failure reported in FS0B_DIAG bit located into FS_SAFE_IOS_1 register too.

Diagnostic of FS0B pin/event is available reading FS_SAFE_IOS_1 register:

- FS0B _DIAG bit reports a FS0B short to high failure.
- FS0B _SNS bit reports real-time FS0B pin state.
- FS0B _DRV bit reports the real-time digital command to drive FS0B low side gate

By default, if FS0B short to high is detected, RSTB pin will be asserted as a redundant path to reset the MCU and assert its FCCU pin. This feature can be disabled with the bit BACKUP_SAFETY_PATH_FS0B in F_I_FSSM register. However, disabling this feature may induce the inability to bring the system in safe state.

5.2.16.3 Fault detection and reaction time

FS0B short to high detection time t_{FSOB_SHORT} (800us) from datasheet

5.2.17 FS1B output

FS1B pin is intended to be used as a secondary safety output. FS1B is a dedicated active low signal integrated into the FS26xyD or FS26xyB which can be activated after a delay (tDELAY) or for a duration (tDUR) when FS0B is activated. FS1B can also be used as an FS0B redundant safety output when tDELAY = 0. In this case, both FS0B and FS1B pins are asserted low at the same time.

This safety output can be used to open the phases of a motor after demagnetization of the coils, to disable an external physical layer for a certain duration to avoid miscommunication when a failure happens, or any other use case where a second safety output is required.

5.2.17.1 Hardware configuration

FS1B is an open-drain output and requires an external pull up resistor to VDDIO or VSUP and a filtering capacitor to GND for immunity. If FS1B is pulled up to VSUP, some current will be taken from VSUP thru the pull up resistor in Standby mode where FS1B is asserted low. FS1B pull up to VSUP shall be used only in applications where VSUP is switched ON/OFF.

When FS1B is used as a global pin (going outside the ECU), an additional serial resistor and capacitor are required. An integrated pull-down resistor guarantees a passive low level to maintain the Fail-safe sate even when the device is completely unpowered. A redundant analog path to VSUP will pull up FS1B low side gate to assert FS1B and maintain the Fail-safe sate in case of loss of the digital command.

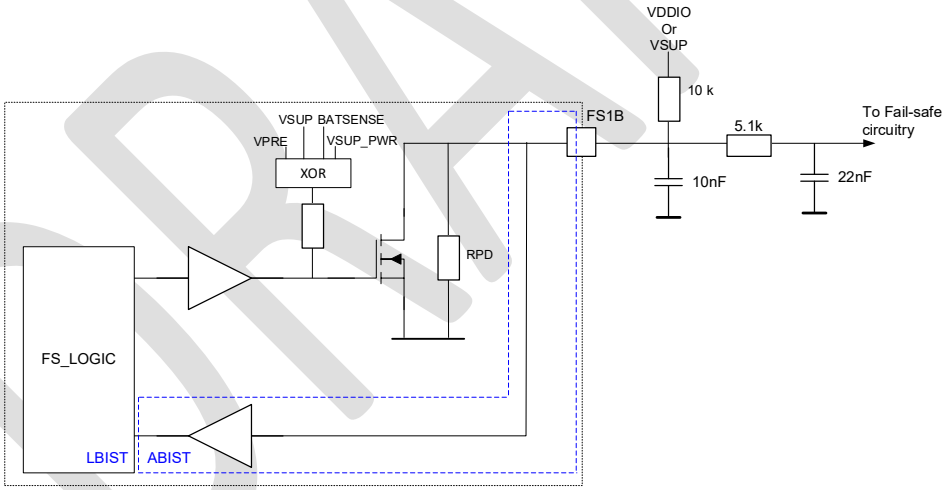

Figure 19 FS1B implementation

System Integration Requirement: [SIR_76] it is the system integrator's responsibility to make sure external components connected to FS1B are available to bring the safety critical outputs to known levels during operation

Rational: To bring the functional safety-critical outputs to a defined voltage level anytime

Implementation hint: FS1B safety path check with FS1B assertion request by MCU (SPI)

System Integration Requirement: [SIR_77] It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS1B only

Rational: To have a redundant path to cover an external FS1B short to high failure mode.

Implementation hint: A redundant signal coming from the MCU with a pull-down resistor to cover passive sate when the MCU is in reset

5.2.17.2 Software configuration and diagnosis

The fault source to activate FS0B is either hard coded or configurable by SPI during the initialization phase as described in **Chapter 5.2.2** .

FS1B assertion can be requested by SPI with the bit FS1B_REQ in FS_SAFE_IOS_1 register. The goal is to verify the hardware connection between the FS1B pin of the FS26 and the safety circuitry connected to FS1B. This request comes from the MCU, which must monitor the good activation and release of the safety switch through a sense path from the safety switch to the MCU.

An internal sense path of the FS1B pin is implemented in the device. The function monitors the output of the pin and compares it with the digital command. If a difference between the digital command and the FS1B internal sense path is detected, the failure reported in FS1B_DIAG bit.

Diagnostic of FS1B pin/event is available reading FS_SAFE_IOS_1 register:

- FS1B _DIAG bit reports a FS1B short to high failure.
- FS1B _SNS bit reports real-time FS1B pin state.
- FS1B _DRV bit reports the real-time digital command to drive FS1B low side gate
-

5.2.17.3 Fault detection and reaction time

FS1B short to high detection time t_{FS1B_SHORT} (800us) from datasheet

5.2.18 Fault Error Counter

The fault error counter counts the number of faults occurring in the system. The fault error counter is incremented by 1, each time the RSTB and/or FS0B pin is asserted. When FS0B is asserted, the fault error counter is incremented by 1, every time the watchdog error counter maximum value is reached.

5.2.18.1 Software configuration and diagnostic

During Initialization phase, the MCU configures the Fault Error Counter with FS_I_FSSM register

- the Fault Error Counter Limit with FLT_ERR_CNT_LIMIT[1:0] bits
- the Fault Error Counter intermediate value impact on RSTB/FS0B with FLT_ERR_REACTION[1:0] bits

By default, the Fault Error Counter limit is 6. The intermediate value can be used to force the FS0B activation or generate a RSTB pulse. The maximum value of the fault error counter is used to transition in Deep Fail-Safe mode.

After each power up or wake up from Standby mode, the Fault Error counter starts at level 1 to ensure the safe state. It is recommended to read the error counter and decrement it to an appropriate value by several consecutive good watchdog refreshes before a reset request by the SPI. The number of watchdogs needed (N) depends on the error counter value (FLT_ERR_CNT [3:0]) and the WD refresh counter (WD_RFR_CNT [2:0]) setup during INIT_FS. N=FLT_ERR_CNT[3:0]x (WD_RFR_CNT[2:0] + 1) to decrement the counter to “0”.

System Integration Requirement: [SIR_78] It is the system integrator’s responsibility to make sure the MCU configures the Fault Error Counter during the initialization phase after each RSTB release.

The Fault Error Counter is triplicated, and a majority voter is implemented to avoid any unexpected change due to a bit flip. In case of a bit flip, the comparison is done with the two other registers and the bit in default is forced to be changed to the right value.

The Fault Error Counter value is available reading FLT_ERR_CNT[3:0] bits in FS_I_FSSM register

5.2.19 Debug mode

In Debug mode, FS0B and FS1B cannot be released to keep the system in safe state because the Watchdog window is fully opened (Watchdog is disabled) to ease the debug of the hardware and software routines.

Debug mode entry can be verified with the bit DBG_MODE in FS_STATES register. DBG_MODE bit must be equal to ‘0’ in application mode.

System Integration Requirement: [SIR_79] it is the system integrator’s responsibility to make sure DBG_MODE bit = ’0’ FS_STATES register before releasing FS0B and FS1B pins.

6 Start-up sequence

After each power up or wake up from WAKE pin, the FS26xyD or FS26xyB executes the regulators power up sequence and verifies the latent faults configured by OTP. Depending on the OTP configuration, the time to release RSTB pin will vary.

6.1 RSTB release

RSTB is released when ABIST1 is done, so RSTB release time depends on ABIST1 OTP configuration. ABIST1 starts when the latest regulator assigned in ABIST1 is started, so it depends on the power up sequence configured by OTP.

Typical power up sequence as soon as VSUP > $V_{SUP\_PWR\_UVH}$:

1- VBOS start up (max 1ms)

2- When VBOS > V_{BOS_UVH}, LBIST execution (max 3ms)

3- When LBIST done, VPRE start up (max 2.3 ms)

4- When VPRE > V_{PRE_UVH}, VREGx power up sequence (OTP dependent, max 1.5 ms with 250 µs slot time)

5- When last regulator assigned to ABIST1 is started, ABIST1 execution

6- When ABIST1 done, RSTB release

When the FS26xyD or FS26xyB RSTB pin is released, all the initialization registers can be accessed and configured. Based on the information in this safety manual, the following is a summary of the minimum safety configuration sequence to do before starting the application.

6.2 Verify

1. **Verify** LBIST and ABIST1 are pass
2. **Verify** Debug mode is not activated
3. **Verify** there is no OTP CRC error

6.3 Configure *FS_I and FS_I_NOT registers*

1. **Configure** all overvoltage and under voltage impact on RSTB and FS0B with VMON_xxx_OV_FS_REACTION and VMON_xxx_UV_FS_REACTION SPI bits.
2. **Configure** the WD window period, the WD window duty cycle, the WD counters limits and its impact on RSTB and FS0B. Ensure the configuration does not violate the FTTI requirement at system level.
3. **Configure** the Fault Error Counter limit and its impact on RSTB and FS0B at intermediate value
4. **Configure** the RSTB pulse duration
5. **Configure** MCU FCCU error monitoring and its impact on RSTB and FS0B
6. **Configure** Ext. IC error monitoring and its impact on RSTB and FS0B
7. **Configure** FS0B short to high impact on RSTB
8. **Configure** FS1B short to high impact on RSTB

6.4 Execute

1. **Close** the initialization phase by sending the first good WD refresh
2. **Clear** all the flags by writing in FS_DIAG_SAFETY1,FS_DIAG_SAFETY2, FS_OVUVREG_STATUS
3. **Clear** the fault error counter to “0” with consecutive good WD refresh
4. **Perform** RSTB path check (steps 1 to 4 must be redo after RSTB is released)
5. **Release** FS0B pin
6. **Perform** FS0B safety path check
7. **Refresh** the WD according to its configuration
8. **Check** FS_GRL_FLAGS register after each WD refresh
9. **Configure** FS1B delay value and duration (if a secondary safety output is needed)
10. **Release** FS1B pin (if a secondary safety output is needed)
11. **Perform** FS1B safety path check (if a secondary safety output is needed)

The FS26xyD or FS26xyB is now ready. If everything is ok for the MCU, it can release its own safety path and the ECU starts.

7 List of safety mechanism integrated in the device

Table 12 – List of safety mechanisms integrated in the device

SM#	Safety mechanism description	FS26xyD Diagnostic Coverage	FS26xyB Diagnostic Coverage	Safety Manual Chapter
SM1	VDDIO Monitoring (OV) thru VMON_LDO1 (OV)	High (99%)	High (99%)	5.2.5
SM2	VDDIO Monitoring (UV) thru VMON_LDO1 (UV)	High (99%)	High (99%)	5.2.5
SM3	VMON_LDO1 (OV)	High (99%)	High (99%)	5.2.5
SM4	VMON_CORE Monitoring (OV)	High (99%)	High (99%)	5.2.4
SM5	VMON_CORE Monitoring (UV)	High (99%)	High (99%)	5.2.4
SM7	VMON_REF Monitoring (UV)	High (99%)	High (99%)	5.2.9
SM8	VMON_TRK1 Monitoring (OV)	High (99%)	High (99%)	5.2.7
SM9	VMON_TRK1 Monitoring (UV)	High (99%)	High (99%)	5.2.7
SM10	VMON_TRK2 Monitoring (OV)	High (99%)	High (99%)	5.2.8
SM11	VMON_LDO1 Monitoring (UV)	High (99%)	High (99%)	5.2.5
SM12	VMON_TRK2 Monitoring (UV)	High (99%)	High (99%)	5.2.8
SM13	VMON_LDO2 (OV)	High (99%)	High (99%)	5.2.6
SM14	VMON_LDO2 (UV)	High (99%)	High (99%)	5.2.6
SM15	VMON_PRE Monitoring (OV)	High (99%)	High (99%)	5.2.3
SM16	VMON_PRE Monitoring (UV)	High (99%)	High (99%)	5.2.3
SM18	Backup safety path (FS0b) in case of FS biasing or logic failure	Low (60%)	Low (60%)	5.2.16
SM19	RESET Request from MCU before safety out released	Low (60%)	Low (60%)	5.2.15
SM20	CHALLENGER WD MONITORING	High (99%)	N/A	5.2.11
SM20 (bis)	SIMPLE WD MONITORING	N/A	Medium (90%)	5.2.3
SM21	redundant RSTB, FSxB Driver supply available	Medium (90%)	Medium (90%)	5.2.15 5.2.16 5.2.17
SM22	VBOS_POR	Medium (90%)	Medium (90%)	5.1.3 5.1.4
SM23	CRC check on SPI com. protocol	High (99%)	High (99%)	5.2.1
SM24	VDIG_OV	High (99%)	High (99%)	5.1.3 5.1.4

Table 13 – List of safety mechanisms integrated in the device (continued)

SM#	Safety mechanism description	FS26xyD Diagnostic Coverage	FS26xyB Diagnostic Coverage	Safety Manual Chapter
SM27	VDIG 1P6_POR and/or VDIG UV detection	Medium (90%)	Medium (90%)	5.1
SM28	VANA UV detection	Medium (90%)	Medium (90%)	5.1
SM29	VDIG_FS POR	Medium (90%)	Medium (90%)	5.1
SM35	Cyclic CRC checks (each 5ms) OTP Bit	High (99%)	High (99%)	5.1
SM40	V5FS_POR	Medium (60%)	Medium (60%)	5.1
SM44	VMON_XXXx Monitoring (OV) (SM1 + SM3 + SM4 + SM8 + SM10 + SM13 + SM15)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM45	VMON_TRKx Monitoring (OV) (SM8 + SM10)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM46	VMON_TRKx Monitoring (UV) (SM9 + SM12)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM47	VMON_REF Monitoring (OV)	High (99%)	High (99%)	5.2.9
SM48	FS / Main Clock Monitoring	Medium (90%)	Medium (90%)	5.1.5
SM49	VMON_LDOx Monitoring (UV) (SM11 + SM14)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM50	VMON_LDOx Monitoring (OV) (SM3 + SM13)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM53	VMON_PRE Monitoring (OV) or VMON_PRE Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM54	VMON_CORE Monitoring (OV) or VMON_CORE Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM55	VMON_LDO1 Monitoring (OV) or VMON_LDO1 Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM56	VMON_LDO2 Monitoring (OV) or VMON_LDO2 Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM57	VMON_TRK1 Monitoring (OV) or VMON_TRK1 Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM58	VMON_TRK2 Monitoring (OV) or VMON_TRK2 Monitoring (UV)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM59	VMON_TRKx Monitoring (UV) (OV) (SM9 + SM12+ SM8 + SM10)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM60	Cyclic CRC checks (each 5ms) OTP Bit	High (99%)	High (99%)	5.1.2

Table 14 – List of safety mechanisms integrated in the device (end)

SM#	Safety mechanism description	FS26xyD Diagnostic Coverage	FS26xyB Diagnostic Coverage	Safety Manual Chapter
SM61	VANA 1P6_FS POR	Medium (90%)	Medium (90%)	5.1
SM62	VMON_XXXx Monitoring (UV) or VBOS_POR (SM2 + SM5 + SM7 + SM9 + SM11 + SM12 + SM14 + SM16+ SM22)	High (99%)	High (99%)	5.2.3 to 5.2.9
SM63	ECC OTP FS	High (99%)	High (99%)	5.1.2
SM64	VBOS_POR and VDIG 1P6_POR and VANA 1P6_POR and Fail safe outputs assertion using analog path (Vsups)	High (99%)	High (99%)	5.1
SM66	VBOS_POR and VDIG 1P6_POR and VANA 1P6_POR and VANA 1P6_FS POR	High (99%)	High (99%)	5.1
SM67	VBOS Under voltage detection	High (99%)	High (99%)	5.1
SM68	VMON_REF Monitoring (OV) or VMON_REF Monitoring (UV)	High (99%)	High (99%)	5.2.9
SM69	VMON_EXT Monitoring (OV)	High (99%)	High (99%)	5.2.10
SM70	VMON_EXT Monitoring (UV)	High (99%)	High (99%)	5.2.10
SM71	VMON_EXT Monitoring (OV) or VMON_EXT Monitoring (UV)	High (99%)	High (99%)	5.2.10

7.1 List of safety mechanism required at application level

Table 15 – List of safety mechanisms required at application level

SMA#	Safety mechanism	Assumed Diagnostic Coverage	[SIR_xx]
SMA1	RSTB request	Low (60%)	[SIR_49]
SMA2	FS0B release check	Low (60%)	[SIR_50]
SMA3	FS1B release check	Low (60%)	[SIR_52]

8 List of Faults and potential cascade effects

Table 16 – Fail Safe Faults and potential cascade effects

Fail-safe Faults	Description	Action in case of Fault	RSTB	FS0B	FS1B	Potential Cascaded effect	RSTB	FS0B	FS1B
VMON_PRE OV	VPRE Overvoltage	VPRE switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_PRE UV	VPRE Undervoltage	VPRE kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_CORE OV	VCORE Overvoltage	VCORE switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_CORE UV	VCORE Undervoltage	VCORE kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_LDO1 OV	LDO1 Reg Overvoltage	LDO1 Reg switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_LDO1 UV	LDO1 Reg Undervoltage	LDO1 Reg kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_LDO2 OV	LDO2 Reg Overvoltage	LDO2 Reg switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_LDO2 UV	LDO2 Reg Undervoltage	LDO2 Reg kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_TRK1 OV	TRK1 Reg Overvoltage	TRK1 Reg switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_TRK1 UV	TRK1 Reg Undervoltage	TRK1 kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_TRK2 OV	TRK2 Reg Overvoltage	TRK2 Reg switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_TRK2 UV	TRK2 Reg Undervoltage	TRK2 kept ON	HIGH	LOW	LOW	-	-	-	-
VMON_VREF OV	VREF Reg Overvoltage	VREF Reg switched OFF	LOW	LOW	LOW	-	-	-	-
VMON_ VREF UV	VREF Reg Undervoltage	VREF Reg kept ON	HIGH	LOW	LOW	-	-	-	-

Fail-safe Faults	Description	Action in case of Fault	RSTB	FS0B	FS1B	Potential Cascaded effect	RSTB	FS0B	FS1B
VMON_EXT OV	Overvoltage on VMONEXT pin	NA	LOW	LOW	LOW	-	-	-	-
VMON_ VREF UV	Undervoltage on VMONEXT pin	NA	HIGH	LOW	LOW	-	-	-	-
V1P6D_FS OV	V1P6D_FS Overvoltage	V1P6D_FS kept ON	LOW	LOW	LOW				
FCCU	MCU FCCU Error monitoring	NA	HIGH	LOW	LOW	Fault recovery timeout	LOW	LOW	LOW
ERRMON	Ext. IC error monitoring	NA	HIGH	LOW	LOW				
WD	WATCHDOG	WD NOT OK during INIT_FS	LOW	LOW	LOW	-	-	-	
		WD_ERR_CNT =MAX	LOW	LOW	LOW	-	-	-	
RSTB short to high	RSTB shorted to high	FS0B & FS1B assertion	HIGH (Ext.)	LOW	LOW	-	-	-	-
FS0B short to high	FS0B shorted to high	RSTB assertion	HIGH	HIGH (Ext.)	LOW	-	-	-	-
FS1B short to high	FS1B shorted to high	RSTB assertion	LOW	LOW	HIGH (Ext.)	-	-	-	-
LBIST	Logic built-in self-test	FS0B & FS1B stuck low	HIGH	LOW	LOW	-	-	-	
ABIST	Analog built-in self-test	FS0B & FS1B stuck low	HIGH	LOW	LOW	-	-	-	
ABIST ON DMEAND	Analog built-in self-test	SPI Flag	HIGH	HIGH	HIGH	-	-	-	
FS_OSC	Fail-safe oscillator drift	-	HIGH	LOW	LOW	-	-	-	
REG CORRUPT	INIT_FS register issue	-	HIGH	LOW	LOW	-	-	-	
OTP CORRUPT	OTP CRC error	-	HIGH	LOW	LOW	-	-	-	

Green	No impact. Device behavior is not configurable
Orange	Impact by default. Device behavior is not configurable
Blue	Device behavior is configurable by the SPI during INIT_FS phase only

Table 17 – Main Faults and potential cascading effects

Main Faults	Description	Action in case of Fault	RSTB	FS0B	Potential Cascade effect	RSTB	FS0B
V1P6D_Main	V1P6D_Main Undervoltage	V1P6D_Main kept ON	LOW	LOW	All regulators will be switched off	LOW	LOW
V1P6A_Main	V1P6A_Main Undervoltage	V1P6A_Main kept ON	LOW	LOW	All regulators will be switched off	LOW	LOW
VBOS_UVL	VBOS Undervoltage	Power down	LOW	LOW	All regulators will be switched off	LOW	LOW
VPRE_FB_OV	VPRE Overvoltage	VPRE switched OFF	LOW	LOW	All regulators will be switched off	LOW	LOW
VPRE_UVL	VPRE Undervoltage	VPRE kept ON	HIGH	LOW	Undervoltage on all regulators	HIGH	LOW
VPRE_ILIM	Current Limitation on Vpre	Duty cycle reduction	HIGH	HIGH	Undervoltage on all regulators	HIGH	LOW
VPRE_TSD	VPRE Thermal Shutdown	VPRE switched OFF	HIGH	HIGH	Undervoltage on VPRE or all regulators	HIGH	LOW
VCORE_UVL	VCORE Undervoltage	VCORE kept ON	HIGH	LOW	Undervoltage on VCOREMON	HIGH	LOW
VCORE_ILIM	Current Limitation on Vcore	Duty cycle reduction	HIGH	HIGH	Undervoltage on VCOREMON	HIGH	LOW
VCORE_TSD	VCORE Thermal Shutdown	VCORE switched OFF	HIGH	HIGH	Undervoltage on VCOREMON	HIGH	LOW
LDO1_ILIM	Current limitation on LDO1	Output voltage value decrease	HIGH	HIGH	Undervoltage on LDO1	HIGH	LOW
LDO1_TSD	LDO1 Thermal Shutdown	LDO1 switched off or global TSD	HIGH	HIGH	Undervoltage on LDO1	HIGH	LOW
LDO2_ILIM	Current limitation on LDO2	Output voltage value decrease	HIGH	HIGH	Undervoltage on LDO2	HIGH	LOW
LDO2_TSD	LDO2 Thermal Shutdown	LDO2 switched off or global TSD	HIGH	HIGH	Undervoltage on LDO2	HIGH	LOW
TRK1_ILIM	Current limitation on TRK1	Output voltage value decrease	HIGH	HIGH	Undervoltage on TRK1	HIGH	LOW
TRK1_TSD	TRK1 Thermal Shutdown	TRK1 switched off	HIGH	HIGH	Undervoltage on TRK1	HIGH	LOW

TRK2_ILIM	Current limitation on TRK2	Output voltage value decrease	HIGH	HIGH	Undervoltage on TRK2	HIGH	LOW
TRK2_TSD	TRK2 Thermal Shutdown	TRK2 switched off	HIGH	HIGH	Undervoltage on TRK2	HIGH	LOW
VREF_ILIM	Current limitation on VREF	Output voltage value decrease	HIGH	HIGH	Undervoltage on VREF	HIGH	LOW

Green	No impact. Device behavior is not configurable
Orange	Impact by default. Device behavior is not configurable
Blue	Device behavior is configurable by the SPI during INIT_FS phase only

9 List of System Integration Requirements

Table 18 – Hardware, software and OTP configuration integration requirements

[SIR_xx]	Description
[SIR_01]	it is the system integrator's responsibility to make sure the MCU checks the FS_GRL_FLAGS and FS_STATES registers after each RSTB or FS0B assertion
[SIR_02]	FMEDA safety metrics are achieved with all internal Safety Mechanism implemented (SMx) and all external Safety Mechanism at Application level implemented (SMAx).
[SIR_03]	it is the system integrator's responsibility to define the OTP configuration desired for its safety application using the latest revision of the GUI to define its desired configuration.
[SIR_04]	it is the system integrator's responsibility to make sure the MCU checks the FS_GRL_FLAGS register after each Watchdog refresh
[SIR_05]	it is the system integrator's responsibility to verify that VPRE_OTP bits are identic to VPRE_V_OTP bits.
[SIR_06]	it is the system integrator's responsibility to configure the correct VPRE monitoring overvoltage and undervoltage thresholds
[SIR_07]	it is the system integrator's responsibility to configure the correct VPRE monitoring overvoltage and undervoltage filtering times
[SIR_08]	it is recommended to assign VPRE monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VPRE monitoring to ABIST1.
[SIR_09]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_10]	it is the system integrator's responsibility to connect VMONPRE to VPRE regulator output.
[SIR_11]	It is the system integrator's responsibility to make sure the MCU configures the VPRE monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_12]	it is the system integrator's responsibility to verify that VCORE_OTP bits are identic to VCORE_V_OTP bits.
[SIR_13]	it is the system integrator's responsibility to configure the correct VCORE monitoring overvoltage and undervoltage thresholds
[SIR_14]	it is the system integrator's responsibility to configure the correct VCORE monitoring overvoltage and undervoltage filtering times
[SIR_15]	it is recommended to assign VCORE monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VCORE monitoring to ABIST1.
[SIR_16]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_17]	it is the system integrator's responsibility to connect VMONPE to VCORE regulator output.
[SIR_18]	It is the system integrator's responsibility to make sure the MCU configures the VCORE monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_19]	it is the system integrator's responsibility to verify that VLDO1_OTP bits are identic to VLDO1_V_OTP bits.
[SIR_20]	it is the system integrator's responsibility to configure the correct LDO1 monitoring overvoltage and undervoltage thresholds
[SIR_21]	it is the system integrator's responsibility to configure the correct LDO1 monitoring overvoltage and undervoltage filtering times
[SIR_22]	it is recommended to assign VLDO1 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VLDO1 monitoring to ABIST1.

[SIR_23]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests
[SIR_24]	It is the system integrator's responsibility to make sure the MCU configures the VLDO1 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_25]	it is the system integrator's responsibility to verify that VLDO2_OTP bits are identic to VLDO2_V_OTP bits.
[SIR_26]	it is the system integrator's responsibility to configure the correct LDO2 monitoring overvoltage and undervoltage threshold
[SIR_27]	it is the system integrator's responsibility to configure the correct LDO2 monitoring overvoltage and undervoltage filtering times
[SIR_28]	it is recommended to assign VLDO2 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VLDO2 monitoring to ABIST1.
[SIR_29]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests
[SIR_30]	It is the system integrator's responsibility to make sure the MCU configures the VLDO2 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_31]	it is the system integrator's responsibility to verify that VTRK1_OTP bits are identic to VTRK1_V_OTP bits
[SIR_32]	it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage thresholds
[SIR_33]	it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage filtering times
[SIR_34]	it is recommended to assign VTRK1 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK1 monitoring to ABIST1.
[SIR_35]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_36]	It is the system integrator's responsibility to make sure the MCU configures the VTRK1 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_37]	it is the system integrator's responsibility to verify that VTRK2_OTP bits are identic to VTRK2_V_OTP bits.
[SIR_38]	it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage thresholds
[SIR_39]	it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage filtering times
[SIR_40]	it is recommended to assign VTRK2 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK2 monitoring to ABIST1.
[SIR_41]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_42]	It is the system integrator's responsibility to make sure the MCU configures the VTRK2 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_43]	it is the system integrator's responsibility to verify that VREF_OTP bits are identic to VREF_V_OTP bits.
[SIR_44]	it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage thresholds
[SIR_45]	it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage filtering times
[SIR_46]	it is recommended to assign VREF monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VREF monitoring to ABIST1.
[SIR_47]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.

[SIR_48]	It is the system integrator's responsibility to make sure the MCU configures the VREF monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_49]	it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage thresholds
[SIR_50]	it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage filtering times
[SIR_51]	it is recommended to assign VMONEXT monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VMONEXT monitoring to ABIST1.
[SIR_52]	if VMONEXT is assign to ABIST1 self-test sequence, it's under the system integrator's responsibility to ensure that the voltage to be monitored on VMONEXT pin is available when ABIST1 sequence is ran by the FS26.
[SIR_53]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_54]	It is the system integrator's responsibility to make sure the MCU configures the VMONEXT monitoring OV and UV impact on RSTB and FS0B, FS1B during initialization phase after each RSTB release.
[SIR_55]	it is the system integrator's responsibility to enable the Watchdog monitoring for safety applications
[SIR_56]	It is the system integrator's responsibility to make sure the MCU configures the Watchdog monitoring during the initialization phase after each RSTB release
[SIR_57]	it is the system integrator's responsibility to make sure the MCU periodically refreshes the FS26xyD/ FS26xyB watchdog
[SIR_58]	it is the system integrator's responsibility to make sure the Watchdog answer calculation is correctly implemented in the MCU software
[SIR_59]	it is the system integrator's responsibility to enable the FCCU monitoring for ASIL D safety applications
[SIR_60]	it is the system integrator's responsibility to select devices with Fault Recovery strategy of the FS26xyD if the Fault Recovery strategy of the MCU is used.
[SIR_61]	it is the system integrator's responsibility to make sure the bi-stable protocol is configured in the NXP MCU for FCCU protocol
[SIR_62]	it is the system integrator's responsibility to make sure the MCU configures the correct FCCU polarity during the initialization phase after each RSTB release.
[SIR_63]	it is the system integrator's responsibility to make sure the correct pull up/down resistor values are properly connected to provide passive error state.
[SIR_64]	It is the system integrator's responsibility to make sure the MCU fault error output is well connected to the FS26xyD FCCUx pin.
[SIR_65]	It is the system integrator's responsibility to make sure the MCU fault error output are capable to modulate high and low level timings and error timings are fitting FS26xyD high and low levels timings limits.
[SIR_66]	It is the system integrator's responsibility to make sure the MCU configures the FCCU settings during INIT_FS after each RSTB release.
[SIR_67]	It is the system integrator's responsibility to make sure the MCU configures the Watchdog Window Recovery period during initialization phase after each RSTB release.
[SIR_68]	it is the system integrator's responsibility to select part number with the ERRMON monitoring.
[SIR_69]	It is the system integrator's responsibility to make sure the error output signal from the external IC is well connected to the FS26 WAKE 2 pin and one MCU GPIO, to ensure the MCU can listen to the fault.
[SIR_70]	It is the system integrator's responsibility to make sure the MCU configures the ERRMON settings during the initialization phase after each RSTB release
[SIR_71]	It is the system integrator's responsibility to make sure the MCU checks that LBIST and ABIST1 are PASS after each power up or wake up from Standb

[SIR_72]	It is the system integrator's responsibility to make sure the appropriate ABIST on demand is run for regulators' monitoring that are not part of the power up sequence.
[SIR_73]	it is the system integrator's responsibility to make sure external components connected to RSTB are available to bring the safety critical outputs to known levels during operation
[SIR_74]	it is the system integrator's responsibility to make sure external components connected to FS0B are available to bring the safety critical outputs to known levels during operation
[SIR_75]	It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS0B only
[SIR_76]	it is the system integrator's responsibility to make sure external components connected to FS1B are available to bring the safety critical outputs to known levels during operation
[SIR_77]	It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS1B only
[SIR_78]	It is the system integrator's responsibility to make sure the MCU configures the Fault Error Counter during the initialization phase after each RSTB release.
[SIR_79]	it is the system integrator's responsibility to make sure DBG_MODE bit = '0' FS_STATES register before releasing FS0B and FS1B pins.
[SIR_32]	it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage thresholds
[SIR_33]	it is the system integrator's responsibility to configure the correct TRK1 monitoring overvoltage and undervoltage filtering times
[SIR_34]	it is recommended to assign VTRK1 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK1 monitoring to ABIST1.
[SIR_35]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_36]	It is the system integrator's responsibility to make sure the MCU configures the VTRK1 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_37]	it is the system integrator's responsibility to verify that VTRK2_OTP bits are identic to VTRK2_V_OTP bits.
[SIR_38]	it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage thresholds
[SIR_39]	it is the system integrator's responsibility to configure the correct TRK2 monitoring overvoltage and undervoltage filtering times
[SIR_40]	it is recommended to assign VTRK2 monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VTRK2 monitoring to ABIST1.
[SIR_41]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_42]	It is the system integrator's responsibility to make sure the MCU configures the VTRK2 monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.
[SIR_43]	it is the system integrator's responsibility to verify that VREF_OTP bits are identic to VREF_V_OTP bits.
[SIR_44]	it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage thresholds
[SIR_45]	it is the system integrator's responsibility to configure the correct VREF monitoring overvoltage and undervoltage filtering times
[SIR_46]	it is recommended to assign VREF monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VREF monitoring to ABIST1.
[SIR_47]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_48]	It is the system integrator's responsibility to make sure the MCU configures the VREF monitoring OV and UV impact on RSTB and FS0B during initialization phase after each RSTB release.

[SIR_49]	it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage thresholds
[SIR_50]	it is the system integrator's responsibility to configure the correct VMONEXT monitoring overvoltage and undervoltage filtering times
[SIR_51]	it is recommended to assign VMONEXT monitoring to ABIST1. However, it is the system integrator's responsibility to configure the assignment of VMONEXT monitoring to ABIST1.
[SIR_52]	if VMONEXT is assign to ABIST1 self-test sequence, it's under the system integrator's responsibility to ensure that the voltage to be monitored on VMONEXT pin is available when ABIST1 sequence is ran by the FS26.
[SIR_53]	it's under the system integrator's responsibility to define the usage and the frequency of the ABIST on demand requests.
[SIR_54]	It is the system integrator's responsibility to make sure the MCU configures the VMONEXT monitoring OV and UV impact on RSTB and FS0B, FS1B during initialization phase after each RSTB release.
[SIR_55]	it is the system integrator's responsibility to enable the Watchdog monitoring for safety applications
[SIR_56]	It is the system integrator's responsibility to make sure the MCU configures the Watchdog monitoring during the initialization phase after each RSTB release
[SIR_57]	it is the system integrator's responsibility to make sure the MCU periodically refreshes the FS26xyD/ FS26xyB watchdog
[SIR_58]	it is the system integrator's responsibility to make sure the Watchdog answer calculation is correctly implemented in the MCU software
[SIR_59]	it is the system integrator's responsibility to enable the FCCU monitoring for ASIL D safety applications
[SIR_60]	it is the system integrator's responsibility to select devices with Fault Recovery strategy of the FS26xyD if the Fault Recovery strategy of the MCU is used.
[SIR_61]	it is the system integrator's responsibility to make sure the bi-stable protocol is configured in the NXP MCU for FCCU protocol
[SIR_62]	it is the system integrator's responsibility to make sure the MCU configures the correct FCCU polarity during the initialization phase after each RSTB release.
[SIR_63]	it is the system integrator's responsibility to make sure the correct pull up/down resistor values are properly connected to provide passive error state.
[SIR_64]	It is the system integrator's responsibility to make sure the MCU fault error output is well connected to the FS26xyD FCCUx pin.
[SIR_65]	It is the system integrator's responsibility to make sure the MCU fault error output are capable to modulate high and low level timings and error timings are fitting FS26xyD high and low levels timings limits.
[SIR_66]	It is the system integrator's responsibility to make sure the MCU configures the FCCU settings during INIT_FS after each RSTB release.
[SIR_67]	It is the system integrator's responsibility to make sure the MCU configures the Watchdog Window Recovery period during initialization phase after each RSTB release.
[SIR_68]	it is the system integrator's responsibility to select part number with the ERRMON monitoring.
[SIR_69]	It is the system integrator's responsibility to make sure the error output signal from the external IC is well connected to the FS26 WAKE 2 pin and one MCU GPIO, to ensure the MCU can listen to the fault.
[SIR_70]	It is the system integrator's responsibility to make sure the MCU configures the ERRMON settings during the initialization phase after each RSTB release
[SIR_71]	It is the system integrator's responsibility to make sure the MCU checks that LBIST and ABIST1 are PASS after each power up or wake up from Standb
[SIR_72]	It is the system integrator's responsibility to make sure the appropriate ABIST on demand is run for regulators' monitoring that are not part of the power up sequence.

[SIR_73]	it is the system integrator's responsibility to make sure external components connected to RSTB are available to bring the safety critical outputs to known levels during operation
[SIR_74]	it is the system integrator's responsibility to make sure external components connected to FS0B are available to bring the safety critical outputs to known levels during operation
[SIR_75]	It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS0B only
[SIR_76]	it is the system integrator's responsibility to make sure external components connected to FS1B are available to bring the safety critical outputs to known levels during operation
[SIR_77]	It is the system integrator's responsibility to ensure the safe state of the system is not driven by the FS1B only
[SIR_78]	It is the system integrator's responsibility to make sure the MCU configures the Fault Error Counter during the initialization phase after each RSTB release.
[SIR_79]	it is the system integrator's responsibility to make sure DBG_MODE bit = '0' FS_STATES register before releasing FS0B and FS1B pins.

10 List of Safety Assumptions

Table 19 – Safety Assumptions

[SA_xx]	Description
[SA_01]	It is assumed that the FS26 product family is used in "12 V Automotive" application where a Fail-safe reaction is expected
[SA_02]	It is assumed that the FS26 product family is used in application for which the battery voltage never exceeds the defined maximum ratings (e.g., 40 V).
[SA_03]	It is assumed the normal operating of the FS26 product family is fulfilled by the compliance to the datasheet.
[SA_04]	It is assumed the FS26 product family shall meet all the datasheet specification after qualification tests.
[SA_05]	It is assumed that the FS26 is used in combination with other devices in the application (e.g. MCU, DDR, other analog IC).
[SA_06]	It is assumed that FS26 product family can be designed in systems that request highest Automotive Safety Integrity Level ASIL D and lower.
[SA_07]	It is assumed that the FS26 is used in application for witch the fault tolerant time interval (FTTI) is ≥ of the FS26 fault detection time plus the FS26 fault reaction time (max 10 ms).
[SA_08]	It is assumed that the multiple point fault interval is ≤ 12 hours then the "Driving Cycle" is assumed to be ≤ 12 hours.
[SA_09]	It is assumed that the number of FS26 pin disconnection, at the same time (i.e. Pin lift on the PCB), is restricted to 1.
[SA_10]	It is assumed the thermal connection of the exposed-pad to the PCB is always ensured thanks to its large size.
[SA_11]	Short circuit between PCB track is not considered in the FS26 (i.e diagnostic, countermeasures).
[SA_12]	External component disconnection is not considered (i.e. diagnostic, countermeasures).
[SA_13]	It is assumed that a power source is always available on the supply pin of the FS26.
[SA_14]	It is assumed the safety signals used to transition the system in safe state is delivered by the MCU and the FS26, to propose redundant and independent safety paths at system level.
[SA_15]	It is assumed that the BMS application safe states is the following: - contactors opened (battery cells isolated from power source)
[SA_16]	It is assumed that one or several contactors (relays) are available to isolate the battery cells for BMS. On different application, a CAN physical layer can be de-activated to isolate the ECU in fault.
[SA_17]	It is assumed that the FS26 product family is used in application for which the battery voltage never exceeds the defined maximum ratings (e.g., 40 V).
[SA_18]	It is assumed the normal operating of the FS26 product family is fulfilled by the compliance to the datasheet.
[SA_19]	It is assumed the FS26 product family shall meet all the datasheet specification after qualification tests.
[SA_20]	It is assumed that the FS26 is used in combination with other devices in the application (e.g. MCU, DDR, other analog IC).
[SA_21]	It is assumed that FS26 product family can be designed in systems that request highest Automotive Safety Integrity Level ASIL D and lower.
[SA_22]	It is assumed that the FS26 is used in application for witch the fault tolerant time interval (FTTI) is ≥ of the FS26 fault detection time plus the FS26 fault reaction time (max 10 ms).
[SA_23]	It is assumed that the FS26 product family is used in application for which the mission profile is the following (or less aggressive)

11 Production related instructions affecting safety

Refer to datasheet for:

- Package soldering
- Storage and handling requirements
- ESD protection capacitance
- EMC coverage

12 Legal information

12.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

12.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

12.3 Licenses

Purchase of NXP <xxx> components
<License statement text>

12.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

12.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

13 Document management

13.1 Abbreviations

Table 20 – Abbreviations

Abbreviation	Description
IC	Integrated Circuit
ABIST	Analog built-in self-test
ADC	Analog-to-digital converter
BIST	Built-in self-test
CCF	Common cause failure
CF	Cascading failure
CMF	Common mode failure
DPF	Dual-point fault
FCCU	Fault collection and control unit
FCRBM	Feedback core resistor bridge monitoring
FMEDA	Failure modes, effects & diagnostic analysis
FSM	Fail-safe machine
FSO	Fail-safe outputs
FSSM	Fail-safe state machine
FTTI	Fault Tolerant Time Interval
GPIO	General purpose I/O
MPFDI	Multiple-point fault detection Interval
LBIST	Logic built-in self-test
LF	Latent fault
LFSR	Linear feedback shift register
MCU	Microcontroller unit
MPF	Multiple-point fault

OV	Overvoltage
OTP	One time programmable
PST	Process safety time
RF	Residual fault
SBC	System basis chip
SF	Safe fault
SPF	Single-point fault
UV	Undervoltage

14 Acceptance Reviews and Approvals

Table 21 – Reviewers

Name	Role	Location	Date

Table 22 – Approvers

Name	Role	Location	Date	Signature (if required)

15 Table of Contents