Document Number: MC33907NL-33908NLSMUG
Rev. 2.0, 7/2015

Safety Manual for 33907 and 33908

Table of Contents

1 Preface

This document discusses requirements for the use of the 33907NL and 33908NL System Basis Chip (SBC) in functional safety relevant applications requiring high functional safety integrity levels.

It is intended to support system and software engineers using the 33907NL and 33908NL available features, as well as achieving additional diagnostic coverage by software measures.

Several measures are prescribed as safety requirements whereby the measure described was assumed to be in place when analyzing the functional safety of this System Basis Chip. In this sense, requirements in the Safety Manual (SM) are driven by assumptions concerning the functional safety of the system that integrates the 33907NL and 33908NL.

- **Assumption**: An assumption being relevant for functional safety in the specific application under consideration (condition of use). It is assumed that the user fulfills an assumption in his design.

Example: **Assumption:** It is system integrator's responsibility that the recommended operating conditions given in the 33907NL and 33908NL data sheet are maintained.

NOTE

Assumptions are marked by a tag of the form "SM_*nnn*" at the beginning of the assumption, and are terminated with an "end". Both of these tags are enclosed within square brackets for easy recognition. These tags could be used to allow importing the assumptions into safety traceability management tools.

NOTE

Since the 33907NL and 33908NL is developed as a "Safety-related Element Out Of Context", the system requirements are NOT available in detail. Therefore, some assumptions are done on the "context of use" of the 33907NL and 33908NL. those assumptions (**S**ystem **R**equirement **A**ssumption) are tagged "**SA + number**".

For the use of the System Basis Chip, means if a specific safety manual assumption is not fulfilled, it has to be rationalized that an alternative implementation is at least similarly efficient concerning the functional safety requirement in question similarly well (for example, provides same coverage, reduces the likelihood of Common Mode Failure (CMF), and so on), or the estimation of an increased failure rate (λ_{SPF}, λ_{RF}, λ_{MPF}, λ_{DU}…) and reduced metrics (SFF: Safe Failure Fraction, SPFM: Single-point Fault Metrics, LFM: Latent Fault Metric) due to the deviation has be specified.

This document also contains guidelines on how to configure and operate the 33907NL and 33908NL for functional safety relevant applications requiring high functional safety integrity levels. These guidelines are preceded by one of the following text statements:

- **Recommendation**: A recommendation is either a proposal for the implementation of an assumption, or a reasonable measure which is recommended to be applied, if there is no assumption in place. The user has the choice whether to follow the recommendation.
- **Rationale**: The motivation for a specific assumption and/or recommendation.
- **Implementation hint**: An implementation hint gives specific hints on the implementation of an assumption and/or recommendation on the 33907NL and 33908NL. The user has the choice whether to follow the implementation hint.

These guidelines are considered to be useful approaches for the specific topics under discussion. The user needs to use discretion in deciding whether these measures are appropriate for their applications.

This document is valid only under the assumption that the System Basis Chip is used in functional safety applications requiring a fail-silent or a fail-indicate System Basis Chip. A fail-operational mode of the 33907NL and 33908NL is not described.

This document targets high functional safety integrity levels. For functional safety goals which do not require high functional safety integrity levels, system integrators need to tailor the requirements for their specific application.

It is assumed, the user of this document is generally familiar with the 33907NL and 33908NL device and ISO 26262 standard.

1.1 Interface Documents

This sections lists all the helpful documentation for the user.

Document Number	Document Type	Description
ISO 26262	Standard	ISO 26262 Road vehicles - Functional safety, November 2011
MC33907-MC33908D2	Data Sheet	Data Sheet for 33907 & 33908
FCTNLSFTYWP	White paper	Addressing the Challenges of Functional Safety in the Automotive and Industrial Markets, White Paper, October 2011
PowerSBCLIN_Dynamic _FMEDA_IEC62380	Dynamic FMEDA	Failure Mode Effects and Diagnostic Analysis Document
201445252A	PPAP	Report summarizing data gathered during qualification of the 33907NL and 33908NL following AECQ100-RevG requirements

1.2 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.

2 General Information

The 33907NL and 33908NL is designed to be used in automotive or industrial applications which need to fulfill functional safety requirements, as defined by functional safety integrity levels (for example, ASIL D of ISO 26262).

The following devices are supported by this Safety Manual:

- MC33907LAE
- MC33908LAE
- MC33907NAE
- MC33908NAE

2.1 Conditions of Operation and System Integration

Assumption: [SM_001] To avoid systematic errors during system integration, It is system integrator's responsibility to follow Freescale recommendations as described in the 33907NL and 33908NL Data Sheet and application note available on www.freescale.com.[END]

Assumption: [SM_002] It is system integrator's responsibility to report all field failures of the devices to the silicon supplier [END]

Rationale: To cover the ISO 26262-7 (6.5.4) and ISO 26262-7 (6.4.2.1).

Assumption: [SM_003] It is system integrator's responsibility to take into account the latest device errata during system design, implementation, and maintenance. For a functional safety-related device such as 33907NL and 33908NL, this also concerns functional safety-related activities such as system level functional safety concept development.[END]

The number of simultaneous pin disconnection (i.e pin lift on the PCB) is restricted to 1.

Thermal connection of the exposed pad to the PCB is always ensures thanks to its large size.

Short-circuit between PCB tracks is not considered.

External component disconnection is not considered.

2.2 Safety Function

Given the application independent nature of the 33907NL and 33908NL, no general safety function can be specified. Therefore, this document specifies a safety function being application independent for the majority of applications. This application independent safety function would have to be integrated into a complete (application dependent) system.

2.3 Safe State

A Safe state of the system is named Safe $state_{system}$ whereas a Safe state of the 33907NL and 33908NL is named Safe $state_{SBC}$. A Safe $state_{system}$ of a system is an operating mode without an unreasonable probability of occurrence of physical injury or damage to the health of persons. A Safe $state_{system}$ may be the intended operating mode or a mode where it has been disabled.

Likewise, a Safe $state_{SBC}$ of the 33907NL and 33908NL is by definition one of following operation modes (see Figure 1):

a) Operating correctly
— Outputs depend on application.
b) Explicitly indicating an error (RESET and/or fail-safe output)
— RESET and fail-safe output are in a state indicating an error (active-low)
c) Reset
— MCU connected is under RESET condition.
d) Completely unpowered

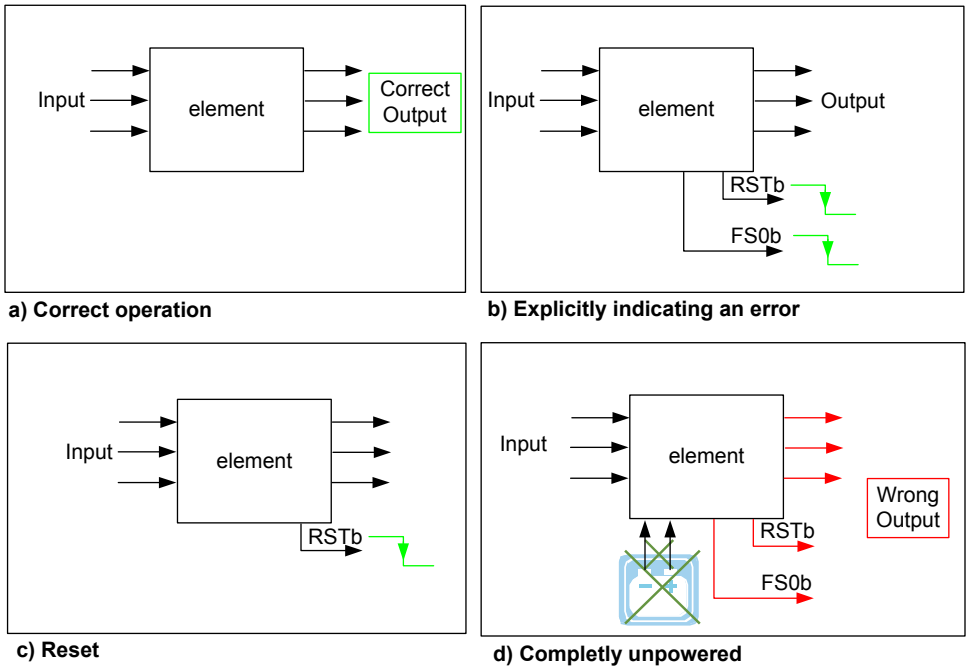


Figure 1. Safe state$_{SBC}$ of the 33907NL and 33908NL

Assumption: [SM_004] It is the system integrator's responsibility to ensure the system transitions itself to a Safe state$_{system}$ when the 33907NL and 33908NL explicitly indicates an error via its fail-safe outputs (Reset and/or FS0b).[END]

Assumption: [SM_005] It is the system integrator's responsibility to ensure the system transitions itself to a Safe state$_{system}$ when the 33907NL and 33908NL is in reset state.[END]

Assumption: [SM_006] It is the system integrator's responsibility to ensure the system transitions itself to a Safe state$_{system}$ when the 33907NL and 33908NL is completely unpowered.[END]

2.4 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 give rise to a hazardous event, and the time by which counteraction has to 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 2 shows the FTTI for a single-point fault occurring in the SBC (Figure 2a) with an appropriate functional safety mechanism to handle the fault (Figure 2b). Without any suitable functional safety mechanism, a hazard may appear after the FTTI elapsed (Figure 2c).

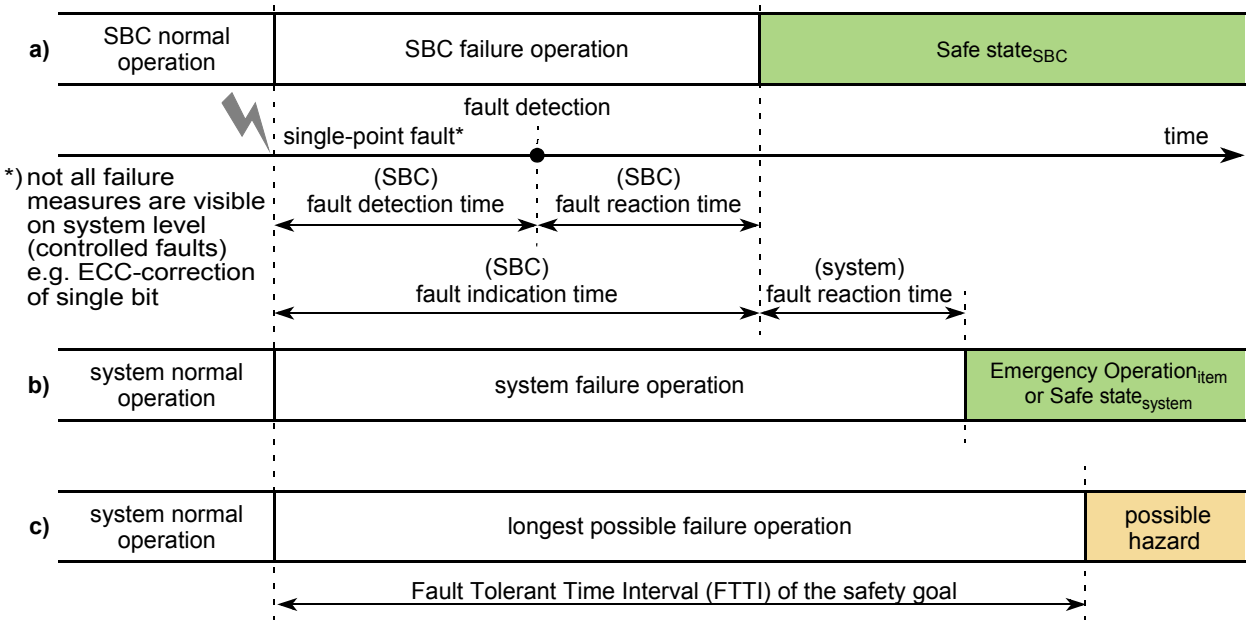


Figure 2. Fault Tolerant Time Interval for Single-point Faults

Fault indication time is the time it takes from the occurrence of a fault to switching into Safe state$_{SBC}$ (for example, indication of that failure by asserting the fail-safe output pins).

Fault indication time of the SBC has three components:

Fault indication time = **Recognition time** + **Internal processing time** + **External indication time**.

Each component of fault indication time is described as follows:

- **Fault detection time** is the maximum time for detection of a fault and consists of:
  - **Recognition time** is the maximum of the recognition time of all involved functional safety mechanisms. The three mechanisms with the longest time are:
    - Recognition time of an overvoltage on regulators takes 234 μs maximum (corresponding to filtering time)
    - Acknowledgement counter used for external IC monitoring is maximum 9.7 ms
  - **Fault reaction time** is the maximum of the reaction time of all involved functional safety mechanisms consisting of internal processing time and external indication time:
  - **Internal processing time** is not the same depending of the origin but the longest time is about 80 μs for an overvoltage detection. All others are below 80 μs.
  - **External indication time** to notify an observer about the failure external to the SBC. This time is 3.0 μs for RSTB and 22 μs for FS0B. Time needed to activate fail-safe outputs when the internal command is sent from digital and activates the analog drivers.

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

2.5 33907NL and 33908NL Assumptions of Use

2.5.1 System Assumptions (SAxxx)

SA001 It is assumed the 33907NL and 33908NL is used in “12 Volts Automotive “applications where FAIL-SAFE reaction is expected.

SA003 It is assumed the 33907NL and 33908NL is used in application for which the mission profile is like in 3.1, Mission Profile (or less aggressive).

SA005 It is assumed the 33907NL and 33908NL is used in application for which the battery voltage (i.e. pin VSUP1, VSUP,2, VSUP3, and VSENSE of the 33907NL and 33908NL) never exceeds the maximum ratings of the 33907NL and 33908NL (i.e 40V). Above this voltage, the 33907NL and 33908NL run the risk of being destroyed and the safety requirements are no longer satisfied.

SA026 It is assumed that normal operating of the 33907NL and 33908NL is fulfilled by the compliance to the 33907NL and 33908NL data sheet.

2.5.2 Technical Assumptions

SA029 It is assumed an out of range operation of the Power Management Integrated Circuit (PMIC: Supply power voltage V_{CORE}, V_{AUX}, and V_{CCA}) of a MCU and potentially others devices, in a context of safety related applications, is considered a violation of at least one of the Safety Goals of the system.

SA012 It is assumed the 33907NL and 33908NL provides the appropriate power management in a context of a safety related application. If a voltage is out of specification (see 33907NL and 33908NL data sheet), a transition to a safe state in the FTTI must be performed.

SA002 It is assumed the 33907NL and 33908NL is used in applications for which the Fault Tolerant Time Interval (FTTI) is ≥ 10 ms. Shorter “Fault Tolerant Time Interval” must be deeply analyzed, taking into account the inherent behavior of the 33907NL and 33908NL (refer to data sheet).

SA017 Faults having a direct impact on violation of SA012 are assumed as single point faults.

SA004 It is assumed when the multiple point fault time interval is ≤12 hours, then the driving cycle is assumed to be ≤ 12hours.

SA006 It is assumed the 33907NL and 33908NL is used in combination with other devices in the application (i.e. MCU, other analog IC).

SA030 It is assumed an abnormal SW & HW execution of the MCU is considered as violating at least one of the safety goals of the system.

SA013 It is assumed the 33907NL and 33908NL provides the safety mechanism for temporal and logical monitoring (Watchdog) of an MCU in a context of safety related applications. If an incorrect behavior is detected by the 33907NL and 33908NL watchdog safety mechanism, transition to a safe state in the FTTI must be performed.

SA018 Faults having a direct impact on the violation of SA013 are assumed as latent faults.

SA019 It is assumed the 33907NL and 33908NL provides the safety mechanism for MCU error monitoring in a context of safety related applications. If an incorrect behavior is detected by this 33907NL and 33908NL MCU error safety mechanism, transition to safe state in the FTTI must be performed.

SA020 Faults having a direct impact on a violation of SA019 are assumed as latent faults.

SA021 It is assumed the 33907NL and 33908NL provides the safety mechanism for IC(s) error monitoring in a context of safety related applications. If an incorrect behavior is detected by this 33907NL and 33908NL error safety mechanism, transition to safe state in the FTTI must be performed.

SA022 Faults having a direct impact on a violation of SA021 are assumed as latent faults.

SA008 It is assumed simultaneous 33907NL and 33908NL pin disconnections (i.e. pin lift on the PCB) are restricted to 1.

SA009 It is assumed the thermal connection of the exposed-pad to the PCB is always ensured due to its large size.

SA023 It is assumed a self-test (LBIST/ABIST) during start-up is performed to ensure the integrity of the system and to prevent latent faults. In case of a latent fault, the application stays in the safe state.

SA024 It is assumed the safe state is defined as in 2.3, Safe State.

SA025 It is assumed an external switch is available to unpower the application and de-energize the actuator(s). This switch is controlled by an MCU and by the 33907NL and 33908NL. The 33907NL and 33908NL provides an active Fail-safe signal to deactivate the external power switch in the event of a request to transition to the safe state.

2.6 Failure Handling

Failure handling can be split into two categories:

- Handling of failures 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.
- Handling of failures during runtime with repetitive supervision while the safety function is enabled. These errors are to be handled in a time shorter than the respective FTTI.

Assumption: [SM_007] 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.[END]

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.

2.7 Tailored Lifecycle Description

The 33907NL and 33908NL is not an item in the sense of ISO 26262, but only is a component in an item developed at a later point in time. Therefore, the 33907NL and 33908NL project follows a tailored “Safety Element out of context” (SEooC) life cycle.

Along with the hardware part, usual documentation (Data sheet including electrical parameters) and safety related documentation (Safety manual, FMEDA) are provided to parties which integrate the 33907NL and 33908NL into systems.

The following table gives detail of the specific tailoring of the safety life cycle applicable for the 33907NL and 33908NL development.

Table 1. Tailoring details

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	NOT Applicable	Under customer responsibility
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	There is no distributed development on the 33907NL and 33908NL development. Qualification of software component: software and the reuse of software components was not part of 33907NL and 33908NL development. No proven in use argument is considered in the context of 33907NL and 33908NL development
9	All sections	ASIL-oriented and safety -oriented analyses	Applicable	There is no ASIL decomposition to consider in the 33907NL and 33908NL development.
10	All sections	Guideline on ISO 26262	NOT Applicable	Information part only

2.8 Customer Tasks Responsibility

In a context of customer applications, this is a list of required customer tasks under their responsibility. The list is delivered as en example and is not exhaustive.

- Use of the latest 33907NL and 33908NL documentation revision (Data sheet, Safety Manual, FMEDA, Application notes, Errata,...).
- 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 33907NL and 33908NL devices as showed in Table 3 of 3.1, Mission Profile.
- Compare system requirements versus 33907NL and 33908NL requirements and make sure there are no deviances.
- Establish validity of assumptions at the system level considered in Section 2.5, 33907NL and 33908NL Assumptions of Use.
  - Verify the Fault Tolerant Time Interval of the 33907NL and 33908NL is under the system FTTI requirement, whatever the faults
  - Violation of the technical assumptions as described in Section 2.5.2, Technical Assumptions
  - Safe state considerations described in 2.3, Safe State
- Perform safety analysis at the system level, taking into account the safety analysis provided for the 33907NL and 33908NL. Consider assumptions like typical mission profile and failure rate data book (IEC 62380).
- During safety analyses, the non-functional blocks (e.g. debug, etc) should also be considered.
- Perform calculation and verify the safety metrics.
- Perform DFA analysis.
- Validate 33907NL and 33908NL outputs behave as expected in the application, and also during of an error condition.
- Consider and verify single point failures and latent failures at system level.
- Consider and verify systematic errors during development.
- Verify the effectiveness of diagnostics at the system level.
- Perform fault injection tests and validate safety mechanisms.
- Consider all recommendations and implementation hints given in this safety manual.
- For completeness of ISO26262 compliance at system level, consider the 2.7, Tailored Lifecycle Description, Table 1
- The installation of the device at the module level is the responsibility of the customer. However, Freescale gives recommendations on Freescale QFP 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 Freescale Semiconductor representative.

3 Failure Rates and FMEDA

The 33907NL and 33908NL 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 33907NL and 33908NL.

The FIT rate model for a semiconductor, per IEC/TR 62380, considers the failure rate model device to be the sum of three subcomponents: the silicon die, the package, and the interface electrical over-stress.

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 33907NL and 33908NL. It then depends on:

- Mission profile of the application in which the 33907NL and 33908NL is operating
- Selection/usage of the functions and functional safety mechanisms implemented in the application

3.1 Mission Profile

The 33907NL and 33908NL is developed to target the highest level of safety integrity (ASIL D) when applying all recommendations and applicability of the system assumptions mentioned in this safety manual, and for the mission profile of typical safety automotive applications.

Table 2 shows the parameters of the mission profile for typical applications. This document is based on these mission profiles, although use of the 33907NL and 33908NL is not limited to these values. Mission profile is a typical automotive profile.

To prevent latent faults accumulating during a very long time of operation, additional diagnostic measures need to be executed in continuous operation within the multiple-point fault detection interval.

Table 2. Mission Profiles

Mission Parameters	Mission profile
Trip time (t_{TRIP})	12 hours
FTTI	10 ms
Lifetime (t_{LIFE})	20 years
Total operating hours	12000 hours

Table 3 shows temperature profiles.

Table 3. Temperature Profile for Mission Profiles

Device type	Temperature range (°C)	Operation time (h)
Packaged device	125	120
	120	960
	76	7800
	23	2400
	-40	720

3.2 FMEDA Overview

The 33907NL and 33908NL 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 and 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 33907NL and 33908NL features implemented for a specific application.

The 33907NL and 33908NL FMEDA sheet is an example only, based on the result of the safety analysis performed for the context of use of the 33907NL and 33908NL, using the mission profile described in Section 3.1, Mission Profile, and when applying all recommendations and assumptions mentioned in this safety manual.

In a context of customer applications, FMEDA is the responsibility of the customer, and then solely responsible for the safety metric values.

The 33907NL and 33908NL FMEDA document associated with the 33907NL and 33908NL failure rate estimation document is available upon request, when covered by a Freescale Semiconductor NDA (contact your local Freescale Semiconductor representative).

NOTE

This 33907NL and 33908NL safety manual, the example of 33907NL and 33908NL FMEDA, and associated documents and information are provided solely to enable hardware system and software engineers to use Freescale products. There are no expressed or implied copyright licenses based on the information in this document.

Freescale reserves the right to make changes without further official notice. Freescale makes no warranty, representation, or guarantee regarding the suitability of the 33907NL and 33908NL for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation, consequential or incidental damages.

All functional and electrical operating of the 33907NL and 33908NL, including the ones in the product data sheet must be validated against each application by the customer’s technical experts.

Local Freescale technical support can be contacted to help understanding and interpreting the Freescale technical documentation.

4 Functional Safety Concept

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.

4.1 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):**
  An SPF 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 3a shows an SPF inside an element generating a wrong output.
- **Latent Fault (LF):**
  An LF is a “multiple-point fault whose presence is not detected by a safety mechanism nor perceived by the driver”. An LF 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 3b shows an LF 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 3c) shows an RF 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 DPF 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 3d shows two LF inside an element generating a wrong output.
- **Multiple-point fault (MPF):**
  An MPF 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 33907NL and 33908NL.
- **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.

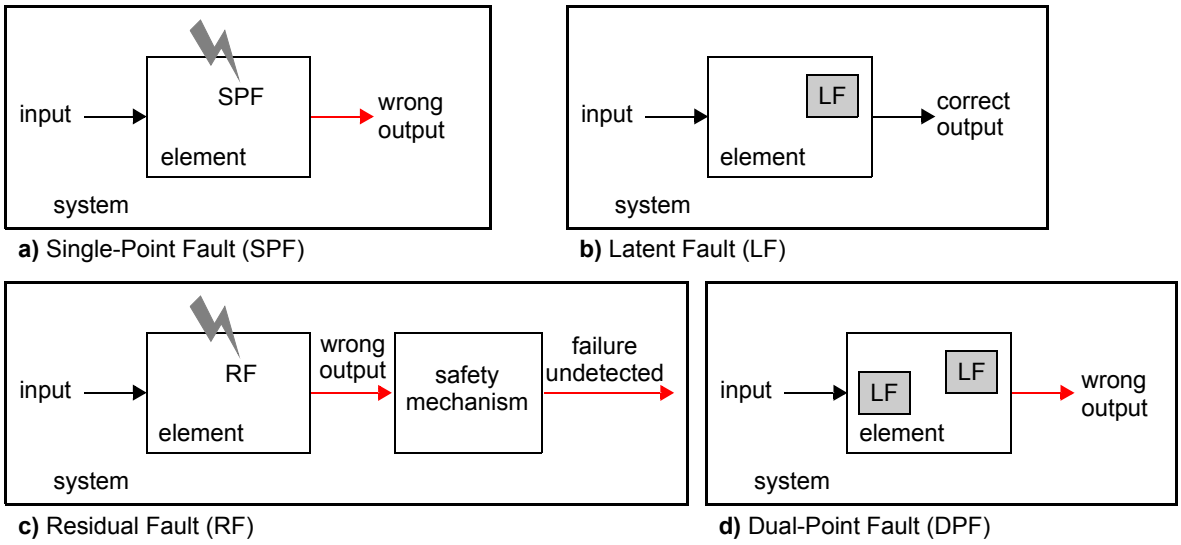


Figure 3. Faults

SPFs must be detected within the FTTI. Latent Faults (dual-point faults) must be detected within the MPFDI. In automotive applications, MPFDI is generally accepted to be once per typical automotive trip time (t_{TRIP}) by test routines (for example, BIST after power-up). This reduces the accumulation time of latent faults from the lifetime of the product t_{LIFE} to t_{TRIP}.

Chapter 3, "Failure Rates and FMEDA" lists a profile with a typical trip time for automotive applications.

4.2 Failures

- **Common Cause Failure (CCF):**
  CCF 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 $\lambda_{\text{single channel}}^{N}$ ($\lambda_{\text{redundant element}} > \lambda_{\text{single channel}}^{N}$).

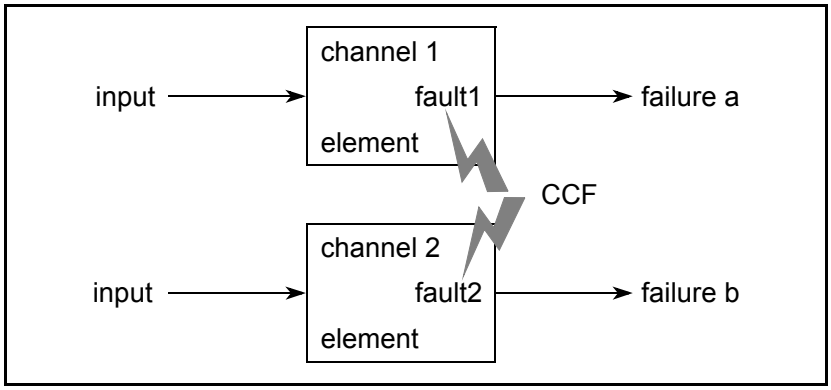


Figure 4. Common Cause Failures

- **Common Mode Failure (CMF):**
  CMF is a subset of CCF. 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 5 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.

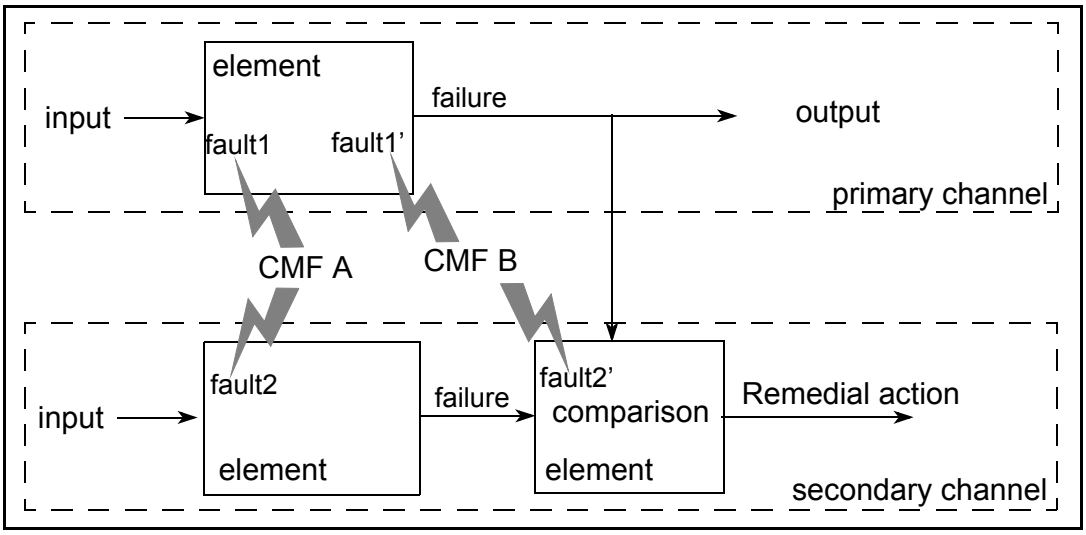


Figure 5. Common Mode Failures

- **Cascading Failure (CF):**
  CFs 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 6 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).

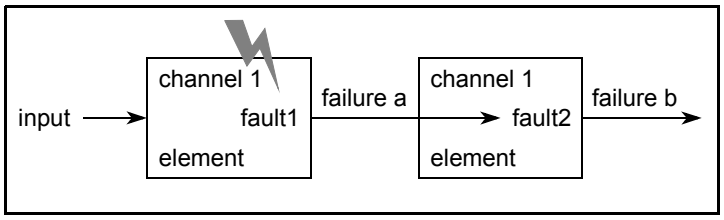


Figure 6. Cascading Failures

4.3 General Functional Safety Concept

Figure 7 shows the block diagram of the 33907NL and 33908NL.

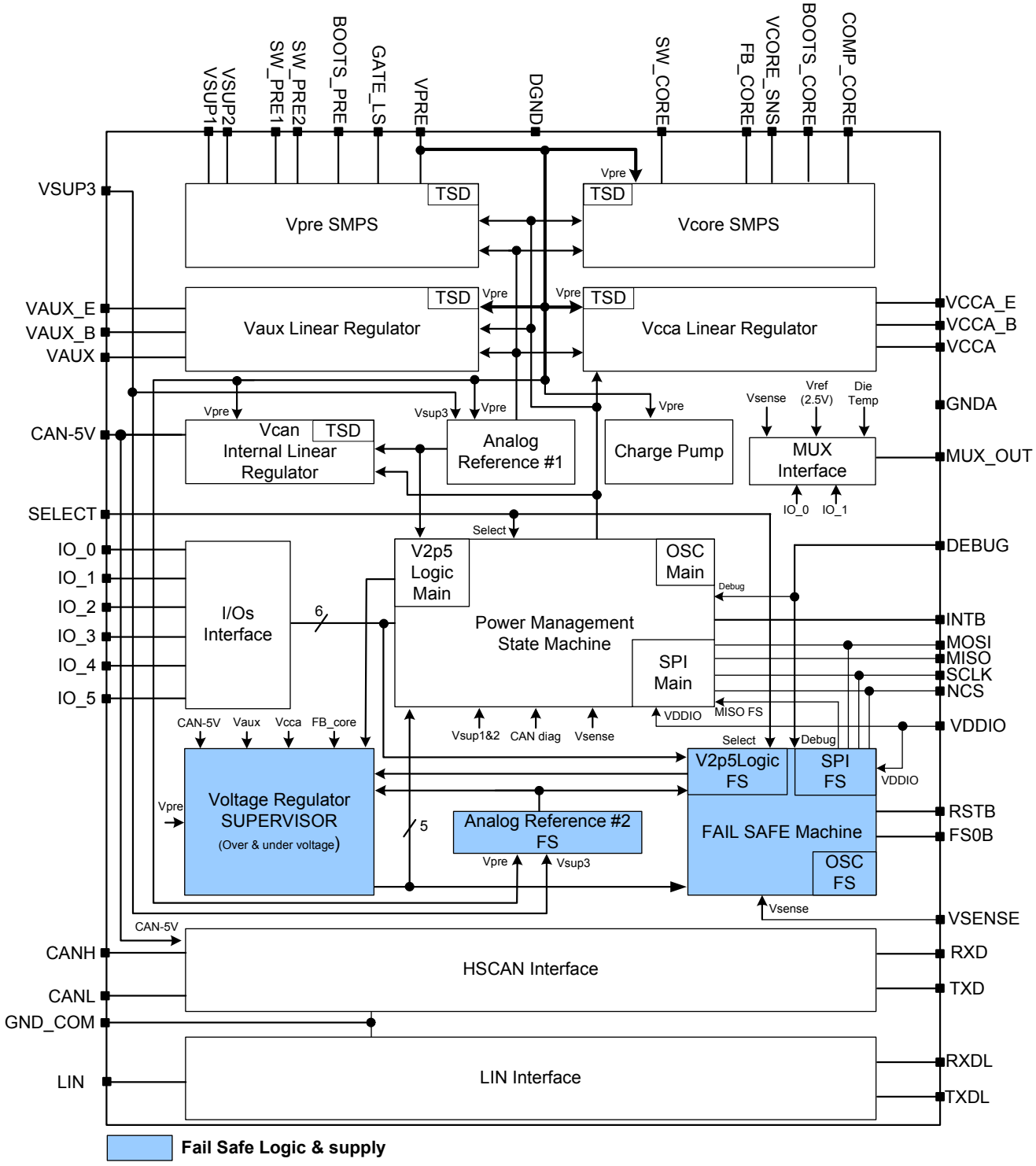


Figure 7. 33907NL and 33908NL Block diagram

Functional Safety integrity measures are as follows:

- Replication of supply pins: three VSUP pins (VSUP1, VSUP2, and VSUP3) are used to supply the product. The loss of VSUP1 or VSUP2 shows the 33907NL and 33908NL is able to continue to work properly thanks to supply redundancy.
- Fail-safe machine is powered by VSUP3, with a redundant supply connection available through VSENSE.
- Fail-safe machine is electrically independent from the rest of the circuit with its own oscillator, own reference voltages (Analog Reference #2FS, V2P5LogicFS), and own SPI register configurations.
- Fail-safe machine internal voltage references are monitored against overvoltage.
- Error correction or detection, or both, to reduce the effect of transient faults and permanent faults is implemented.
- Internal supplies and clock are supervised by dedicated monitors.
- Monitoring of the external voltages (FB_{CORE}, V_{CCA}, V_{AUX}) are provided through the voltage supervisor. Internal reference voltages like V2P5 Main analog (Analog reference#1), V2P5 LogicMain, V2P5 FS analog (Analog Reference #2), V2P5LogicFS are also monitored.
- Built-in self tests (ABIST and LBIST) are implemented in hardware to detect, in general, latent faults only and therefore reduce the risk of coincident latent faults (multiple-point faults).
- The 33907NL and 33908NL can react to failure notifications coming from the Freescale microcontroller, using FCCU (Fault Collection and Control Unit) or external error IC monitoring.
- The risk of CMFs are reduced by a set of measures for both control and reduction of CMFs, spanning system level approaches (such as temperature and non-functional signal monitoring), physical separation, or diversity.
- The use of internal (and external) watchdogs or timeout measures.
- A dedicated mechanism is provided to check the functionality of the safety path (such as by an application).
- A dedicated mechanism is provided to measure external component drift connected on FB_CORE (V_{CORE}).

5 Hardware Requirements at the System Level

This section lists necessary or recommended measures on the system level for the 33907NL and 33908NL to achieve the functional system safety goal(s).

The 33907NL and 33908NL offer an integrated functional safety architecture, a variety of replicated function blocks, self-test unit, and other items to detect faults. By these means, single point failures and latent failure can be detected with a high diagnostic coverage.

However, not all failure modes may be detected on a complete system by the 33907NL and 33908NL. So it is assumed a separate circuitry is used to bring the system into the Safe state$_{system}$ (MCU) in such cases.

Figure 8 depicts the functional safety related elements of the 33907NL and 33908NL.

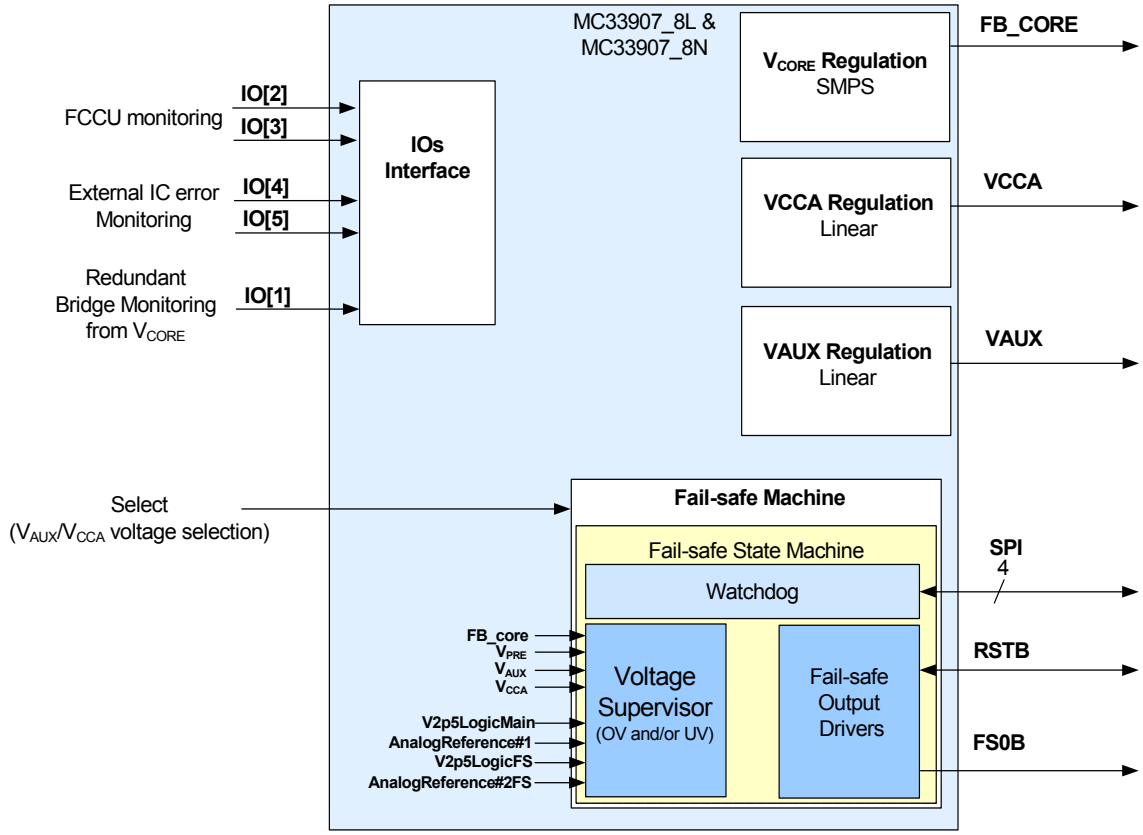


Figure 8. 33907NL and 33908NL Functional Safety Blocks

- V_{PRE} is a voltage mode SMPS regulator supplying several block inside the 33907NL and 33908NL like internal reference voltage, linear, and SMPS regulators.
- V_{CORE} is a voltage mode SMPS regulator. It is dedicated to the MCU core supply (1.2 V, or 3.3 V), configurable through an external resistor bridge.
- V_{CCA} is a 5.0 V/3.3 V linear voltage regulator dedicated usually to the MCU ADC reference voltage.
- V_{AUX} is a linear voltage regulator dedicated usually to auxiliary functions (3.3 V/5.0 V) or sensor supply (tracking of V_{CCA}).
- The SELECT pin is the pin to configure the voltage level of the V_{CCA} and V_{AUX} regulators.
- Based on safety requirements, the IOs can be used to monitor external error signals coming from the MCU or from other integrated circuits in the system. IO[1] can be used to monitor V_{CORE} as a redundant path.
- The Fail-safe machine (FSM) is part of the safety system partitioning. This FSM is made of three main blocks which are:
  - Voltage supervisor (VS)
  - Fail-safe output drivers (FSO)
  - Watchdog (WD)

Figure 9 depicts a simplified application schematic for a functional safety relevant application in conjunction with an MCU (only functional safety-related elements shown). The 33907NL and 33908NL supply the MCU with the required supply voltages (1.2 V, or 3.3 V). Although for most applications the 1.2 V for digital core supply is generated by an external ballast transistor from the 3.3 V supply. Voltages generated by the 33907NL and 33908NL are monitored for overvoltage by the embedded voltage supervision.

The 33907NL and 33908NL also monitor the state of the error out signals FCCU_F[n] (error monitor) using bi-stable protocol only.

Via the SPI communication interface, the 33907NL and 33908NL repetitively trigger the watchdog from the MCU with a valid answer. A dedicated fail-safe state machine is implemented to bring and maintain the application in Safe $state_{system}$. During a failure (e.g. watchdog not serviced correctly), RSTB is asserted LOW to reset the MCU. A fail-safe output (FS0B) is available to control or deactivate any fail-safe circuitry (e.g. power switch) in redundancy with the MCU.

[covers: SMA8-FMEDA]. 33907NL and 33908NL include Built-in-self-tests.

An interrupt output (INTB) for error information is connected to the NMI input of the MCU.

By a connection of the signal MUX_OUT to an ADC-input of MCU further diagnostic measures are possible (e.g. reading temperature or measuring V_{BATT}). Digital inputs (IO_0, IO_1, IO_4, IO_5) may be used for monitoring error signal handling of other devices. Additionally, 33907NL and 33908NL may act as a physical interface to connect the MCU directly with a CAN or LIN bus.

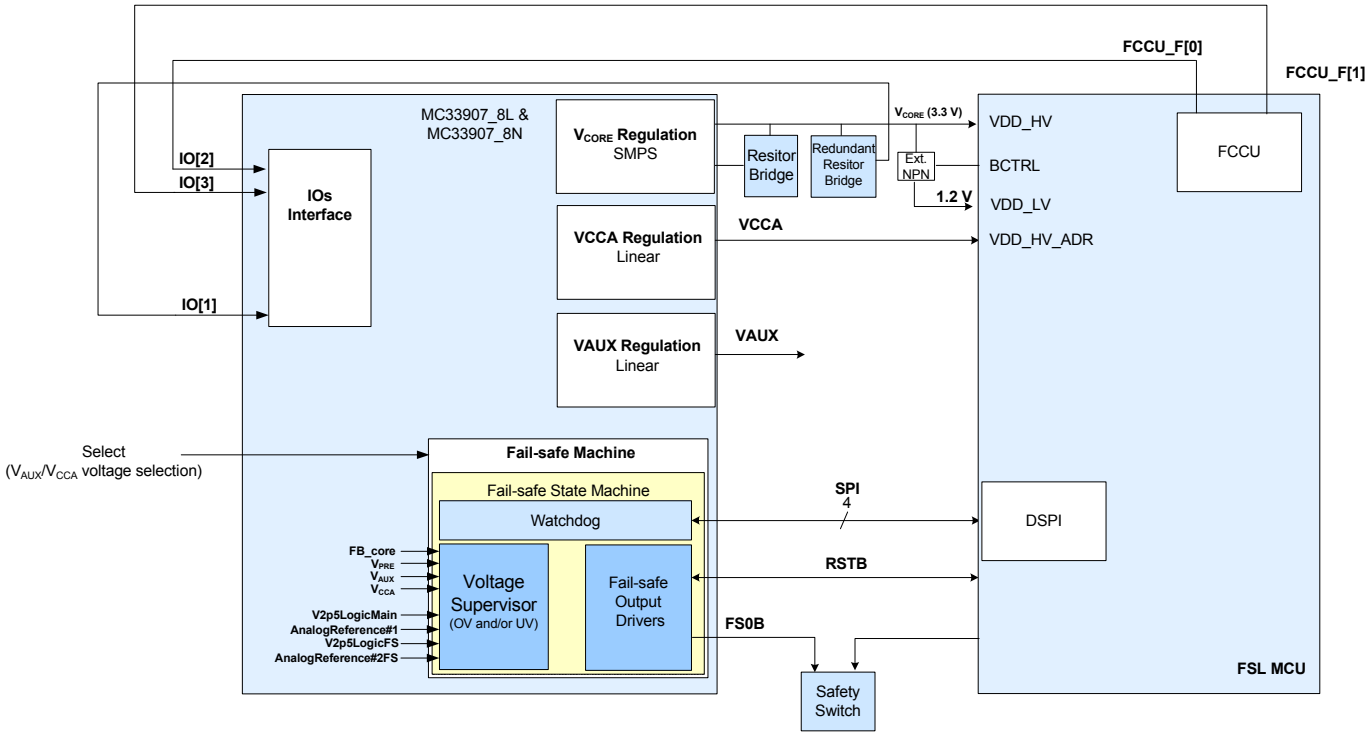


Figure 9. Functional Safety-related Connection to the MCU

NOTE

As an example, on Power Steering applications, the Safety Switch is usually connected between the battery and the three phase MOSFET bridge driving the current to the electric motor. During a fault in the system, the safety switch is opened and the electric motor is no longer powered.

6 Safety Interoperation with Separate Circuitry (MCU)

This section describes safety inter operation with 33907NL and 33908NL and external circuitry like MCU for application requiring high functional safety integrity levels. Failure rates of external devices have to be included in the system FMEDA by the system integrator.

Device Power-up

When the device is powered up, the fuses are loaded into a register bank (to fine tune internal electrical parameters) and checked by means of a hamming code.

[SM_026] if the result of this check is bad due to errors which cannot be corrected, a flag is set in the bit0 “FS_reg_ECC” of the “WD_answer” register, and the RSTB and the FS0B are asserted low. This Error Detection Correction measure is called SPI DED.

This check is used as a safety integrity measure to detect latent faults. [END]

[covers: SM11-FMEDA]

6.1 Power Supply

6.1.1 V_{PRE}

A highly flexible SMPS pre-regulator is implemented in the 33907NL and 33908NL. It can be configured as “Non-inverting Buck-boost converter” or “Standard Buck converter”, depending on the external configuration (Low-side connection).
The pre-regulator delivers a voltage output of 6.5 V, which is used internally.

6.1.1.1 Buck or Buck Boost Configuration

An external low-side logic level MOSFET (N-type) is required to operate the “Non-inverting buck-boost converter”. The connection of the external MOSFET is detected automatically during the start-up phase.

If the low-side is not connected (GATE_LS pin connected to PGND), the product is configured as a standard buck converter.

Assumption: [SM_023] It is the system integrator’s responsibility to make sure the MCU checks the configuration of the buck/or boost configuration after system startup or after LPOFF mode, by reading LS_ detect bit in HW_CONFIG register.[END]

[covers: SMA7-FMEDA]

Rationale: To ensure the system can still be supplied by the device if the battery reaches a very low level due to cranking (Boost option).

Table 4. HW_CONFIG - LS_detect

Read																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	LS_detect	Vaux not used	Vcca_PNP_detect	Vcca_HW	Vaux_HW	1	0	DBG

LS_detect	Description	Report the hardware configuration of V_{PRE} (Buck only or Buck-Boost)
	0	Buck-Boost
	1	Buck only
	Reset Condition	Power On Reset / Refresh after LPOFF

6.1.1.2 V_{PRE} Undervoltage

In case of a V_{PRE} undervoltage, the consequences could be visible on the other regulators available on the device. This is because the V_{PRE} is the supply of all the regulators, so by cascade effect an undervoltage can occurs on V_{CORE}, V_{CCA}, and V_{AUX}.

If the V_{PRE} undervoltage has no consequence on the other regulators, it could still have an impact on the external circuitry potentially connected to V_{PRE} (another external linear regulator for instance).

Assumption: [SM_024] It is system integrator's responsibility to make sure the MCU checks the V_{PRE} undervoltage flag, in case an external circuitry is connected to the V_{PRE} as a supply of this circuitry, by reading the VPRE_UV bit in the DIAG VREG1 register.[END]

Rationale: To ensure the system is aware of this undervoltage and the consequences.

Table 5. DIAG VREG1 - VPRE_UV

Read																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Others_G	Vsns_uv	Vsup_uv_7	Tsd_pre	Vpre_OV	Vpre_uv	Tsd_core	Vcore_OV	Vcore_uv

V_{PRE_UV}	Description	V_{PRE} undervoltage detection
	0	No undervoltage ($V_{PRE} > V_{PRE\_UV}$)
	1	Undervoltage detected ($V_{PRE} < V_{PRE\_UV}$)
	Reset Condition	Power On Reset/Read

6.1.2 V_{CORE}

The 33907NL and 33908NL provide a dedicated voltage supply rail for the main input voltage of the MCU or directly for the core of the MCU (i.e. V_{CORE}).

The voltage level of V_{CORE} supply is configurable through an external resistor bridge. The accuracy of V_{CORE} is ±2.0% without taking account the accuracy of the external resistor bridge.

It is mandatory to select an appropriate resistor tolerance for the external resistor bridge (inferior or equal to ±1.0%).

Assumption:[SM_008] It is the system integrator's responsibility to make sure the right resistor values are well connected between V_{CORE_SNS} and ground, with the middle point connected to $FB_{\_CORE}$ to configure the right voltage to MCU.[END]

Rationale: To ensure overall operation of the MCU according to its datasheet

Figure 10 shows how to configure external resistor bridge for two ranges of supply level (3.3 V and 1.2 V).

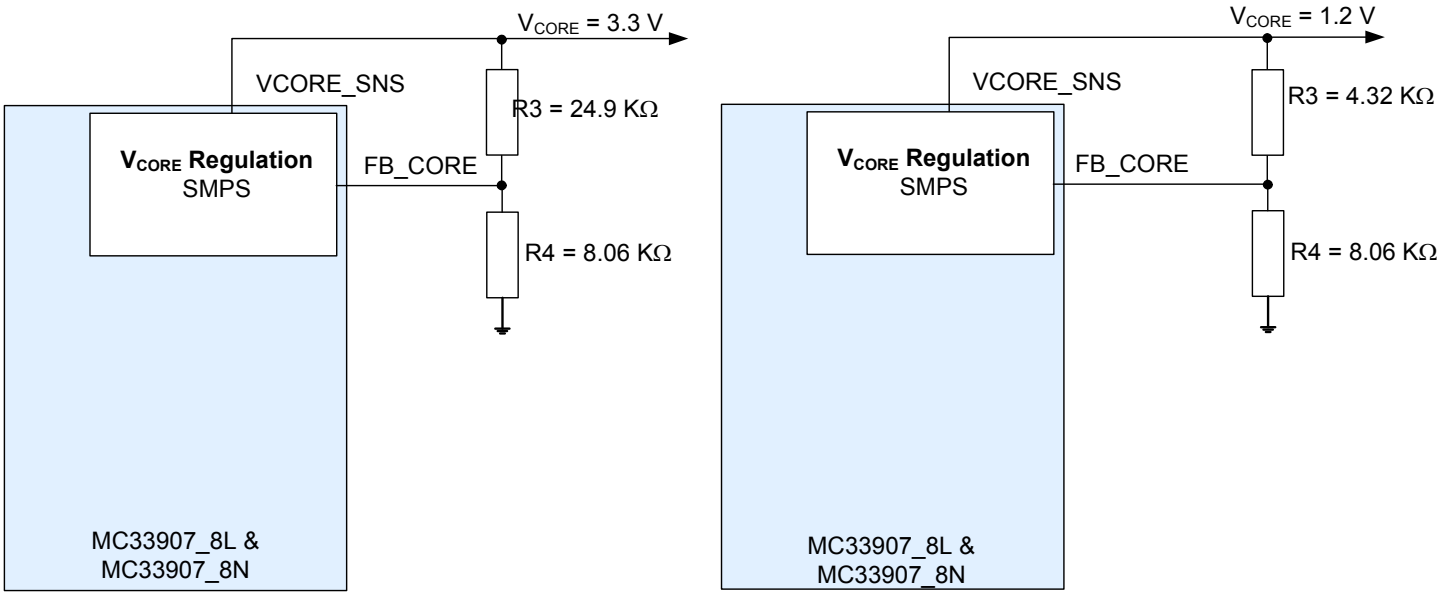


Figure 10. V_{CORE} External Resistor Bridge Configuration

This supply voltage must be in the specified operating range of the MCU, because an overvoltage might cause permanent damage to the MCU even if the MCU is kept in reset. It is therefore either required to de-energize the MCU or to decommission/replace the MCU after an overvoltage event. An undervoltage might lead to an unexpected behavior of the MCU.

Recommendation: It is recommended at the system level to avoid V_{CORE} overvoltage and/or undervoltage, or to permanently disable (Safe $state_{system}$) the system in the event of an overvoltage/undervoltage.

Rationale: To ensure overall operation of the MCU according to its datasheet.

Implementation hint: The 33907NL and 33908NL provide an overvoltage/undervoltage monitoring of the $FB_{\_CORE}$. V_{CORE} voltage is set with an external resistor bridge. If the $FB_{\_CORE}$ is above or below the value specified in the 33907NL and 33908NL decathlete, the MCU is kept powerless by switching off $FB_{\_CORE}$, and the SBC switches the system to a Safe $state_{system}$ within the FTTI and maintains Safe $state_{system}$ through fail-safe outputs (FS0B, RSTB)

[covers: SM1-FMEDA, SM2-FMEDA]

- Internal register configuration:

  In the 33907NL and 33908NL, a register can be configured during the initialization phase to manage the impact at the system level of such overvoltage/undervoltage on V_{CORE}.

  INIT SUPERVISOR 1 register - **Vcore_FS1:0** bits can be configured to perform actions on Fail-safe outputs if there is overvoltage and/or undervoltage on V_{CORE}.

  By default, both V_{CORE_OV} and V_{CORE_UV} do have an impact on RSTB and FS0B.

  The values of overvoltage and undervoltage as well as the filtering time to avoid any sporadic detection, are specified in the 33907NL and 33908NL Data Sheet.

  The voltage supervisor is able also to detect any spikes, oscillations, or drifts of the $FB_{\_CORE}$ voltage if the defined spikes, oscillations, or drifts are in the range of the detection capability (filtering time and voltage threshold specified on $FB_{\_CORE}$).

Table 6. INIT SUPERVISOR 1- Vcore_FS1:0

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	0	0	1	P	Vcore_ FS1	Vcore_ FS0	VCCA_ FS1	VCCA_ FS0	Secure _3	Secure _2	Secure _1	Secure _0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_ G	Vothers _G	SPI_FS _err	SPI_FS _CLK	SPI_FS _Req	SPI_FS _Parity	Vcore_ FS1	Vcore_ FS0	VCCA_ FS1	VCCA_ FS0

	Description	V_{CORE} Safety Input
Vcore_FS1:0	00	No effect on V_{CORE_OV} and V_{CORE_UV} on RSTB and FS0B
	01	V_{CORE_OV} DOES HAVE an impact on RSTB and FS0B. V_{CORE_UV} DOES HAVE an impact on RSTB
	10	V_{CORE_OV} DOES HAVE an impact on RSTB and FS0B. No effect of V_{CORE_UV} on RSTB and FS0B
	11	Both V_{CORE_OV} and V_{CORE_UV} DO HAVE an impact on RSTB and FS0B
	Reset Condition	Power On Reset

In addition, to the Vcore overvoltage / undervoltage monitoring ensured by the voltage supervisor of the 33907NL and 33908NL, the device offers the possibility to detect a drift of the external resistor bridge leading to a drift of the Vcore supply during system lifetime.

Assumption: [SM_009] It is the system integrator's responsibility to make sure the value of the external resistor bridge stays within its nominal value.[END]

Rationale: To avoid a non absolute desired voltage core supply as FB_core is checked for overvoltage and undervoltage.

Implementation Hint: Connect a second external resistor bridge where the middle point is routed to the IO[1] of the 33907NL and 33908NL. This second resistor bridge must be equivalent to the first resistor bridge in charge of the Vcore voltage setting. [covers: SM3-FMEDA]

On the first resistor bridge, the 33907NL and 33908NL regulates the middle point to 0.8V and Vcore voltage is settled according to resistor values. The second resistor bridge takes the Vcore voltage value as the reference voltage and the middle point (connected to IO[1]) is measured and compared to the 0.8V regulated by the devices itself. If the difference is higher than 100mV(maximum), the 33907NL and 33908NL will bring the system in Safe $state_{System}$ within the FTTI and will maintain Safe $state_{System}$ via its safe outputs pins (FS0B, RSTB).

Figure 11 shows the good connections of the external resistor bridges.

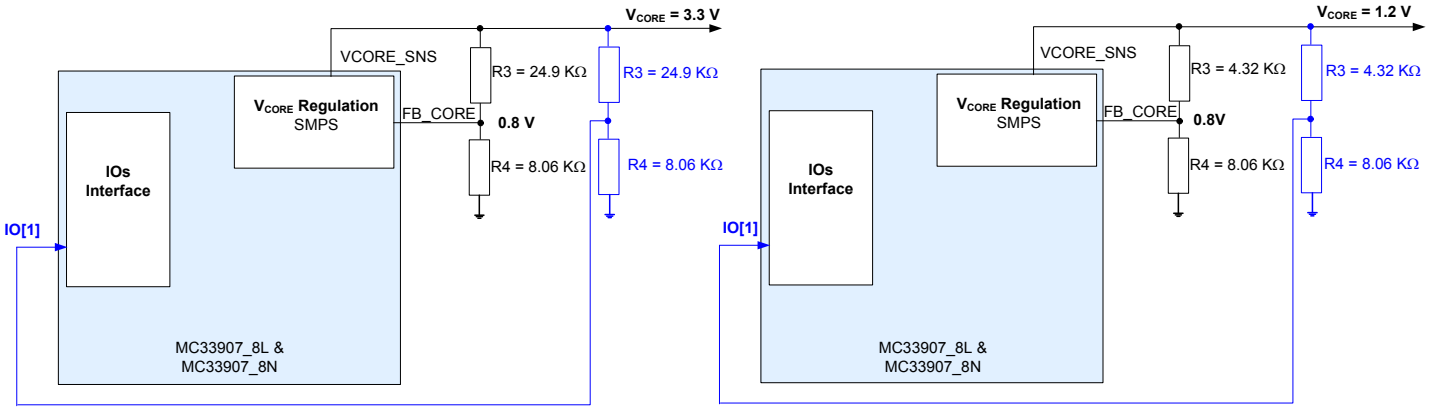


Figure 11. Connection of the second resistor bridge

- Internal register configuration:

  In the 33907NL and 33908NL a register must be configured during initialization phase to enable this safety function and configure IO[1] to measure the middle point of the second external resistor bridge.

  INIT FSSM1 register - IO_1_FS bit must be configured as safety critical.

  By default, IO_1_FS is configured as not safety input.

Table 7. INIT FSSM1 - IO_1_FS

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	0	0	P	IO_01_FS	IO_01_FS	IO_45_FS	Rstb_low	Secure_3	Secure_2	Secure_1	Secure_0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	IO_01_FS	IO_01_FS	IO_45_FS	Rstb_low

IO_1_FS	Description	Configure the IO_1 as Safety Input
	0	NOT SAFETY
	1	SAFETY CRITICAL
	Reset Condition	Power On Reset

6.1.3 V_{CCA}

The 33907NL and 33908NL provide a dedicated voltage supply rail for the Analog to Digital converter of an MCU or for a local ECU supply.

The supply voltage must stay in its specified operating range, because an overvoltage might cause permanent damage to the MCU (if connected as reference voltage of an Analog to Digital converter, for example), even if the MCU is kept in reset.

An undervoltage might lead to an unexpected behavior of the external circuitry, for example where V_{CCA} is the main supply or creates bad conversion results, if V_{CCA} is used as a reference voltage for the Analog to Digital converter of an MCU.

Assumption: [SM_019] It is the system integrator's responsibility to make sure the MCU checks the VCCA output voltage level after system startup, or after LPOFF mode by reading the VCCA_HW bit in the HW_CONFIG register.[END]

[covers: SMA7-FMEDA]

Rationale: To ensure the output voltage level is as good as expected by the system requirements (3.3 V or 5.0 V).

Table 8. HW_CONFIG - VCCA_HW

Read																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	LS_detect	Vaux not used	Vcca_PNP_detect	Vcca_HW	Vaux_HW	1	0	DBG

VCCA_HW	Description	Report the hardware configuration for VCCA
	0	3.3 V
	1	5.0 V
	Reset Condition	Power On Reset

Assumption:[SM_010] It is the system integrator's responsibility where measures at the system level maintain the Safe state$_{system}$ when the V_{CCA} supply voltage is above or below the specified operational range.[END]

Rationale: To ensure overall operation of the analog to digital converter of the MCU or the external circuitry where V_{CCA} is connected.

Implementation hint: The 33907NL and 33908NL provide an overvoltage/undervoltage monitoring of the V_{CCA}. If V_{CCA} is above or below the value specified in the 33907NL and 33908NL Data Sheet, and according to its nominal value (5.0 V or 3.3 V), the MCU or external circuitry is kept powerless, and the SBC switches the system to a Safe state$_{system}$ within the FTTI and maintains Safe state$_{system}$ through fail-safe outputs (FS0B, RSTB).

[covers: SM1-FMEDA, SM2-FMEDA]

- Internal register configuration:

  In the 33907NL and 33908NL, a register can be configured during the initialization phase to manage the impact at the system level of such an overvoltage/undervoltage on V_{CCA}.

  INIT_SUPERVISOR 1 register - **Vcca_FS1:0** bits must be configured to perform actions on fail-safe outputs if there is an overvoltage and/or undervoltage on V_{CCA}. By default, both V_{CCA_OV} and V_{CCA_UV} do have an impact on RSTB and FS0B.

  The values of overvoltage and undervoltage are specified in the 33907NL and 33908NL Data Sheet, as well as the filtering time to avoid any sporadic detection.

  The voltage supervisor is able also to detect any spikes, oscillations, or drifts on the V_{CCA} voltage, if the defined spikes, oscillations, or drifts are in the range of the detection capability (filtering time and voltage threshold specified on V_{CCA}).

Table 9. INIT SUPERVISOR 1 - VCCA_FS1:0

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	0	0	1	P	Vcore_ FS1	Vcore_ FS0	VCCA_ FS1	VCCA_ FS0	Secure _3	Secure _2	Secure _1	Secure _0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_ G	Vothers _G	SPI_FS _err	SPI_FS _CLK	SPI_FS _Req	SPI_FS _Parity	Vcore_ FS1	Vcore_ FS0	VCCA_ FS1	VCCA_ FS0

	Description	V_{CCA} Safety Input
Vcca_FS1:0	00	No effect on V_{CCA_OV} and V_{CCA_UV} on RSTB and FS0B
	01	V_{CCA_OV} DOES HAVE an impact on RSTB and FS0B. V_{CCA_UV} DOES HAVE an impact on RSTB
	10	V_{CCA_OV} DOES HAVE an impact on RSTB and FS0B. No effect of V_{CCA_UV} on RSTB and FS0B
	11	Both V_{CCA_OV} and V_{CCA_UV} DO HAVE an impact on RSTB and FS0B
	Reset Condition	Power On Reset

6.1.4 V_{AUX}

The 33907NL and 33908NL provide a dedicated voltage supply rail for the IOs of an MCU. It can be configurable to supply external sensors.

This supply voltage must stay in its specified operating range, because an overvoltage might cause permanent damage to the MCU, sensors, or local ECU supply. An undervoltage might lead to an unexpected behavior of the external circuitry, for example where V_{AUX} is the main supply.

Assumption: [SM_020] It is the system integrator's responsibility to make sure the MCU checks the VAUX output voltage level after system startup or after LPOFF mode by reading the VAUX_HW bit in the HW_CONFIG register. [END]

[covers: SMA7-FMEDA]

Rationale: To ensure the output voltage level is as good as expected by the system requirements (3.3 V or 5.0 V).

Table 10. HW_CONFIG - VAUX_HW

Read																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	LS_detect	Vaux not used	Vcca_PNP_detect	Vcca_HW	Vaux_HW	1	0	DBG

VAUX_HW	Description	Report the hardware configuration for VAUX
	0	5.0 V
	1	3.3 V
	Reset Condition	Power On Reset

Assumption: [SM_011] It is the system integrator's responsibility to measure at the system level and maintain the Safe $state_{system}$ when the V_{AUX} supply voltage is above or below the specified operational range.[END]

Rationale: To ensure overall operation of the MCU or external circuitry (sensors) where V_{AUX} is connected.

Implementation hint: The 33907NL and 33908NL provide an overvoltage/under voltage monitoring of the V_{AUX}. If V_{AUX} is above or below the value specified in the 33907NL and 33908NL Data Sheet and according to its nominal value (5.0 V or 3.3 V), the MCU or external circuitry is kept powerless, and the SBC switches the system to a Safe $state_{system}$ within the FTTI and maintains Safe $state_{system}$ through the fail-safe outputs (FS0B, RSTB)

[covers: SM1-FMEDA, SM2-FMEDA]

- Internal register configuration:

  In the 33907NL and 33908NL, a register can be configured during the initialization phase to manage the impact at the system level of such an overvoltage/undervoltage on V_{AUX}.

  INIT_SUPERVISOR 2 register - **Vaux_FS1:0** bits must be configured to perform actions on fail-safe outputs if there is an overvoltage and/or undervoltage on V_{AUX}. By default, both V_{AUX_OV} and V_{AUX_UV} do have an impact on RSTB and FS0B.

  The values of overvoltage and undervoltage are specified in the 33907NL and 33908NL Data Sheet as well as the filtering time, to avoid any sporadic detection.

  The voltage supervisor is able to detect any spikes, oscillations, or drifts on the V_{AUX} voltage, if the defined spikes, oscillations, or drifts are in the range of the detection capability (filtering time and voltage threshold specified on V_{AUX})

Table 11. INIT SUPERVISOR 2 - VAUX_FS1:0

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	0	1	0	P	Vaux_FS1	Vaux_FS0	0	DIS_8s	Secure_3	Secure_2	Secure_1	Secure_0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	0	DIS_8s	Vaux_FS1	Vaux_FS0

Vaux_FS1:0	Description	V_{AUX} Safety Input
	00	No effect on V_{AUX_OV} and V_{AUX_UV} on RSTB and FS0B
	01	V_{AUX_OV} DOES HAVE an impact on RSTB and FS0B. V_{AUX_UV} DOES HAVE an impact on RSTB
	10	V_{AUX_OV} DOES HAVE an impact on RSTB and FS0B. No effect of V_{AUX_UV} on RSTB and FS0B
	11	Both V_{AUX_OV} and V_{AUX_UV} DO HAVE an impact on RSTb and FS0b
	Reset Condition	Power On Reset

6.1.5 V_{AUX} - Sensor Supply

V_{AUX} can be used as a sensor supply in a system. To ensure ratiometric conversion between sensors supplied by the V_{AUX} and the analog to digital converter supplied by V_{CCA}, the V_{AUX} must be configured as a tracker of V_{CCA}.

Assumption: [SM_012] It is the system integrator's responsibility to make sure the V_{CCA} linear regulator is used as reference voltage of the analog to digital converter of the MCU.[END]

Rationale: to ensure ratiometric conversion on sensors data output powered by V_{AUX}.

Implementation hint: During initialization phase, the **INIT_VREG2** register must be configured to activate the Vaux_trk_EN bit. V_{AUX} is then the tracker of V_{CCA} with a tracking accuracy of ±15 mV. By default the V_{AUX} tracker is not activated.

Table 12. INIT Vreg 2 - VAUX_trk_EN

Write															
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	0	0	0	0	1	0	P	0	Tcca_lim_off	Icca_lim	0	0	Taux_lim_off	Vaux_trk_EN	0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	0	Tcca_lim_off	Icca_lim	0	0	Taux_lim_off	Vaux_trk_EN	0

Vaux_trk_EN	Description	Configure V_{AUX} regulator as a tracker
	0	No tracking.
	1	Tracking enabled
	Reset Condition	Power On Reset

6.2 Safety Inputs - IOs

6.2.1 IO[2] & IO[3] MCU Error Monitoring - FCCU

The 33907NL and 33908NL measure internal errors coming from the Freescale MCU. If the MCU signals an internal failure via its error out pins (FCCU[0] and FCCU[1]), the system may no longer rely on the integrity of the device's outputs for safety functions. If an error out is indicated, the system switches and remains in the Safe $state_{system}$. The SBC switches the system to a Safe $state_{system}$ within the FTTI and maintains the Safe $state_{system}$ through the Fail-safe outputs (FS0B, RSTB) as a reaction to the indicated error out.

Only the "Bi-stable" protocol is covered on the 33907NL and 33908NL to use with the FCCU pins coming from the Freescale Microcontroller. Refer to the respective Freescale MCU data sheet.

Assumption: [SM_013] It is the system integrator's responsibility to make sure the bi-stable protocol is configured in the Freescale MCU for FCCU protocol.[END]

Rationale: To monitor the Freescale MCU error out signals for correct functionality of the device. The system (for example ECU) may not rely on any I/O other than FCCU_F[0] and FCCU_F[1], when those signals indicate an error.

Implementation hint: Connect MCU FCCU_F[0] error output to the 33907NL and 33908NL IO[2] input, and the MCU FCCU_F[1] error output to the 33907NL and 33908NL IO[3] input. A pull-down must be connected to FCCU_F[0]/IO[2] and a pull-up must be connected to the FCCU_F[1]/IO[3].

[covers: SM8-FMEDA]

Figure 12 shows the connections of MU FCCU and 33907NL and 33908NL IOs.

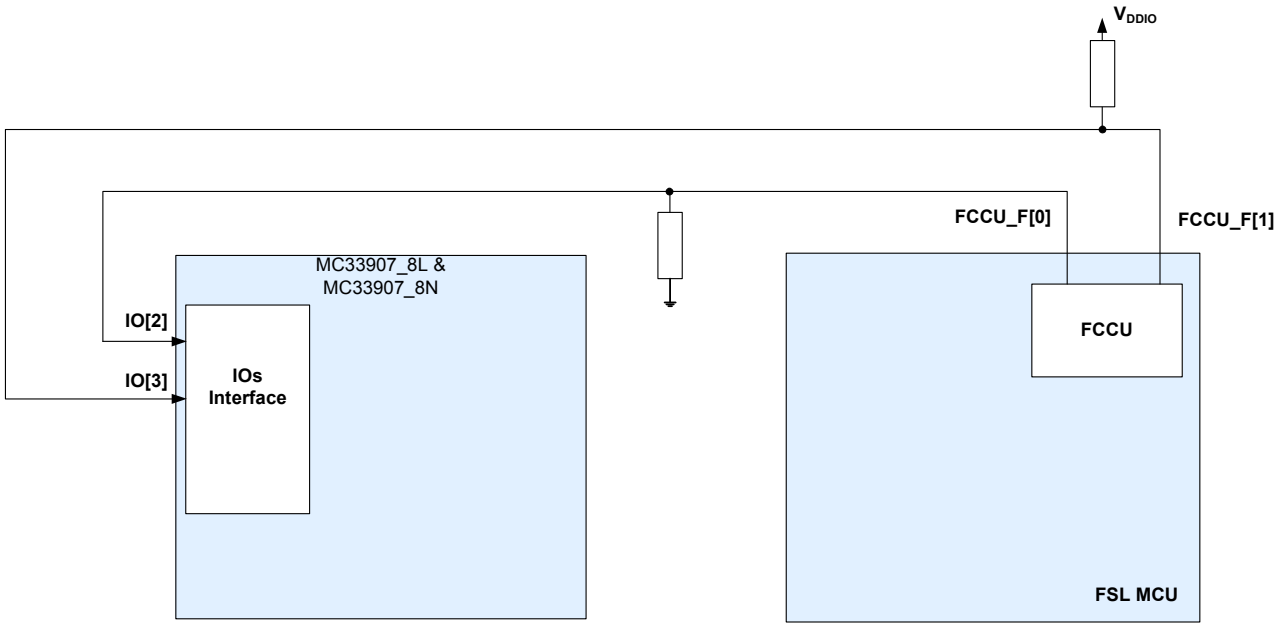


Figure 12. FCCU Connection with 33907NL and 33908NL IOs

- Internal register configuration:
  In the 33907NL and 33908NL, a register must be configured during initialization phase to activate the FCCU error out monitoring.
  INIT_FSSM2 register - **IO_23_FS** bits must be configured as safety inputs
  By default, **IO_23_FS** bit is activated.

Table 13. INIT_FSSM2 - IO_23_FS

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	0	1	P	RSTb_err_FS	IO_23_FS	PS	0	Secure_3	Secure_2	Secure_1	Secure_0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	RSTb_err_FS	IO_23_FS	PS	0

IO_23_FS	Description	Configure the couple of IO_3:2 as safety inputs for FCCU monitoring
	0	NOT SAFETY
	1	SAFETY CRITICAL
	Reset Condition	Power On Reset

6.2.2 IC Error Signal Monitoring

The 33907NL and 33908NL, out of the Freescale MCU FCCU monitoring, can monitor error signals coming from an external IC. This is possible by using digital inputs (IOs) by pair.

On each pair of digital inputs, one must be dedicated to monitor the output error signal coming from the external circuitry, and the other one must be connected to an output of the MCU, to listen for the acknowledgement of the error by the MCU itself.

If the external IC is not in the ECU (local) but outside (global), a serial resistor (5.1 kΩ) must be connected on the right IO to limit the input current during high transients on the line.

When an error from the external circuitry is NOT acknowledged by the MCU within a specific “acknowledgment timing”, the 33907NL and 33908NL switch the system to a Safe $state_{system}$ within the FTTI and maintains the Safe $state_{system}$ through the fail-safe outputs (FS0B).

Assumption: [SM_014] It is the system integrator’s responsibility to make sure the error output signal from external IC is well connected to one SBC IO and one MCU GPIO, to ensure the MCU is able to listen to the fault.[END]

Rationale: Monitor a safety function realized in the ECU, out of the MCU, and bring the system to the Safe $state_{system}$ during a fault.

Implementation hint: In the 33907NL and 33908NL, a register can be configured during the initialization phase to manage the impact at the system level of such error monitoring using IOs by pair out of IO[2] & IO[3], which are dedicated to FCCU monitoring.

IO[0] & IO[1] AND/OR IO[4] & IO[5] can be used to enable this safety function.

INIT FSSM1 register - **IO_01_FS** bits must be configured as **safety critical** to perform actions on fail-safe outputs (FS0B) if there is an error reported by an external IC on IO[0] and not acknowledged by the MCU on IO[1]. Refer to the 33907NL and 33908NL Data Sheet.

By default, IO_01_FS are not configured as safety critical inputs.

INIT FSSM1 register - **IO_45_FS** bits must be configured as **safety critical** to perform actions on fail-safe outputs (FS0B, RSTB) if there is an error reported by external IC on IO[4] and not acknowledged by the MCU on IO[5]. Refer to the 33907NL and 33908NL Data Sheet.

By default, IO_45_FS are not configured as safety critical inputs.

Table 14. INIT_FSSM1 - IO_01_FS - IO_45_FS

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	0	0	P	IO_01_FS	IO_1_FS	IO_45_FS	RSTb_low	Secure_3	Secure_2	Secure_1	Secure_0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	IO_01_FS	IO_1_FS	IO_45_FS	RSTb_low

IO_01_FS	Description	Configure the couple of IO_1:0 as safety inputs
	0	NOT SAFETY
	1	SAFETY CRITICAL
	Reset Condition	Power On Reset
IO_45_FS	Description	Configure the couple of IO_5:4 as safety inputs
	0	NOT SAFETY
	1	SAFETY CRITICAL
	Reset Condition	Power On Reset

Figure 13 shows a connection example of an external IC error out on IO[4] connected in the ECU and the MCU acknowledgement on IO[5]

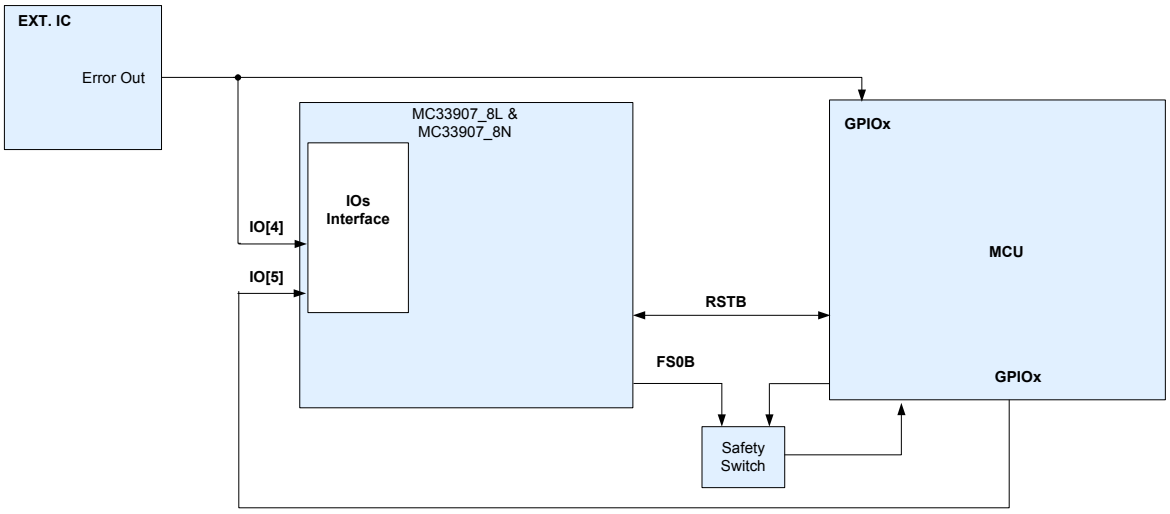


Figure 13. External IC Error Connection - External Circuitry Designed in the ECU (Local)

Figure 14 shows the signal in case of an error on the external IC with or without MCU acknowledgement.

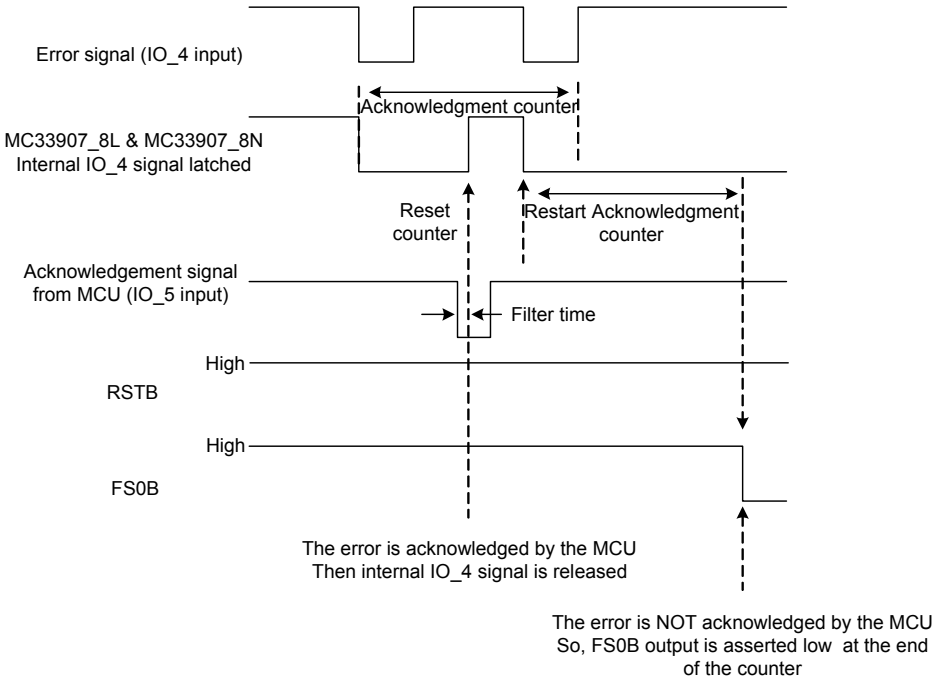


Figure 14. External IC Error Monitoring (Timing)

Refer to the 33907NL and 33908NL Data Sheet for filtering time, and counters.

[covers: SM9-FMEDA]

6.2.3 IC Error Signal Monitoring or How to Verify the Safety Path in a System

If an error is reported to IO[4] and if the MCU doesn't acknowledge the fault, the SBC asserts only the FS0B output to bring the system into Safe state$_{system}$. The RSTB is not asserted low in this specific case.

The external IC error out can also be replaced by the MCU itself using a GPIO.

Recommendation: at each startup of the system it is recommended to verify the safety path.

[covers: SMA9-FMEDA]

Rationale: to ensure the system is well in the Safe state$_{system}$ when the FS0B is asserted low before starting the application.

Implementation hint: connection of one MCU GPIO to IO[4] and a second GPIO to IO[5], and drive the first GPIO (IO[4]) like the error output of an external IC. Bit IO_45_FS in register shown in Table 14 must be configured.

Figure 15 shows the connection for the verification of safety path each startup.

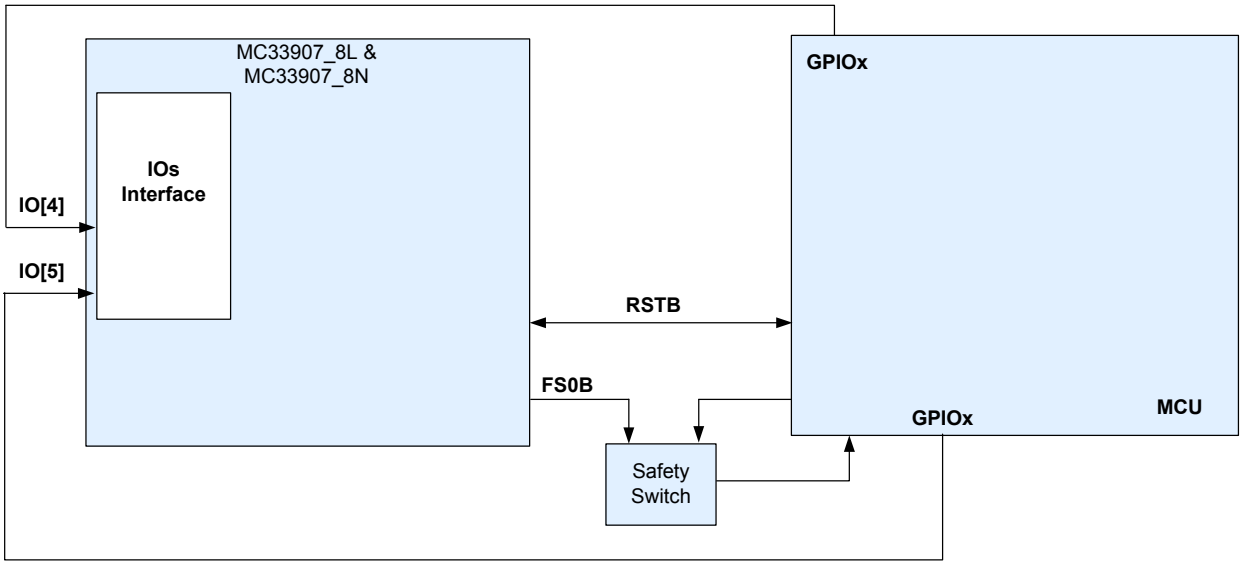


Figure 15. Safety Path Verification

6.3 Watchdog

A common mode failure may lead to a state where an MCU is not able to signal an internal failure via its error out pins (see IO[2] & IO[3] MCU Error Monitoring - FCCU). With the use of an item (system) level timeout function (e.g. watchdog), the likelihood that common mode failures affecting the functional safety of the system can be reduced significantly.

In general, the external watchdog covers common mode failures which are related to:

- missing/wrong power
- missing/wrong clocks
- missing/wrong resets
- general destruction of internal components (e.g. latch-up at redundant input pads)
- errors in mode change (e.g. test, debug, sleep/wake-up)

Since these errors do not result in subtle output variations of the MCU, but typically in a complete failure, a simple watchdog is sufficient.

The watchdog function is required to be sufficiently independent to the SBC (e.g regarding clock generation, power supply, implementation, etc.).

The 33907NL and 33908NL act as a supervisor of the operation, and as a consequence, include a windowed watchdog which needs to be refreshed periodically by the MCU. It means the 33907NL and 33908NL watchdog function is in permanent communication with the MCU. As soon as there is no correct communication, after repetitive and defined tries, the SBC switches the system to Safe state$_{system}$ within the FTTI. Thus either the MCU or the SBC can switch the system to Safe state$_{system}$.

Assumption: [SM_015] It is the system integrator's responsibility to make sure the MCU refresh periodically the 33907NL and 33908NL watchdog.[END]

Rationale: to cover situations, when MCU is not able to signal a failure.

Implementation hint: The duration of the watchdog window is configurable to allow different MCU handshake strategies. The duty cycle of the window is fixed and is 50%. Therefore the first half of the window is said "closed" and the second half of the window is said "open". "Open" window is the window where the watchdog must be refreshed.

[covers: SM5-FMEDA]

- Internal register:

  In the 33907NL and 33908NL, a register can be configured during initialization phase or in normal operation. Doing the change in normal operation allow the system integrator to configure the watchdog window duration on the fly (the new WD window duration will be taken into account when the previous one is finished).

  WD WINDOW register - **WD_Window_x** bits (where x=0 to 3) can be configured

  By default, a window of 3.0 ms is configured.

Table 15. WD_Window

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	1	0	P	WD_Window_3	WD_Window_2	WD_Window_1	WD_Window_0	Secure_3	Secure_2	Secure_1	Secure_0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	WD_Window_3	WD_Window_2	WD_Window_1	WD_Window_0

WD_Window_3:0	Description	Configure the couple of IO_1:0 as safety inputs
	0000	Disable
	0001	1.0 ms
	0010	2.0 ms
	0011	3.0 ms
	0100	4.0 ms
	0101	6.0 ms
	0110	8.0 ms
	0111	12 ms
	1000	16 ms
	1001	24 ms
	1010	32 ms
	1011	64 ms
	1100	128 ms
	1101	256 ms
	1110	512 ms
	1111	1024 ms
	Reset Description	Power On Reset

Figure 16 shows the refresh slot allowed during WD refresh

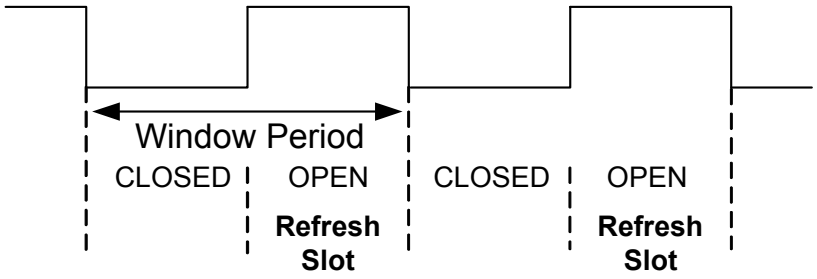


Figure 16. WD Refresh Slot

The windowed watchdog is based on an 8-bit pseudo-random word generated by means of a Linear Feedback Shift Register implemented in the SBC. A default LFSR value (0xB2) is available in the WD_LFSR register at startup and the MCU, during the SBC initialization phase, can read back the LFSR to start its own calculation and then perform the watchdog answer.

- Internal register:

  In the 33907NL and 33908NL, a register can be checked during initialization phase or even in normal operation to read back the LFSR value. It is also possible for the MCU to write its own LFSR. The new LFSR is taken by the SBC to perform its own calculation.

  WD_LFSR register - **WD_LFSR_x** bits (where x=0 to 7) - Read or Write allowed.

When the MCU reads back the LFSR from the 33907NL and 33908NL, the MCU must start the calculation using simple formula. Refer to the 33907NL and 33908NL Data Sheet.

As soon as the result is available and when the window is open, the MCU must send the result to the SBC. The two results (MCU & SBC) are then compared.

- Internal register:

  In the 33907NL and 33908NL, a register is available to write the result of the simple calculation based on the LFSR.

  WD ANSWER register - **WD_answer_x** bits (where x=0 to 7) - Read or Write allowed.

Table 16 shows when a Watchdog answer is considered as right or wrong.

Table 16. Watchdog Error Table

		WINDOW	
		CLOSED	**OPEN**
SPI	**BAD Key**	WD_NOK	WD_NOK
	Good Key	WD_NOK	WD_OK
	None (Timeout)	No_issue	WD_NOK

Three counters are involved each time a right or wrong watchdog refresh is performed. Refer to the 33907NL and 33908NL Data Sheet to understand how they interact each others.

- WD_error counter
- WD_refresh counter
- Reset error counter

NOTE

After consecutive bad watchdog refreshes, the 33907NL and 33908NL switches the system in Fail-safe sate when reset error counter reaches intermediate level. Then, any correct watchdog refresh is also monitored to allow the MCU to “get out” from a Fail-safe state, because the MCU behaves again as expected.

Too many consecutive bad watchdog refreshes (if reset error counter reaches final value) definitively switch the system to a deep Fail-safe mode. Only a key off/Key on sequence at the system level can help to recover the situation. Refer to the 33907NL and 33908NL Data Sheet.

The FTTI requirement at system level (e.g. 10 ms) must be considered, and by consequence the watchdog window period must be configured accordingly. The WD error counter can also be configured to define the number of consecutive bad WD refreshes allowed by the system before tripping a reset. Basically, it can be 3, 2, or only 1.

6.4 Debug Mode Operation

A debug mode is available on the device to help the system engineer to develop its software without asserting the watchdog in a periodic manner.

In this mode, the FS0B output is asserted low at startup as in normal mode, but as soon as the FS0B is released to a “high” via the SPI (Good 1st WD answer and FS_OUT writing), this pin never asserts low, even if a fault is reported.

For example, in debug mode, any errors from the watchdog are ignored (No reset and No fail-safe), even if the whole functionality of the watchdog is kept ON (Seed, LFSR, WD_refresh counter, WD error counter). This allows an easy debug of the hardware and software routines (i.e. SPI commands).

When the Debug mode is activated, the CAN transceiver is set to Normal operation mode. This allows communication with the MCU, in case the SPI communication is not available (case of MCU not programmed).

Assumption: [SM_022] It is the system integrator’s responsibility to make sure the MCU checks of the Debug mode is not activated after system startup or after LPOFF mode by reading the DBG bit in HW_CONFIG register.[END]

[covers: SMA7-FMEDA]

Rationale: To ensure the product is not working in debug mode and by consequence is able to assert the safety output FS0B low during a fault.

Table 17. HW_CONFIG - DBG

Read																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	LS_detect	Vaux not used	Vcca_PNP_detect	Vcca_HW	Vaux_HW	1	0	DBG

DBG	Description	Report the configuration of the DEBUG mode
	0	Normal operation
	1	DEBUG mode selected
	Reset Condition	Power On Reset / Refresh after LPOFF

To activate the Normal mode at startup, the debug pin of the device must have an external pull-down. Refer to 33907NL and 33908NL data sheet.

6.5 Safety Outputs - FS0B, RSTB

The safety outputs are used to switch the system in the Fail-safe state (Safe $state_{system}$).

6.5.1 RSTB

RSTB is a dedicated active low signal integrated in the 33907NL and 33908NL to bring the MCU under RESET during an SBC internal fault or a fault reported by the system.

Assumption: [SM_016] an output in high-impedance is not considered safe at the system level, 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.[END]

Rationale: to bring at the functional safety-critical outputs to a defined voltage level anytime.

Implementation: an external pull-down capacitor (filtering) and an external pull-up resistor must be connected to the right voltage rail (5.0 V or 3.3 V).

Figure 17 shows the connection of external components to insure good safety operation of RSTB.

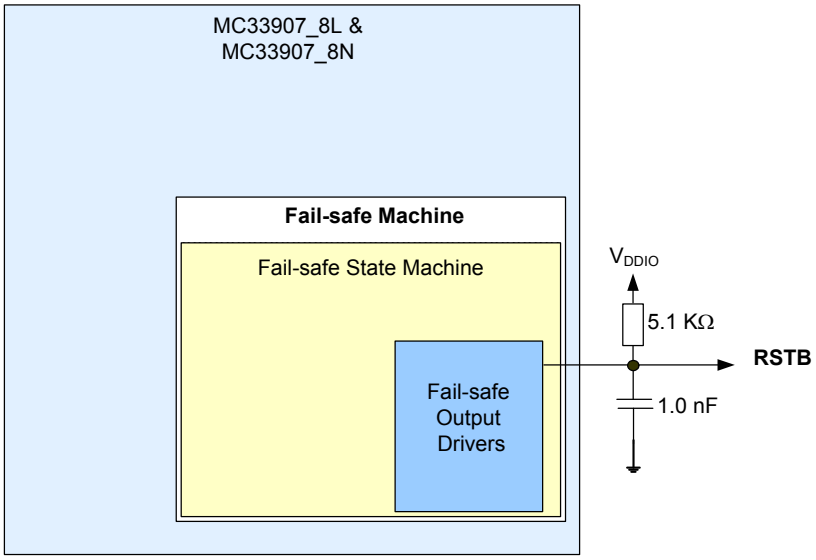


Figure 17. External Components on RSTB

The duration of the reset is configurable during initialization phase of the SBC.

- Internal register:

  In the 33907NL and 33908NL, a register can be configured only during initialization phase to define the reset duration when it is asserted low.

  INIT FSSM1 register - **RSTB_low** bits (1.0 ms or 10 ms low level duration available).

  By default, the reset low duration time is set to 10 ms

Table 18. INIT_FSSM1 - RSTB_low

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	0	0	P	IO_01_FS	IO_1_FS	IO_45_FS	RSTb_low	Secure_3	Secure_2	Secure_1	Secure_0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	IO_01_FS	IO_1_FS	IO_45_FS	RSTb_low

RSTB_Low	Description	Configure the Reset low duration time
	0	10 ms
	1	1.0 ms
	Reset Condition	Power On Reset

An RSTB low pulse can also be requested by the SPI to check hard connection between the MCU reset pin and the 33907NL and 33908NL. This request comes from the MCU itself and is a software request.

This action must be done before releasing the FS0B to a “high”. The goal is to verify the good RSTB hardware connection between the MCU and the 33907NL and 33908NL.

[covers: SMA4-FMEDA]

- Internal register:
  In the 33907NL and 33908NL, a write command can be send by the MCU to request a low reset pulse
  RSTB_request register - **RSTB_request** bit.
  By default, the **RSTB_request** bit is not activated.

Table 19. RSTB_request

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	1	0	1	0	P	0	0	Rstb_request	0	Secure_3	Secure_2	Secure_1	Secure_0
MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	0	0	0	0	0	0	0	0

RSTb_Request	Description	Request a RSTB low pulse
	0	No request
	1	Request a RSTB low pulse
	Reset Condition	Power On Reset / When RSTB is done

The RSTB pin is bi-directional, so the 33907NL and 33908NL can bring the MCU under RESET and the MCU can maintain the RSTB low even if the 33907NL and 33908NL is ready to release it. All the reset numbers asserted by the 33907NL and 33908NL are populated in the reset error counter.

The reset error counter manages the reset events and count the number of reset occurring in the system. This counter is incremented by 1 each time a reset is generated.

The reset error counter has two outputs values (intermediate and final). The intermediate output value is used to handle the transition from reset (RSTB is asserted low) to reset and fail, where RSTB and FS0B are activated. The final value is used to handle the transition from reset and fail to deep reset and fail (deep Fail-safe mode) where all regulators are off, reset and FS0B are asserted low, and a power on reset or a transition on IO[0] is needed to recover.

Rationale: if reset error counter reaches its final value, it means a critical permanent issue is reported at the stem level and the SBC completely switches the MCU off, and maintains the system in the fail-safe state (Safe $state_{system}$).

implementation hint: In the 33907NL and 33908NL, a register, INIT_FSSM2 can be configured during the initialization phase for the intermediate and final values of the reset error counter.

- Internal register:
  INIT_FSSM2 register - **RSTB_err_FS** bit
  By default, the **RSTB_err_FS** bit is configured for an intermediate value = 3 and a final value = 6.

Table 20. INIT_FSSM2 - RSTB_err_FS

Write																
	bit15	bit14	bit13	bit12	bit11	bit10	bit9	bit8	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
MOSI	1	1	0	0	1	0	1	P	RSTb_err_FS	IO_23_FS	PS	0	Secure_3	Secure_2	Secure_1	Secure_0

MISO	SPI_G	WU	CAN_G	LIN_G	IO_G	Vpre_G	Vcore_G	Vothers_G	SPI_FS_err	SPI_FS_CLK	SPI_FS_Req	SPI_FS_Parity	RSTb_err_FS	IO_23_FS	PS	0

RSTB_err_FS	Description	Configure the values of reset error counter
	0	Intermediate = 3; final = 6
	1	Intermediate = 1; final = 2
	Reset Condition	Power On Reset

Conditions which can lead to an incrementation of the RSTB error counter and according to product configuration are:

- Watchdog error counter = 6 (if WD_CNT_error_1:0 from INIT_WD register = 00, or 01)
- Watchdog refresh not OK during INIT phase or watchdog timeout
- IO_23 error detection FCCU
- Undervoltage
- Overvoltage
- Delta voltage of the second resistor bridge connected on Vcore
- FS0B shorted to VDD
- SPI DED
- Reset request by SPI (software request)
- External reset

[SM_025] The reset error counter is triplicated and a majority voter is implemented to avoid any unexpected change due to a bit flip, for example. 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 by the right value.

A flag is set in the “FS_ECC” bit of the “WD_answer” register available for MCU diagnostic. [End]

[Covers: SM10-FMEDA]

6.5.1.1 Reset Error Counter at Startup or Resuming from LPOFF Mode

At startup or when resuming from LPOFF mode the reset error counter starts at level 1.

6.5.2 FS0B

FS0B is a dedicated active low signal integrated in the 33907NL and 33908NL to bring the system in fail-safe state (Safe $state_{system}$) when needed. This safety output can be used for opening the power supply line, opening a security MOSFET is a series with a Motor/Valve,...

Assumption: [SM_017] an output in high-impedance is not considered safe at the system level, It is the system integrator's responsibility to make sure external components connected to FS0B are available to bring the safety critical outputs to a known level during operation. [END]

Rationale: in order to bring the functional safety-critical outputs to a defined voltage level at anytime.

Implementation: an external pull-down capacitor (filtering) and an external pull-up resistor must be connected to the right voltage rail (up to battery voltage).

Assumption: [SM_021] It is the system integrator's responsibility to make sure, opening the safety switch in a system must not be driven by he FS0B only at a fault event, but also by the MCU.[END]

[covers: SMA8-FMEDA]

Rationale: In order to have a redundant path in some specific case (i.g low power mode OFF and FS0B shorted to high).

Implementation: a redundant signal coming from the MCU must be connected to the safety switch with a pull-down resistor.

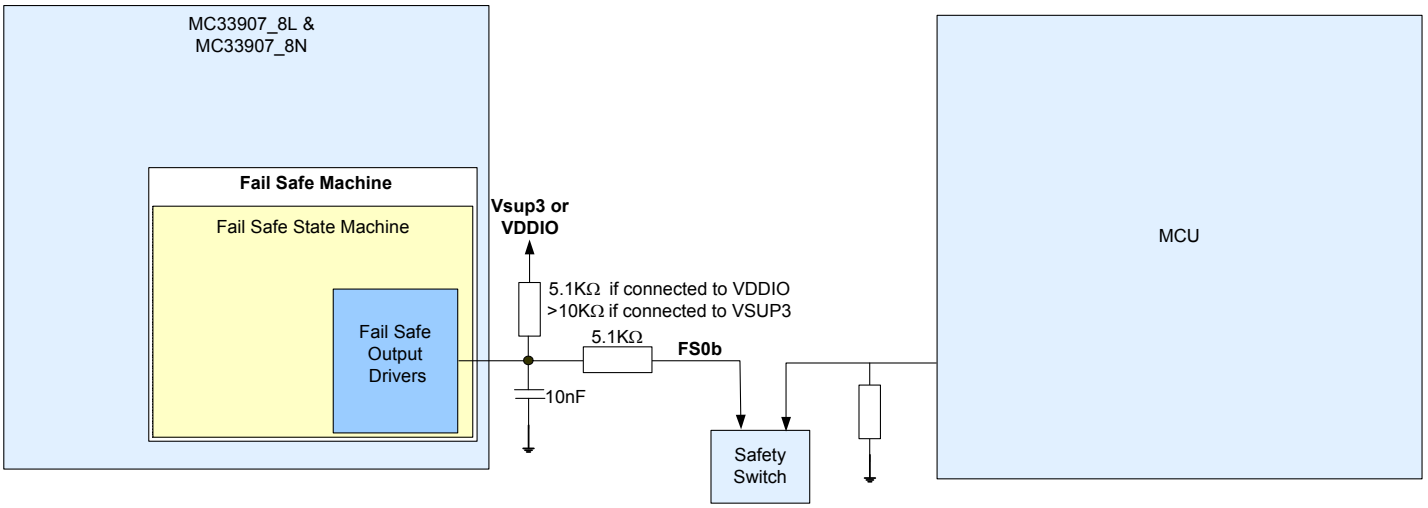


Figure 18. Redundant Safety Path with Pull-down

Assumption: [SM_018] It is system integrator's responsibility to make sure a resistor in series is well connected to FS0B.[END]

Rationale: FS0B can be connected externally to the system. In that case, it must be robust against automotive transients which can appears on the battery line.

Implementation: A resistor of 5.1 kΩ must be connected in series on FS0B.

Figure 19 shows the connection of external components to insure good safety operation of FS0B

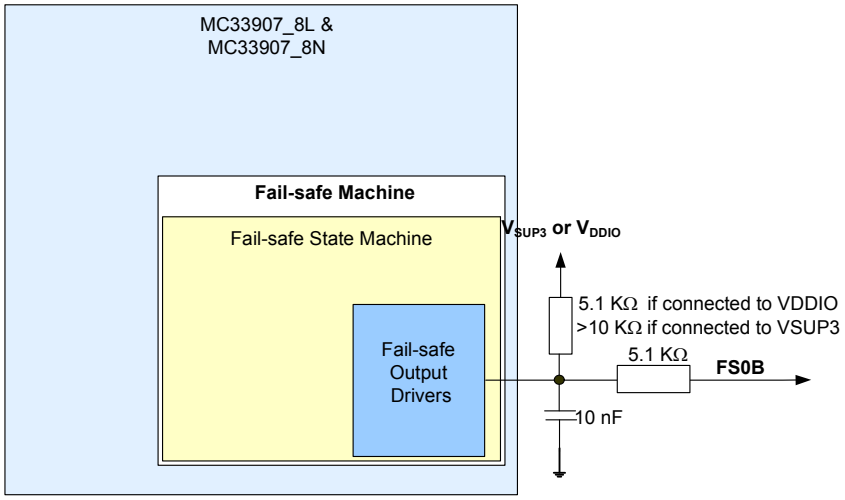


Figure 19. FS0B Connection

Condition leading to a fail-safe activation are the following, but also depend on product configuration.

Table 21. List of Fail-safe Error Handling

Error Flag	Description	Main action in case of fault	RSTb	FS0b	Comments
Vpre_OV	Overvoltage on V_{PRE}	V_{PRE} switched OFF	LOW	LOW	-
Vcore_OV	Overvoltage on V_{CORE}	V_{CORE} switched OFF	LOW	LOW	Fail-safe impact selectable through the SPI
Vcore_UV	Undervoltage on V_{CORE}	V_{CORE} kept ON	LOW	LOW	Fail-safe impact selectable through the SPI
Vcca_OV	Overvoltage on V_{CCA}	V_{CCA} switched OFF	LOW	LOW	Fail-safe impact selectable through the SPI
Vcca_UV	Undervoltage on V_{CCA}	V_{CCA} kept ON	LOW	LOW	Fail-safe impact selectable through the SPI
Vaux_OV	Overvoltage on V_{AUX}	V_{AUX} switched OFF	LOW	LOW	Fail-safe impact selectable through the SPI
Vaux_UV	Undervoltage on V_{AUX}	V_{AUX} kept ON	LOW	LOW	Fail-safe impact selectable through the SPI
IO_0:1	External IC error handling	-	HIGH	LOW	-
IO_1	R,bridge drift monitoring (Vcore)	V_{CORE} kept on	LOW	LOW	-
IO_2:3	MCU FCCU error handling	-	LOW	LOW	-
IO_4:5	External IC Error Handling	-	HIGH	LOW	-
WD	Watchdog	WD error counter / WD refresh counter	LOW	HIGH	-
RSTb shorted to High	Short-circuit	-	HIGH (Externally)	LOW	-
FS0b shorted to High	Short-circuit	-	LOW	HIGH (Externally)	-
SPI DED	Dual error detection in SPI	-	LOW	LOW	-
V2P5 main analog	Overvoltage on internal reference voltage for main V2P5 analog	-	LOW	LOW	-
V2P5 main digital	Overvoltage on internal reference voltage for main V2P5 digital	-	LOW	LOW	-

Table 21. List of Fail-safe Error Handling (continued)

V2P5 FS analog	Overvoltage on internal reference voltage for Fail-safe V2P5 analog	-	LOW	LOW	-
V2P5 FS digital	Overvoltage on internal reference voltage for Fail-safe V2P5 digital	-	LOW	LOW	-
LBIST	Logic Built-in Self Test	Keep device stuck in reset	LOW	LOW	-
ABIST	Analog Built-in Self Test	Bring system in Fail-safe	LOW	LOW	-

6.5.3 RSTB, FS0B Internal Monitoring

An internal sense path of the RSTB and FS0B pins is implemented in the device. The function monitors the output of each pin and compares it with the digital command.

- If a difference between the digital command and the RSTB internal sense path is detected, the impossibility to bring the system in safe state, by the RSTB pin, is reported (FS0_G bit in the WD answer register) and the FS0B pin is asserted low.

  (i.e. external short to high when the device asserts the RSTB low).
- If a difference between the digital command and the FS0B internal sense path is detected, the impossibility to bring the system in safe state, by the FS0B, is reported (FS0_G bit in the WD answer register) and the RSTB pin is asserted low.

  (i.e. external short to high when the device asserts the FS0B low).

[covers: SM7-FMEDA]

6.6 Built-in Hardware Self Tests (BIST)

Built-in hardware self-test (BIST) is a mechanism that permits circuitry to test itself.

Not every fault expresses itself immediately. For example, a fault may remain unnoticed if a component is not used or the context is not causing an error or the error is masked.

If faults are not detected over a long time (latent faults), they can pile up once they propagate. ISO 26262 requires a latent-fault metric for ASIL D ≥ 90%, ≥ 80% for ASIL C, and ≥ 60% for ASIL B. Typically hardware assisted BIST is therefore used as a safety integrity measure to detect latent faults.

The 33907NL and 33908NL is equipped with a built-in hardware self-test:

- Logic (LBIST, executed at startup, and going out from LPOFF mode)
  - during LBIST the device tests the functional logic of the fail-safe machine against stuck at fault
- Analog (ABIST, executed at start-up, and going out from LPOFF mode)
  - during ABIST the product tests the analog monitoring functions showed in Table 22:

Table 22. ABIST checks

Parameters	ABIST Checks			Comments
	Overvoltage	Undervoltage	OK / NOK	
V_{PRE}	X			
V_{CORE}	X	X		
V_{CCA}	X	X		
V_{AUX}	X	X		
V2P5 Main Digital	X			undervoltage not checked because undervoltage means power on reset state
V2P5 Main Analog	X			undervoltage not checked because undervoltage means power on reset state
V2P5 Fail-safe Digital	X			undervoltage not checked because undervoltage means power on reset state

Table 22. ABIST checks (continued)

Parameters	ABIST Checks			Comments
V2P5 Fail-safe Analog	X			undervoltage not checked because undervoltage means power on reset state
Osc Fail-safe			X	
2nd resistor bridge monitoring (IO_1)			X	
RSTB			X	Internal Sense path is checked for high and low level
FS0B			X	Internal Sense path is checked for high and low level

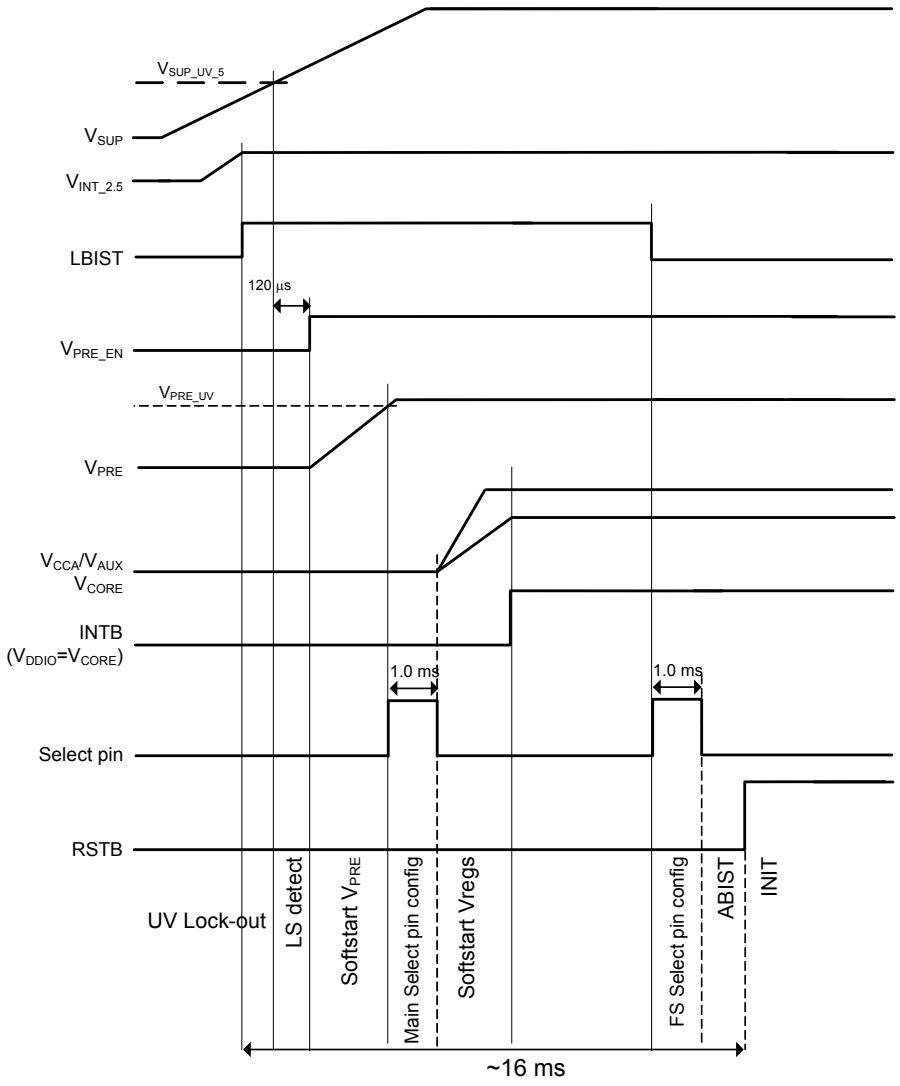
[SM_027]A self-test during start-up or resuming from LPOFF mode is performed to ensure the integrity of the system. If a latent fault is detected, the application stays in the safe state.[END]

Rationale: To prevent latent faults.

Implementation Hint: The LBIST and ABIST are performed automatically after the occurrence of a Power on reset or resuming from LPOFF. No software request is expected. All startup tests are executed before application software starts, because during this time the SBC maintain its own reset and as a consequence keep the MCU in reset. After approximately 16 ms RSTB is released and operation can start. If failed, the 33907NL and 33908NL do not leave Safe state$_{SBC}$. The RSTB stays low and the MCU never starts.

7 Start-up sequence recommendations

At startup, when the reset is released after around ~16 ms, all the regulators are ON, the FS0B pin is asserted low (Safe state$_{SBC}$), and the device is ready to be configured. At this stage, the device is in the INIT phase.



Starting when the reset is released, the MCU has an open window of 256 ms to configure the device and to send the first WD refresh. if the first WD is not asserted after 256 ms, a reset is sent to the MCU.

After five consecutive resets (because at startup the reset error counter starts at 1), the device falls in Deep Fail-safe mode.

7.1 INIT Phase

During this phase all the initialization registers can be accessed and configured. Refer to the 33907NL and 33908NL decathlete to know which registers can be configured during the INIT mode only.

Based on the informations in this safety manual here are the important things to do before to release the safety pin (FS0B).

- Configure the V_{CORE}, V_{CCA}, and V_{AUX} overvoltage and undervoltage impact on RSTB and FS0B.
- On V_{CORE}, if the second resistor bridge is connected externally, configure the IO_1_FS bit of the INIT FSSM1 register
- Read the V_{CCA} and V_{AUX} voltage configuration (3.3 V or 5.0 V) - bit VCC_HW and Vaux_HW of the HW_Config register and confirm the values are the expected ones.
- If you're using V_{AUX} to supply sensors and V_{CCA} as an MCU ADC ref voltage, configure V_{AUX} as tracker of V_{CCA}, Vaux_trk_en of Init Vreg2 register.
- If you are using an FSL MCU and the FCCU output connected to IO[2] and IO[3], ensure the IO_23_FS bit of the INIT FSSM2 register is well configured as safety critical. If you are not using it, then don't forget to remove this option, Otherwise an error is automatically generated when moving to normal WD running mode.
- Ensure the debug mode is not activated by checking the DBG bit of the HW_config register.
- Ensure the LS_detect bit of the HW_CONFIG register is not activated in case the buck boost operation is needed.
- Configure the WD window period in the WD_Window register. 3.0 ms by default is selected, which is in aligned with an FTTI below 10 ms. Ensure to not configure a WD window period above the FTTI requirement at system level.

  Also check the WD error counter configuration.

  Implementation example: if the WD error counter is configured at six then three, consecutive bad WD refreshes must be done before to assert a reset (WD error counter is incremented by two each bad WD refresh)

  If the WD window period is configured for 3.0 ms, then worst case is 3 * 3.0 ms = 9.0 ms before a reset is asserted.

  Refer to the 33907NL and 33908NL data sheet to understand the counter behavior and interactions.
- Once all the configuration is done, send the first good WD.
- At this stage (FS0B is still asserted low), the initialization registers are locked (no change possible), the IO[2] and IO[3] monitors the FCCU MCU outputs, and the WD must be asserted according to the WD window period configured previously.
- After seven good consecutive WD refreshes, the RST error counter is at level 0 (if no other faults are reported - Refer to the 33907NL and 33908NL data sheet to see the faults which can increment the RST error counter)
- The release of the FS0B can be done by writing the good word in the FS_OUT register (refer to 33907NL and 33908NL decathlete). The MCU must maintain its own safety path to low because the safety path check as not been yet done.
- Finally, the safety path check must be done to ensure the good HW connection between the device and the safety switch. This is done by the MCU driving IO_4 low, and IO_5 to a high level. After the acknowledge counter period < 10 ms, the FS0B is asserted low whereas the RSTB is maintained high.
- MCU must check the signal is well toggling from high to low on the safety switch side.
- Then again the FS0B must be released to high by writing in the FS_OUT register (RSTB error counter = 0)
- A word must be send in the INIT_INT register (Main state machine is moving from initialization phase to normal operation)
- The 33907NL and 33908NL is now ready. If everything is ok for the MCU, it can release its own safety path and the ECU starts.

8 List of Fail-safe Errors and Potential Cascade Effects

Impacts on Fail-safe activation (RSTB and FS0B) depends on the product configuration.

Table 23. List of Fail-safe Error Handling and potential cascade effect

Error Flag	Description	Main action in case of fault	RSTB	FS0B	Potential Cascade effect	RSTb	FS0b
Vpre_OC	Overcurrent	V_{PRE} switched OFF	HIGH	HIGH	Undervoltage reported on all regulators	LOW	LOW
Vpre_Ilim	Current limitation	duty cycle reduction	HIGH	HIGH	Undervoltage reported on all regulators	LOW	LOW
Vpre_OV	Overvoltage on V_{PRE}	V_{PRE} switched OFF	LOW	LOW	All regulators will be switched off	-	-
Vpre_UV(1)	Undervoltage on V_{PRE}	V_{PRE} kept ON	HIGH	HIGH	Undervoltage reported on all regulators	LOW	LOW
VPRE_TSD	Thermal shutdown	V_{PRE} switched OFF	HIGH	HIGH	Undervoltage reported on all regulators	LOW	LOW
Vcore_OV	Overvoltage on V_{CORE}	V_{CORE} switched OFF	LOW	LOW	-	-	-
Vcore_UV	Undervoltage on V_{CORE}	V_{CORE} kept ON	LOW	LOW	-	-	-
Vcore_Ilim	Current limitation	duty cycle reduction	HIGH	HIGH	Undervoltage on V_{CORE}	LOW	LOW
Vcore_TSD	Thermal shutdown	Vcore switched OFF	HIGH	HIGH	Undervoltage on V_{CORE}	LOW	LOW
Vcca_OV	Overvoltage on V_{CCA}	V_{CCA} switched OFF	LOW	LOW	-	-	-
Vcca_UV	Undervoltage on V_{CCA}	V_{CCA} kept ON	LOW	LOW	-	-	-
VCCA_ILIM	Current limitation	-	HIGH	HIGH	-	-	-
Vcca_TSD	Thermal shutdown (internal Pmos)	V_{CCA} switched off	HIGH	HIGH	Undervoltage on V_{CCA}	LOW	LOW
Vaux_OV	Overvoltage on V_{AUX}	V_{AUX} switched OFF	LOW	LOW	-	-	-
Vaux_UV	Undervoltage on V_{AUX}	V_{AUX} kept ON	LOW	LOW	-	-	-
Vaux_Ilim	Current limitation		HIGH	HIGH	-	-	-
Vaux_TSD	Thermal shutdown (internal reverse transistor)	V_{AUX} switched off	HIGH	HIGH	Undervoltage on V_{AUX}	LOW	LOW
Vcan _OV	Overvoltage on V_{CAN}	V_{CAN} switched off and CAN Physical layer off	HIGH	HIGH	-	-	-
Vcan _UV	Undervoltage on V_{CAN}	CAN physical OFF	HIGH	HIGH	-	-	-
Vcan_ILIM	Current limitation		HIGH	HIGH	-	-	-
Vcan_TSD	Thermal shutdown	V_{CAN} switched off and Physical layer OFF	HIGH	HIGH	-	-	-
IO_0:1	External IC error handling	-	HIGH	LOW	-	-	-
IO_1	R bridge drift monitoring (Vcore)	Vcore kept on	LOW	LOW			
IO_2:3	MCU FCCU error handling	-	LOW	LOW	-	-	-
IO_4:5	External IC Error Handling	-	HIGH	LOW	-	-	-
WD	Watchdog	WD error counter / WD refresh counter	LOW	HIGH	Fail-safe low depending of intermediate value configuration and level on reset error counter.	-	-
RSTb shorted to High	Short-circuit	-	HIGH (Externally)	LOW	-	-	-
FS0b shorted to High	Short-circuit	-	LOW	HIGH (Externally)	-	-	-
SPI DED	Dual error detection in SPI		LOW	LOW	-	-	-

Table 23. List of Fail-safe Error Handling and potential cascade effect (continued)

Error Flag	Description	Main action in case of fault	RSTB	FS0B	Potential Cascade effect	RSTb	FS0b
LBIST	Logic Built In Self Test	Keep device stuck in reset	LOW	LOW	Deep fail-safe (RSTB = 8.0 s)	-	-
ABIST	Analog Built In Self Test	Bring system in Fail-safe	LOW	LOW	Deep fail-safe (RSTB = 8.0 s)	-	-

Note:

1. No action either on RSTB nor on FS0B exists following V_{PRE} undervoltage event. if V_{PRE} is used to supply a function in the ECU, a safety mechanism at application level must be taken in case of undervoltage, if considered as a safety regulator.

9 Acronyms and abbreviations

A short list of acronyms and abbreviations used in this document is summarized for completeness:

Table 24. Acronyms and Abbreviations

Terms	Meanings
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
FMEDA	Failure Modes, Effects & Diagnostic Analysis
FSM	Fail-safe Machine
FSO	Fail-safe Outputs
FSSM	Fail-safe State Machine
FTTI	Single-Point 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
PST	Process Safety Time
RF	Residual Fault
SBC	System Basis Chip
SF	Safe Fault
SPF	Single-Point Fault
UV	Undervoltage

9.1 Safety Tags

Table 25 shows all tags of the safety application guide

Table 25. Safety Tags

Tag	Assumption
[SM_001]	It is assumed that the recommended operating conditions given in the 33907NL and 33908NL Data Sheet are maintained
[SM_002]	It is assumed that all field failures of the devices are reported to silicon supplier.
[SM_003]	It is assumed that the latest device errata is taken into account during system design, implementation, and maintenance. For a functional safety-related device such as 33907NL and 33908NL, this also concerns functional safety-related activities such as system level functional safety concept development.
[SM_004]	It is assumed that the system transitions itself to a Safe $state_{system}$ when the 33907NL and 33908NL explicitly indicates an error via its fail-safe outputs (Reset and FS0b).
[SM_005]	It is assumed that the system transitions itself to a Safe $state_{system}$ when the 33907NL and 33908NL is in reset state.
[SM_006]	It is assumed that the system transitions itself to a Safe $state_{system}$ when the 33907NL and 33908NL is completely unpowered
[SM_007]	It is assumed that 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.
[SM_008]	It is assumed the right resistor values are well connected between V_{CORE_SNS} and ground, with the middle point connected to $FB_{\_CORE}$ to configure the right voltage to the MCU.
[SM_009]	It is assumed the value of the external resistor bridge stays within its nominal value.
[SM_010]	It is assumed that measures at system level maintain the Safe $state_{system}$ during and after V_{CCA} supply voltage above or under the specified operational range.
[SM_011]	It is assumed that measures at system level maintain the Safe $state_{system}$ during and after V_{AUX} supply voltage above or under the specified operational range.
[SM_012]	It is assumed the V_{CCA} linear regulator is used as reference voltage of analog to digital converter of the MCU.
[SM_013]	It is assumed the bi-stable protocol has been configured in the Freescale MCU for FCCU protocol.
[SM_014]	It is assumed the error output signal from external IC is well connected to one SBC IO and one MCU IO to ensure the MCU is able to listen the fault
[SM_015]	It is assumed the MCU refresh periodically the 33907NL and 33908NL watchdog.
[SM_016]	An output in high-impedance is not considered safe at system level, it is assumed that external components connected to RSTB are available to bring the safety critical outputs to known level during operation.
[SM_017]	An output in high impedance is not considered safe at system level, it is assumed that external components connected to FS0B are available to bring the safety critical outputs to a known level during operation.
[SM_018]	It is assumed resistor in series is well connected to FS0B.
[SM_019]	It is assumed the MCU check the VCCA output voltage level after system startup or after LPOFF mode by reading VCCA_HW bit in HW_CONFIG register.
[SM_020]	It is assumed that MCU check the VAUX output voltage level after system startup or after LPOFF mode by reading VAUX_HW bit in HW_CONFIG register.
[SM_021]	In case of fault, opening the safety switch in a system must not be drived by he FS0B only, but also by the MCU.
[SM_022]	It is assumed that MCU checks the debug mode is not activated after system startup or after LPOFF mode by reading DBG bit in HW_CONFIG register.
[SM_023]	It is assumed that MCU checks the configuration of the buck/or boost configuration after system startup or after LPOFF mode by reading LS_ detect bit in HW_CONFIG register. It covers the safety mechanism SMA7 in the FMEDA.
[SM_024]	It is assumed that MCU checks the Vpre undervoltage flag, in case an external circuitry is connected to the Vpre as a supply of this circuitry, by reading the VPRE_UV bit in the DIAG VREG1 register.
[SM_025]	The reset error counter is triplicated and a majority voter is implemented to avoid any unexpected change due to bit flip for example. In case of bit flip, the comparison is done with the two other registers and the bit in default is forced to be changed by the right value. A flag is set in the “FS_ECC” bit of the “WD_answer” register available for MCU diagnostic.

Table 25. Safety Tags (continued)

[SM_026]	if the result of this check is bad due to errors that cannot be corrected, a flag is set in the bit0 “FS_reg_ECC” of the “WD_answer” register, the RSTb and the FS0b are asserted low. This Error Detection Correction measure is called SPI DED. This check is used as safety integrity measure to detect latent faults.
[SM_027]	It is assumed that a self-test during start-up or resuming from LPOFF mode is performed to ensure the integrity of the system. In case of detection of latent fault the application stays in safe state

10 Document Revision History

Table 26 summarizes revisions to this document.

Table 26. Revision history

Revision	Date	Description of changes
1.0	5/2015	• Initial release
2.0	7/2015	• Updated document format

How to Reach Us:

Home Page:
freescale.com

Web Support:
freescale.com/support

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document.

Freescale reserves the right to make changes without further notice to any products herein. Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer’s technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at the following address: freescale.com/SalesTermsandConditions.

Document Number: MC33907NL-33908NLSMUG
Rev. 2.0
7/2015