AN13322

NXP SBC solution for Infineon AURIX TC2xx/TC3xx series MCU

Rev. 4.0 — 31 July 2026 Application note

Document information

Information	Content
Keywords	FS65/FS45, FS26, FS23, FS85/FS84, Infineon AURIX TC2xx/TC3xx, AUTOSAR, power management, functional safety, ASIL B, ASIL D
Abstract	This application note provides design guidelines on how to supply any Infineon AURIX TC2xx/TC3xx MCU using NXP's FS system basis chip (FS65/FS45, FS23, FS26 and FS85/FS84) family of devices for automotive and industrial systems.

1 Introduction

This application note provides design guidelines on how to supply any Infineon AURIX TC2xx/TC3xx MCU using NXP's FS system basis chip (SBC) family of devices (FS65/FS45, FS23, FS26, and FS85/FS84) for automotive and industrial systems. AURIX™ is a trademark of Infineon Technologies.

This document discusses system level details and recommendations when using the dedicated FS device to supply Infineon AURIX TC2xx/TC3xx and other peripherals as part of the full system. Using I/Os and built-in functional safety features, the system designer can maximize the safety level up to Automotive Safety Integrity Level (ASIL) D.

A section is dedicated to each of the four safety SBC devices: Section 3 "FS65/FS45 solution" covers the FS65/FS45, Section 4 "FS26 solution" covers the FS26, and Section 5 "FS85/FS84 solution" covers the FS85/FS84, and Section 6 covers the FS23.. These four sections provide specific information about each device and offer power tree proposals related to the AURIX MCUs.

2 Attaching NXP safety SBC to AURIX safety MCU

The NXP safety SBC portfolio offers multiple supply solutions for AURIX TC2xx/TC3xx safety MCUs and other system components (peripherals, low voltage power management integrated circuits (PMICs), external sensors, a second AURIX MCU, etc.), without requiring additional external software safety mechanisms. NXP safety SBCs provide both HW and SW safety management capabilities that reach ASIL D level performance.

The following subsections describe various ways of supplying the AURIX MCU. Subsequent sections map NXP safety SBC vs. AURIX MCU versions, to help designers achieve optimized and cost effective solutions.

2.1 Guidelines for supplying AURIX MCU

The AURIX MCU features two embedded voltage regulators (EVR) that provide 3.3 V (EVR33) and 1.25 V (EVR13) internally from a single external voltage supply (5 V). EVR33 is a linear regulator (LDO) whereas EVR13 is a DC-DC buck controller that needs two external metal-oxide-semiconductor field-effect transistors (MOSFETs) to regulate its core supply.

Each rail can also be powered externally by an NXP safety SBC, which allows all rails to be monitored without an additional discrete regulator on the high-end AURIX MCU. In between are multiple supply configurations depicted below.

In the interest of simplicity, analog-to-digital converter (ADC) supply and reference pins are not shown in the drawings below. These pins can either be supplied with a dedicated regulator with high accuracy or share the MCU common supply (e.g. VEXT).

2.1.1 Single-supply configurations

The AURIX MCU is supplied by a single voltage rail at the VEXT pin. The voltage level can be either 5 V or 3.3 V (with ±10 % tolerance). EVRx regulators generate the 3.3 V and 1.25 V internally, when needed.

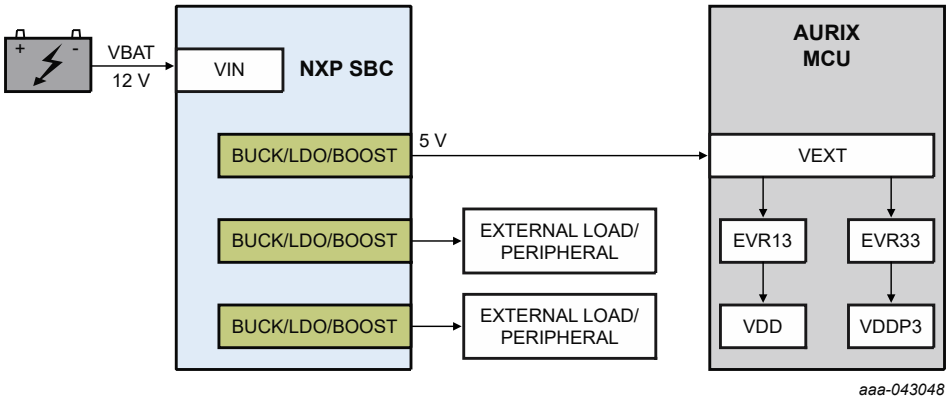


Figure 1. Single-supply use case where VEXT = 5 V

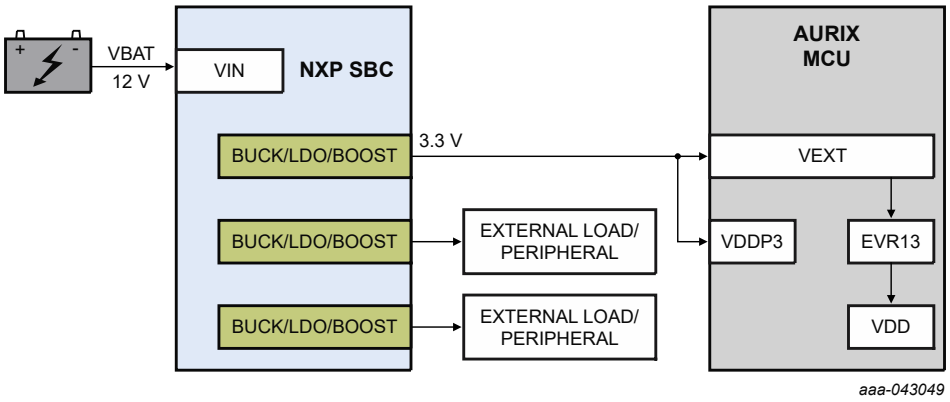


Figure 2. Single-supply use case where VEXT = VDDP3 = 3.3 V

2.1.2 Multiple-supply configurations

The AURIX MCU is supplied by two or three voltage rails through VEXT, VDD and VDD3 pins (5 V, 1.25 V and 3.3 V respectively, with a ±10 % tolerance). In the first use case, EVR33 is generates the 3.3 V internally when other rails are externally supplied. In the second use case, all rails are externally supplied and EVRx regulators are not used.

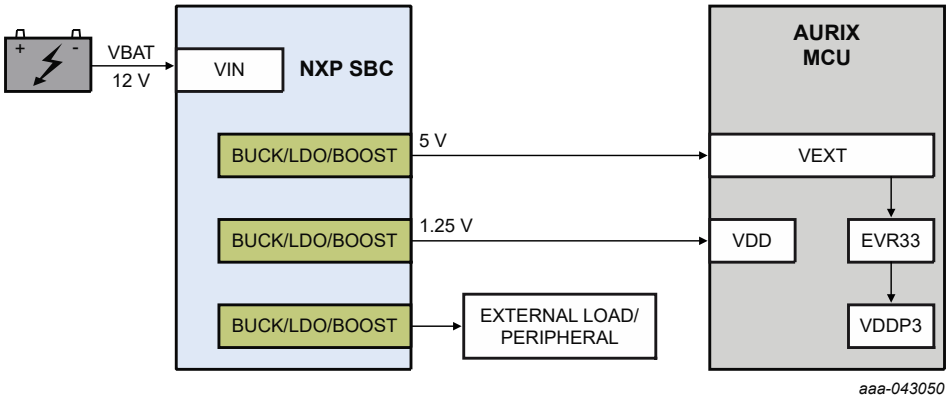


Figure 3. Dual supply use case where VEXT = 5 V and VDD = 1.25 V

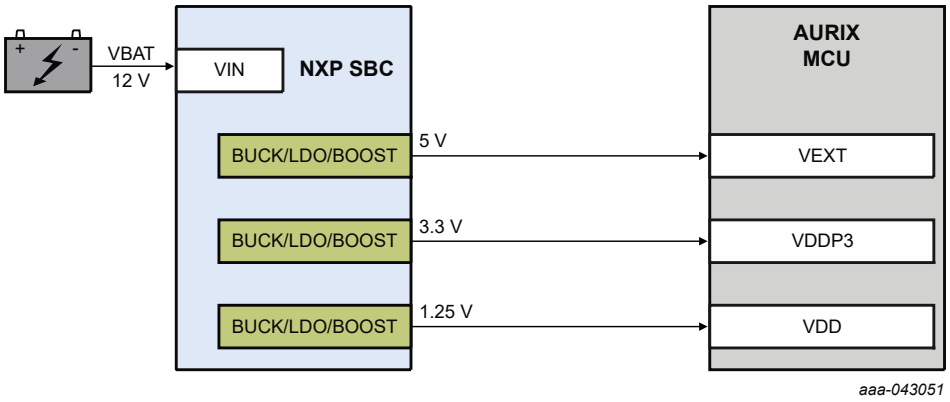


Figure 4. All external supply use case where VEXT = 5 V, VDDP3 = 3.3 V and VDD = 1.25 V

2.1.3 Power-up and power-down sequences

When supplying the AURIX MCU with two or more rails, VEXT, VDD and VDDP3 external rails can ramp up or down, regardless of their sequence. It is preferred, but not mandatory, that VEXT starts before VDD and VDDP3 to avoid potential overshoots on VDD/VDDP3.

2.1.4 Low-power modes

NXP safety SBCs offer different Low-power mode strategies and benefits for the system and low current consumption for longer duration of the stored energy. These modes, along with the Run mode, are detailed below as a reference:

- **Run mode**: regulators are ON with full current capability and application is in Normal mode until requested to move to Low-power mode.
- **Low-power ON (LPON) or Standby (STBY) mode**: specific regulators are ON with limited current capability, allowing low quiescent current to reduce battery discharge. The MCU is already powered (memory and some critical functions are kept alive) in order to allow fast system wakeup.
- **Low-power OFF (LPOFF) mode**: all regulators are OFF, which means the MCU is unpowered, with low quiescent current to reduce battery discharge (mainly SBC low-power budget). The SBC can wake-up the system using the Wake/IO pin or CAN (if available).

To allow standby mode with the Infineon AURIX MCU, the VERSB pin should be supplied independently by a standby-capable regulator with the same voltage as VEXT, depending on the use case (5 V or 3.3 V).

The table below gives an overview of what can be achieved with NXP SBCs, depending on the use case:

Table 1. NXP SBCs and AURIX MCU attach strategy depending on the required Low-power mode

TC2xx/TC3xx supply only	LPOFF mode required	LPON mode required
	FS65/FS45	FS26
TC2xx/TC3xx supply + system features (LDT, trackers …)	FS65/FS45	FS26, FS23
TC2xx/TC3xx supply + peripherals (low-voltage PMIC, 2nd AURIX MCU …)	FS84/FS85	VR5510 [1]

[1] VR5510 will be developed in next AN revision

2.1.5 AURIX MCU ADC supply

Regarding the AURIX MCU ADC compliancy, ADC analog reference (VAREF) and ADC supply (VDDM) should share the same supply rail.

This is the prerequisite involving VDDM and VAREF, to ensure ADC performance:

$(V_{DDM} \times 0.9) \leq V_{AREF} \leq (V_{DDM} + 0.05\ V)$

Similarly, the prerequisite on the ADC grounds is:

$(V_{SSM} \times 0.9) \leq V_{AGND} \leq (V_{SSM} + 0.05\ V)$

2.2 NXP SBC vs AURIX MCU mapping

To help designers choose the most appropriate NXP safety SBC at a glance, Table 2 provides a mapping between SBC and AURIX MCU variations, based on the AURIX MCU supply requirements only. Depending on the system aspects (the peripherals, the safety level target, etc.) more appropriate solutions can be found.

When a safety SBC can supply a given AURIX MCU version, it is assumed lower versions can easily be addressed using the same SBC.

Table 2. NXP safety SBC vs. AURIX MCU mapping

NXP safety SBC (VCORE / BUCKx current)		TC2 series				TC3 series				
		TC21/ TC22/ TC23	TC26	TC27	TC29	TC33	TC36	TC37	TC38	TC39
LPOFF capable	FS450x (0.5 A)	X				X				
	FS650x (0.8 A)		X	X			X	X		
	FS651x (1.5 A)				X				X	
	FS652x (2.2 A)									X
	FS84/85 (2.5 A)[1]				X					X
LPON + LPOFF capable	FS260x/1x (0.8 A)	X	X	X		X	X	X		
	FS262x/3x (1.65 A)				X				X	X[2]
	FS23xx (0.1 A/0.25 A/0.6 A)	X	X	X		X	X			

[1] FS84/FS85 device is not only suited to supply high-end AURIX MCU but is also capable of supplying two AURIX MCUs.
[2] When FS262x/3x attach TC39x, TC39x work modes should be considered to see if 1.65 A is enough for TC39x core supply.

3 FS65/FS45 solution

3.1 Product overview

The FS65 and the FS45 are multi-output power supply integrated circuits dedicated to the automotive market. The devices simplify system implementation by providing ISO 26262 system solutions, documentation and an optimized MCU interface enabling customers to minimize the cost and complexity of their designs. The FS65 and the FS45 integrated electromagnetic compatibility (EMC) and electrostatic discharge (ESD) protections also facilitate less complex system designs with increased functional reliability.

NXP analog ICs are manufactured using the SMARTMOS process, a combinational BiCMOS manufacturing flow that integrates precision analog, power functions, and dense complementary metal–oxide–semiconductor (CMOS) logic together on a single cost-effective die.

This application note applies to all FS65 and FS45 part numbers. Local interconnect network (LIN) and FS1B functions are exclusive. The differentiation is made by part numbers. When LIN is available, FS1B is not, and vice versa. Other exceptions are specifically indicated.

3.1.1 Documentation references

- **FS45 Device Webpage**
- **FS65 Device Webpage**

The above links point to web pages that contain a variety of material related to the FS65/FS45 family. These web pages provide more detailed information about specific topics:

• **FS45: Grade 1 and grade 0 data sheets**: information such as features, functional description, parametric description, and register mapping.

• **FS65: Grade 1 and grade 0 data sheets**: information such as features, functional description, parametric description, and register mapping.

• **F65/FS45 functional safety manual (ASIL B and ASIL D)**: descriptions of how to use the FS65/FS45 in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level.

• **AN5238**: information such as application schematic, bill of material, placement and layout guidelines, and application validation data [ISO/non-ISO pulses, electromagnetic compatibility (EMC)].

• **AN12786**: application note with details on how to attach AURIX MCU TC2xx/TC3xx in battery management system (BMS) applications.

3.1.2 Typical block diagram

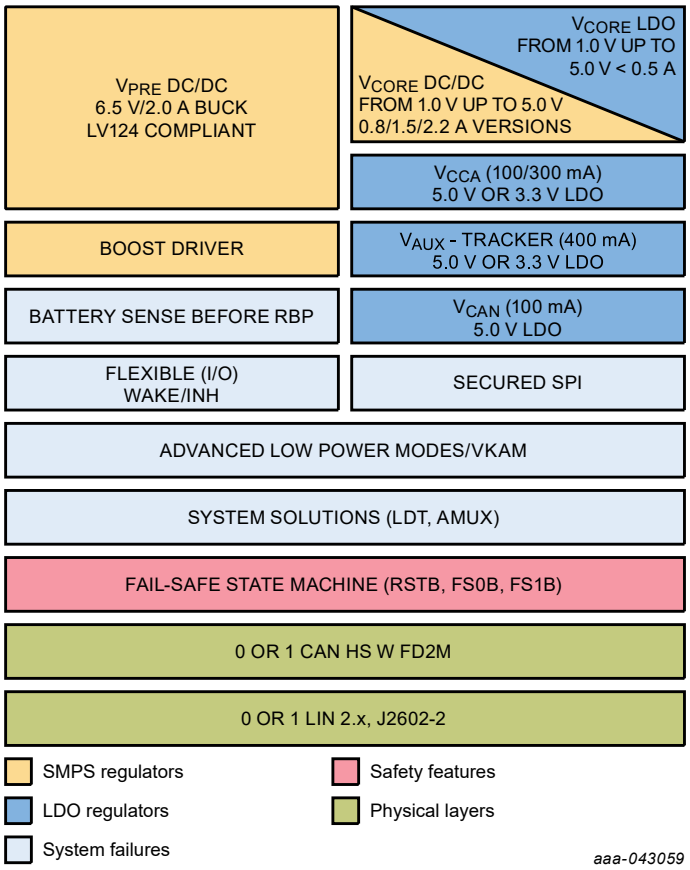


Figure 5. FS65/FS45 functional block diagram

3.1.3 Key features

The FS65/FS45 device presents different types of power management blocks, with an independent safety island for supporting ASIL B or ASIL D applications.

Below is a summary of the different power management blocks:

- Input supply up to 40 V DC for 12 V systems
- HV BUCK/BOOST (also named VPRE), 6.5 V, up to 2.0 A DC, 440 kHz asynchronous with integrated MOSFETs allowing ultra-low-voltage operation down to 2.7 V
- VCORE: low-dropout (LDO) or DC-DC with adjustable VCORE voltage from 1.0 V to 5.0 V
- Part number selection for max current: 0.5 A (FS450x) or 0.8 A (FS650x) or 1.5 A (FS651x) or 2.2 A (FS652x)
- VCCA LDO 3.3 V or 5 V, 100 mA / 1 % or 300 mA 3 %
- VAUX TRACKER 3.3 V or 5 V, 400 mA, with 15 mV offset
- VCAN LDO 5 V, 100 mA
- Low-power OFFmode, with wakeup by I/Os, CAN/LIN

The device also presents some system features such as:

- Wakeup via dedicated pins, CAN, LIN
- Long duration timer (LDT) feature – counter from a few seconds up to 6 months
- AMUX: Battery voltage monitoring, internal safety critical voltages, precise VREF and temperatures

- Controller area network flexible data rate (CAN FD) 2M PHY and LIN (optional part numbers)
- Control via 16-bit serial-peripheral interface (SPI) (including parity check)
- Low-power OFF mode with low quiescent current: 32 µA
- Several part numbers are pin-to-pin compatible with optional FS1B, long-duration timer (LDT), controller area network protocol (CAN), LIN

But this device also provides functional safety:

- Fail silent – configurable state machine with independent safety monitoring unit
- Fit for ASIL D solution: OV/UV, challenger W/D, HW system on chip (SoC) monitoring pins (fault collection and control unit – FCCU), dual FSb, built-in self-test (BIST), ERRMON, etc.

3.2 Safety management with AURIX MCU

To fulfill the safety-critical applications, a dedicated Fail-safe machine (FSM) is provided. The FSM is composed of three main sub-blocks:

- Voltage supervisors
- Reset output;
- Two HW SoC monitoring pins (FCCU) inputs for NXP and non-NXP MCU monitoring
- Fail-safe output driver (FSO)
- Built-in self-test (BIST)

The FSM is independent from the rest of the circuitry to avoid common-cause failures. The FSM has its own voltage regulators (analog and digital), dedicated bandgap, and oscillator. This block is physically independent from the rest of the circuitry, due to dedicated layout placement and trench isolation.

3.2.1 Safety outputs

In normal operation when FS0B (and FS1B, if used) and RSTB are released, the fault error counter is incremented when a fault is detected by the FS65 and FS45 Fail-safe state machine.

Table 3 lists the faults and their impact on RSTB, FS0B and FS1B pins according to the default device configuration. The faults that are configured to not assert RSTB and FS0B (and FS1B, if used) will not increment the fault error counter. In that case, only the flags are available for MCU diagnostics. When FS0B is asserted, the fault error counter continues to be incremented by one each time the WD error counter reaches its maximum value. Refer to the safety manual for more details on the safety implementation.

Table 3. Application-related fail-safe fault list and reaction

In orange, the reaction is not configurable.
In green, the reaction is configurable by SPI during the INIT_FS state.

Apps related fail-safe faults	Fault error counter increment	FS0B assertion	RSTB assertion
VPRE power rail overvoltage	+1	VMON_PRE_OV_FS_REACTION[0]	VMON_PRE_OV_FS_REACTION[1]
VCORE power rail overvoltage	+1	VMON_CORE_OV_FS_REACTION[0]	VMON_CORE_OV_FS_REACTION[1]
VLDO1 power rail overvoltage	+1	VMON_LDO1_OV_FS_REACTION[0]	VMON_LDO1_OV_FS_REACTION[1]
VLDO2 power rail overvoltage	+1	VMON_LDO2_OV_FS_REACTION[0]	VMON_LDO2_OV_FS_REACTION[1]
VTRK1 power rail overvoltage	+1	VMON_TRK1_OV_FS_REACTION[0]	VMON_TRK1_OV_FS_REACTION[1]
VTRK2 power rail overvoltage	+1	VMON_TRK2_OV_FS_REACTION[0]	VMON_TRK2_OV_FS_REACTION[1]
VREF power rail overvoltage	+1	VMON_VREF_OV_FS_REACTION[0]	VMON_VREF_OV_FS_REACTION[1]
Overvoltage on the analog input monitoring	+1	VMON_EXT_OV_FS_REACTION[0]	VMON_EXT_OV_FS_REACTION[1]
VPRE power rail undervoltage	+1	VMON_PRE_UV_FS_REACTION[0]	VMON_PRE_UV_FS_REACTION[1]
VCORE power rail undervoltage	+1	VMON_CORE_UV_FS_REACTION[0]	VMON_CORE_UV_FS_REACTION[1]
VLDO1 power rail undervoltage	+1	VMON_LDO1_UV_FS_REACTION[0]	VMON_LDO1_UV_FS_REACTION[1]

Table 3. Application-related fail-safe fault list and reaction...*continued*

In orange, the reaction is not configurable.
In green, the reaction is configurable by SPI during the INIT_FS state.

Apps related fail-safe faults	Fault error counter increment	FS0B assertion	RSTB assertion
VLDO2 power rail undervoltage	+1	VMON_LDO2_UV_FS_REACTION[0]	VMON_LDO2_UV_FS_REACTION[1]
VTRK1 power rail undervoltage	+1	VMON_TRK1_UV_FS_REACTION[0]	VMON_TRK1_UV_FS_REACTION[1]
VTRK2 power rail undervoltage	+1	VMON_TRK2_UV_FS_REACTION[0]	VMON_TRK2_UV_FS_REACTION[1]
VREF power rail undervoltage	+1	VMON_VREF_UV_FS_REACTION[0]	VMON_VREF_UV_FS_REACTION[1]
Undervoltage on the analog input monitoring	+1	VMON_EXT_UV_FS_REACTION[0]	VMON_EXT_UV_FS_REACTION[1]
An error is sent by the MCU on FCCU1 and FCCU2 pins (dual wire protocol)	+1	yes	FCCU12_FS_REACTION
An error is sent by the MCU on FCCU1 pin (single wire protocol)	+1	yes	FCCU1_FS_REACTION
An error is sent by the MCU on FCCU2 pin (single wire protocol)	+1	yes	FCCU2_FS_REACTION
An external IC is driving to the error state the signal connected on ERRMON pin	+1	yes	ERRMON_FS_REACTION
Watchdog error counter reaches its maximum value (WD_ERR_CNT[3:0] = @WD_ERR_LIMIT[1:0])	+1	WD_FS_REACTION[0]	WD_FS_REACTION[1]
The fault error counter reaches its intermediate value: (@WD_ERR_LIMIT[1:0])/2	No	FLT_ERR_REACTION[0]	FLT_ERR_REACTION[1]
Wrong WD refresh in INIT_FS state	+1	yes	yes
No WD refresh in INIT_FS	+1	yes	yes
RSTB pin asserted externally	+1	no[1]	yes (low externally)
RSTB pulse request by MCU	No	no[1]	yes
RSTB short to high	+1	yes	No (high externally)
FS0B short to high	+1	no (high externally)	BACKUP_SAFETY_PATH_FS0B
FS0B request by the MCU	No	yes	no
FS1B hort to high	+1	no	BACKUP_SAFETY_PATH_FS1B
FS1B request by the MCU	No	yes	no
REG_CORRUPT = 1	+1	yes	no
OTP_CORRUPT = 1	+1	yes	no
GOTO_INIT request by MCU	No	no[1]	no

[1] By cascaded effect, FS0B is asserted LOW in the INIT_FS state.

Table 3 shows the mapping between the NXP safety SBC and the Aurix family for the use case when the VCORE regulator of the SBC is used to supply the VDD core voltage of the respective Aurix MCU directly, without using the EVR of the Aurix MCU.

For the use case where the EVR of the Aurix MCU is used (see Figure 1 and Figure 2), an SBC with lower VCORE current capability can be used to supply the MCU with a 5 V or 3.3 V power supply. The system integrator is responsible for the correct dimensioning of the SBC, depending on MCU power consumption for the selected application use case, the additional loads on the VCORE rail, and the temperature conditions.

3.2.2 Watchdog

The FS65 and FS45 act as supervisors of the application operation, and as a consequence, include a windowed watchdog (temporal and logical monitoring) that needs to be refreshed periodically by the MCU. This means that the FS65 and FS45 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 a safe state system within the fault-tolerant time interval (FTTI). Thus, either the MCU or the SBC can switch the system to a safe state.

The duration of the watchdog window is configurable to allow different MCU handshake strategies. The duty cycle of the window is fixed at 50 % ± 10 %. Therefore, the first half of the window is said to be closed and the second half is said to be open. The watchdog must be refreshed during the open window (see Figure 6).

After a good or a bad watchdog refresh, a new window period starts immediately in order for the MCU to remain synchronized with the windowed watchdog. The first good watchdog refresh closes the INIT_FS. Then the watchdog window is running, and the MCU must refresh the watchdog in the open window of the watchdog window period. The duration of the watchdog window is configurable from 1.0 ms to 1024 ms using the WDW_PERIOD[3:0] bits. The new watchdog window is effective after the next watchdog refresh. The watchdog window can be disabled only during INIT_FS. The watchdog disable is effective when the INIT_FS is closed.

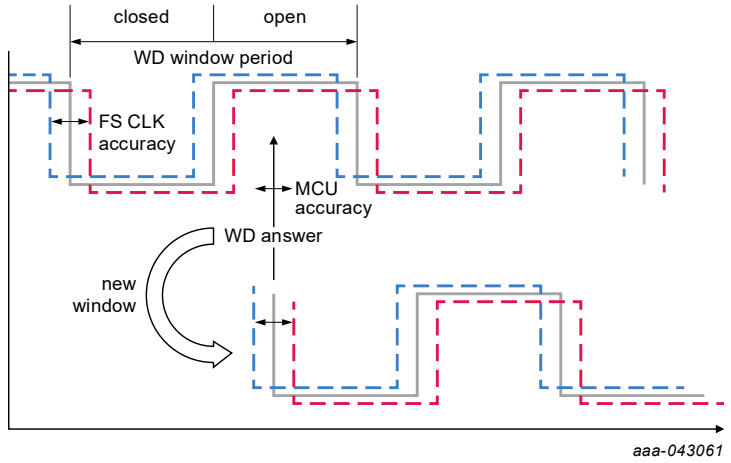


Figure 6. Windowed watchdog

3.2.3 HW SoC monitoring (FCCU)

3.2.3.1 Steady-state mode

FCCU monitoring is meant to detect any HW failures from the MCU. It is active as soon as the Fail-safe machine is in Normal_WD. In the FS45 and the FS65, a register must be configured during the initialization phase to activate the FCCU error-out monitoring: the INIT_FSSM register. In this register, the IO_23_FS bit must be set to logic 1 to configure IO[2] and IO[3] as safety critical inputs. These two I/Os are supposed to work in a bistable protocol with NXP MCUs, but are also capable of monitoring non-NXP MCUs such as AURIX TC2xx/TC3xx.

When connected to the AURIX MCU, the FCCU input pins must be configured as shown in Figure 7 to work with a single error-out pin from the AURIX safety management unit (SMU).

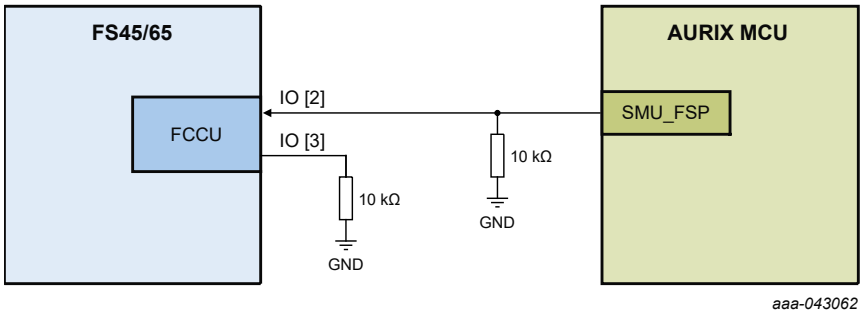


Figure 7. FCCU connection to AURIX SMU in single output fault mode

With the FCCU default polarity configuration, a pulldown must be connected to IO[2] to provide a passive fault detection in case the MCU does not drive its SMU_FSP (fault signaling protocol) output pins.

Assuming IO[2] and IO[3] are connected as shown in Figure 7, these are the steps to follow to enable the FCCU with the AURIX SMU:

1. Configure FS device: IO[2] and IO[3] as safety critical inputs
2. Configure the AURIX SMU in steady state mode
3. Proceed to a latent failure to avoid shorted pin: at INIT phase, toggle the pin and check the IO[2] flag status. The flag follows the pin status
4. FCCU/SMU function is checked and operational

3.2.3.2 PWM mode

The FS45 and the FS65 are also capable of monitoring AURIX MCU through the SMU_FSP signal in pulse-width modulation (PWM) mode (toggling signal) with some limitations. To make this possible, the system engineer must take into account the filtering time of IO[2] and IO[3], which is specified to be 4 µs < FCCU filtering time < 8 µs.

In PWM mode, FCCU must not be triggered accidentally, meaning T_{ON} and T_{OFF} timings must not last more than 4 µs each. To prevent that from happening, the minimum frequency should be 125 kHz with a maximum duty cycle of 50 %. Higher frequencies are safe to be used with a duty cycle never reaching either 0 % or 100 %.

This way, a stuck-LOW or stuck-HIGH signal on IO[2] (depending on the preset pin polarity) is detected as an error, as shown in Figure 8 (a). However, if IO[2] happens to be stuck to its non-fault state (depending on the polarity configuration), this event cannot be detected (see Figure 8 (b) and Figure 9) unless the MCU performs a latent-failure check on this pin at initialization.

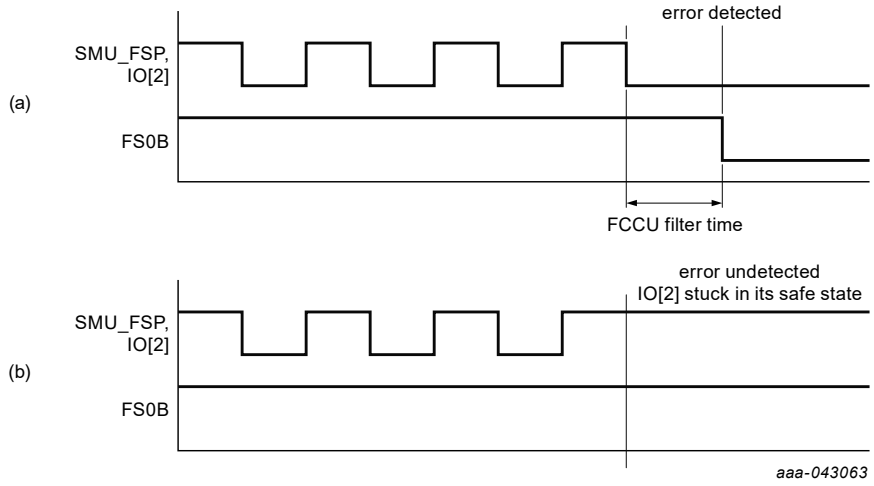


Figure 8. FCCU monitoring and error detection when SMU_FSP signal gets stuck LOW (a) or HIGH (b)

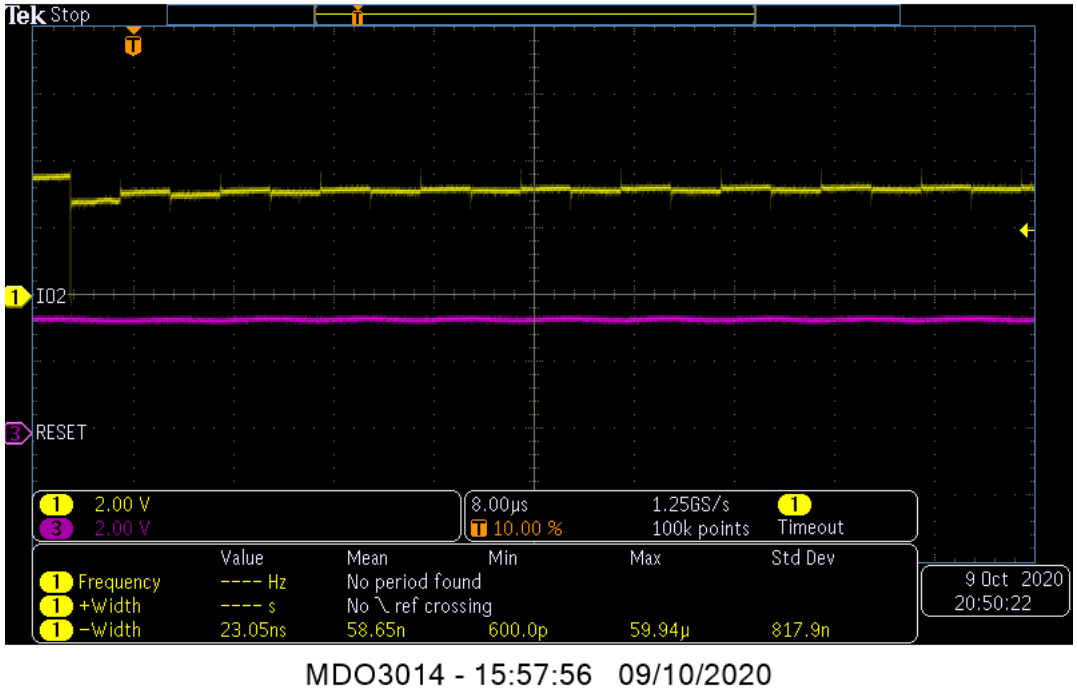


Figure 9. IO[2] shorten to VDDIO - fault not detected and RESET not asserted

If the PWM frequency drifts lower, which is considered an MCU failure, the drift will be detected when it drops below 125 kHz.

If the PWM frequency drifts higher, the FS device will not be able to detect this failure event only through FCCU monitoring (see Figure 10). In this situation, T_{On} and T_{Off} timings will always be under the 4 µs filtering time, preventing the FS device from detecting the drift.

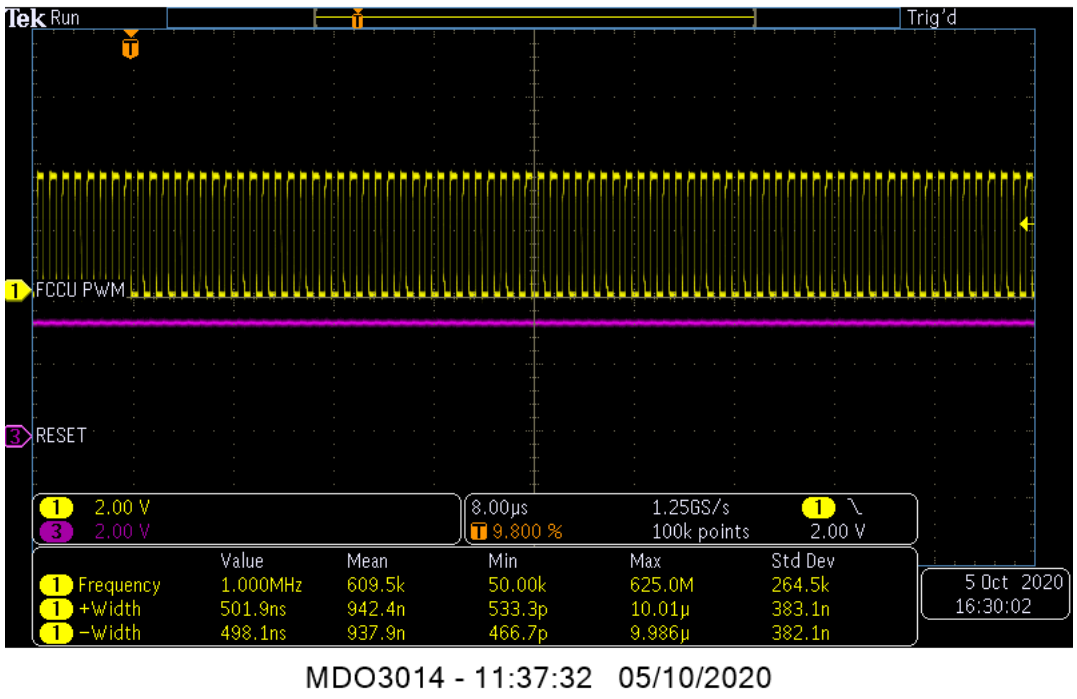


Figure 10. Frequency drift (up) fault not detected and RESET not asserted (f = 1 MHz/T_{On} = 501.9 ns/T_{Off} = 498.1 ns

To be able to detect such an event, the windowed WD monitoring can be used in a variety of ways. An increasing drift in the MCU's clock frequency inevitably impacts its WD answer frequency and leads to multiple WD errors.

The MCU must always trigger the WD in the open WD window, or else an error is generated. Here are the steps during the handshake:

1. FS65/FS45 generates a pseudo random code using a linear-feedback shift register(LFSR)
2. MCU reads the code
3. Both MCU and FS65/FS45 calculate the WD answer using the same formula
4. MCU sends its WD answer and FS65/FS45 compares that answer with its own
5. If the WD answer is wrong or sent in the closed WD window, a WD error is generated. If the good WD answer is sent in the open WD window, a new WD window opens and the handshake restarts

From here, there are two different ways to improve detectability:

- One can choose to reduce the WD window period, to capture the MCU frequency drift as quickly as possible, taking into account the ± 10 % accuracy of the FS65/FS45 clock, but also the MCU accuracy.
- One can decide to have the MCU WD answer sent at the very beginning of the WD open window. This workaround is more severe, and would allow detection to occur faster than any MCU frequency drift increase. Again, the MCU and the FS65/FS45 clock accuracies must be taken into the equation to prevent a false WD answer.

Example: *Down to 1 ms, the WD period can be between 0.9 ms and 1.1 ms (1 ms ± 10 %). With a 50 % duty cycle, the MCU WD answer should be sent in the middle of the open window, between 0.55 ms (worst case is 60 % of 0.5 ms) and 0.9 ms (see Figure 6).*

Assuming again IO[2] and IO[3] are connected as shown in Figure 7, these are the steps to follow to enable FCCU with the AURIX SMU:

1. Configure FS device: IO[2] and IO[3] are safety critical inputs
2. Configure the AURIX SMU in PWM mode
3. Proceed to a latent failure check to detect shorted pins: at INIT phase, toggle the pin and check the IO[2] flag status. The flag must follow the pin status
4. Set IO[2] in its valid state (HIGH level in this use case) when closing the INIT_FS phase before entering Normal mode
5. FCCU/SMU function is checked and operational. AURIX can switch to the PWM SMU_FSP signal

Figure 11 through Figure 13 show lab test results when sending a PWM signal with various frequencies to IO[2] in standard configuration and following the steps described above. IO[2] and IO[3] are set as safety-critical inputs and the pins' polarity is default. Thus, IO[3] is pulled down to GND (safe state) and IO[2] safe state is HIGH (LOW indicates a fault) before closing the INIT phase and entering Normal mode.

As both IOs are safety critical inputs, the RESET pin is asserted LOW upon a fault, and the IO_23 flag is set to logic 1 in the DIAG_FS_IOS register.

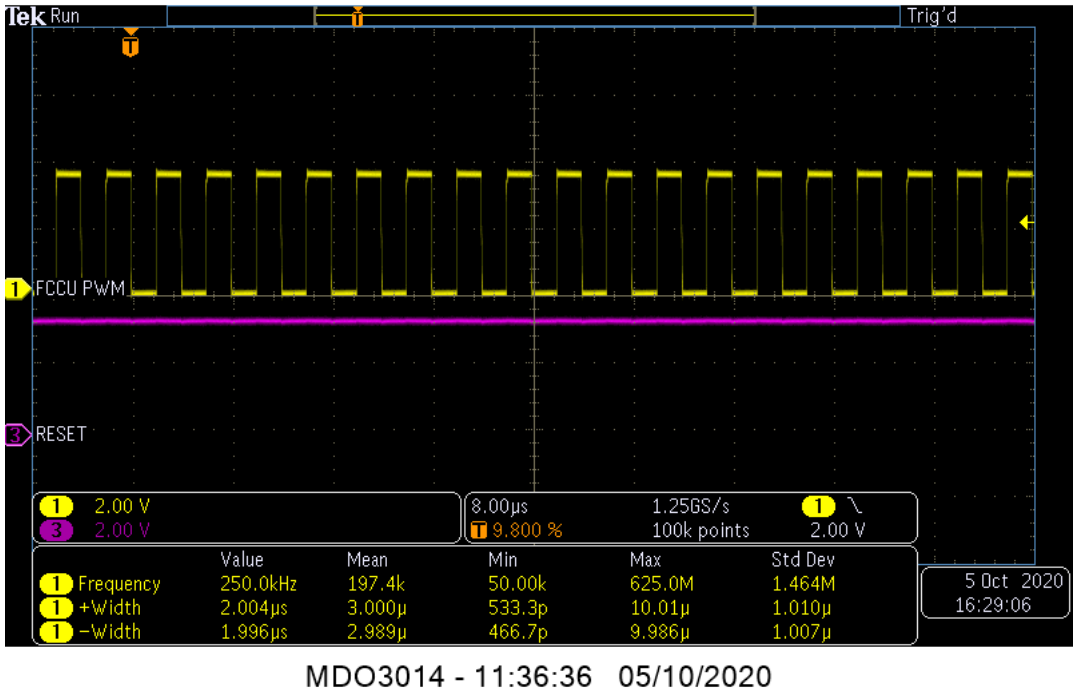


Figure 11. Reference state — no fault / RESET not asserted — f = 250 kHz / T_{On} = 2.004 µs / T_{Off} = 1.996 µs

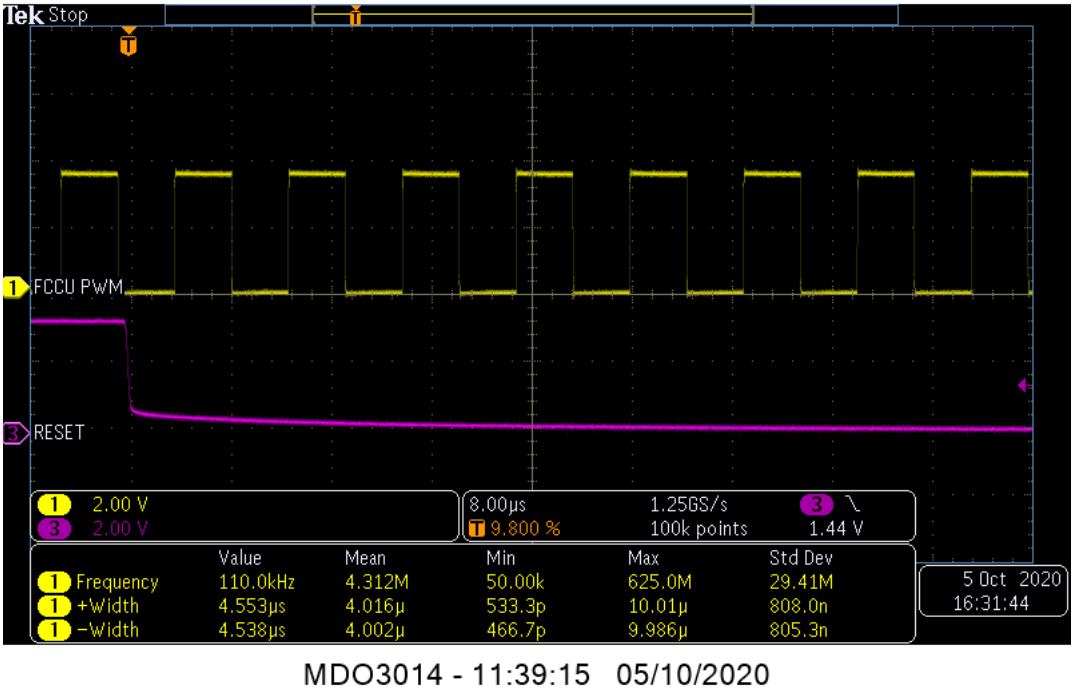


Figure 12. Frequency drift (down) fault detected / RESET asserted f = 110 kHz / T_{On} = 4.553 µs / T_{Off} = 4.538 µs

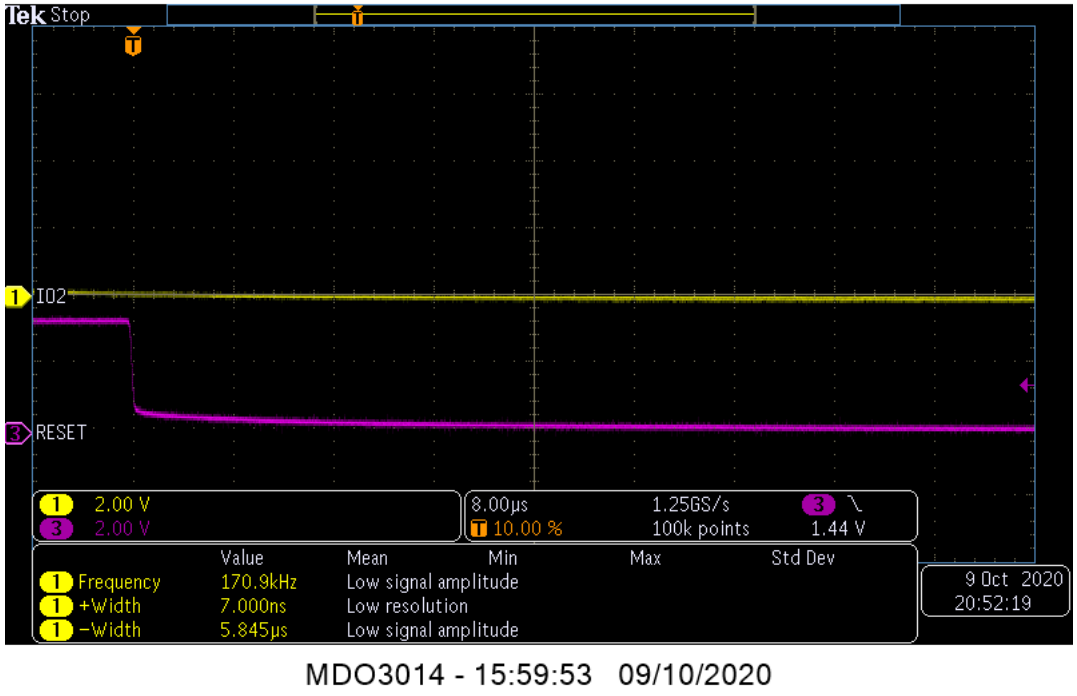


Figure 13. IO[2] short to GND fault detected / RESET asserted f = 125 kHz / T_{On} = 4.007 µs / T_{Off} = 3.993 µs

Given the right configuration and strategy, the FS65/FS45 is able to support the AURIX SMU FSP signal in steady-state mode and in PWM mode.

3.3 Power management with AURIX MCU

The following diagrams and tables show the connections between the FS65/FS45 and AURIX TC2xx/TC3xx MCUs.

3.3.1 FS450x + TC23x

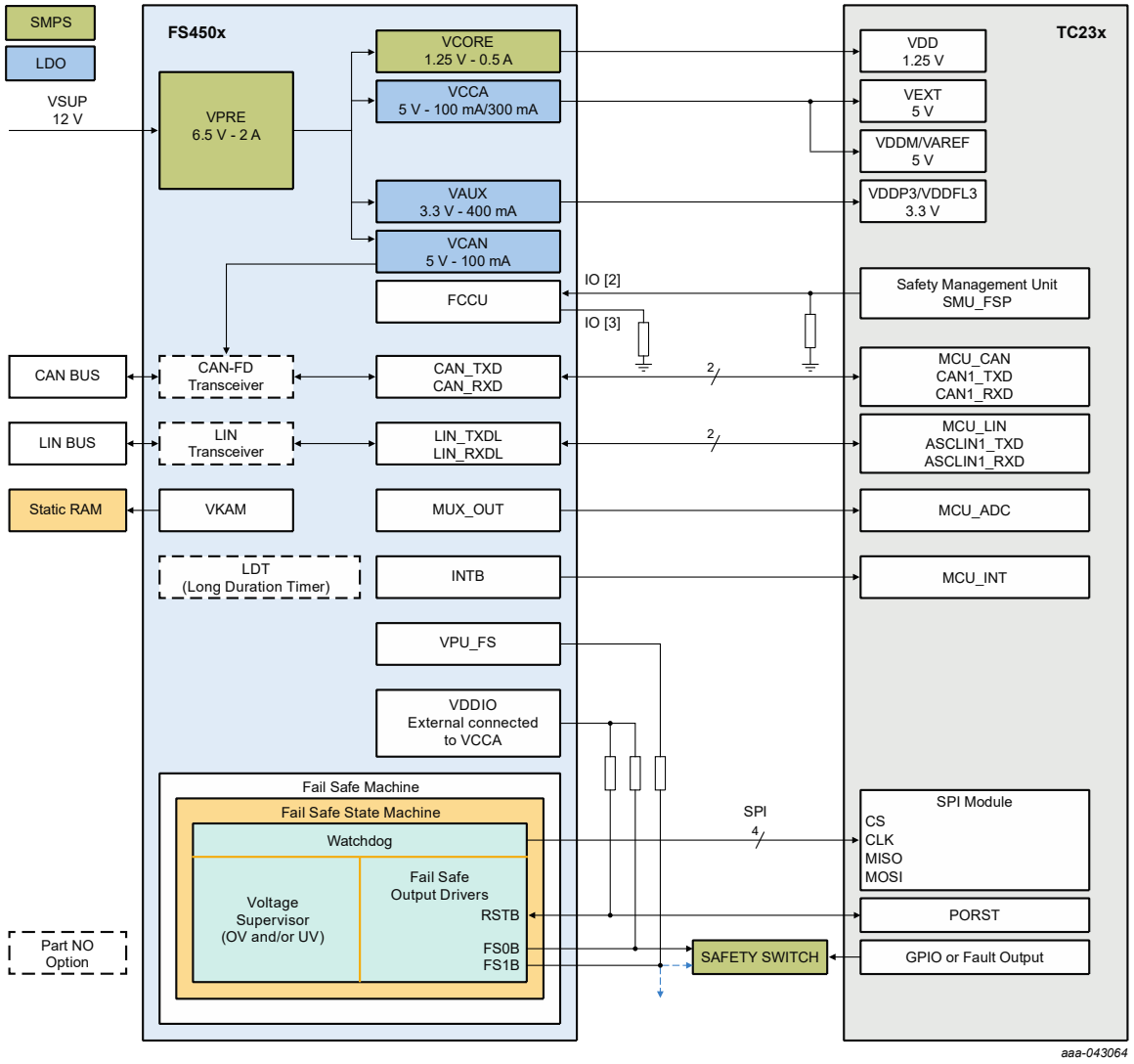


Figure 14. FS450x attached to TC23x AURIX MCU

Table 4. FS450x-TC23x connections summary

FS450x connection	TC23x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to 1.3 V VDD in TC23x
VCCA	VEXT, VDDM and VAREF	VCCA provides 5.0 V voltage rail to VEXT, VDDM and VAREF with ± 1 % accuracy in TC23x
VAUX	VDDP3	VAUX provides 3.3 V voltage rail to VDDP3 in TC23x
4 lines SPI	4 lines SPI	SPI connections between FS450x to TC23x

Table 4. FS450x-TC23x connections summary*...continued*

FS450x connection	TC23x connection	Description
IO_2	SMU_FSP	SMU connection with pull-down resistor
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection
MUX_OUT	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC23x
CAN/LIN signal	CAN/LIN signal	CAN bus/LIN bus communication signal

3.3.2 FS650x + TC27x

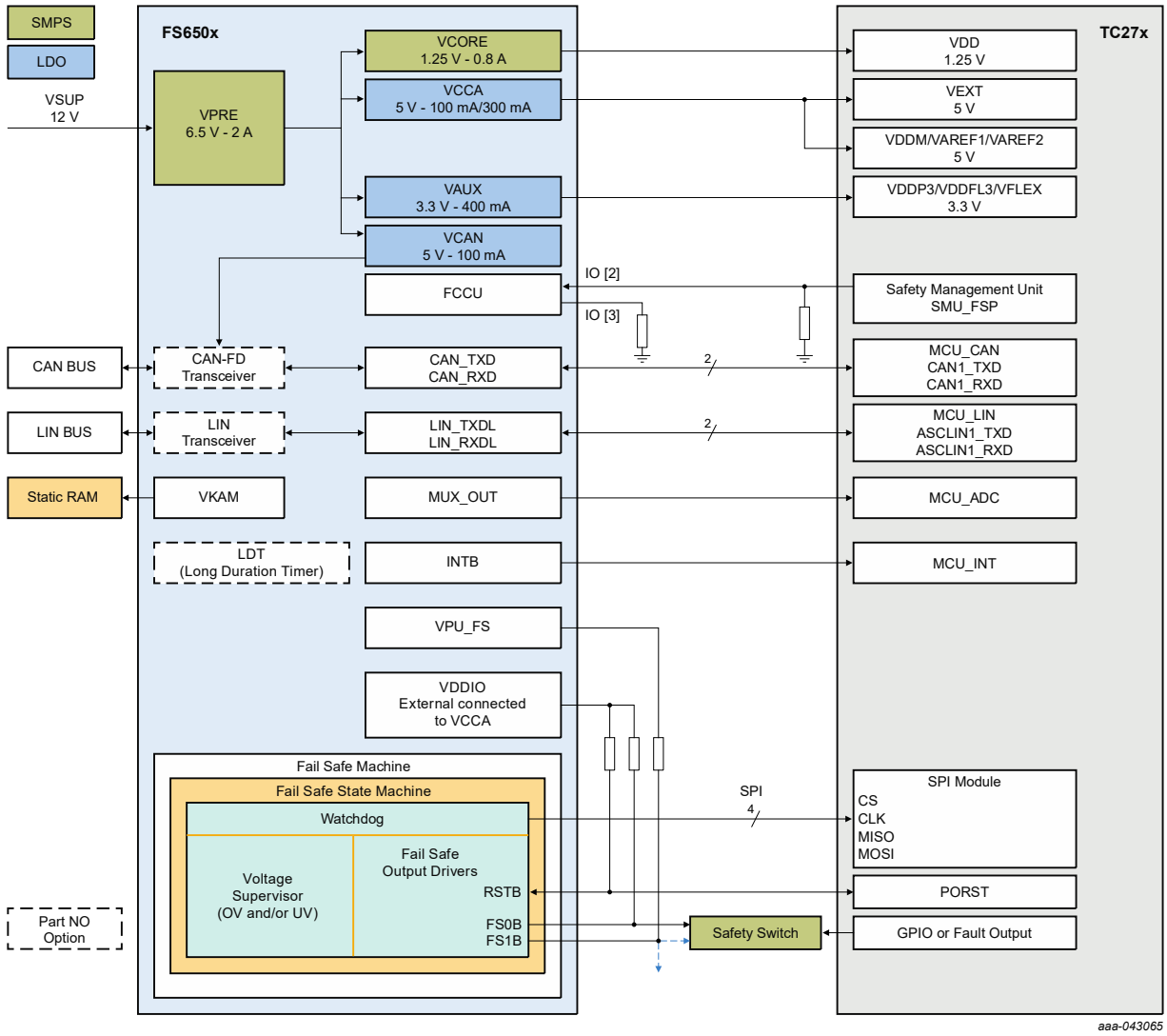


Figure 15. FS650x attached to TC27x AURIX MCU

Table 5. FS650x-TC27x connections summary

FS450x connection	TC23x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC27x
VCCA	VEXT, VDDM and VAREF1/2	VCCA provides 5.0 V voltage rail to VEXT, VDDM and VAREF1/2 with ±1 % accuracy in TC27x
VAUX	VDDP3, VDDFL3, and VFLEX	VAUX provides 3.3 V voltage rail to VDDP3, VAREF1/2, VDDFL3, VFLEX, and VEXT in TC27x
4 lines SPI	4 lines SPI	SPI connections between FS450x to TC27x
IO_2	SMU_FSP	SMU connection with pull-down resistor
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection

Table 5. FS650x-TC27x connections summary*...continued*

FS450x connection	TC23x connection	Description
MUX_OUT	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC27x
CAN/LIN signal	CAN/LIN signal	CAN-bus/LIN-bus communication signal

3.3.3 FS651x + TC29x

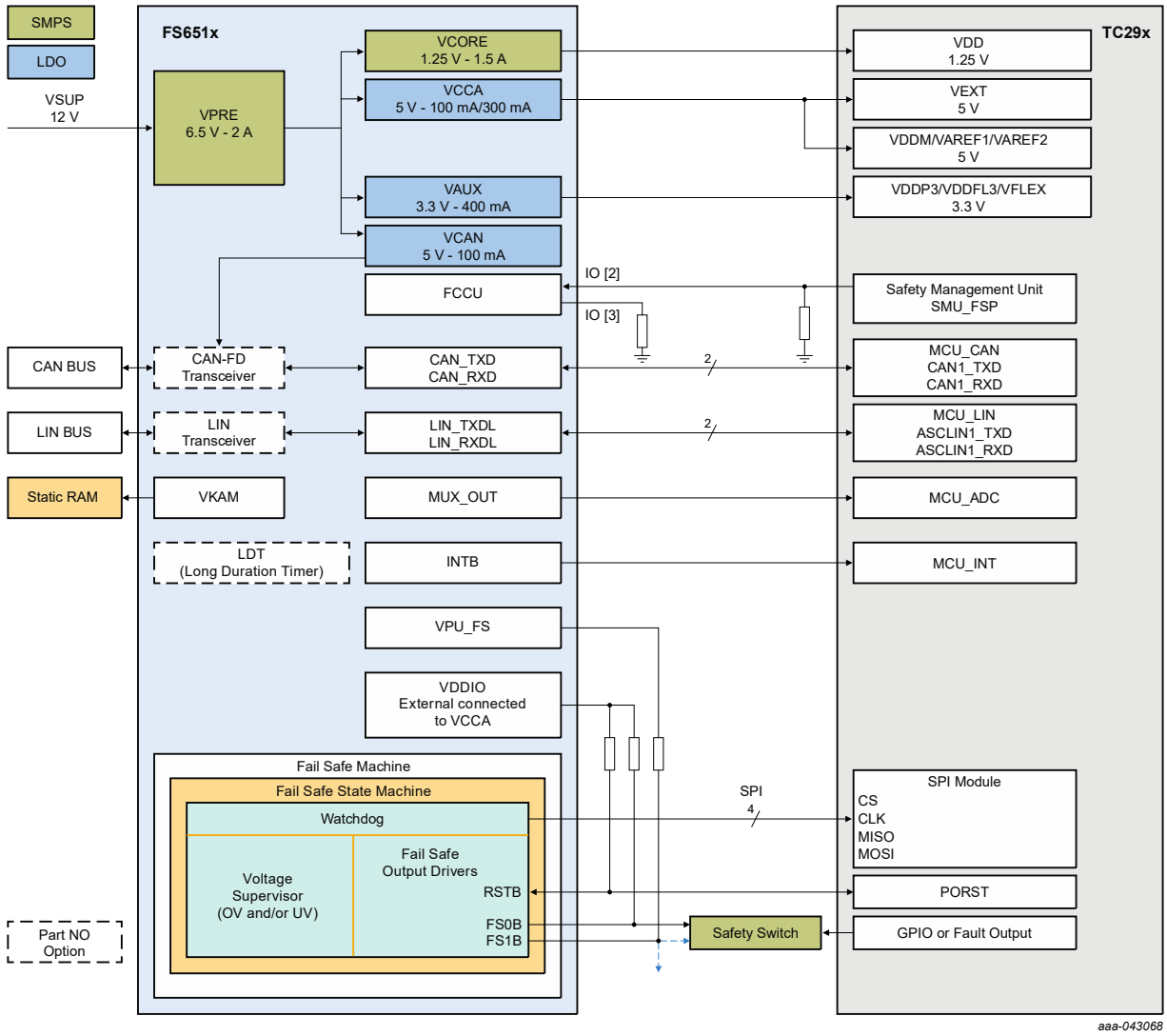


Figure 16. FS651x attached to TC29x AURIX MCU

Table 6. FS651x-TC29x connections summary

FS651x connection	TC29x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC29x
VCCA	VEXT, VDDM and VAREF1/2	VCCA provides or 5.0 V voltage rail to VEXT, VDDM and VAREF1/2 with ± 1 % accuracy in TC29x
VAUX	VDDP3, VDDFL3 and VFLEX	VAUX provides 3.3 V voltage rail to VDDP3, VDDFL3 and VFLEX in TC29x
4 lines SPI	4 lines SPI	SPI connections between FS651x to TC29x
IO_2	SMU_FSP	SMU connection with pulldown resistor
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection

Table 6. FS651x-TC29x connections summary*...continued*

FS651x connection	TC29x connection	Description
MUX_OUT	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC29x
CAN/LIN signal	CAN/LIN signal	CAN bus/LIN bus communication signal

3.3.4 FS652x + TC39x

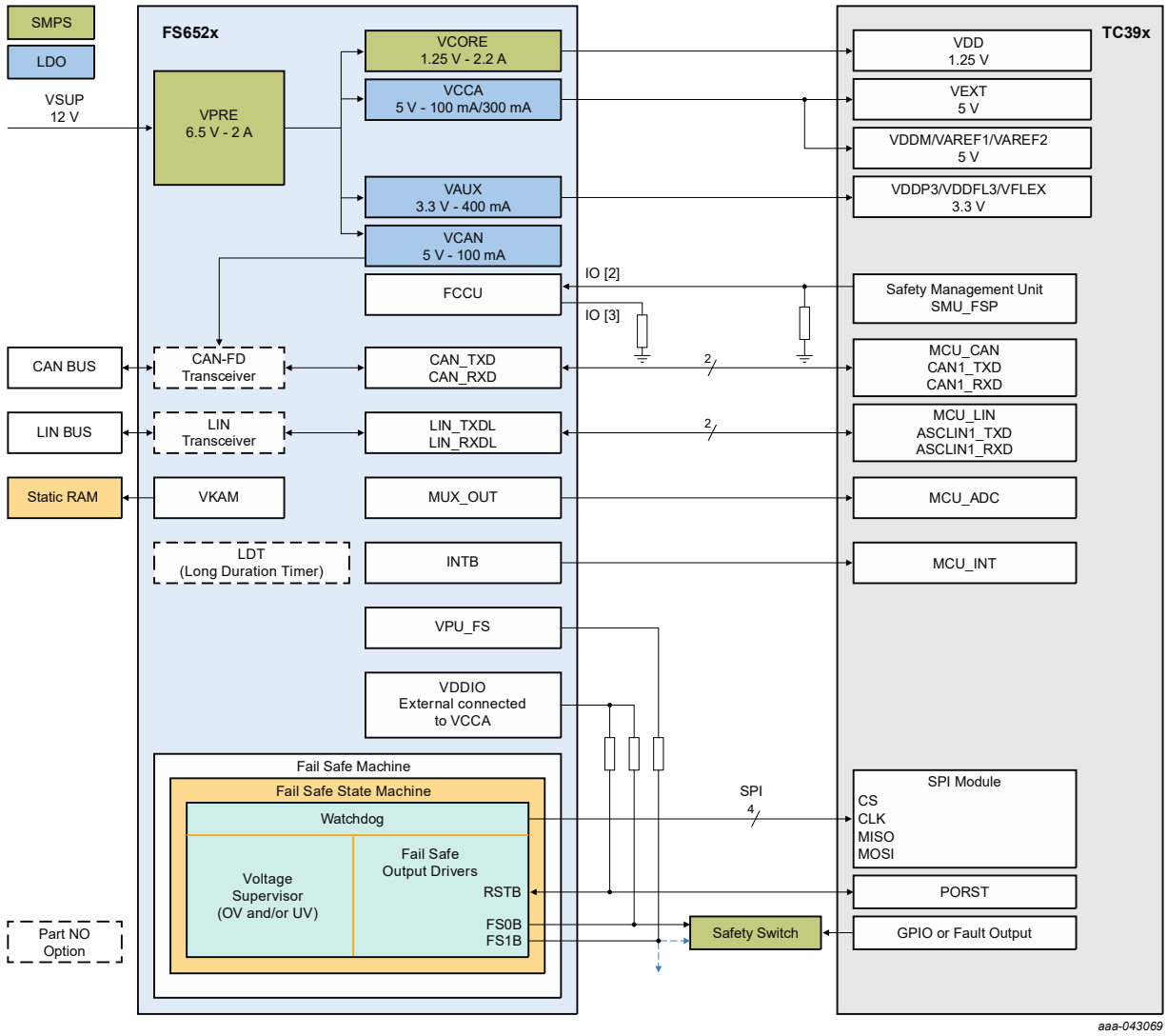


Figure 17. FS652x attached to TC39x AURIX MCU

Table 7. FS652x-TC39x connections summary

FS652x connection	TC39x connection	Description
VCORE	VDD_1.3 V and VDDSB	VCORE provides 1.3 V voltage rail to 1.3 V VDD in TC39x
VCCA	VDDM and VAREF1/2	VCCA provides 3.3 V or 5.0 V voltage rail to VDDM and VAREF1/2 with ± 1 % accuracy in TC39x
VAUX	VDDP3, VDDFL3, VEXT,VFLEX, VEVRSB and VEXTLVDS	VAUX provides 3.3 V voltage rail to VDDP3, VDDFL3, VEXT, VFLEX, VEVRSB, and VEXTLVDS in TC39x
4 lines SPI	4 lines SPI	SPI connections between FS652x to TC39x
IO_2	SMU_FSP	SMU connection with pull-down resistor
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection

Table 7. FS652x-TC39x connections summary*...continued*

FS652x connection	TC39x connection	Description
MUX_OUT	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC39x
CAN/LIN signal	CAN/LIN signal	CAN bus/LIN bus communication signal

3.3.5 FS65/FS45 + TC2xx/TC3xx alternative

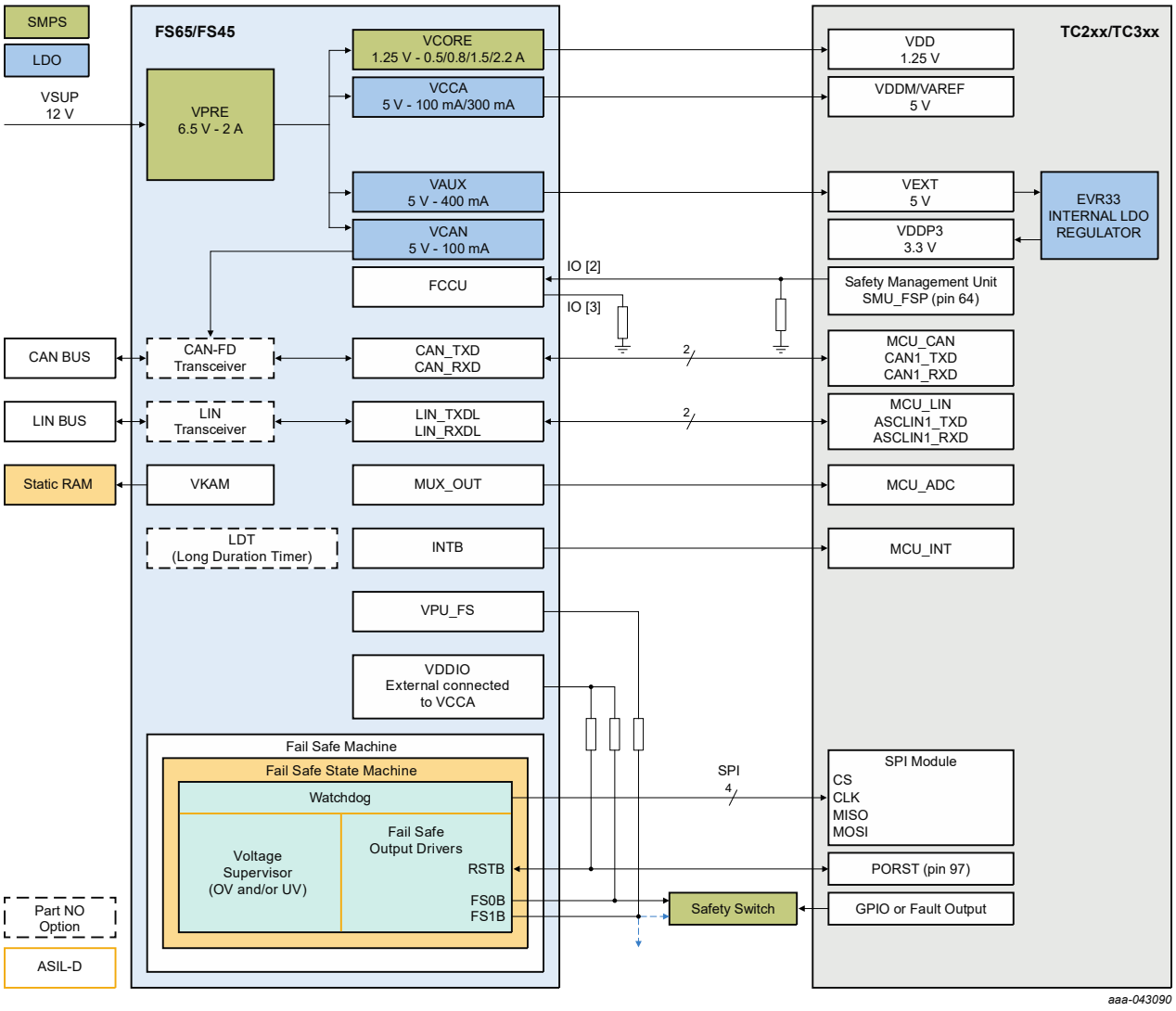


Figure 18. FS65/FS45 attached to TC2xx/TC3xx AURIX MCU - alternative solution

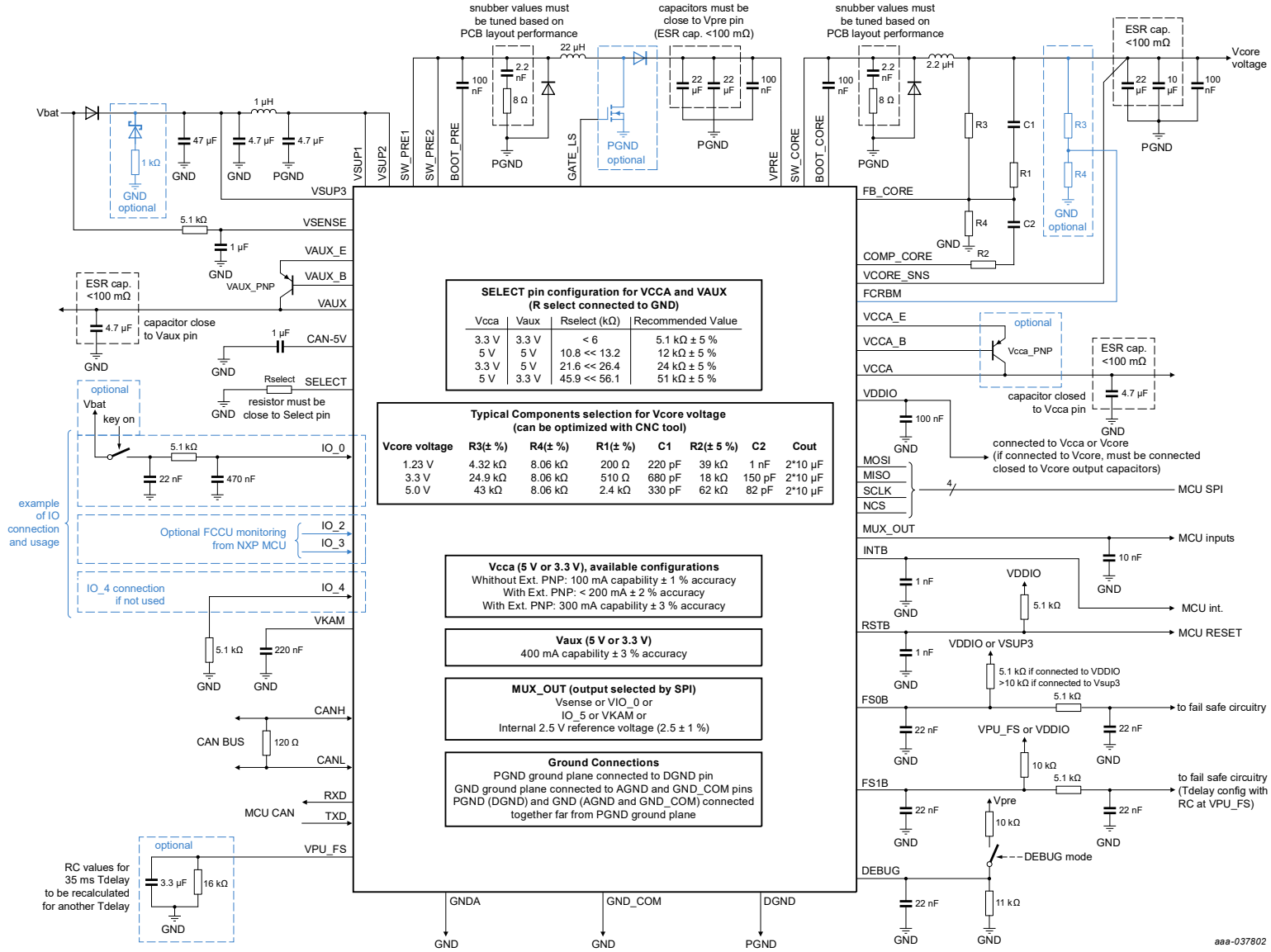
Table 8. FS65/FS45 other system connections summary

FS450x connection	TC23x connection	Description
VKAM	Ssatic RAM	VKAM provides power rail to static RAM
IO_3	pulldown resistor to GND	works with IO2 for SMU function
FS0B	connect to safety switch	Works with FS1B together as safety switch output to bring the system into a safe state. The connection may vary based on customer requirements.
FS1B	connect to safety switch	Works with FS0B together as safety switch output to bring the system into a safe state. The connection may vary based on customer requirements. .
VDDIO	connect to RSTB and FS0B	pull up voltage source for RSTB and FS0B (also FS1B if available) with resistors

Table 8. FS65/FS45 other system connections summary*...continued*

FS450x connection	TC23x connection	Description
VPU_FS	connect to FS1B	pull up voltage source of FS1B with resistor
Debug	connect to resistor ladder in series of switch	for Debug mode enable/disable
Select	connect to R_{SELECT} to GND or VPRE	to set VCCA and VAUX voltage and Deep Fail-safe mode enable/disable

3.4 Application schematic



SELECT pin configuration for VCCA and VAUX (R select connected to GND)

Vcca	Vaux	Rselect (kΩ)	Recommended Value
3.3 V	3.3 V	< 6	5.1 kΩ ± 5 %
5 V	5 V	10.8 << 13.2	12 kΩ ± 5 %
3.3 V	5 V	21.6 << 26.4	24 kΩ ± 5 %
5 V	3.3 V	45.9 << 56.1	51 kΩ ± 5 %

Typical Components selection for Vcore voltage (can be optimized with CNC tool)

Vcore voltage	R3(± %)	R4(± %)	R1(± %)	C1	R2(± 5 %)	C2	Cout
1.23 V	4.32 kΩ	8.06 kΩ	200 Ω	220 pF	39 kΩ	1 nF	2*10 µF
3.3 V	24.9 kΩ	8.06 kΩ	510 Ω	680 pF	18 kΩ	150 pF	2*10 µF
5.0 V	43 kΩ	8.06 kΩ	2.4 kΩ	330 pF	62 kΩ	82 pF	2*10 µF

Vcca (5 V or 3.3 V), available configurations
Whithout Ext. PNP: 100 mA capability ± 1 % accuracy
With Ext. PNP: < 200 mA ± 2 % accuracy
With Ext. PNP: 300 mA capability ± 3 % accuracy

Vaux (5 V or 3.3 V)
400 mA capability ± 3 % accuracy

MUX_OUT (output selected by SPI)
Vsense or VIO_0 or
IO_5 or VKAM or
Internal 2.5 V reference voltage (2.5 ± 1 %)

Ground Connections
PGND ground plane connected to DGND pin
GND ground plane connected to AGND and GND_COM pins
PGND (DGND) and GND (AGND and GND_COM) connected together far from PGND ground plane

Figure 19. FS65/FS45 automotive schematic used for BOM list

3.5 BOM

Table 9. FS65/FS45 BOM reference

Domain	item name	value	unit	description	optional
IO_O ignition connection	R_IO	5.1	kΩ	load dump serial resistor protection	X
	COUT1_IO	470	nF	load dump serial capacitor protection	X
	COUT2_IO	22	nF	ESD protection capacitor	X
IO_2/3 FCCU monitoring	FCCU_PU	5.1	kΩ	pullup resistor for FCCU1/ IO_3	X
	FCCU_PD	10	kΩ	pulldown resistor for FCCU2/ IO_2	X
VDDIO	COUT_VDDIO	100	nF	decoupling capacitor close to the pin for immunity	
AMUX	COUT_MUX	10	nF		
INTB	COUT_INTB	1	nF		
VSUP power dupply	FB			ferrite bead	X
	RP diode	—		reverse protection diode	
	DIP	Zener 30 V		external Zener diode and serial resistor to discharge CBAT capacitor (needed to sustain ISO pulses on VBAT in LPOFF)	X
	RIP	1	kΩ		X
	CBAT	47	µF	decoupling capacitor	
	CPI1	4.7	µF	pi filter components	
	LPI	1	µH		
	CPI2	4.7	µF		
	RSENSE	5.1	kΩ	current limit resistor	
	CSENSE	1	µF	decoupling capacitor	
VPRE pre-regulator	NMOSFET	—		VPRE in BUCK BOOST mode	X
	Diode	—			X
	CSNU_VPRE	2.2	nF	snubber capacitor for VPRE	
	RSNUB_VPRE	8	Ω	snubber resistor for VPRE	
	CBOOT_PRE	100	nF	bootstrap capacitor	
	D_VPRE	Diode		diode	
	L_VPRE	22	µH	power inductor	
	LS_BB	—		low-side MOSFET	X
	D_BB	—		Schottky diode	X
	COUT_VPRE	10 or 22	µF	output capacitors	
FS65 VCORE regulator (BUCK)	L_VCORE	2.2	µH	power inductor	
	D_VCORE	—		diode	

Table 9. FS65/FS45 BOM reference*...continued*

Domain	item name	value	unit	description	optional
	CBOOT_CORE	100	nF	bootstrap capacitor	
	RSNUB_VCORE	8	Ω	VCORE snubber	
	CSNUB_VCORE	2.2	nF		
	R4	8.06	kΩ	ext resistor bridge	
	R3	43	kΩ	ext resistor bridge	
	R1	2.4	kΩ	compensation network	
	C1	330	pF		
	R2	62	kΩ		
	C2	82	pF		
	COUT_VCORE	4 x 10 or 22 x 2	µF	output capacitors	
	EMI COUT_ VCORE	100	nF	electromagnetic interference (EMI) capacitor values to be adjusted at printed-circuit board (PCB) level	X
	EMI VCORE_SNS	330	pF		X
	EMI_FB_CORE	22	pF		X
FS45 VCORE regulator (LDO)	COUT_VCORE	10 or 22	µF	output capacitor	
VAUX Regulator	VAUX_PNP	—		PNP	
	COUT_VAUX	4.7	µF	output capacitor	
	RSELECT	5.1	kΩ	VAUX/VCCA voltage configuration	
VCCA	COUT_VCCA	4.7	µF	output capacitor	
VCAN	COUT_VCAN	1	µF	output capacitor	X
CAN BUS	R_CAN	120	Ω	CAN bus resistor connected between CANH and CANL	X
Reset and Fail-safe outputs	COUT_RSTB	1	nF	RSTB capacitor	
	PU_RSTB	5.1	kΩ	RSTB pullup resistor	
	COUTx_FS0B	2 x 10 to 22	nF	FS0B capacitors	
	COUTx_FS1B	2 x 10 to 22	nF	FS1B capacitors	X
	PU_FS0B	5.1	kΩ	FS0B pullup resistor	
	PU_FS1B	10	kΩ	FS1B pullup resistor	X
	RFS0B	5.1	kΩ	FS0B resistor	
	RFS1B	5.1	kΩ	FS1B resistor	X
	RPD	to be calculated	Ω	backup delay resistor for FS1B	X
	CPD	to be calculated	F	backup delay capacitor for FS1B	X

For more detailed information on product guidelines, refer to the dedicated application note: AN5238.

3.6 Timing sequence

3.6.1 Flowchart

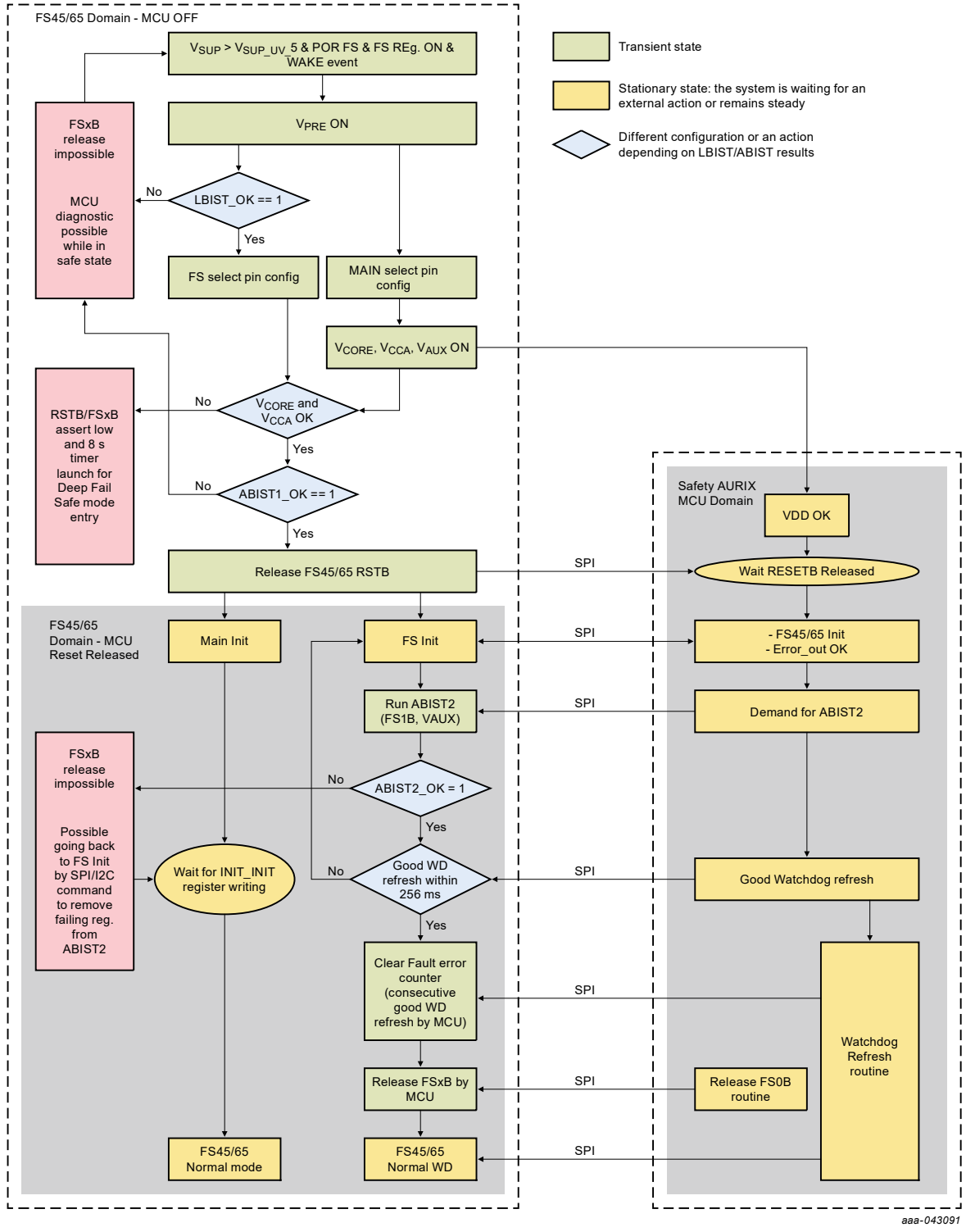


Figure 20. Power-up sequence flowchart block diagram

The following domain information details some specific states from the flowchart in Figure 20.

FS65/FS45 domains:

- **Select pin configuration:** VAUX and VCCA voltages are configured according to the resistor value connected between the SELECT pin and ground or VPRE. The same applies to the Main state machine and the deep fail-safe configuration. In the Fail-safe machine, this detection is used to set internally the UV/OV threshold on VCCA and VAUX for the voltage supervision, and enable/disable the deep fail-safe feature.
- **Main init:** When RSTB is released, the initialization phase starts where the MCU configures the device via the SPI bus. Once the INIT register configurations are complete, a last register called INIT_INT must be configured to switch to Normal mode.
- **Fail-safe init:** A window of 256 ms after the release of RSTB is available to configure the initialization register of the FS65/FS45. The MCU can configure watchdog, error counters, safety reaction mechanisms and similar behaviors in this window using the SPI bus. In order to close this window before timeout, the MCU must send a good watchdog refresh. Otherwise, it will be considered to be a fault.
- **FS65/FS45 Normal mode:** In order for the FS65/FS45 to enter Normal mode, the FS0B pin must be released. To release the FS0B pin, send several consecutive good watchdog commands to clear the error counter down to 0. Finally, send a SPI bus command to release the FS0B.

AURIX TC2xx/TC3xx MCU domains:

- MCU VDD OK: Depending on the system architecture, VDD (equivalent for VCORE) from the MCU can be supplied by the FS65/FS45 or by an external source.
- MCU waits for RESETB to be released: The pin RESETB from the FS65/FS45 is chosen in this application note for releasing the RESET of the MCU.

3.6.2 FS65/FS45 power sequencing

A system power-up sequence is shown in Figure 21:

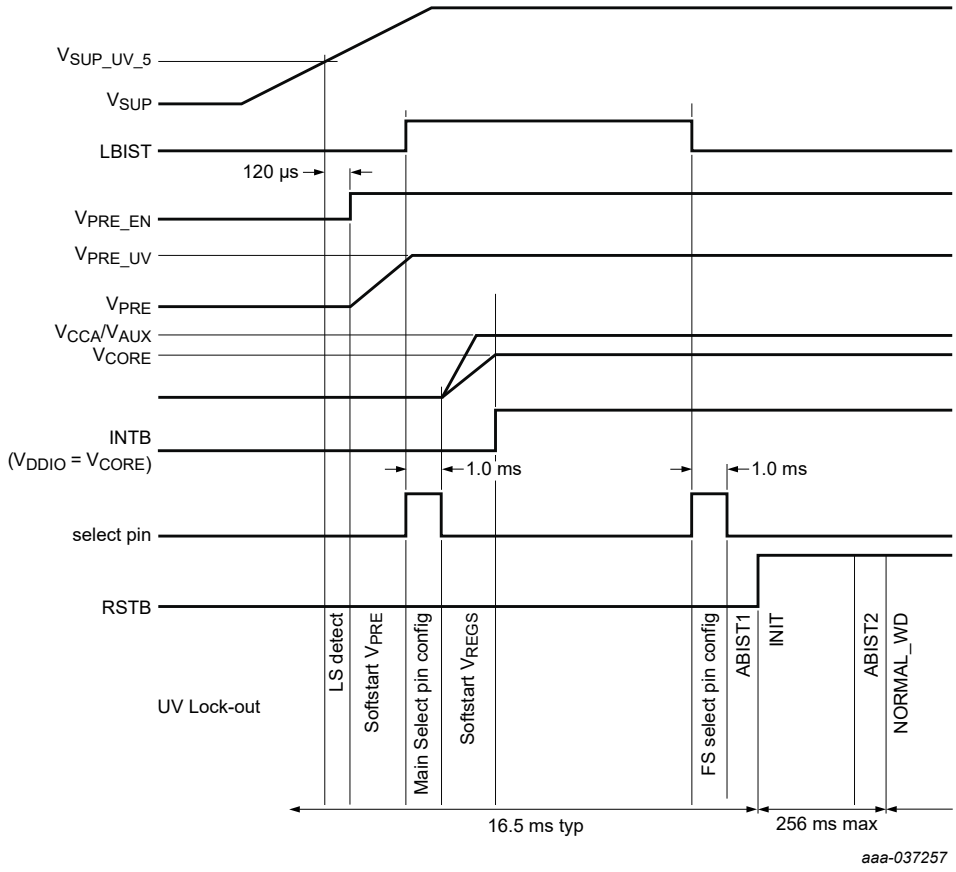


Figure 21. Power-up sequence

To provide a safe and well-known start-up sequence, the FS65/FS45 includes an undervoltage lockout. This VSUP_UV_5 undervoltage lockout applies when the device is under a power-on reset condition or released from LPOFF. All the different voltage rails start automatically as described in Figure 21.

The final value of VAUX and VCCA depends on the hardware configuration (resistor values at the SELECT pin). The typical start-up sequence takes around 16.5 ms to release RSTB. RSTB can be pulled LOW after those 16.5 ms by the TC2xx/TC3xx, if it is not ready to run.

3.7 Fault management and recovery

When the system is operating in Normal mode, various types of faults can occur on the FS65/FS45, on the MCU, or on external peripherals. Fault use cases that the system might face and its reaction to each one are explained in this section.

Fault management use cases between FS65/FS45 and AURIX TC2xx/TC3xx are described in Section 3.7.1 "AURIX TC2xx/TC3xx VCORE overvoltage" through Section 3.7.5 "Other recovery". Other faults, such as overtemperature, follow the same sequence.

Table 10. Fault list

Fault number	Fault location	Fault type
1	FS65/FS45 AURIX VCORE supply	Over-voltage

Table 10. Fault list*...continued*

Fault number	Fault location	Fault type
2	FS65/FS45 AURIX VCORE supply	Under-voltage
3	FS65/FS45 AURIX SPI	Watchdog Fault
4	FS65/FS45 IO_23	FCCU fault

3.7.1 AURIX TC2xx/TC3xx VCORE overvoltage

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- VCORE_FS_OV_1:0 = 11 (default value), VCCA_OV does have an impact on RSTB and FS0B
- RSTB_DURATION = 0 (default value), set to configure the RSTB LOW duration time to 10 ms
- TDLY_TDUR = 0, set the FS1B in T_{DELAY} mode
- FS1B_TIME_3:0 = 1011, FS1B_TIME_RANGE = 1, set the T_{DELAY} = 1103 ms
- Deep Fail-safe (DFS) function is enabled (SELECT pin connected to ground)

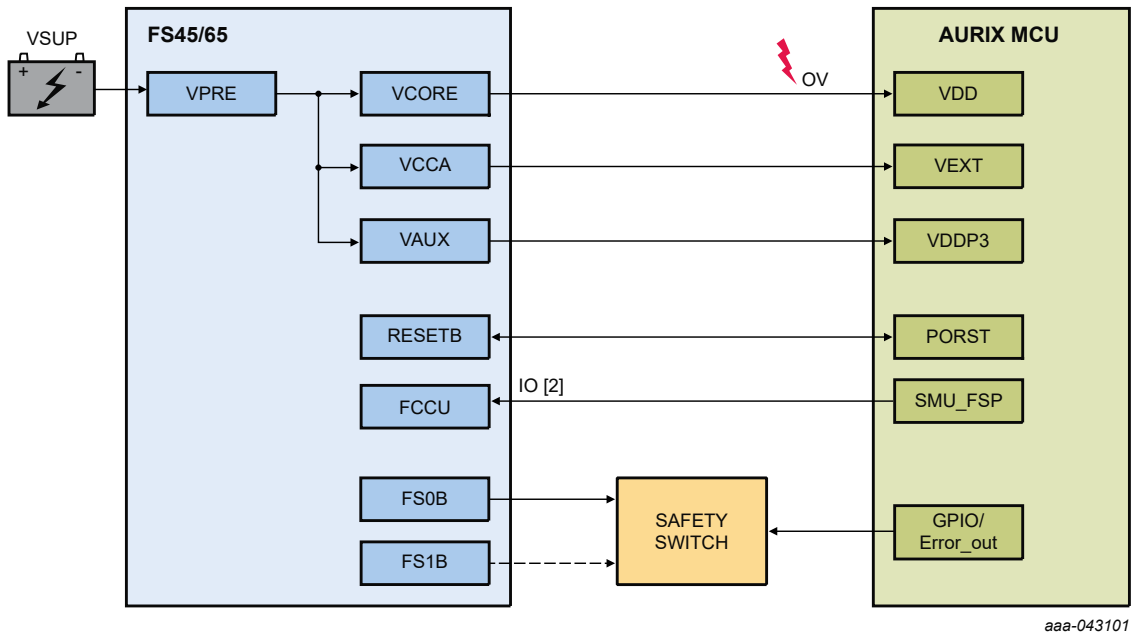


Figure 22. VCORE OV fault simplified schematic

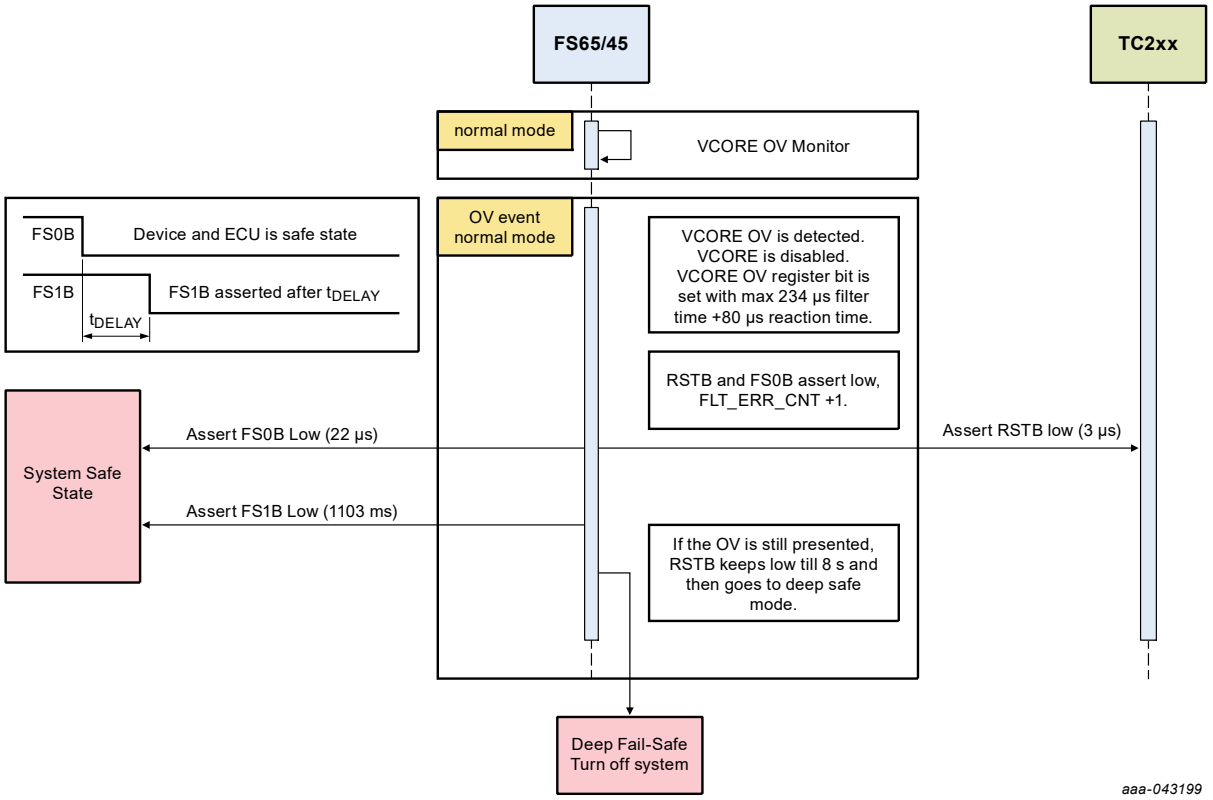


Figure 23. VCORE OV fault management sequence diagram (to DFS)

1. FS65/FS45 VCORE voltage is internally monitored.
2. OV event occurs on VCORE. FS65/FS45 triggers a fault after max 234 µs filter time + 80 µs reaction time. VCORE regulator is disabled. FS65/FS45 increments FLT_ERR_CNT by one.
3. FS65/FS45 asserts RSTB and FS0B LOW according to VCORE_FS_OV_1:0 configuration
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms
5. If the OV condition remains, RSTB stays LOW
6. If RSTB stays LOW for 8 s, FS65/FS45 goes to Deep Fail-safe mode

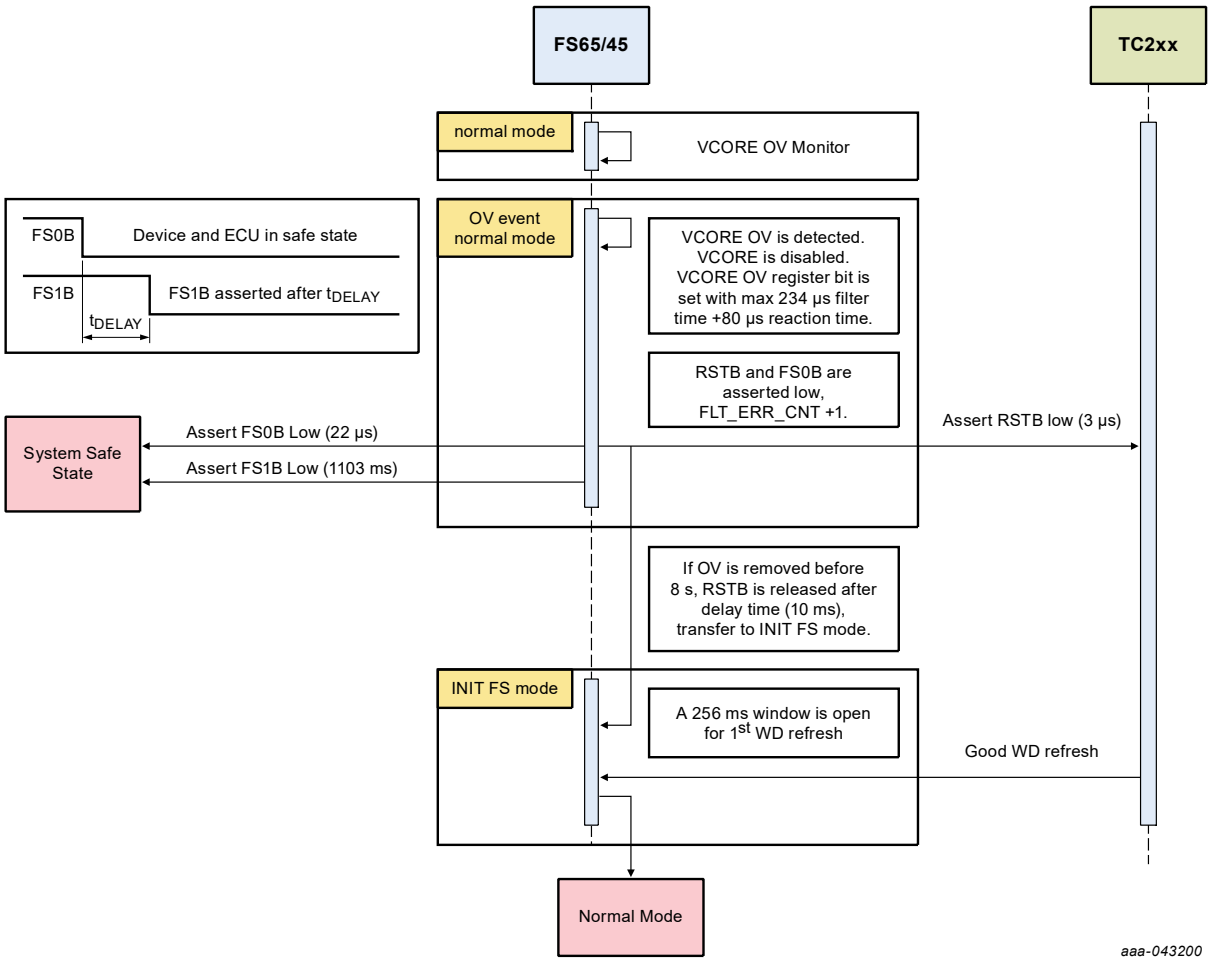


Figure 24. VCORE OV fault management sequence diagram (to recovery)

1. FS65/FS45 VCORE voltage is internally monitored.
2. OV event occurs on VCORE. FS65/FS45 triggers a fault after max 234 µs filter time + 80 µs reaction time. VCORE is disabled. FS65/FS45 increments FLT_ERR_CNT by one.
3. FS65/FS45 asserts RSTB and FS0B LOW according to VCORE_FS_OV_1:0 configuration.
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms.
5. If the OV condition is removed before 8 s, after 10 ms delay, RSTB is released. FS65/FS45 transfers to INIT_FS mode, opens a 256 ms window and waits for a new WD refresh from AURIX.
6. FS65/FS45 returns to Normal mode as a result of a good WD refresh. If good WD refreshes continue, FLT_ERR_CNT decrements to 0.

3.7.2 AURIX TC2xx/TC3xx VCORE undervoltage

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- VCORE_FS_UV_1:0 = 10 (default value), $V_{CORE\_FB\_UV}$ has an impact only on FS0B
- IO_23_FS = 1 (default value), set to configure the couple of IO_3:2 as safety inputs for FCCU monitoring
- TDLY_TDUR = 0, set the FS1B in T_{DELAY} mode
- FS1B_TIME_3:0 = 1011, FS1B_TIME_RANGE = 1, set the T_{DELAY} = 1103 ms
- Deep fail-safe (DFS) function is enabled (SELECT pin connected to ground)

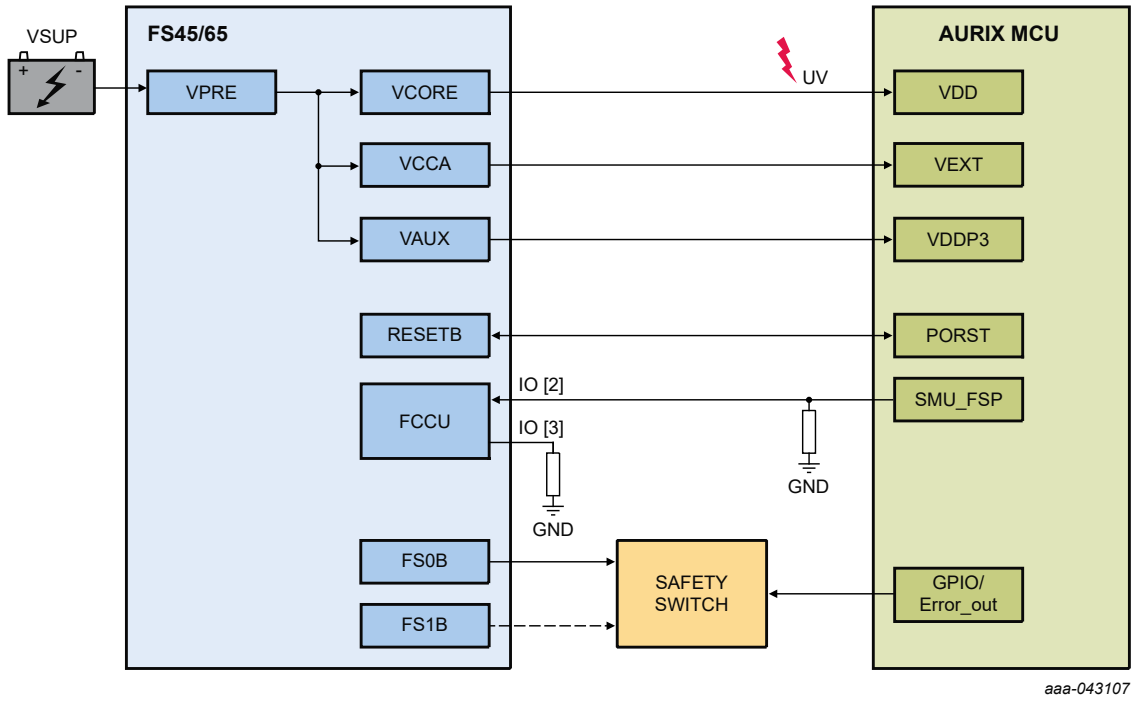


Figure 25. VCORE UV fault simplified schematic

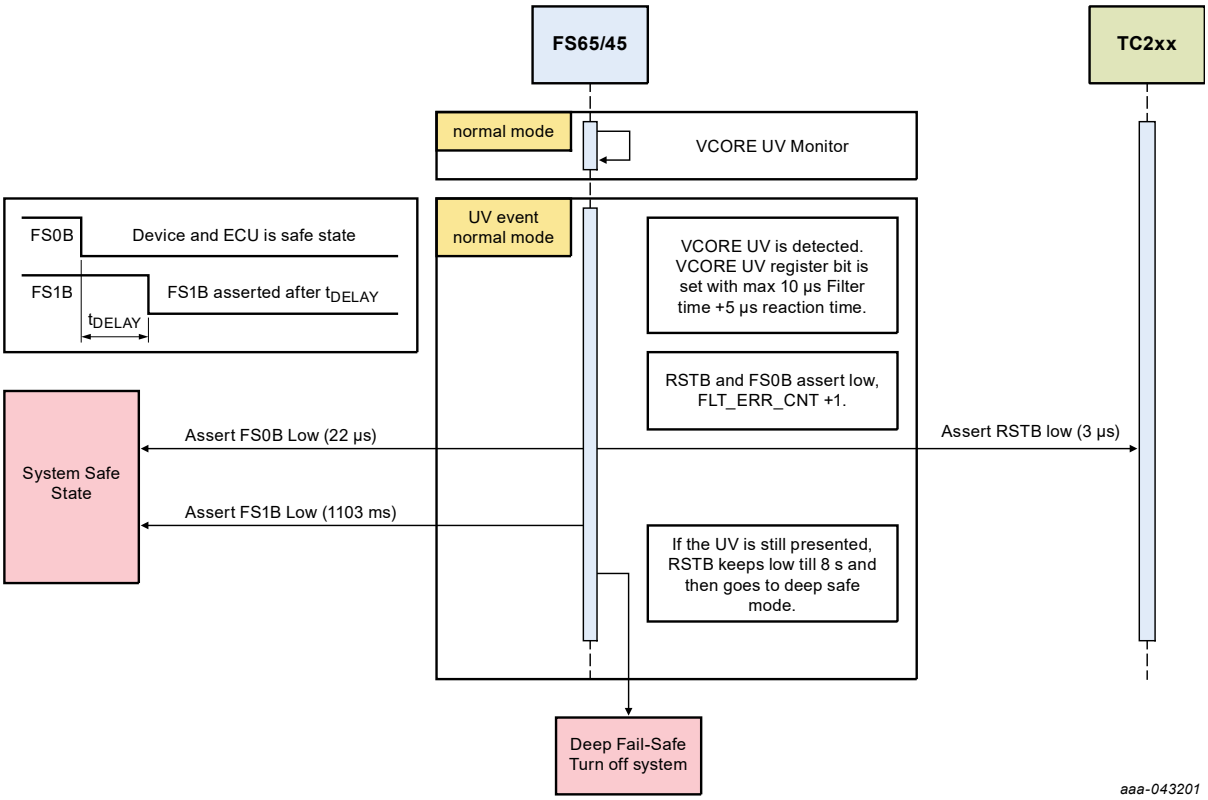


Figure 26. VCORE UV fault management sequence diagram (to DFS)

1. FS65/FS45 VCORE is internally monitored in Normal mode

2. UV event occurs on VCORE; FS65/FS45 triggers a VCORE UV fault with max 10 µs filter time + 5 µs reaction time; FS65/FS45 increments its fault error counter to 1
3. FS65/FS45 asserts RSTB and FS0B LOW according to VCORE_FS_UV_1:0
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms
5. If the UV condition is continually presented, RSTB stays LOW
6. If RSTB stays low for 8 s, FS65/FS45 goes to Deep Fail-safe mode

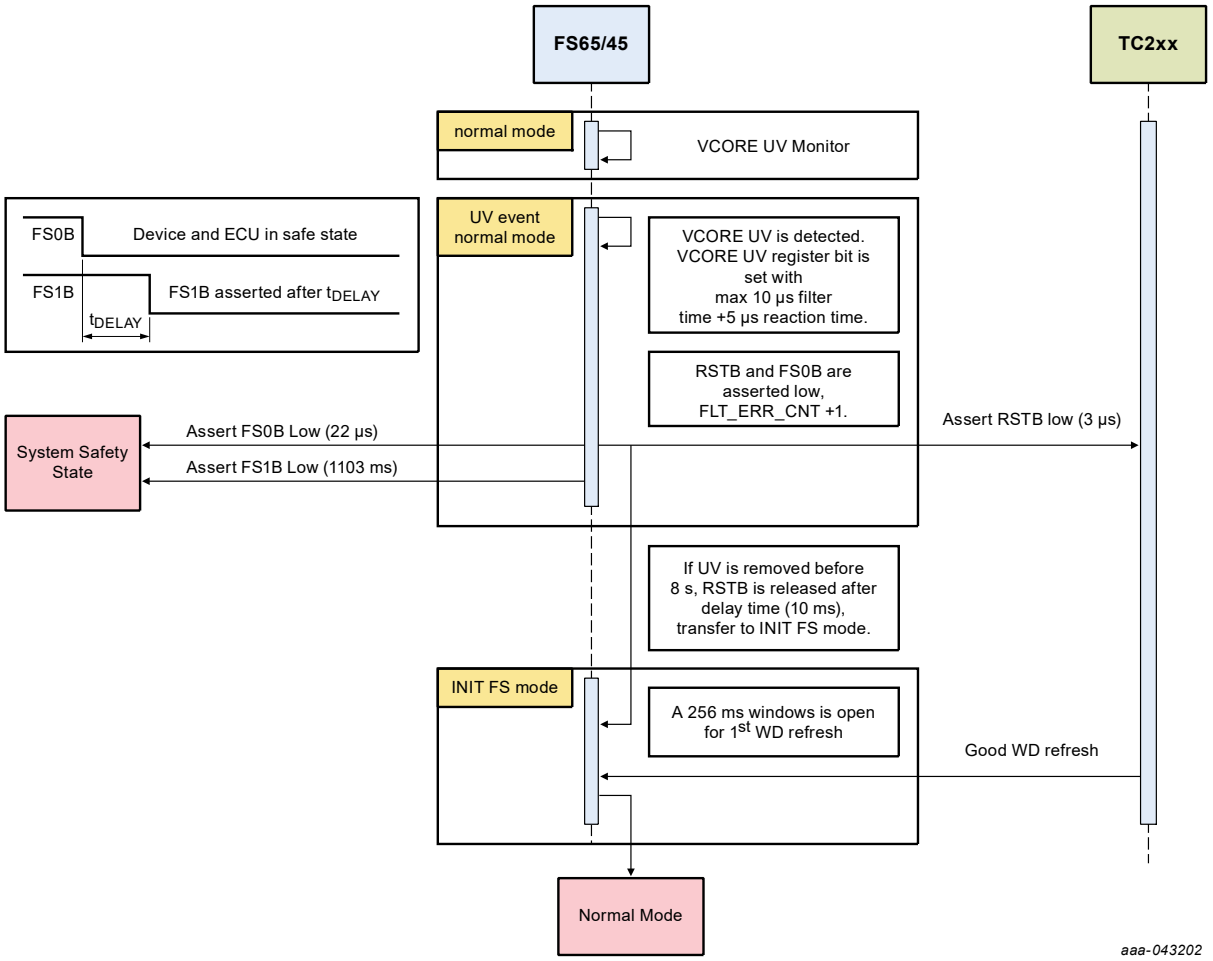


Figure 27. VCORE UV fault management sequence diagram (to recovery)

1. FS65/FS45 VCORE is internally monitored in Normal mode.
2. UV event occurs on VCORE. FS65/FS45 triggers a VCORE UV fault with max 10 µs filter time + 5 µs reaction time. FS65/FS45 increments its fault error counter to 1.
3. FS65/FS45 asserts RSTB and FS0B LOW according to VCORE_FS_UV_1:0.
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms.
5. If the UV condition is removed before 8 s, after 10 ms delay time, RSTB is released. FS65/FS45 transfers to INIT FS mode and opens a 256 ms window for new WD refresh from AURIX.
6. FS65/FS45 returns to Normal mode as a result of a good WD refresh. As a result of successive good WD refreshes, FLT_ERR_CNT decrements to 0.

3.7.3 AURIX TC2xx/TC3xx watchdog fault

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- WD_WINDOW_3:0 = 0011, WD window is set to 6 ms with 50 % duty cycle
- WD_IMPACT_1:0 = 10, FS0B only is asserted LOW if WD error counter = WD_CNT_ERR[1:0]
- WD_CNT_ERR_1:0 = 00, max value of WD error counter is set to 6
- RSTB_DURATION = 0 (default value), set to configure the RSTB LOW duration time to 10 ms
- FS65/FS45 FLT_ERR_FS = 0, to set the counter intermediate value to 3 and maximum limit to 6
- FLT_ERR_IMP_1:0 = 10, RSTB is asserted LOW if FLT_ERR_CNT ≥ intermediate value and WD error counter = WD_CNT_ERR[1:0]
- TDLY_TDUR = 0, set the FS1B in T_{DELAY} mode
- FS1B_TIME_3:0 = 1011, FS1B_TIME_RANGE = 1, set the T_{DELAY} = 1103 ms
- DFS function is enabled (SELECT pin connected to ground)

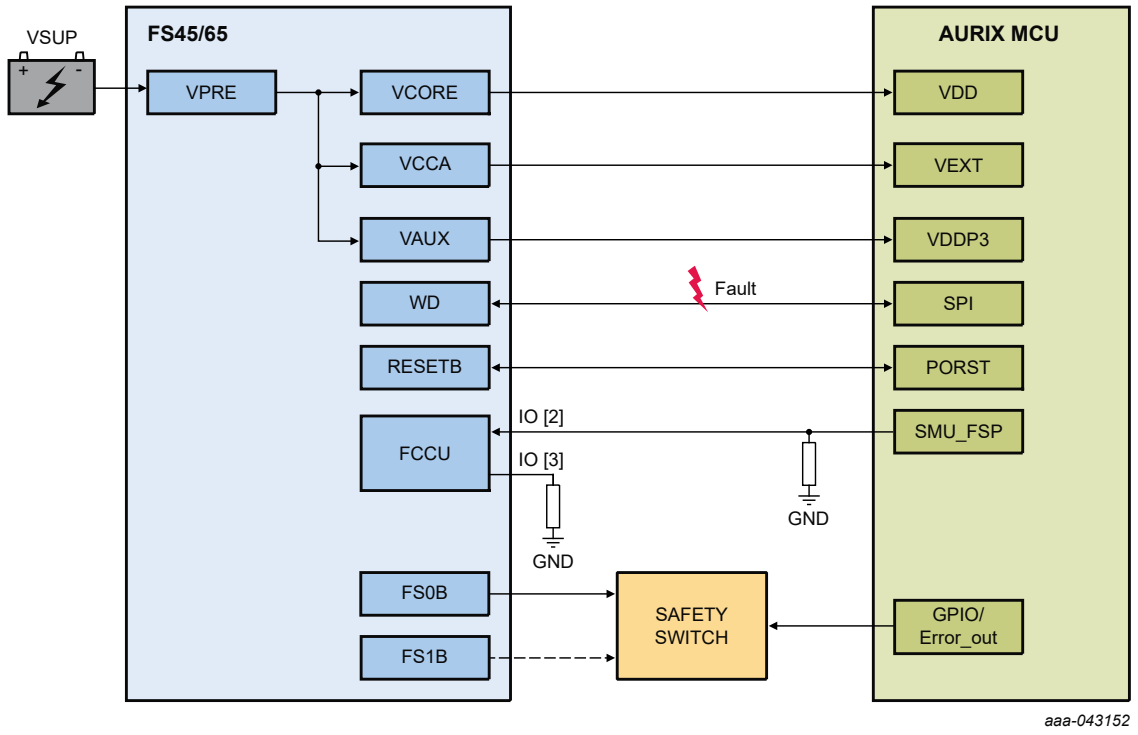


Figure 28. WD fault simple schematic

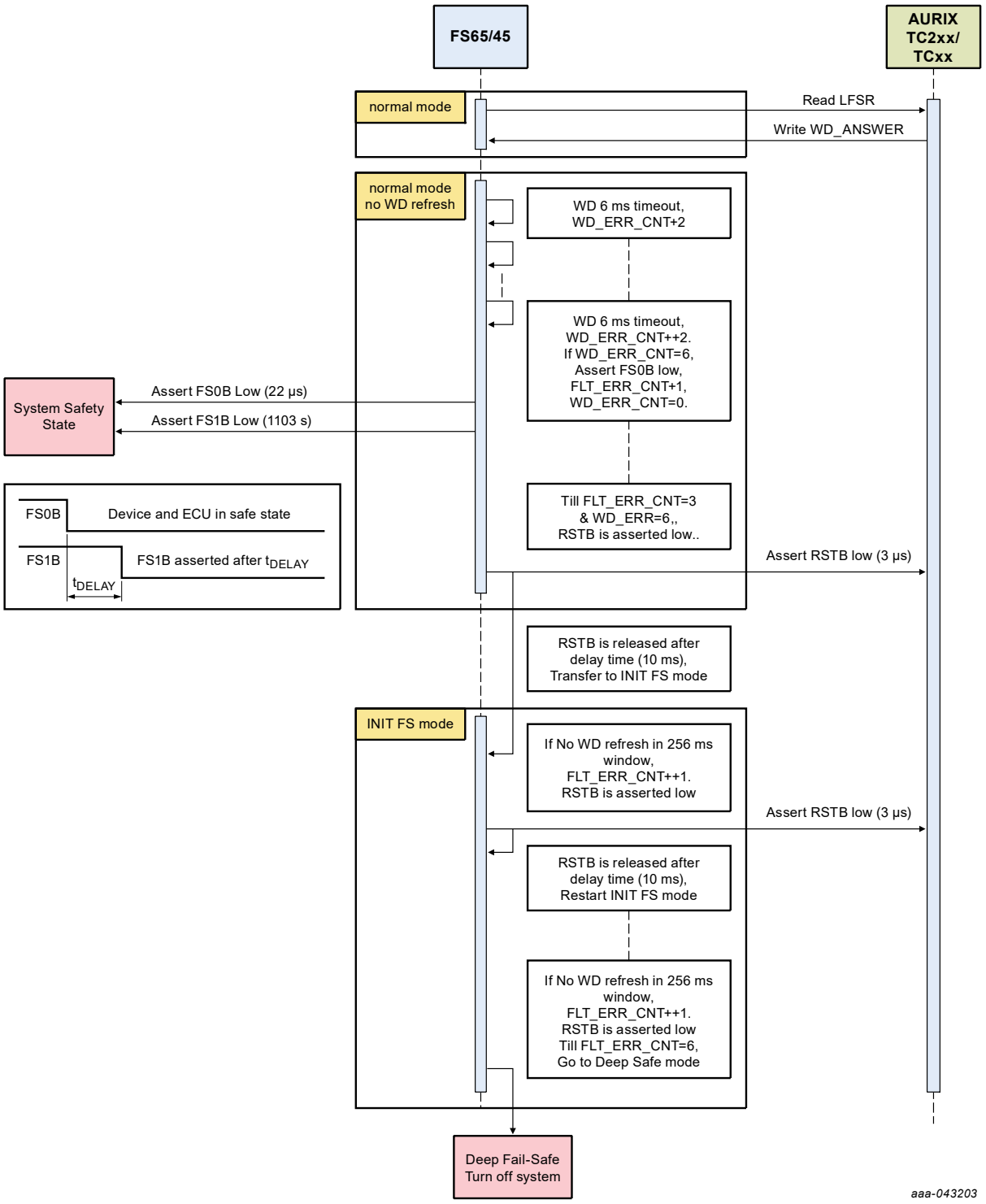


Figure 29. WD fault management sequence (to DFS)

1. FS65/FS45 window WD opens a 6 ms window with 50 % duty cycle in Normal mode .
2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2 .
3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2;.

4. When the WD_ERR_CNT = 6, FS0B is asserted LOW according to the WD_IMPACT_1:0 and WD_CNT_ERR_1:0 configuration, and FLT_ERR_CNT increment to 1;.
5. WD_ERR_CNT is set back to 0 .
6. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_CNT_ERR = 6, RSTB and FS0B are asserted LOW
7. FS65/FS45 asserts FS1B LOW following FS0B status after a 1103 ms delay .
8. AURIX MCU is reset .
9. After a 10 ms delay time, RSTB is released. FS65/FS45 transfers to INIT_FS mode, opens a 256 ms window and waits for a new WD refresh from the AURIX MCU.
10. In the absence of a good WD refresh, FLT_ERR_CNT is incremented and RSTB is asserted LOW again.
11. In the absence of a good WD refresh, the device loops from step 9 to step 10 until FLT_ERR_CNT = 6 (max value). FS65/FS45 then goes to DFS mode.

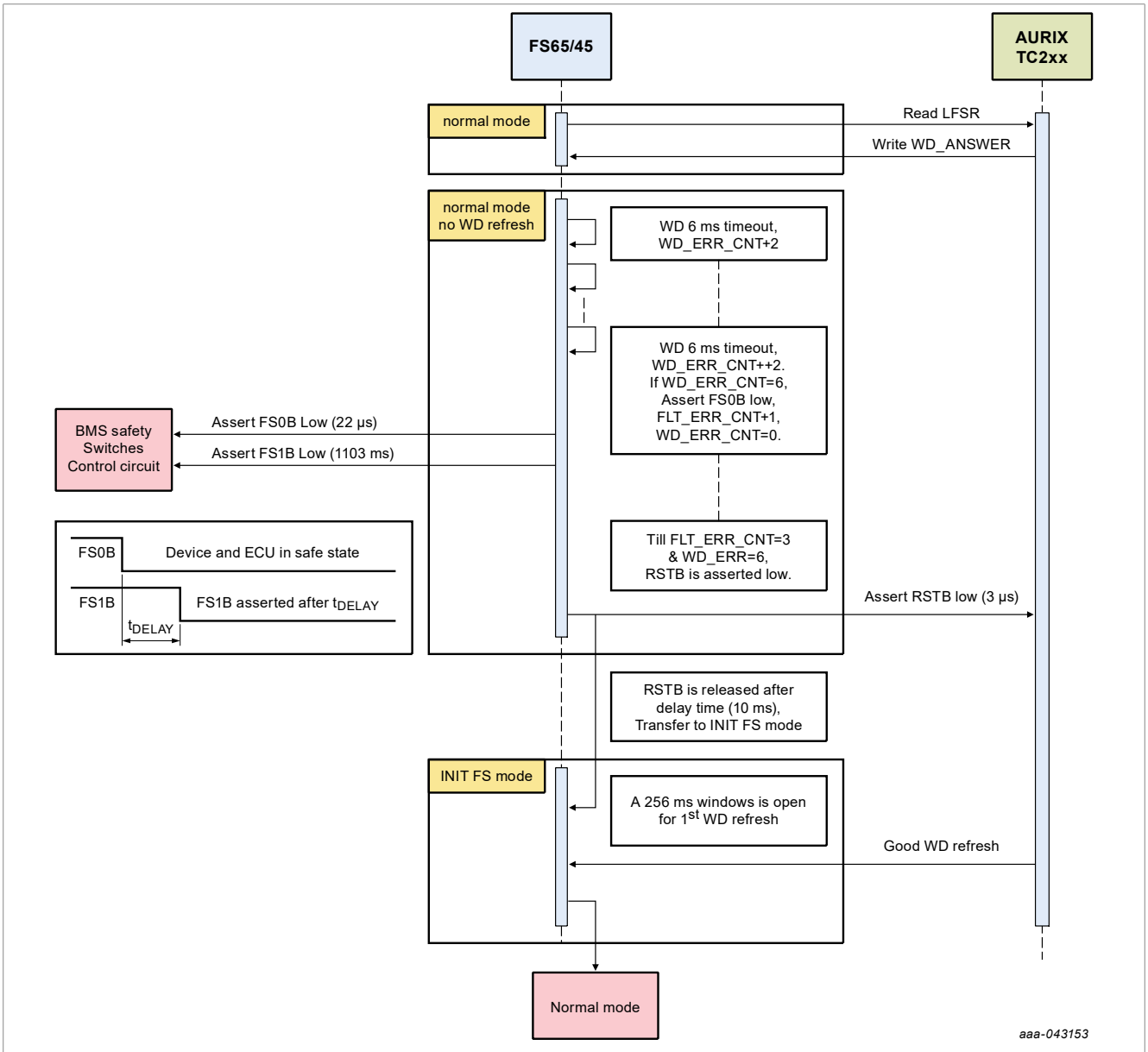


Figure 30. WD fault management sequence (to recovery)

1. FS65/FS45 window WD opens a 6 ms window with 50 % duty cycle in Normal mode
2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2;'.
3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2.
4. When the WD_ERR_CNT = 6, FS0B is asserted LOW according to WD_IMPACT_1:0 and WD_CNT_ERR_1:0 configuration and FLT_ERR_CNT increments to 1.
5. WD_ERR_CNT is set back to 0;.
6. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_CNT_ERR = 6, RSTB and FS0B are asserted LOW;.
7. FS65/FS45 asserts FS1B LOW following FS0B status after a 1103 ms delay;.
8. AURIX MCU is reset.
9. After a 10 ms delay time, RSTB is released. FS65/FS45 transfers to INIT_FS mode, opens a 256 ms window and waits for a new WD refresh from the AURIX MCU.
10. The WD handshake is recovered between FS65/FS45 and AURIX MCU. FS65/FS45 returns to Normal mode as a result of a good WD refresh. Due to successive good WD refreshes, FLT_ERR_CNT decrements to 0.

3.7.4 AURIX TC2xx/TC3xx FCCU fault

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- IO_23_FS = 1 (default value), set to configure the couple of IO_3:2 as safety inputs for FCCU monitoring
- FS65/FS45 FLT_ERR_FS = 0, to set counter intermediate value to 3 and maximum limit to 6
- FS65/FS45 PS = 0, FCCU_eaout_1:0 active HIGH
- FLT_ERR_IMP_1:0 = 11, FS0B and RSTB are asserted LOW if FLT_ERR_CNT ≥ intermediate value
- TDLY_TDUR = 0, set the FS1B in T_{DELAY} mode
- FS1B_TIME_3:0 = 1011, FS1B_TIME_RANGE = 1, set the T_{DELAY} = 1103 ms
- DFS function is enabled (SELECT pin connected to ground)

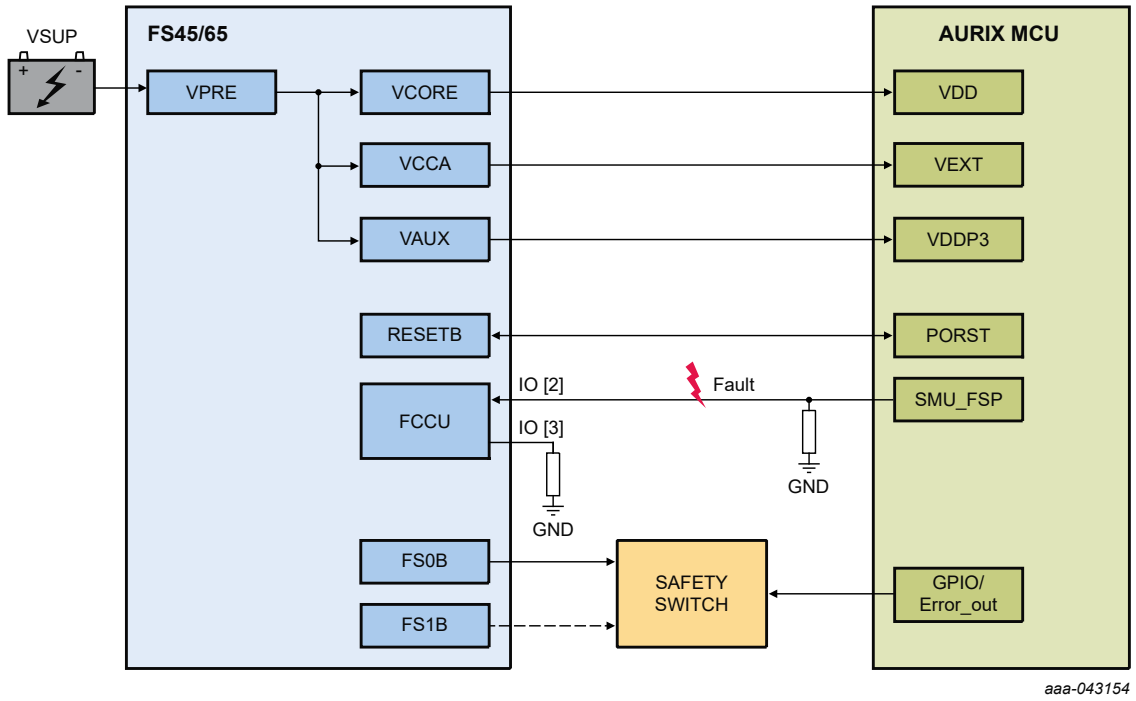


Figure 31. FCCU fault management simple schematic

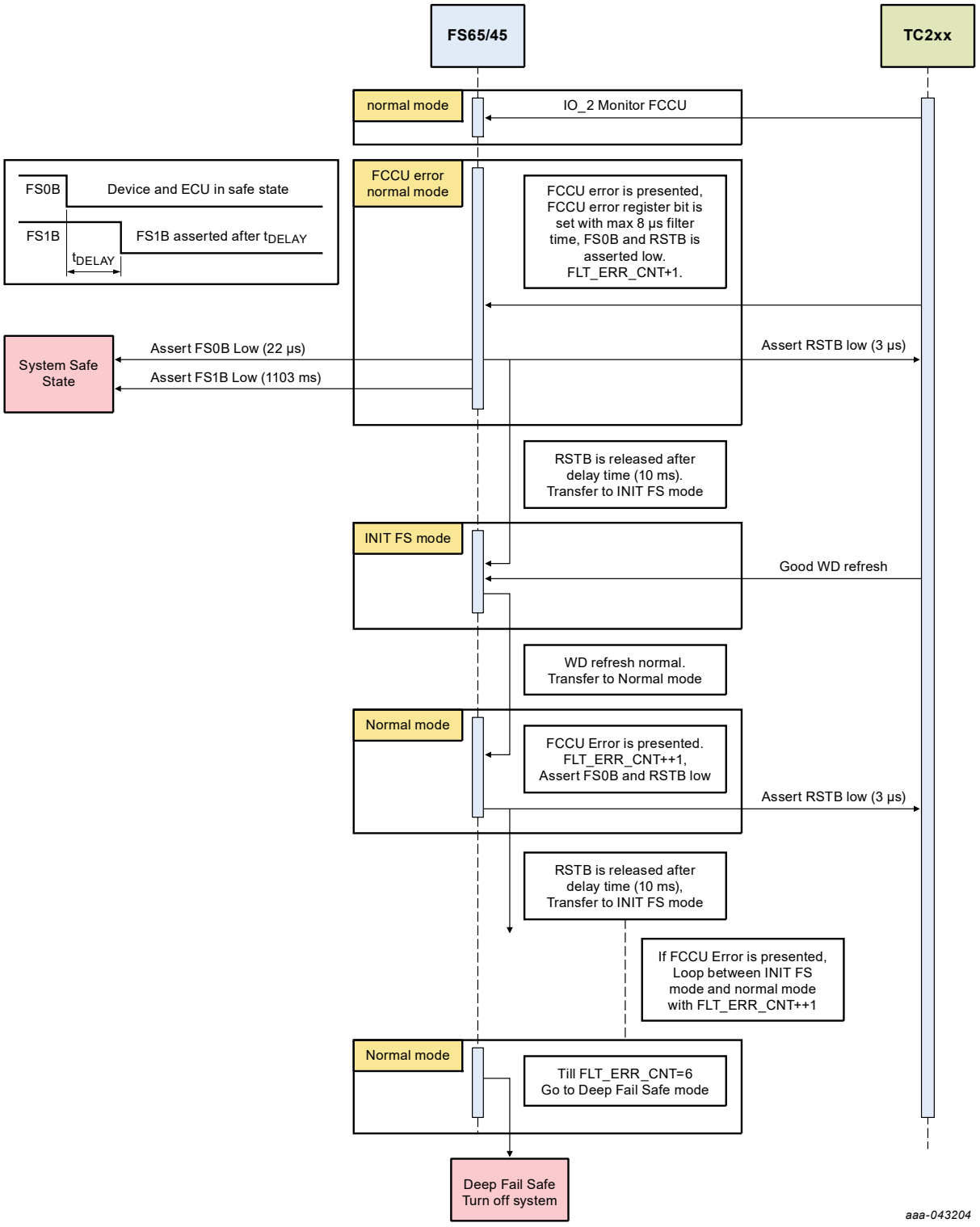


Figure 32. FCCU fault management sequence diagram (to DFS)

1. FS65/FS45 is using IO_23 to monitor AURIX FCCU in Normal mode.
2. FCCU error occurs on IO_23; FS65/FS45 triggers an FCCU fault with max 8 µs filter time; FS65/FS45 increments FLT_ERR_CNT by one.

3. FS65/FS45 asserts RSTB and FS0B LOW according to FLT_ERR_FS configuration.
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms.
5. AURIX MCU is reset.
6. After a 10 ms delay, RSTB is released. FS65/FS45 is transferred to INIT_FS mode and opens a 256 ms window for new WD refresh from AURIX.
7. A good WD refresh is sent from AURIX and FS65/FS45 is transferred to Normal mode.
8. If an FCCU error is still presented, the device loops from step 2 to step 7 until FST_ERR_CNT = 6 (counter final value). Then FS65/FS45 goes to DFS mode.

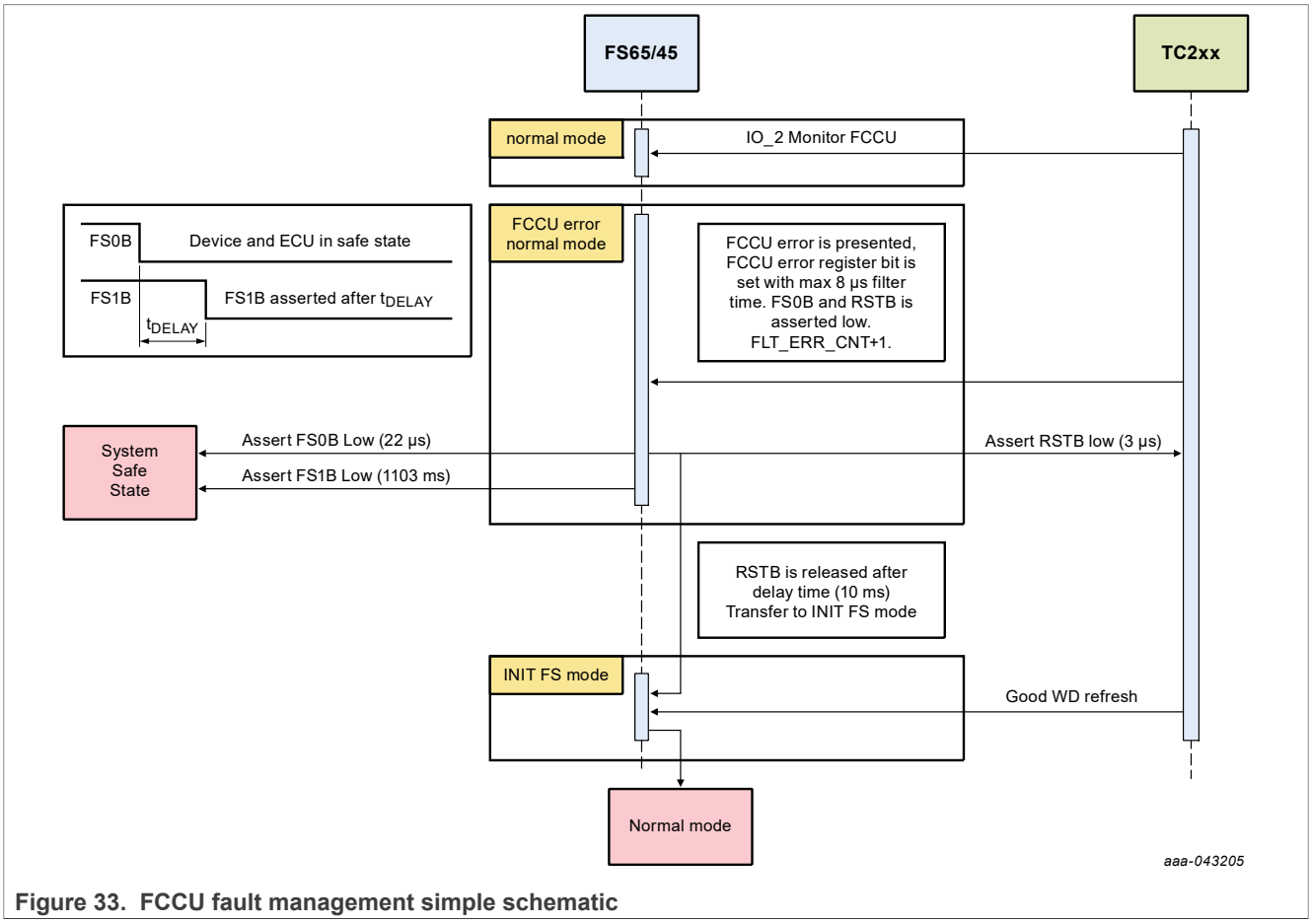


Figure 33. FCCU fault management simple schematic

1. FS65/FS45 is using IO_23 to monitor AURIX FCCU in Normal mode.
2. An FCCU error occurs on IO_23. FS65/FS45 triggers an FCCU fault with max 8 µs filter time; FS65/FS45 increments FLT_ERR_CNT by one.
3. FS65/FS45 asserts RSTB and FS0B LOW according to FLT_ERR_FS configuration.
4. FS65/FS45 asserts FS1B LOW to follow FS0B status after 1103 ms;.
5. AURIX MCU is reset.
6. After a 10 ms delay time, RSTB is released; FS65/FS45 is transferred to INIT_FS mode and a 256 ms window opens for new WD refresh from AURIX.
7. A good WD refresh is sent from AURIX and FS65/FS45 is transferred to Normal mode.
8. FS65/FS45 comes back to Normal mode due to good WD refreshes. If an FCCU error is not presented, and good WD refreshes continue to be received, FLT_ERR_CNT decrements to 0.

3.7.5 Other recovery

When a fault occurs, both fail-safe outputs FS0B and FS1B are asserted LOW. Thereafter, some conditions must be fulfilled before allowing the device to release these pins again. These conditions are:

- ABIST2_FS1B_OK = 1 if part number with FS1B
- ABIST2_VAUX_OK = 1, except if VAUX_FS_OV_1:0 = VAUX_FS_UV_1:0 = 00
- Fault is removed
- Fault error counter must be at 0
- Close the S1 switch if FS1B backup delay was engaged (FS1B_DLY_DRV bit = 1)
- RELEASE_FSxB register must be filled with the right value

When the device is in DFS state, all the regulators are off (except VKAM if VKAM was on), and RSTB, FS0B, and FS1B are activated. To exit this state, a key-off/key-on action is needed. IO_0 is typically connected to a key signal. Key off (IO_0 LOW) moves the device to LPOFF-deep FS, and key on (IO_0 HIGH) wakes up the device.

4 FS26 solution

4.1 Product overview

The FS26 is a family of automotive safety SBC devices with multiple power supplies designed to support entry- and mid-range safety microcontrollers like the S32K3 series, while maintaining flexibility to work with other microcontrollers. Targets include automotive electrification, such as power train, chassis, safety and low-end gateway applications.

The FS26 features multiple switch mode regulators, as well as LDO voltage regulators to supply the microcontroller, sensors, peripheral ICs, and communication interfaces. It offers a high-precision voltage reference available to the system as well as reference voltages for two independent voltage tracking regulators. The FS26 also offers various functionalities for system control and diagnostics, including as an analog multiplexer, GPIOs and selectable wake-up events from I/O, long duration timer, or SPI communication.

The FS26 is developed in compliance with the ISO 26262 standard. It includes enhanced safety features with multiple fail-safe outputs, and can be part of a safety-oriented system partitioning covering both ASIL B and ASIL D safety integrity levels, with the latest on-demand latent fault monitoring.

4.1.1 Documentation references

- **FS26 device webpage**
- **Secure Files webpage**

Through the Secure Files webpage, various materials are available regarding the FS26 family that can be used to access more detailed information about specific topics:

- **FS26 data sheet**: information such as features, functional description, parametric description, register mapping
- **FS26 functional safety manual (ASIL B and ASIL D)**: describes how to use the FS26 in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level
- **AN12995**: information such as application schematics, bill of materials, placement and layout guidelines, and application validation data (ISO/non-ISO pulses and EMC)
- **Recommended OTP configurations**: MFS2621HMDABAD (AURIX TC38x, TC29x), SFS2623HMDF5AD (TC377 for BMS application), SFS2631HMDDYAD (TC387 for inverter application), SFS2631HMDEXAD (TC387 for DC/DC application), SFS2633HMDDZAD (TC377 for inverter application).

4.1.2 Typical block diagram

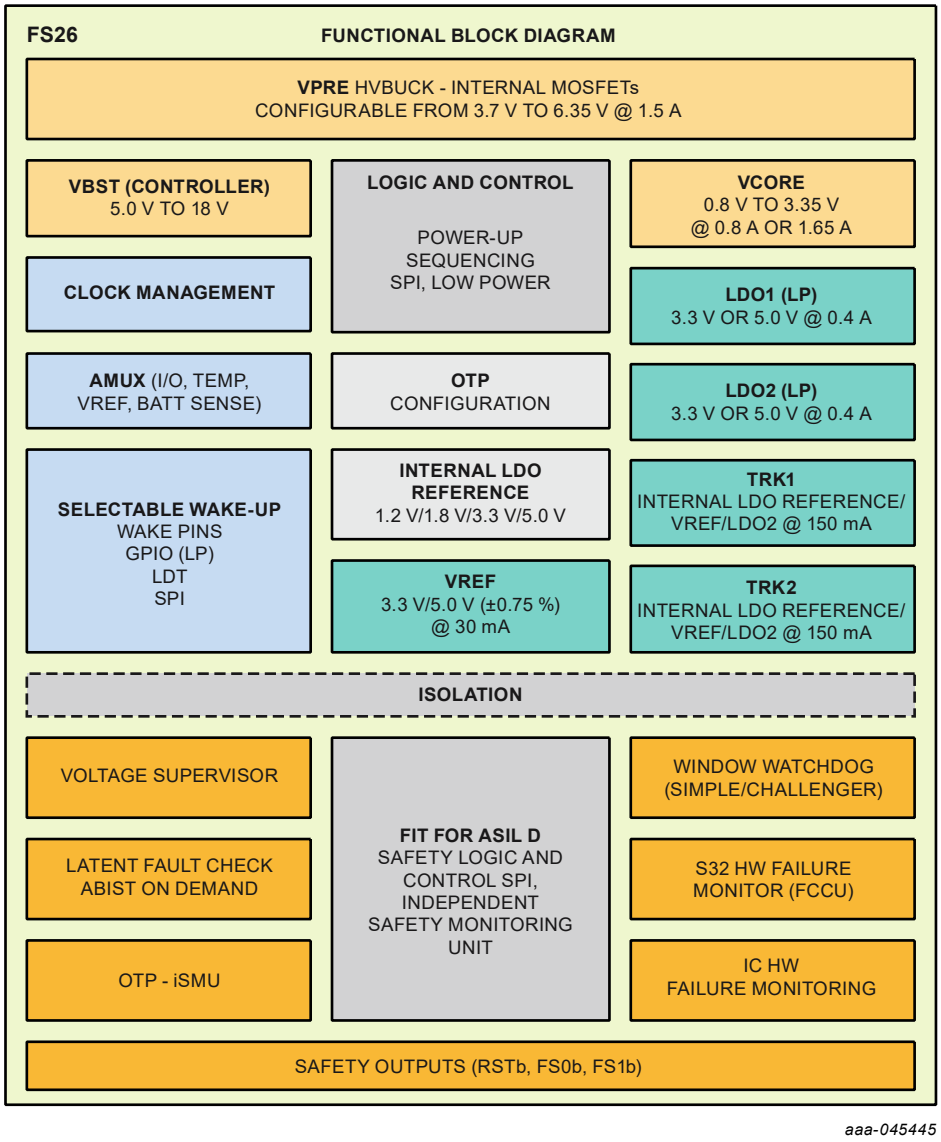


Figure 34. FS26 functional block diagram

4.1.3 Key features

The FS26 device presents various types of power management blocks, with an independent safety island for supporting ASIL B or ASIL D applications.

Below is a summary of the different power management blocks:

- 40 V DC maximum input voltage
- Supports operating voltage range down to battery 3.2 V with VBST
- Supports operating voltage range down to battery 6 V without VBST
- Low-power Off mode with 30 µA quiescent current
- Low-power Standby mode with 29 µA quiescent current, with VPRE active. LDO1 or LDO2 activation selectable via one-time programmable (OTP) configuration. GPIO1 or GPIO2 activation selectable via SPI communication.

- VPRE: Synchronous buck converter with integrated FETs. Configurable output voltage and switching frequency, output DC current capability up to 1.5 A and pulse frequency modulation (PFM) mode for Low-power Standby mode operation.
- VCORE: Synchronous buck converter with integrated FETs. VCORE is dedicated for microcontroller core supply. Output DC current up to 0.8 A or 1.65 A (depending on part number), output voltage range setting from 0.8 V to 3.35 V.
- VBST: Asynchronous boost controller with external low-side switch, diode, and current sense resistor. VBST is configurable as front-end supply to withstand low voltage cranking profiles or in back-end supply with configurable output voltage and scalable output DC current capability.
- LDO1: LDO regulator for microcontroller I/O support with selectable output voltage between 3.3 V and 5.0 V and up to 400 mA current capability
- LDO2: LDO regulator for system peripheral support with selectable output voltage between 3.3 V and 5.0 V and up to 400 mA current capability
- VREF: High-precision reference voltage with 0.75 % accuracy for external ADC reference and internal tracking reference
- TRK1 and TRK2: Voltage tracking regulators with selectable output voltage between VREF, LDO2, or internal LDO reference. Support for high-voltage protection for electronic control unit (ECU) off-board operation. Each tracker has a current capability up to 150 mA.

The device also presents system features such as:

- Two wake-up inputs with high-voltage support for system robustness
- Two programmable GPIOs with wake-up capability or HS/LS driver
- Programmable LDT for system shutdown and wake-up control
- Monitoring of system voltages (including battery voltage monitoring) through the analog multiplexer
- Selectable wake-up sources from: WAKE/GPIO pins, LDT, or SPI activity
- Device control via 32-bit SPI interface with cyclic redundancy checks (CRC)

The FS26 also provides functional safety:

- Scalable portfolio from ASIL B to D
- Independent monitoring circuitry, dedicated interface for microcontroller monitoring, simple or challenger watchdog function
- Analog built-in self-test (ABIST) and logic built-in self-test (LBIST) at start up
- Analog built-in self-test (ABIST) on-demand
- Safety outputs with latent fault detection mechanism (RSTB, FS0B, FS1B)

Compliance:

- Electromagnetic compatibility (EMC) optimization techniques for switching regulators including spread spectrum, slew rate control, and manual frequency tuning
- Electromagnetic interference (EMI) robustness supporting various automotive EMI test standards

4.2 Safety management with AURIX MCU

To fulfill the safety-critical applications, a dedicated Fail-safe machine (FSM) is provided. The FSM is composed of three main sub-blocks:

- Voltage supervisors
- Reset output;
- Two HW SoC monitoring pins (FCCU) inputs for NXP and non-NXP MCU monitoring
- Fail-safe output driver (FSO)
- Built-in self-test (BIST)

The FSM is independent from the rest of the circuitry to avoid common-cause failures. The FSM has its own voltage regulators (analog and digital), dedicated bandgap, and oscillator. This block is physically independent from the rest of the circuitry, due to dedicated layout placement and trench isolation.

4.2.1 Safety outputs

In normal operation, when FS0B (and FS1B if used) and RSTB are released, the fault error counter is incremented when a fault is detected by the FS26 Fail-safe state machine.

Table 11 lists the faults and their impacts on RSTB, FS0B, and FS1B pins, according to the device configuration. The faults that are configured to not assert RSTB and FS0B (and FS1B if used) will not increment the fault error counter. In that case, only the flags are available for MCU diagnostics. When FS0B is asserted, the fault error counter continues to be incremented by +1 each time the WD error counter reaches its maximum value. Refer to the safety manual for more details on the safety implementation.

Table 11. Application-related fail-safe fault list and reactions

Apps relate fail-safe faults	Fault error counter update	FS0B assertion [1][2]	RSTB assertion[1][2]
VPRE power rail overvoltage	+1	VMON_PRE_OV_FS_REACTION[0]	VMON_PRE_OV_FS_REACTION[1]
VCORE power rail overvoltage	+1	VMON_CORE_OV_FS_REACTION[0]	VMON_CORE_OV_FS_REACTION[1]
VLDO1 power rail overvoltage	+1	VMON_LDO1_OV_FS_REACTION[0]	VMON_LDO1_OV_FS_REACTION[1]
VLDO2 power rail overvoltage	+1	VMON_LDO2_OV_FS_REACTION[0]	VMON_LDO2_OV_FS_REACTION[1]
VTRK1 power rail overvoltage	+1	VMON_TRK1_OV_FS_REACTION[0]	VMON_TRK1_OV_FS_REACTION[1]
VTRK2 power rail overvoltage	+1	VMON_TRK2_OV_FS_REACTION[0]	VMON_TRK2_OV_FS_REACTION[1]
VREF power rail overvoltage	+1	VMON_VREF_OV_FS_REACTION[0]	VMON_VREF_OV_FS_REACTION[1]
Overvoltage on the analog input monitoring	+1	VMON_EXT_OV_FS_REACTION[0]	VMON_EXT_OV_FS_REACTION[1]
VPRE power rail undervoltage	+1	VMON_PRE_UV_FS_REACTION[0]	VMON_PRE_UV_FS_REACTION[1]
VCORE power rail undervoltage	+1	VMON_CORE_UV_FS_REACTION[0]	VMON_CORE_UV_FS_REACTION[1]
VLDO1 power rail undervoltage	+1	VMON_LDO1_UV_FS_REACTION[0]	VMON_LDO1_UV_FS_REACTION[1]
VLDO2 power rail undervoltage	+1	VMON_LDO2_UV_FS_REACTION[0]	VMON_LDO2_UV_FS_REACTION[1] ERRMON_FS_REACTION[1]
VTRK1 power rail undervoltage	+1	VMON_TRK1_UV_FS_REACTION[0]	VMON_TRK1_UV_FS_REACTION[1]
VTRK2 power rail undervoltage	+1	VMON_TRK2_UV_FS_REACTION[0]	VMON_TRK2_UV_FS_REACTION[1]

Table 11. Application-related fail-safe fault list and reactions*...continued*

Apps relate fail-safe faults	Fault error counter update	FS0B assertion [1][2]	RSTB assertion[1][2]
Undervoltage on the analog input monitoring	+1	VMON_EXT_UV_FS_REACTION[0]	VMON_EXT_UV_FS_REACTION[1]
An error is sent by the MCU on FCCU1 and FCCU2 pins (dual wire protocol)	+1	FCCU12_FS_REACTION[0]	FCCU12_FS_REACTION[1]
An error is sent by the MCU on FCCU1 pin (single wire protocol)	+1	FCCU1_FS_REACTION[0]	FCCU1_FS_REACTION[0]
An error is sent by the MCU on FCCU2 pin (single wire protocol)	+1	FCCU2_FS_REACTION[0]	FCCU2_FS_REACTION[0]
nAn external IC is driving the signal connected on the ERRMON pin to the error state.	+1	ERRMON_FS_REACTION[0]	ERRMON_FS_REACTION[1]
Watchdog error counter reaches its maximum value (WD_ERR_CNT = WD_ERR_LIMIT)	+1	WD_FS_REACTION[0]	WD_FS_REACTION[0]
The fault error counter reaches its intermediate value: (WD_ERR_LIMIT)/2	none	FLT_ERR_REACTION[0]	FLT_ERR_REACTION[1]
Wrong WD refresh in INIT_FS state	+1	yes	yes
No WD refresh in INIT_FS	+1	yes	yes
RESET pin asserted externally	+1	yes	yes (low externally)
RSTB pulse request by MCU	no	no	yes
RSTB short to high	+1	yes	no (high externally)
FS0B short to high	+1	no (high externally)	BACKUP_SAFETY_PATH_FS0B[0]
FS0B request by the MCU	no	yes	no
FS1B short to high	+1	no (high externally)	BACKUP_SAFETY_PATH_FS1B[0]
FS1B request by the MCU	no	yes	no
REG_CORRUPT = 1	+1	yes	no
OTP_CORRUPT = 1	+1	yes	no

[1] In orange, the reaction is not configurable.
[2] In green, the reaction is configurable by OTP for and by SPI only during the INIT_FS phase.

Table 11 shows the mapping between the NXP Safety SBC and the Aurix family for the use case when the VCORE regulator of the SBC is used to supply the VDD core voltage of the respective Aurix MCU directly, without using the EVR of the Aurix MCU.

For the use case where the EVR of the AURIX MCU is used (see Figure 1 and Figure 2), an SBC with lower VCORE current capability can be used to supply the MCU with a 5 V or 3.3 V power supply. The system integrator is responsible for the correct dimensioning of the SBC, depending on MCU power consumption for the selected application use case, the additional loads on the VCORE rail, and temperature conditions.

4.2.2 Watchdog

The FS26 acts as a supervisor of the application operation, and as a consequence, includes a windowed watchdog (temporal and logical monitoring) that needs to be refreshed periodically by the MCU. This means that the FS26 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 a safe state system within the FTTI. Thus, either the MCU or the SBC can switch the system to a safe state.

The duration of the watchdog window is configurable to allow different MCU handshake strategies. The duty cycle of the window is configurable from 31.25 % to 68.75 % (50 % by default) with the WDW_DC[2:0] bits. The first part of the window is said to be closed and the second is said to be open. The watchdog must be refreshed during the open window (see Figure 35).

After a good or a bad watchdog refresh, a new window period starts immediately in order for the MCU to remain synchronized with the windowed watchdog. The first good watchdog refresh closes the INIT_FS. Then the watchdog window is running and the MCU must refresh the watchdog in the open window of the watchdog window period. The duration of the watchdog window is configurable from 1.0 ms to 1024 ms with the WDW_PERIOD[3:0] bits. The new watchdog window is effective after the next watchdog refresh. The watchdog window can be disabled only during INIT_FS. The watchdog disablement is effective when the INIT_FS is closed.

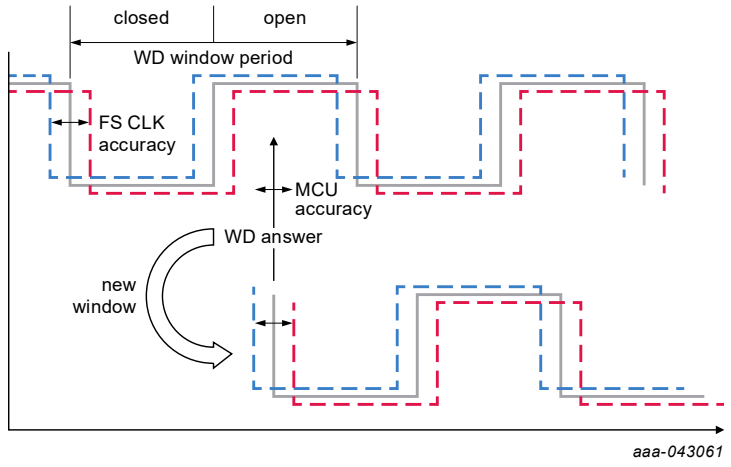


Figure 35. Windowed watchdog

4.2.3 HW SoC monitoring (FCCU)

The FCCU monitoring feature is available for FS26xyD devices (ASIL D) but also for FS26xyB derivatives (optional). The FCCU input pins are in charge of monitoring HW failures from the MCU. They can be configured by pair, as single independent inputs, or as monitoring a PWM signal on one pin, or both. The FCCU monitoring is active as soon as the initialization phase is closed (exit of INIT_FS state) by the first good watchdog refresh.

When connected to the AURIX MCU, the FCCU input pins can be configured as shown in Figure 36 to work in PWM mode with the AURIX SMU. The frequency range in this case should be between 10 kHz and 45 kHz. The FCCU input pins should be set with the FCCU_CFG[2:0] bits in PWM mode, either using FCCU1 only, FCCU2 only or both (when monitoring two AURIX MCUs, for instance):

- FCCU_CFG[2:0] = 101, PWM monitoring enabled on FCCU1 and FCCU2 pins

- FCCU_CFG[2:0] = 110, PWM monitoring enabled on FCCU1 pin and level monitoring only on FCCU2
- FCCU_CFG[2:0] = 111, PWM monitoring enabled on FCCU2 pin and level monitoring only on FCCU1

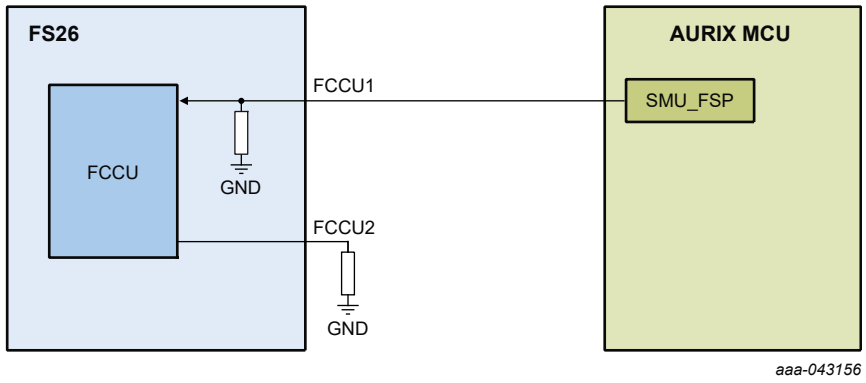


Figure 36. FCCU connection to AURIX SMU in PWM mode – FCCU_CFG = 110

With the FCCU default polarity configuration, a pulldown must be connected externally to FCCU2, forcing the pin into a safe state. FCCU1, though, has an integrated pulldown resistor providing a passive fault detection in case the MCU does not drive its SMU_FSP (fault signaling protocol) output pin.

In time-monitoring mode (PWM), FCCU12_FILT OTP setting does not apply. When the SMU_FSP signal frequency drifts below 5 kHz (F_{FCCU12_BLF}) or above 90 kHz (F_{FCCU12_BHF}), the FS2600 assumes that the MCU has an internal error. The reaction on safety outputs can also be configured by the FCCU1_FS_REACTION or FCCU2_FS_REACTION SPI bit during the initialization phase. SPI bit descriptions in this section are valid only if FCCU_CFG[2:0] ≠ 00 or 01.

Assuming FCCU1 and FCCU2 are connected as shown in Figure 36, below are the steps for enabling FCCU with the AURIX SMU:

1. At start-up, the FS2600 proceeds to a latent failure check (LBIST) to verify the correct functionality of the safety logic monitoring, including FCCU block.
2. During INIT_FS phase, configure the FS2600 device using the FCCU_CFG[2:0], FCCU1_FS_REACTION and/or FCCU2_FS_REACTION bits.
3. Configure the AURIX SMU in PWM mode.
4. FCCU/SMU function is checked and operational.

The timing diagram in Figure 37 describes different possible phases that can happen during PWM monitoring in the application. An error is triggered because the incoming signal on the FCCU1 pin is drifting below the filtering time. This example is only valid for FCCU_CFG[2:0] = 101 and FCCUx_FS_REACTION = 1.

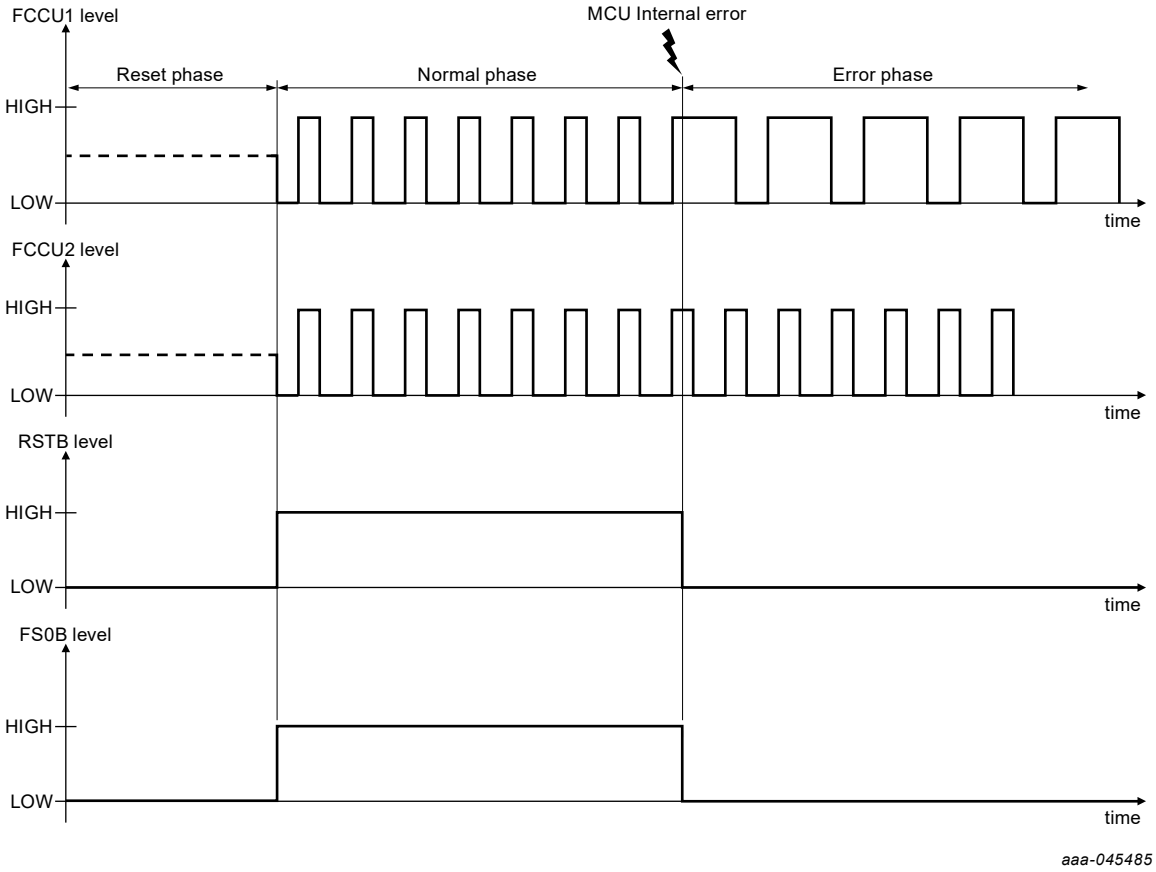


Figure 37. Dual PWM input monitoring example with two AURIX MCUs

4.2.3.1 Steady-state mode

FCCU monitoring is meant to detect any HW failures from the MCU. It is active as soon as the Fail-safe machine is in Normal_WD. In the FS45 and the FS65, a register must be configured during the initialization phase to activate the FCCU error-out monitoring: the INIT_FSSM register. In this register, the IO_23_FS bit must be set to logic 1 to configure IO[2] and IO[3] as safety critical inputs. These two I/Os are supposed to work in a bistable protocol with NXP MCUs, but are also capable of monitoring non-NXP MCUs such as AURIX TC2xx/TC3xx.

When connected to the AURIX MCU, the FCCU input pins must be configured as shown in Figure 38 to work with a single error-out pin from the AURIX safety management unit (SMU).

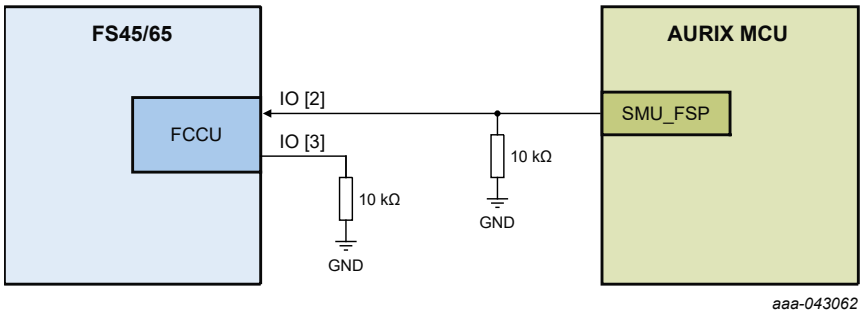


Figure 38. FCCU connection to AURIX SMU in single output fault mode

With the FCCU default polarity configuration, a pulldown must be connected to IO[2] to provide a passive fault detection in case the MCU does not drive its SMU_FSP (fault signaling protocol) output pins.

Assuming IO[2] and IO[3] are connected as shown in Figure 38, these are the steps to follow to enable the FCCU with the AURIX SMU:

1. Configure FS device: IO[2] and IO[3] as safety critical inputs
2. Configure the AURIX SMU in steady state mode
3. Proceed to a latent failure to avoid shorted pin: at INIT phase, toggle the pin and check the IO[2] flag status. The flag follows the pin status
4. FCCU/SMU function is checked and operational

4.2.3.2 PWM mode

The FS45 and the FS65 are also capable of monitoring AURIX MCU through the SMU_FSP signal in pulse-width modulation (PWM) mode (toggling signal) with some limitations. To make this possible, the system engineer must take into account the filtering time of IO[2] and IO[3], which is specified to be 4 µs < FCCU filtering time < 8 µs.

In PWM mode, FCCU must not be triggered accidentally, meaning T_{ON} and T_{OFF} timings must not last more than 4 µs each. To prevent that from happening, the minimum frequency should be 125 kHz with a maximum duty cycle of 50 %. Higher frequencies are safe to be used with a duty cycle never reaching either 0 % or 100 %.

This way, a stuck-LOW or stuck-HIGH signal on IO[2] (depending on the preset pin polarity) is detected as an error, as shown in Figure 39 (a). However, if IO[2] happens to be stuck to its non-fault state (depending on the polarity configuration), this event cannot be detected (see Figure 39 (b) and Figure 40) unless the MCU performs a latent-failure check on this pin at initialization.

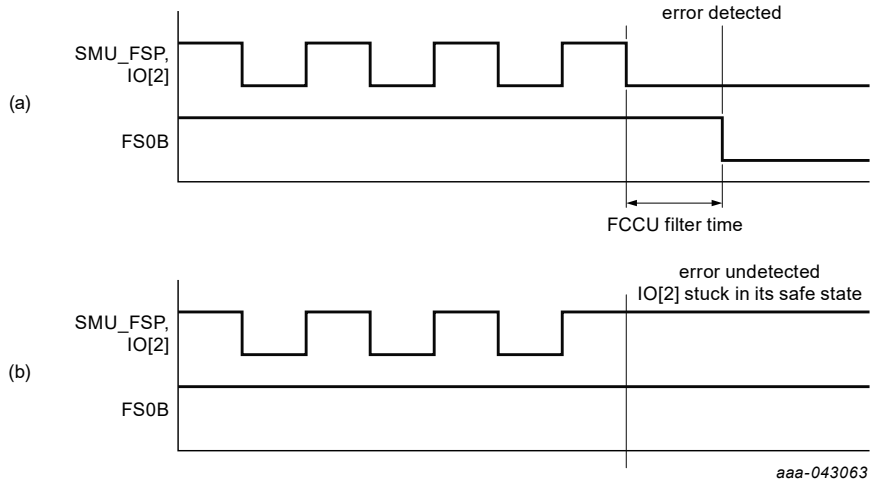


Figure 39. FCCU monitoring and error detection when SMU_FSP signal gets stuck LOW (a) or HIGH (b)

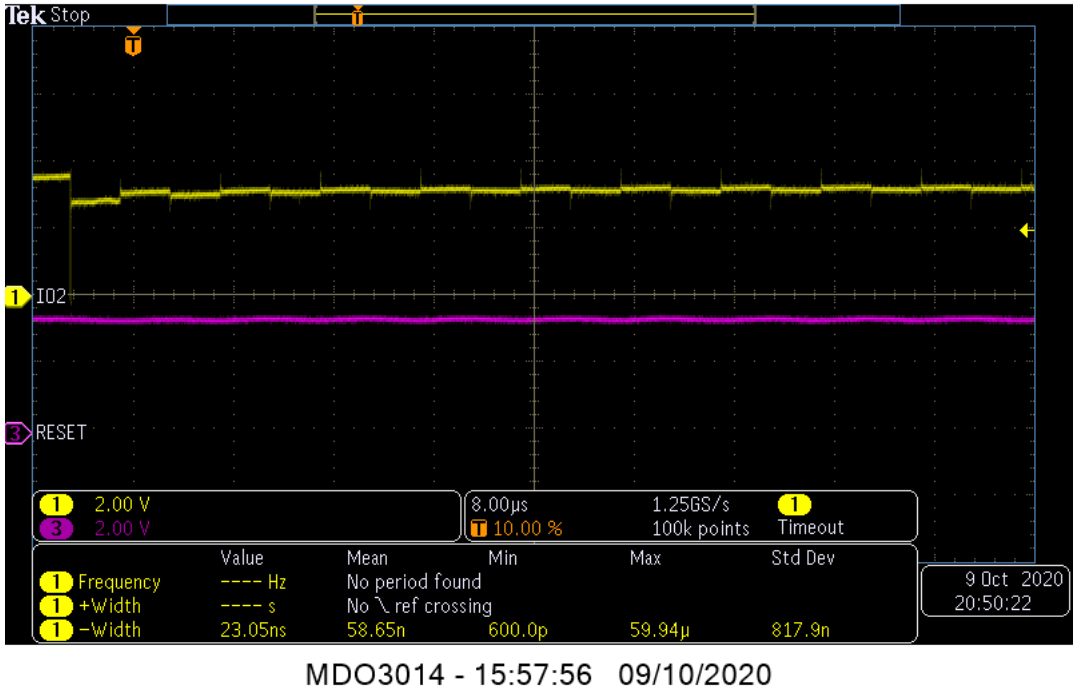


Figure 40. IO[2] shorten to VDDIO - fault not detected and RESET not asserted

If the PWM frequency drifts lower, which is considered an MCU failure, the drift will be detected when it drops below 125 kHz.

If the PWM frequency drifts higher, the FS device will not be able to detect this failure event only through FCCU monitoring (see Figure 41). In this situation, T_{On} and T_{Off} timings will always be under the 4 µs filtering time, preventing the FS device from detecting the drift.

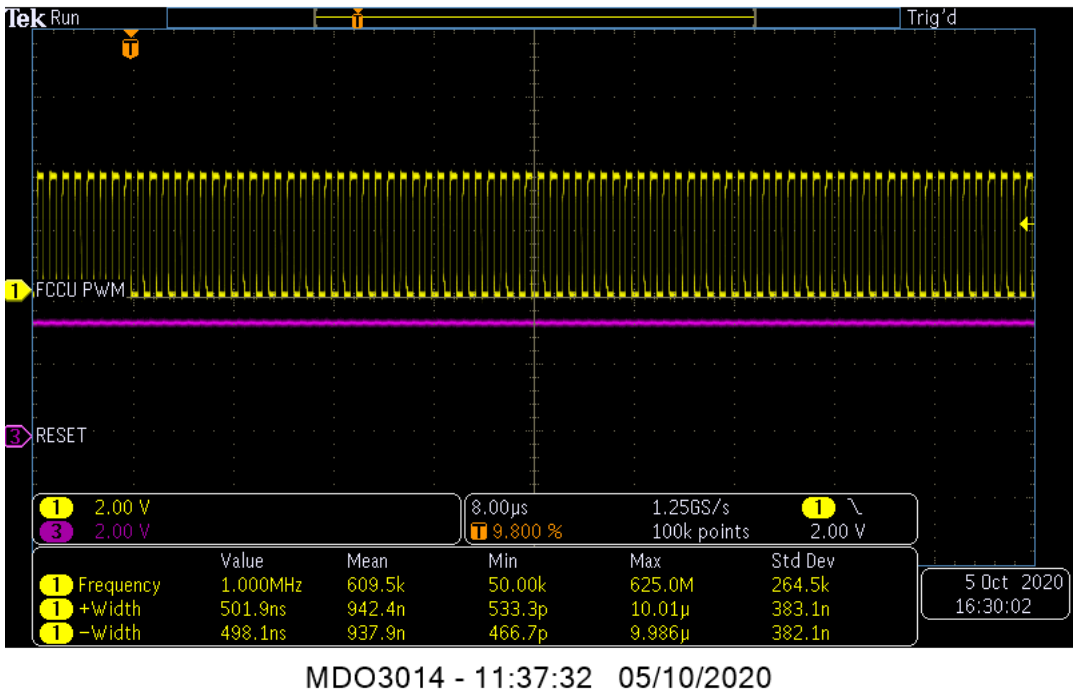


Figure 41. Frequency drift (up) fault not detected and RESET not asserted (f = 1 MHz/T_{On} = 501.9 ns/T_{Off} = 498.1 ns

To be able to detect such an event, the windowed WD monitoring can be used in a variety of ways. An increasing drift in the MCU's clock frequency inevitably impacts its WD answer frequency and leads to multiple WD errors.

The MCU must always trigger the WD in the open WD window, or else an error is generated. Here are the steps during the handshake:

1. FS65/FS45 generates a pseudo random code using a linear-feedback shift register(LFSR)
2. MCU reads the code
3. Both MCU and FS65/FS45 calculate the WD answer using the same formula
4. MCU sends its WD answer and FS65/FS45 compares that answer with its own
5. If the WD answer is wrong or sent in the closed WD window, a WD error is generated. If the good WD answer is sent in the open WD window, a new WD window opens and the handshake restarts

From here, there are two different ways to improve detectability:

- One can choose to reduce the WD window period, to capture the MCU frequency drift as quickly as possible, taking into account the ± 10 % accuracy of the FS65/FS45 clock, but also the MCU accuracy.
- One can decide to have the MCU WD answer sent at the very beginning of the WD open window. This workaround is more severe, and would allow detection to occur faster than any MCU frequency drift increase. Again, the MCU and the FS65/FS45 clock accuracies must be taken into the equation to prevent a false WD answer.

Example: *Down to 1 ms, the WD period can be between 0.9 ms and 1.1 ms (1 ms ± 10 %). With a 50 % duty cycle, the MCU WD answer should be sent in the middle of the open window, between 0.55 ms (worst case is 60 % of 0.5 ms) and 0.9 ms (see Figure 6).*

Assuming again IO[2] and IO[3] are connected as shown in Figure 7, these are the steps to follow to enable FCCU with the AURIX SMU:

1. Configure FS device: IO[2] and IO[3] are safety critical inputs
2. Configure the AURIX SMU in PWM mode
3. Proceed to a latent failure check to detect shorted pins: at INIT phase, toggle the pin and check the IO[2] flag status. The flag must follow the pin status
4. Set IO[2] in its valid state (HIGH level in this use case) when closing the INIT_FS phase before entering Normal mode
5. FCCU/SMU function is checked and operational. AURIX can switch to the PWM SMU_FSP signal

Figure 42 through Figure 44 show lab test results when sending a PWM signal with various frequencies to IO[2] in standard configuration and following the steps described above. IO[2] and IO[3] are set as safety-critical inputs and the pins' polarity is default. Thus, IO[3] is pulled down to GND (safe state) and IO[2] safe state is HIGH (LOW indicates a fault) before closing the INIT phase and entering Normal mode.

As both IOs are safety critical inputs, the RESET pin is asserted LOW upon a fault, and the IO_23 flag is set to logic 1 in the DIAG_FS_IOS register.

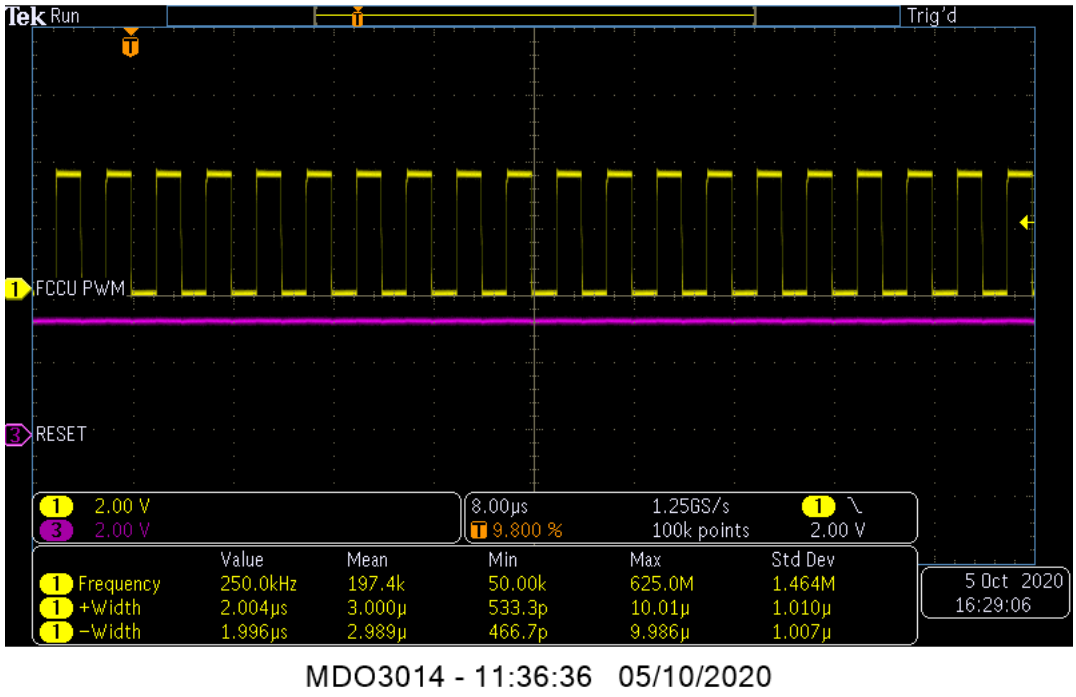


Figure 42. Reference state — no fault / RESET not asserted — f = 250 kHz / T_{On} = 2.004 µs / T_{Off} = 1.996 µs

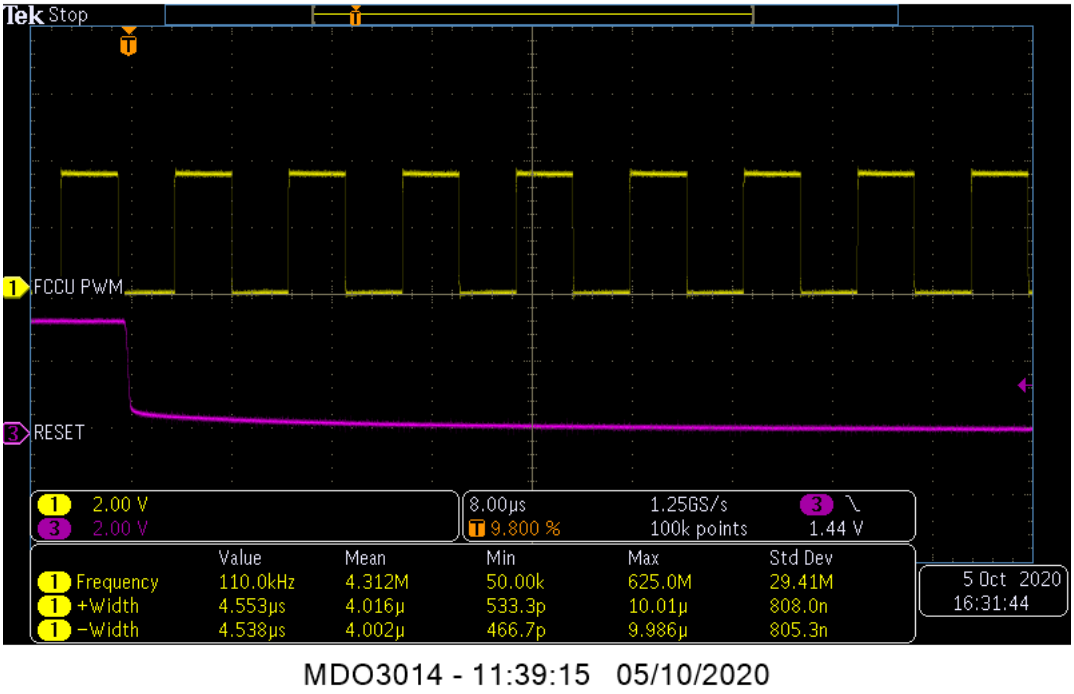


Figure 43. Frequency drift (down) fault detected / RESET asserted f = 110 kHz / T_{On} = 4.553 µs / T_{Off} = 4.538 µs

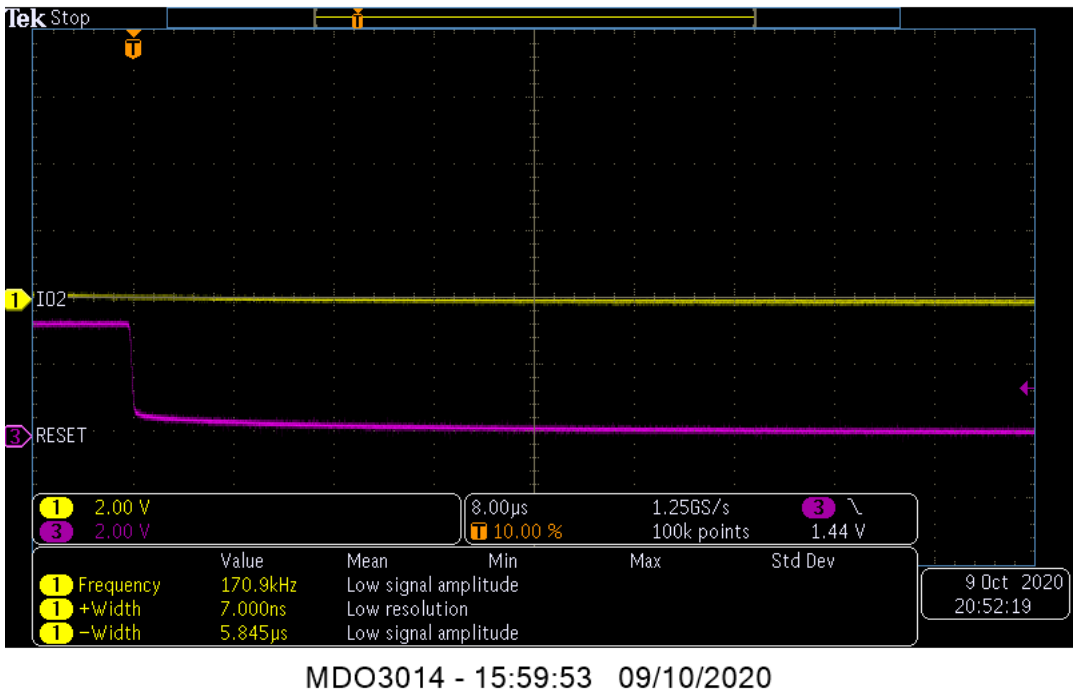


Figure 44. IO[2] short to GND fault detected / RESET asserted f = 125 kHz / T_{On} = 4.007 µs / T_{Off} = 3.993 µs

Given the right configuration and strategy, the FS65/FS45 is able to support the AURIX SMU FSP signal in steady-state mode and in PWM mode.

4.3 Power Management with AURIX MCU

Below diagrams and tables show the power connections between FS26 and AURIX TC2xx/TC3xx MCUs.

4.3.1 FS260x/FS261x + TC26x/TC27x/TC36x/TC37x

4.3.1.1 Option A

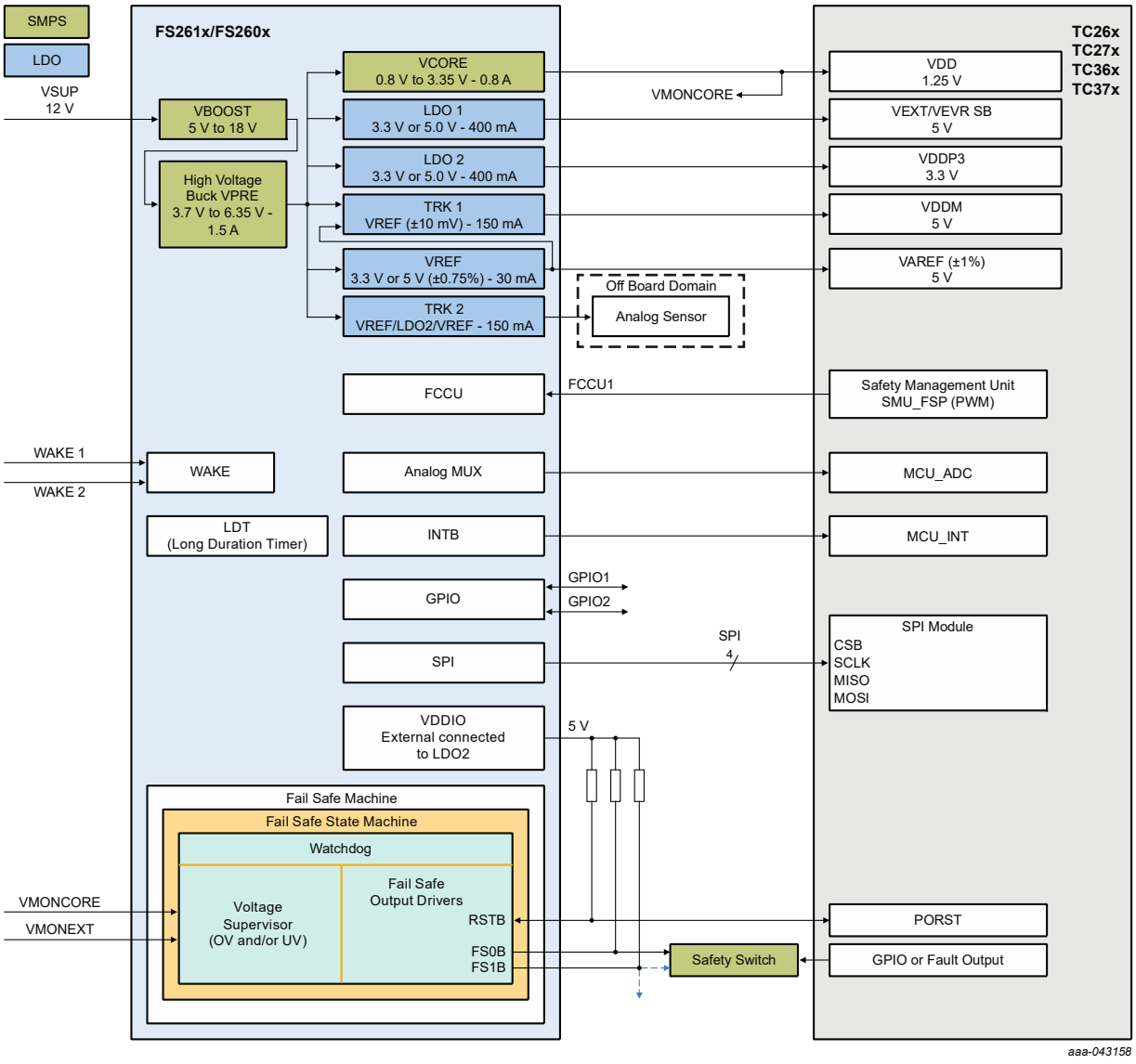


Figure 45. FS260x/FS261x attached to TC26x/TC27x/TC36x/TC37x AURIX MCU (option A)

Table 12. FS260x/FS261x - TC26x/TC27x/TC36x/TC37x connections summary (option A)

FS2600 connection	TC26x/TC27x/ TC36x/TC37x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC26x, TC27x, TC36x or TC37x
LDO1	VEXT/VEVRSB	LDO1 provides either 3.3 V or 5 V voltage rail to VEXT and VEVRSB in TC26x, TC27x, TC36x or TC37x
LDO2	VDDP3	LDO2 provides 3.3 V voltage rail to VDDP3 in TC26x, TC27x, TC36x or TC37x

Table 12. FS260x/FS261x - TC26x/TC27x/TC36x/TC37x connections summary (option A)*...continued*

FS2600 connection	TC26x/TC27x/ TC36x/TC37x connection	Description
VREF	VAREF	VREF provides 3.3 V or 5.0 V voltage rail to VAREF with ±0.75 % accuracy in TC26x, TC27x, TC36x or TC37x
TRK1	VDDM	TRK1 tracks VREF voltage providing VREF ±10 mV voltage rail to VDDM in TC26x, TC27x, TC36x or TC37x
4 lines SPI	4 lines SPI	SPI connections between FS260x/FS261x and TC26x, TC27x, TC36x or TC37x
FCCU1	SMU_FSP	SMU connection to FCCU monitoring
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection
AMUX	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC26x, TC27x, TC36x or TC37x

4.3.1.2 Option B

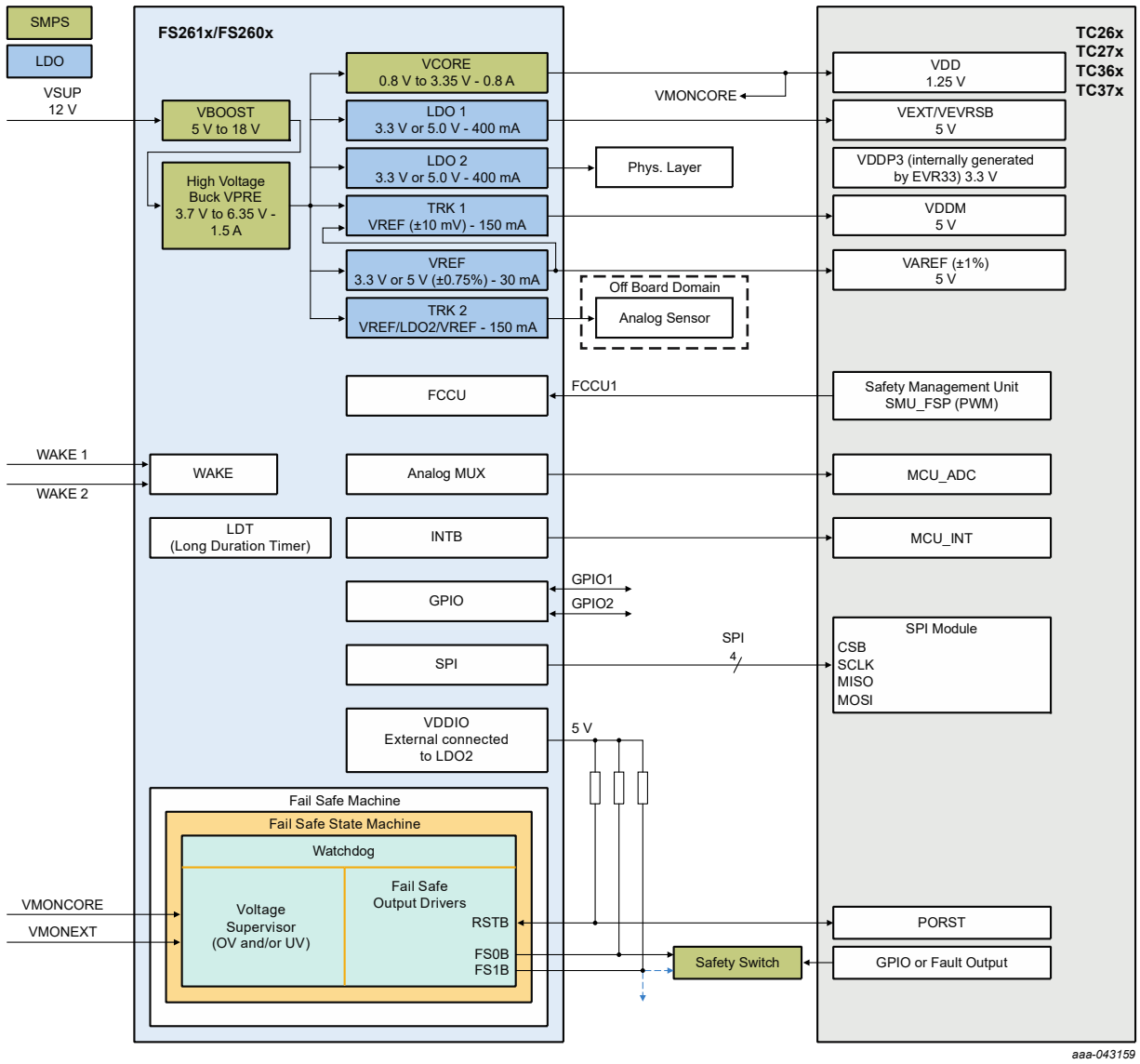


Figure 46. FS260x/FS261x attached to TC26x/TC27x/TC36x/TC37x AURIX MCU (option B)

Table 13. FS260x/FS261x - TC26x/TC27x/TC36x/TC37x connections summary (ption B)

FS2600 connection	TC26x/TC27x/ TC36x/TC37x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC26x, TC27x, TC36x or TC37x
LDO1	VEXT/VEVRSB/ VDDP3	LDO1 provides 3.3 V voltage rail to VEXT, VEVRSB and VDDP3 in TC26x, TC27x, TC36x or TC37x
VREF	VAREF	VREF provides 3.3 V or 5.0 V voltage rail to VAREF with ±0.75 % accuracy in TC26x, TC27x, TC36x or TC37x
TRK1	VDDM	TRK1 tracks VREF voltage providing VREF ±10 mV voltage rail to VDDM in TC26x, TC27x, TC36x or TC37x

Table 13. FS260x/FS261x - TC26x/TC27x/TC36x/TC37x connections summary (ption B)*...continued*

FS2600 connection	TC26x/TC27x/ TC36x/TC37x connection	Description
4 lines SPI	4 lines SPI	SPI connections between FS260x/FS261x and TC26x, TC27x, TC36x or TC37x
FCCU1	SMU_FSP	SMU connection to FCCU monitoring
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection
AMUX	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC26x, TC27x, TC36x or TC37x

4.3.2 FS262x/FS263x + TC29x/TC38x/TC39x

4.3.2.1 Option A

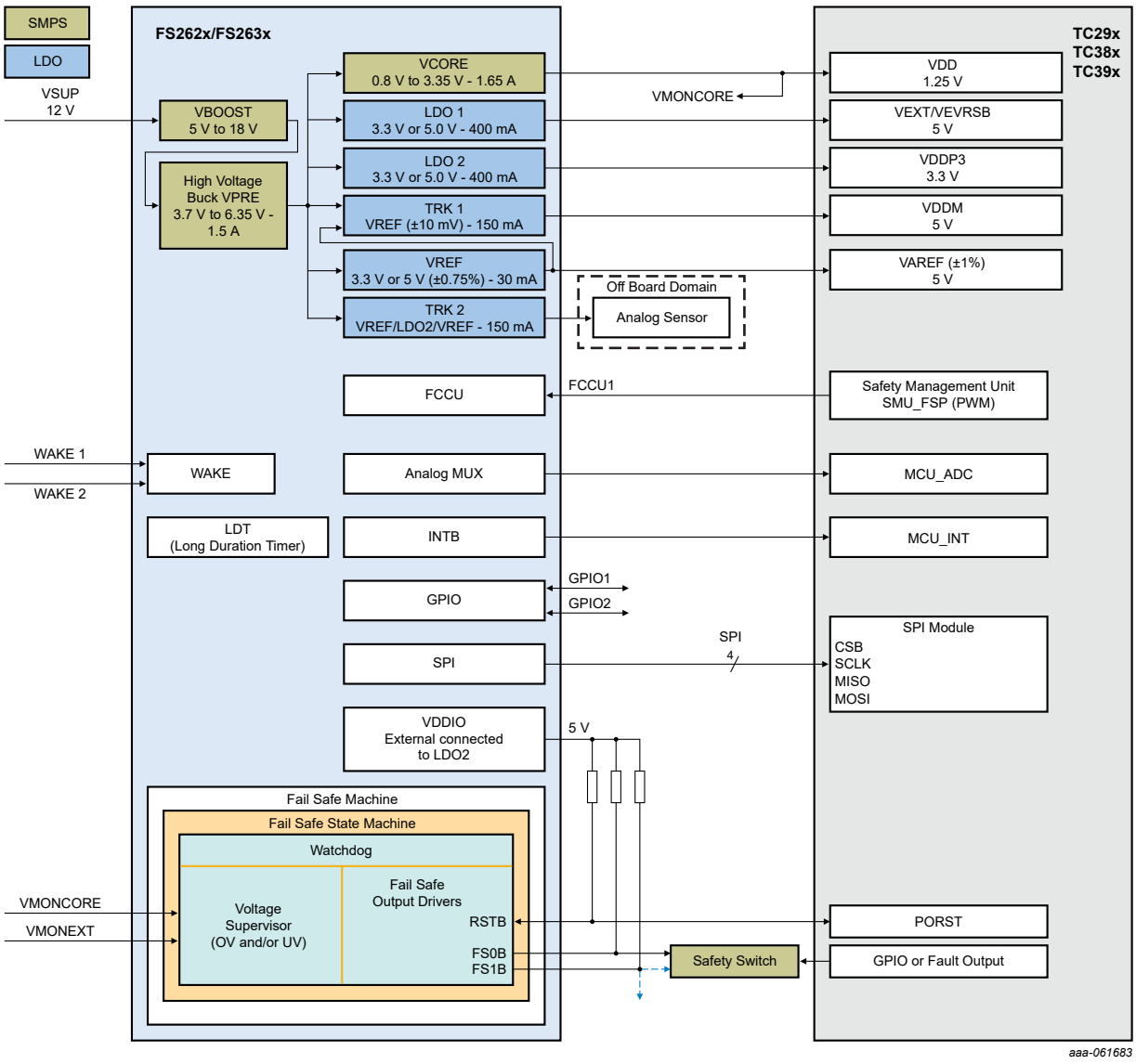


Figure 47. FS262x/FS263x attached to TC29x/TC38x/TC39x AURIX MCU (option A)

Table 14. FS262x/FS263x - TC29x/TC38x/TC39x connections summary (option A)

FS2600 connection	TC29x/TC38x/TC39x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC29x, TC38x, or TC39x
LDO1	VEXT/VEVRSB	LDO1 provides either 3.3 V or 5 V voltage rail to VEXT and VEVRSB in TC29x, TC38x, or TC39x
LDO2	VDDP3	LDO2 provides 3.3 V voltage rail to VDDP3 in TC29x, TC38x, or TC39x

Table 14. FS262x/FS263x - TC29x/TC38x/TC39x connections summary (option A)*...continued*

FS2600 connection	TC29x/TC38x/TC39x connection	Description
VREF	VAREF	VREF provides 3.3 V or 5.0 V voltage rail to VAREF with ±0.75 % accuracy in TC29x, TC38x, or TC39x
TRK1	VDDM	TRK1 tracks VREF voltage providing VREF ±10 mV voltage rail to VDDM in TC29x, TC38x, or TC39x
4 lines SPI	4 lines SPI	SPI connections between FS260x/FS261x and TC29x, TC38x, or TC39x
FCCU1	SMU_FSP	SMU connection to FCCU monitoring
INTB	MCU_INT	Interrupt signal connection
RSTB	PORST	RSTB connection
AMUX	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC29x, TC38x, or TC39x

4.3.2.2 Option B

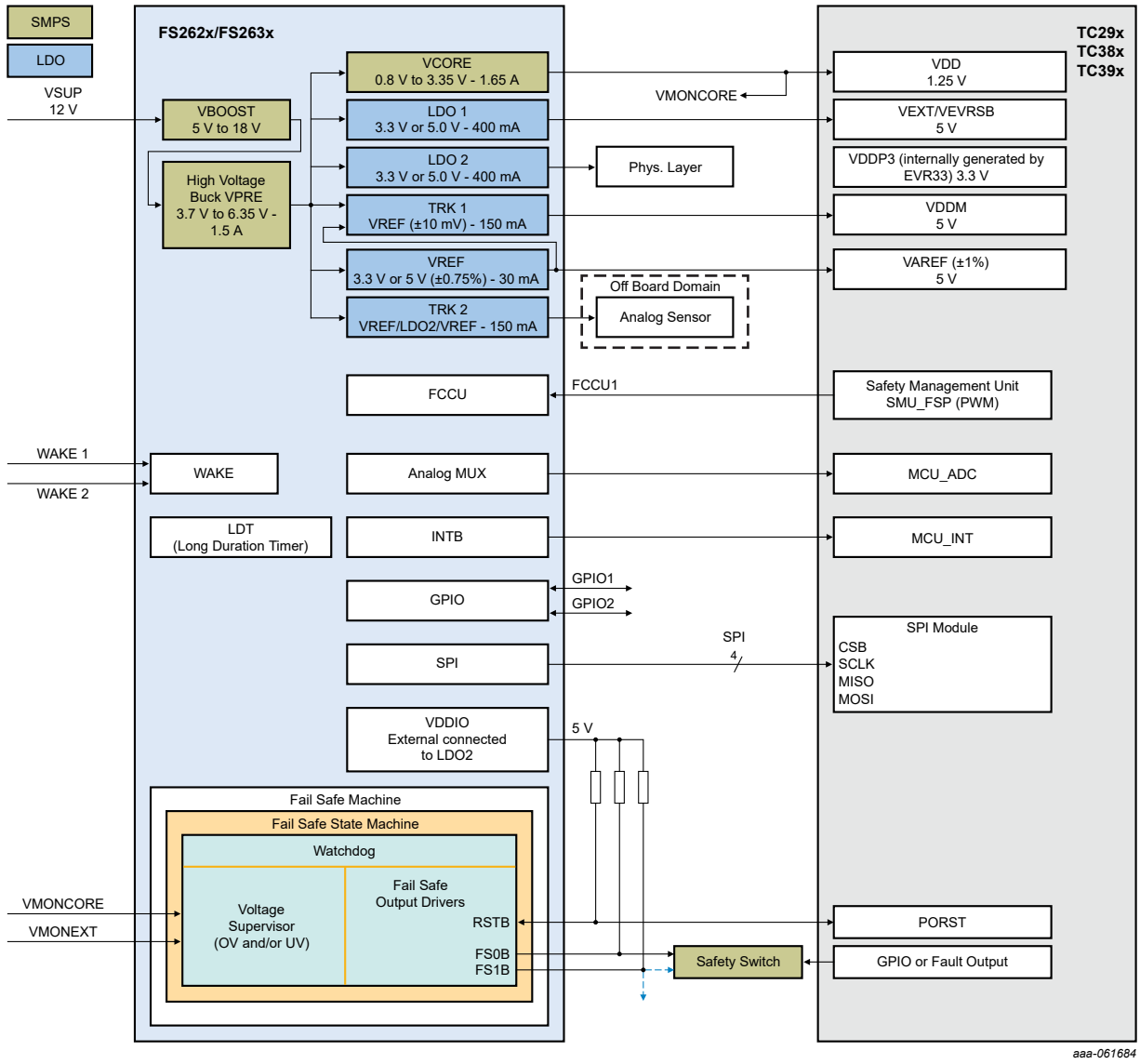


Figure 48. FS262x/FS263x attached to TC29x/TC38x/TC39x AURIX MCU (option B)

Table 15. FS262x/FS263x - TC29x/TC38x/TC39x connections summary (option B)

FS2600 connection	TC29x/TC38x/TC39x connection	Description
VCORE	VDD	VCORE provides 1.25 V voltage rail to VDD in TC29x, TC38x, or TC39x
LDO1	VEXT/VEVRSB/VDDP3	LDO1 provides 3.3 V voltage rail to VEXT, VEVRSB and VDDP3 in TC29x, TC38x, or TC39x
VREF	VAREF	VREF provides 3.3 V or 5.0 V voltage rail to VAREF with ±0.75 % accuracy in TC29x, TC38x, or TC39x
TRK1	VDDM	TRK1 tracks VREF voltage providing VREF ±10 mV voltage rail to VDDM in TCTC29x, TC38x, or TC39x

Table 15. FS262x/FS263x - TC29x/TC38x/TC39x connections summary (option B)*...continued*

FS2600 connection	TC29x/TC38x/TC39x connection	Description
4 lines SPI	4 lines SPI	SPI connections between FS260x/FS261x and TC29x, TC38x, or TC39x
FCCU1	SMU_FSP	SMU connection to FCCU monitoring
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB connection
AMUX	MCU_ADC	monitor signal from MUX_OUT to ADC input in TC29x, TC38x, or TC39x

4.3.3 FS26 other pins connection

Table 16. FS26 other system connections summary

FS26 connection	TC2xx/TC3xx connection	Description
FCCU2	pulldown resistor to GND	to be set in the right state if not used
FS0B	connect to safety switch	Works with FS1B together as safety switch output to bring the system into safe state. The connection may vary based on different customer requirements.
FS1B	connect to safety switch	Works with FS0B together as safety switch output to bring the system into a safe state. The connection may vary based on different customer requirements.
VDDIO	connect to RSTB and FS0B	pullup voltage source for RSTB and FS0B (also FS1B if available) with resistors
DEBUG	-	For debug mode entry, apply VDBG voltage to this pin prior to applying any voltage on VSUP pin.
VMONEXT	connect to any external IC	monitors a voltage generated by another part in the application

4.4 Application schematic

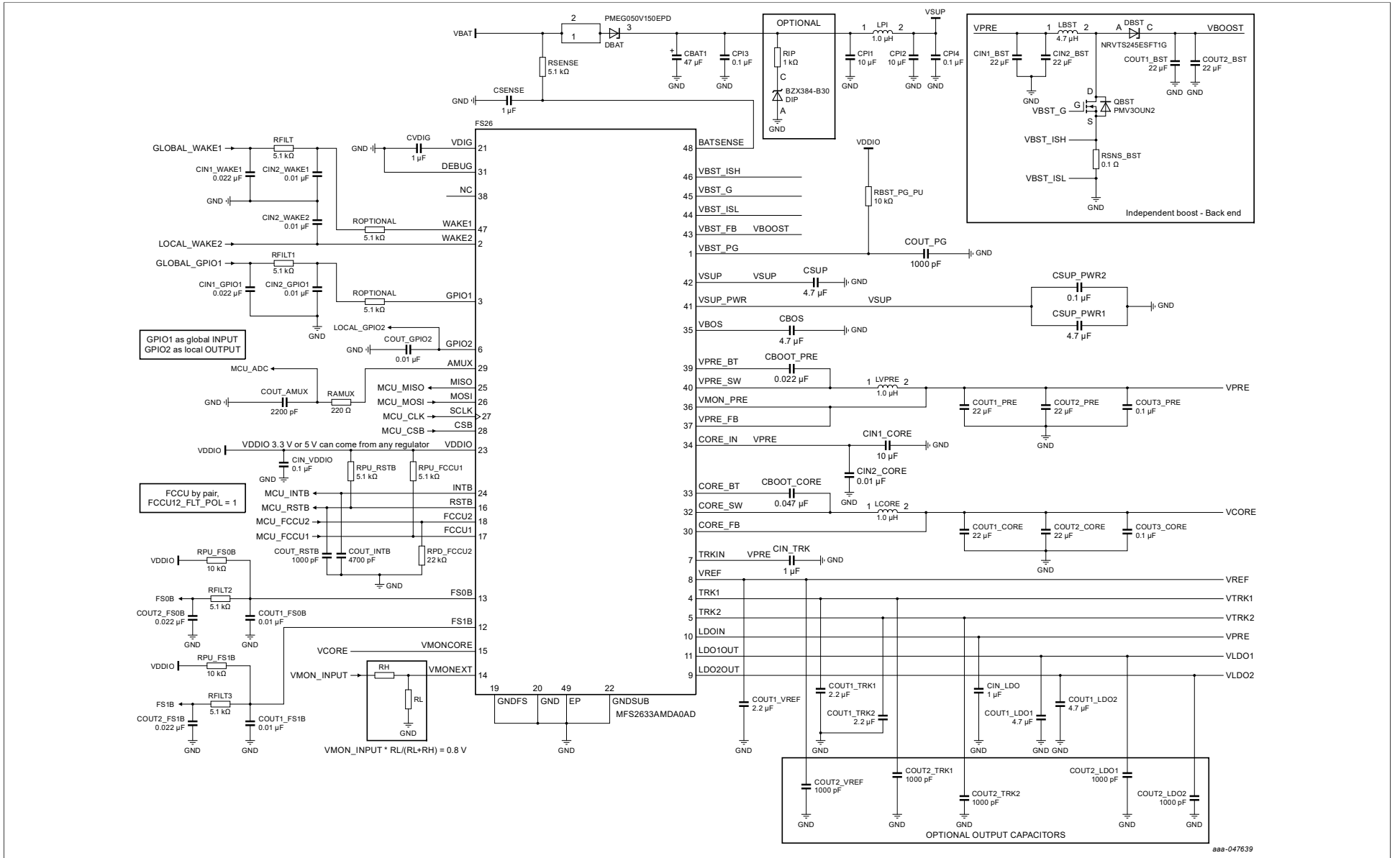


Figure 49. FS26 automotive schematic with BOOST in back-end configuration (a)

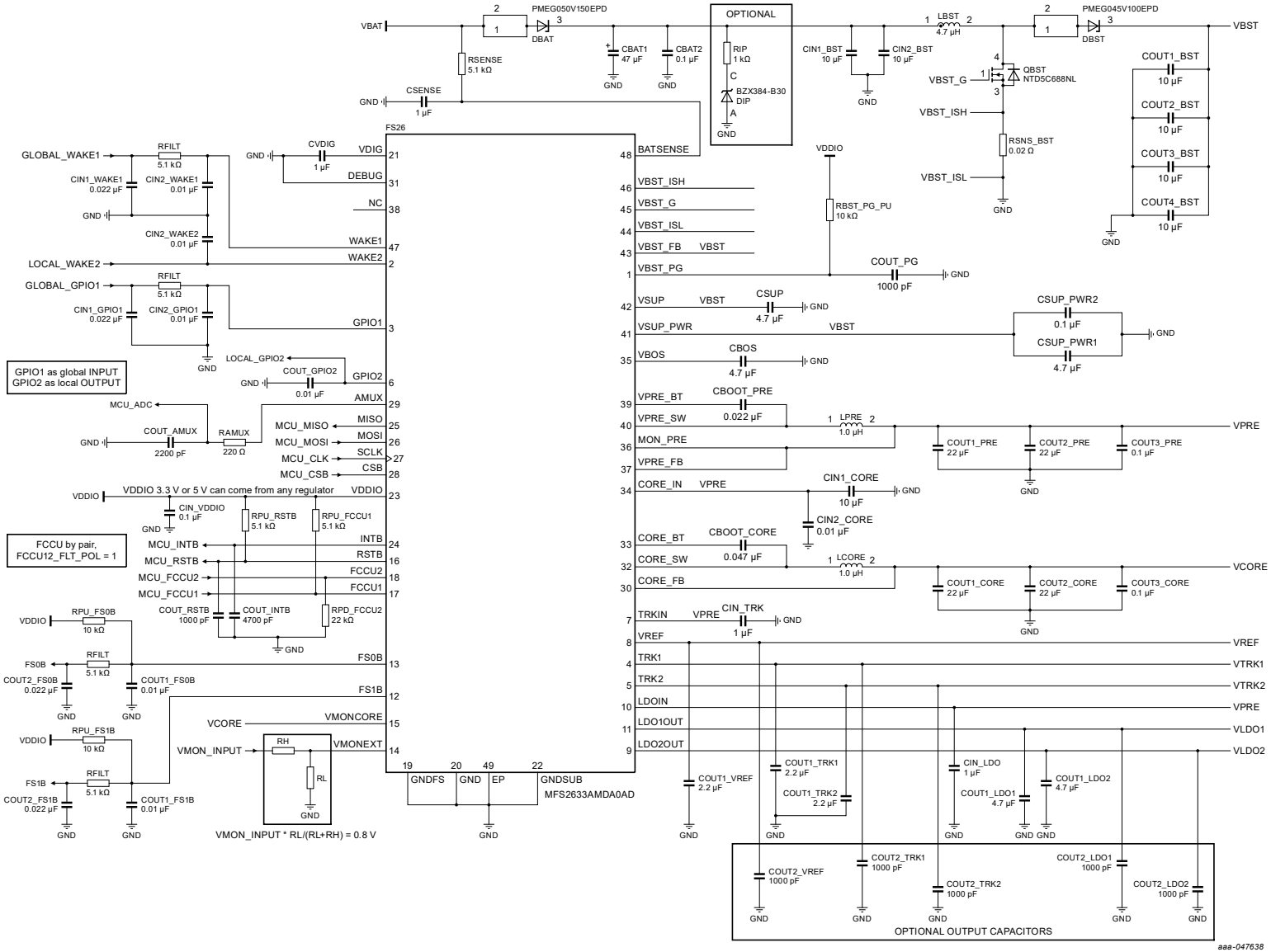


Figure 50. FS26 automotive schematic with BOOST in front-end configuration (b)

4.5 BOM

Table 17. FS26xy BOM reference

Domain	item name	value	unit	description	optional
FCCU monitoring	FCCU_PU	5.1	kΩ	pullup resistor for FCCU1 to VDDIO	X
	FCCU_PD	22	kΩ	pulldown resistor for FCCU2	X
VSUP power supply	DBAT	—		reverse battery diode	
	CBAT	47	µF	decoupling capacitor	
	pi filter (BOOST in back-end)	1	µH	pifilter components and decoupling capacitors for conducted emission	X
		2 x 10	µF		
		2 x 100	nF		
	CSUP	4.7	µF	decoupling capacitor	
	CSUP_PWR	4.7 + 0.1	µF	decoupling capacitors	
	RSENSE	5.1	kΩ	current limit resistor	
	CSENSE	1	µF	decoupling capacitor	
BOOST regulator	PUVBST_PG	10	kΩ	PGOOD pullup resistor to VDDIO	
	CIN_BOOST	2 x 22 or 2 x 10	µF	input capacitor	
	LBOOST	4.7	µH	power inductor	
	QBST	—		power diode	
	DBOOST	—		Schottky diode	
	RSNS_BOOST	—	Ω	BOOST sensing resistor for current limitation = (VBST_ILIM_TH/RSNS_BST)	
	COUT_BOOST	2 x 22 or 4 x 10	µF	output capacitors	
VPRE pre-regulator	CBOOT_PRE	22	nF	bootstrap capacitor	
	L_VPRE	2.2 or 10	µH	power inductor	
	COUT_VPRE	2 x 22 + 1 x 0.1	µF	output capacitors	
VCORE regulator	CIN_CORE	10	µH	input capacitor	
	CBOOT_CORE	47	nF	bootstrap capacitor	
	LCORE	1 or 2.2	µH	power inductor	
	COUT_CORE	2 x 22	µF	output capacitors	
LDO1 and LDO2 regulators	CIN_LDO	1	µF	input capacitor	
	COUT_LDOx	2 x 4.7	µF	output capacitors	
	$C_{OUT\_LDOx\_OP}$	2 x 1	nF	output capacitors if VREF accuracy target is 0.75%	X
VREF	COUT_VREF	2.2	µF	output capacitor	

Table 17. FS26xy BOM reference*...continued*

Domain	item name	value	unit	description	optional
regulator	$C_{OUT\_VREF\_OP}$	1	nF	output capacitors if VREF accuracy target is 0.75%	X
TRK1 and TRK2 regulators	CIN_TRKx	1	µF	input capacitor	
	COUT_TRKx	2 x 2.2	µF	output capacitors (only one if one tracker is used)	
	$C_{OUT\_TRKx\_OP}$	2 x 1	nF	output capacitors if FPRE = 2.2 MHz or if FPRE = 450 kHz and TRKx is tracking LDO2	X
VBOS	COUT_VBOS	4.7	µF	best of supply decoupling output capacitor	
wake pins	CIN_WAKE	2 x 22 + 2 x 10	nF	input capacitors	
	R_WAKE	2 x 5.1	kΩ	resistors to limit the current	
GPIO	COUT_GPIO	1 x 22 + 2 x 10	nF	output capacitors	
	R_GPIO	2 x 5.1	kΩ	resistors to limit the current	
VDDIO	COUT_VDDIO	0.1	µF	decoupling capacitor close to the pin for immunity	
INTB	COUT_INTB	4.7	nF	decoupling capacitor close to the pin for immunity	
VMONEXT	R_VMONEXT	—	kΩ	resistor bridge for VMONEXT; R18 and R16 must satisfy: Vx * R18 / (R18 + R16) = 0.8 V (Vx is the monitored voltage)	X
AMUX Pin	R_AMUX	220	Ω	resistor and capacitor required for buffer stability	
	C_AMUX	2.2	nF		
reset and Fail-safe outputs	COUT_RSTB	1	nF	RSTB decoupling capacitor	
	PU_RSTB	5.1	kΩ	RSTB pullup resistor to VDDIO	
	COUT2_FS0B	22	nF	FS0B capacitor to damp ESD gun stress	
	COUT2_FS1B	22	nF	FS1B capacitor to damp ESD gun stress	X
	COUT1_FS0B	10	nF	FS0B decoupling capacitor close to the pin for immunity	
	CIN_FS1B	10	nF	FS1B decoupling capacitor close to the pin for immunity	X
	PU_FS0B	10 or 5.1	kΩ	FS0B pullup resistor to VDDIO	
	PU_FS1B	10 or 5.1	kΩ	FS1B pullup resistor to VDDIO	X
	RFS0B	5.1	kΩ	FS0B resistor to limit current	
	RFS1B	5.1	kΩ	FS1B resistor to limit current	X

For more detailed information on product guidelines, refer to the dedicated application note AN12995.

4.6 Flowchart

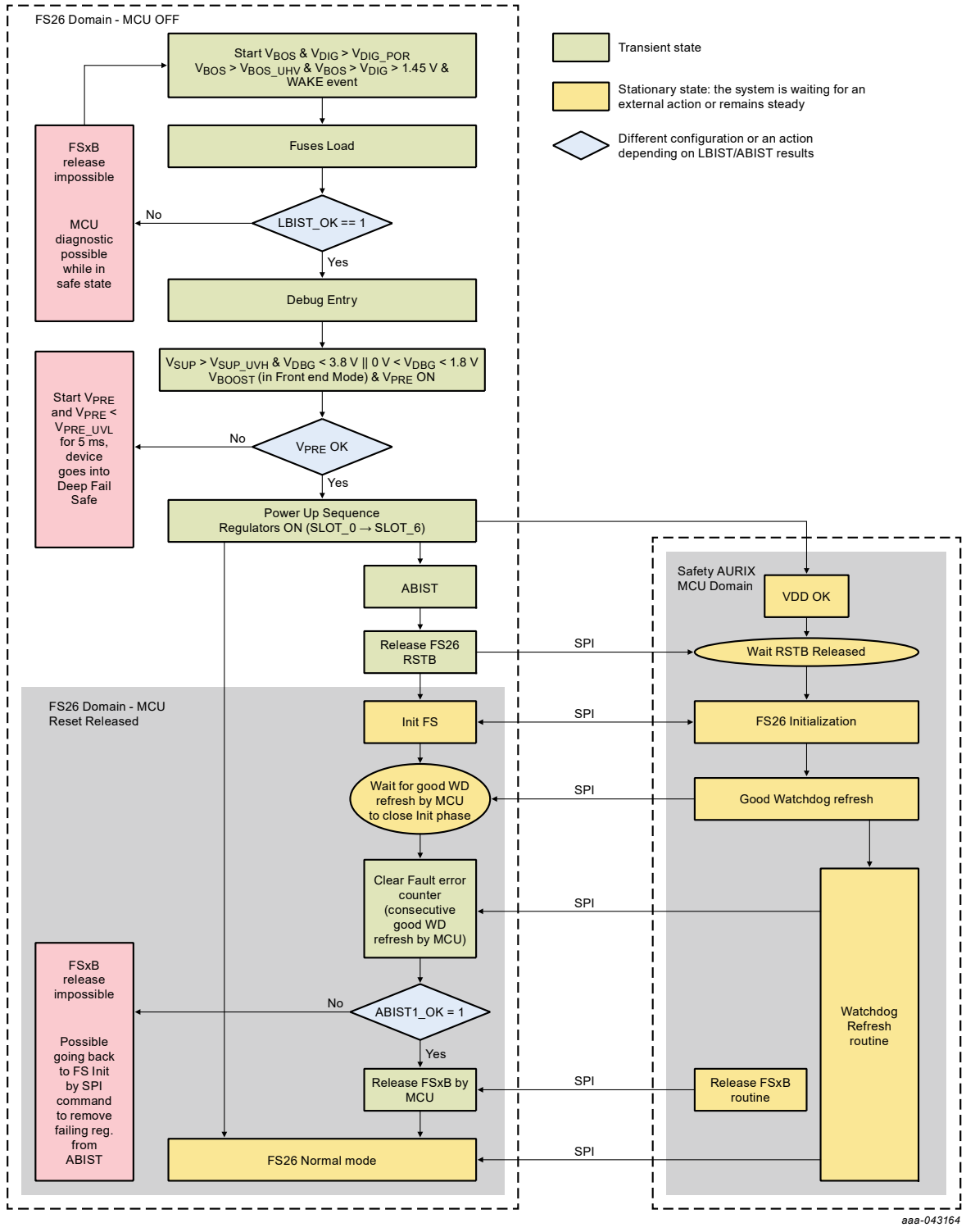


Figure 51. Power-up sequence flow chart block diagram

The FS26 operation is divided in two independent logic blocks to achieve best in class functional safety coverage. The Main state machine manages the power management, the low power modes, and the wake-up

sources while the Fail-safe state machine manages the monitoring of the power management, the monitoring of the microcontroller and the monitoring of an external IC.

The following domain information details some specific states from the flowchart in Figure 51.

FS26 domains:

- Fuses load: FS26 loads its preset configuration through fuse memory (OTP).
- Fail-safe init: A window of 256 ms after the release of RSTB is available to configure the initialization register of the FS26. The MCU can configure watchdog, error counters, safety reaction mechanisms and similar behaviors in this window by SPI. In order to close this window before timeout, the MCU must send a good watchdog refresh. Otherwise, it will be considered a fault.
- Normal mode: This is intended to be the fully functional mode, with all power supplies enabled as required by the system, as well as availability to all the system functionality provided by the FS26 device. During the Normal mode, the Fail-safe state machine is available and provides full monitoring and operation of all the safety features in the device. To enter Normal mode, the FSxB pin must be released. To release the FSxB pins, send several consecutive good watchdog commands to clear the fault error counter down to 0. Finally send a SPI command to release the FSxB safety outputs.

AURIX TC2xx/TC3xx MCU domains:

- MCU VDD OK: Depending on the system architecture, VDD (equivalent for VCORE) from the MCU can be supplied by the FS26 or by an external source.
- MCU waits for RESETB to be released: The pin RESETB from the FS26 is chosen in this application note for releasing the RESET of the MCU.

4.6.1 FS26 power sequencing

A system power-up sequence is shown in Figure 52 :

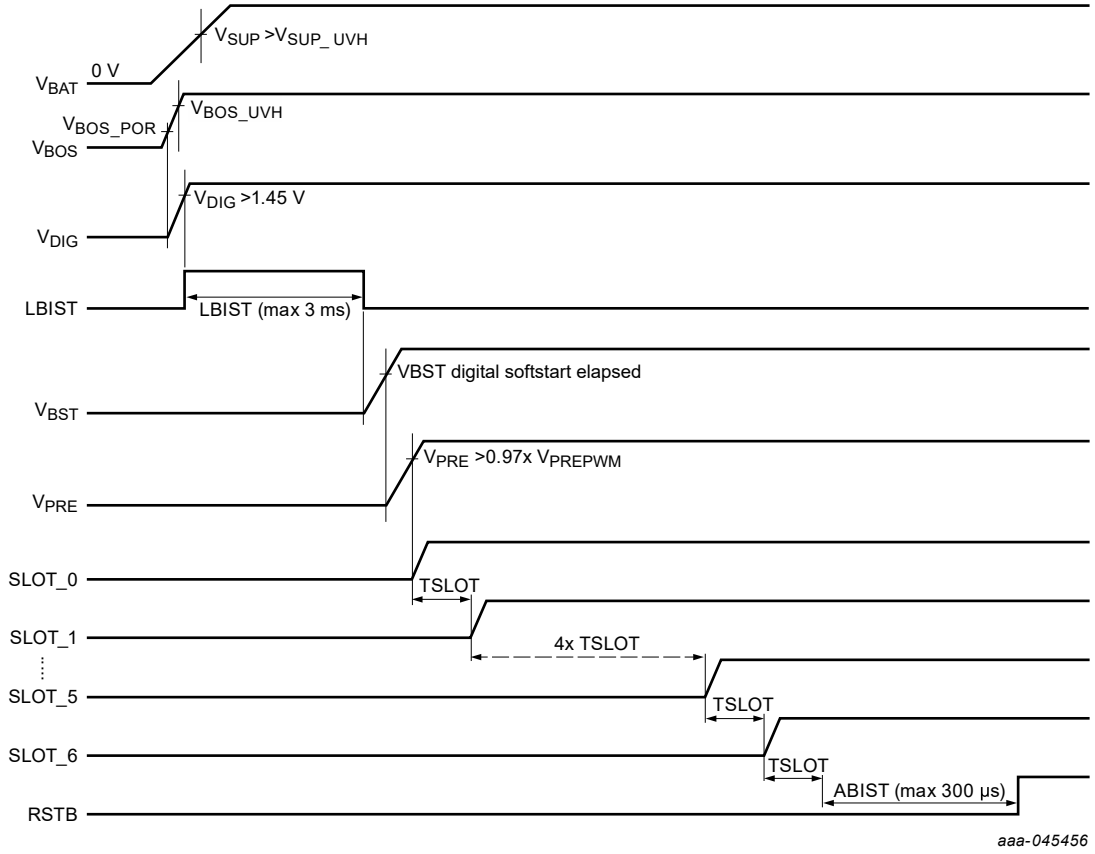


Figure 52. 12 Power-up sequence with VBST as front-end supply

Seven slots are available to program the start-up sequence of VCORE, LDO1, LDO2, VREF, VTRK1 and VTRK2 as well as the GPIO1 and GPIO2 signals for external control.

The power-up sequence starts at SLOT0 and ends at SLOT6 with a TSLOT_OTP delay between each slot. Regulators assigned *off* are not started during the power-up sequence but can be enabled later in Normal mode via a SPI command. When VBST is used as a back end supply, it can only be enabled via a SPI command once the device is in the Normal mode.

Each regulator is assigned a slot by OTP configuration using the dedicated OTP bits. To reduce the power-up timing, an OTP configuration is provided to allow the sequencer to run until reaching the selected slot and bypassing all preceding regulators. When the power-up is finished, the Main state machine is in Normal mode, which is the application running mode with all the regulators ON. If the MCU is not ready to run, RSTB can be pulled low by the MCU after its release.

During a power-down event, the device uses the same slot bits to turn off the voltage regulators in reverse order from the power-up sequence.

4.7 Fault management and recovery

When the system is operating in Normal mode, various types of faults can occur on the FS26, the MCU, or on external peripherals. Fault use cases that the system might face and its reaction to each are explained in this section.

Fault management use cases between FS26 and AURIX TC2xx/TC3xx are described in this section. Other faults, like overtemperature, follow the same sequence.

Table 18. Fault list

Fault number	Fault location	Fault type
1	FS26 AURIX VCORE supply	overvoltage
2	FS26 AURIX SPI	watchdog fault
3	FS26 FCCU1/2	FCCU fault

4.7.1 AURIX TC2xx/TC3xx VCORE overvoltage

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- VMONCORE pin must be connected to VCORE regulator output
- VMON_CORE_OVTH[3:0] OTP bits, set VCORE monitoring overvoltage thresholds between +4.5 % to +12 % in increments of +0.5 %
- VMON_CORE_OVDGLT_OTP bit, set VCORE monitoring overvoltage filtering time (25 µs or 45 µs)
- VMON_CORE_ OV_FS_REACTION[1:0] = 11, VCORE OV does have an impact on RSTB and FS0B
- RSTB_DUR = 0, set to configure the RSTB LOW duration time to 10 ms
- FS1B_TDELAY[4:0] = 11001, FS1B_TDUR = 11111, set FS1B in Delay mode with T_{DELAY} = 1 s
- DFS_DIS_OTP = 0 by OTP (register CFG_OVUV_3_OTP), DFS function is enabled

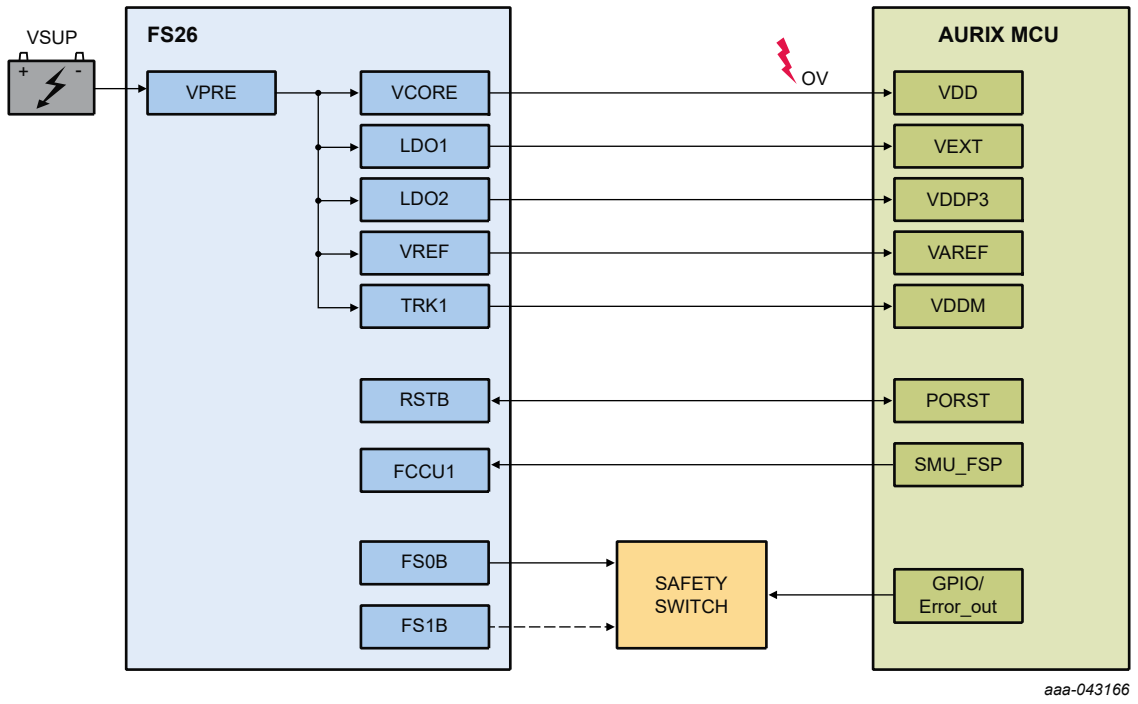


Figure 53. VCORE OV fault simplified schematic

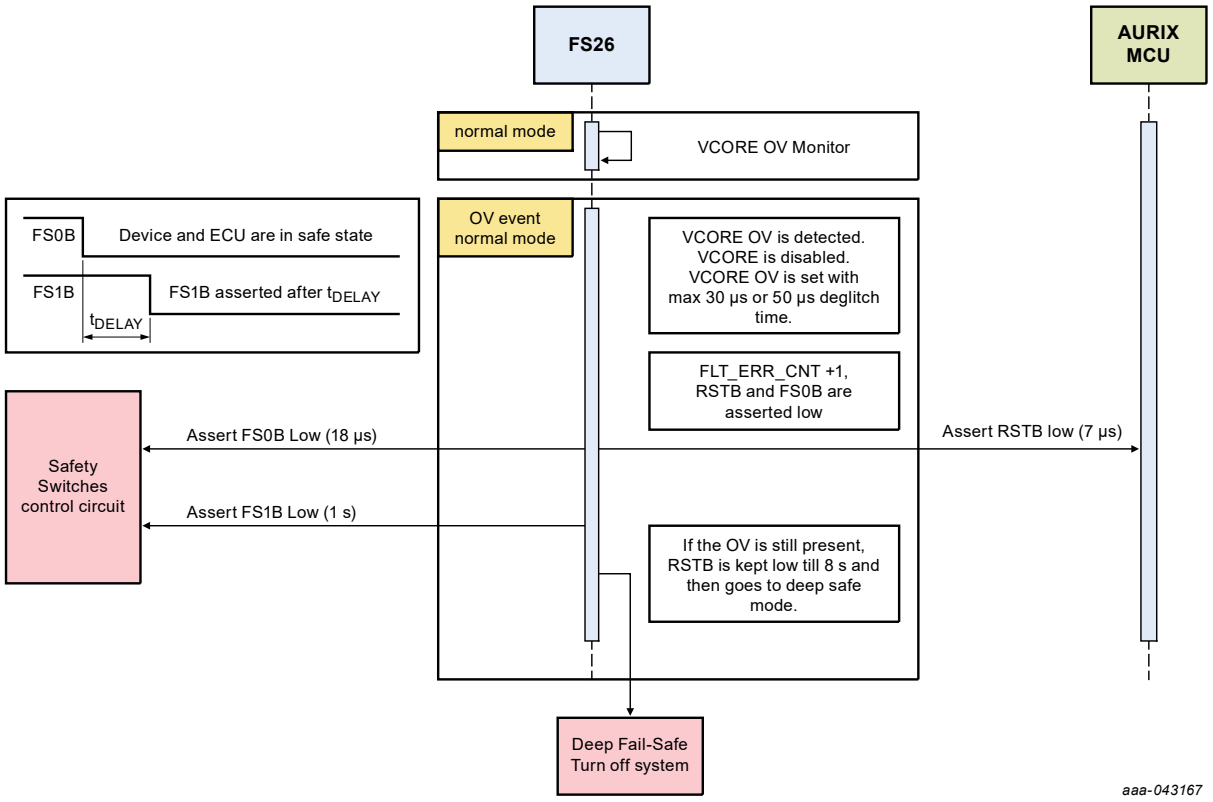


Figure 54. VCORE OV fault management sequence diagram (to DFS)

1. FS26 VCORE voltage is internally monitored through the VMONCORE pin
2. OV event occurs on VCORE; FS26 triggers a fault after maximum 30 µs or 50 µs deglitch time; VCORE regulator is disabled; FS26 increments FLT_ERR_CNT by one.
3. FS26 asserts RSTB and FS0B LOW according to the VMON_CORE_OV_FS_REACTION configuration
4. FS26 asserts FS1B low following FS0B status after a 1 s delay
5. If the OV condition remains, RSTB stays LOW
6. If RSTB stays LOW for 8 s, FS26 goes to DFS mode

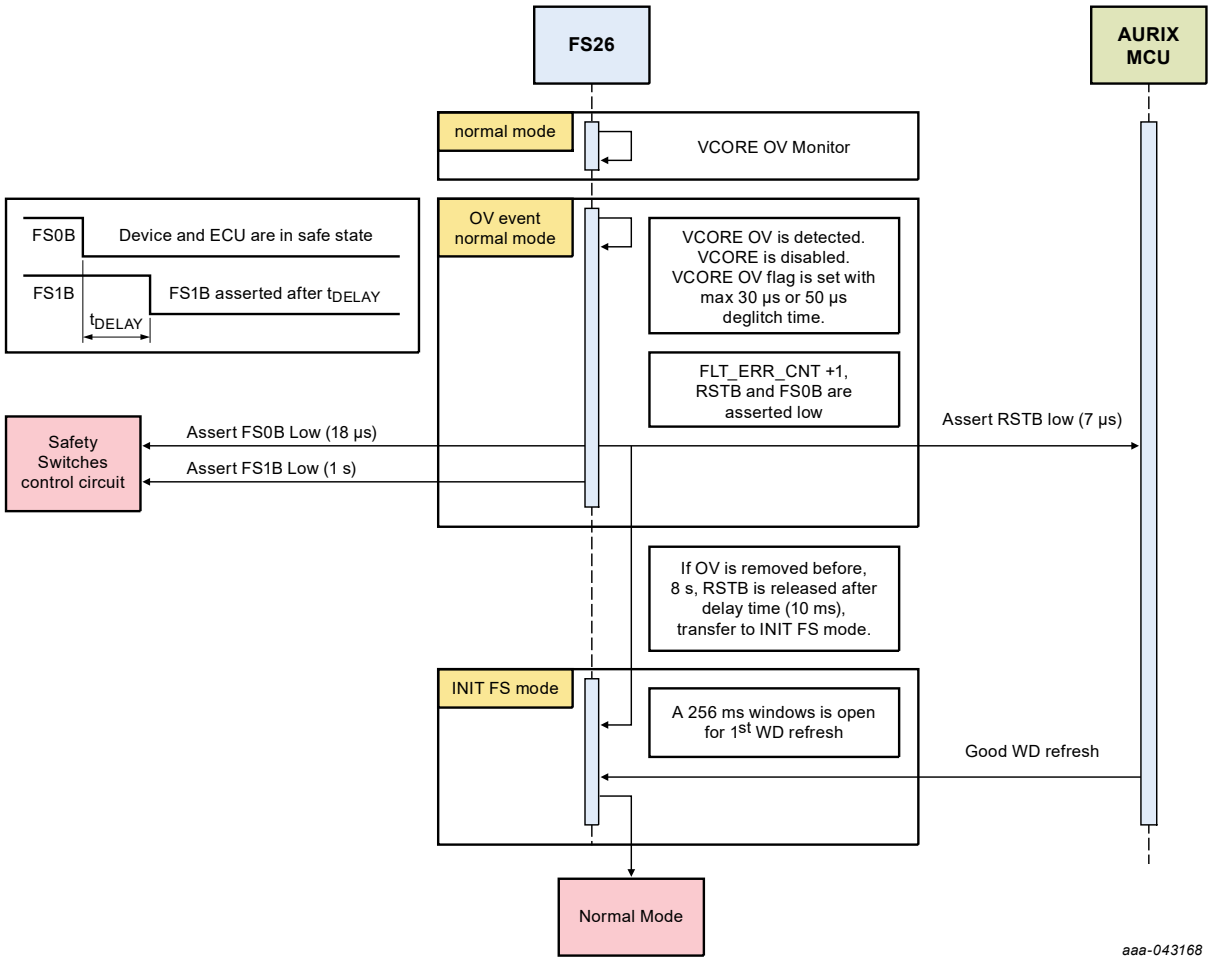


Figure 55. VCORE OV fault management sequence diagram (to recovery)

1. FS26 VCORE voltage is internally monitored through the VMONCORE pin.
2. OV event occurs on VCORE; FS26 triggers a fault after maximum 30 µs or 50 µs deglitch time; VCORE regulator is disabled; FS26 increments FLT_ERR_CNT by one.
3. FS26 asserts RSTB and FS0B LOW according to VMON_CORE_ OV_FS_REACTION configuration.
4. FS26 asserts FS1B LOW following FS0B status after a 1 s delay.
5. If the OV condition is removed before 8 s, after a 10 ms delay, RSTB is released; FS26 transfers to INIT_FS mode, opens a 256 ms window and waits for a new WD refresh from AURIX.
6. AURIX sends a first good WD refresh, closing the INIT_FS phase, then decrements FLT_ERR_CNT to 0 and releases the safety outputs. At this point, the FS26 is back in Normal mode.

4.7.2 AURIX TC2xx/TC3xx watchdog fault

Use assumptions:

- System is running in normal mode (RSTB and FSxB are released)
- WDW_PERIOD[3:0] = 0101 and WDW_DC[2:0] = 010, WD window is set to 6 ms with 50 % duty cycle
- WD_FS_REACTION[1:0] = 01, FS0B only is asserted LOW if WD_ERR_CNT = WD_ERR_LIMIT
- WD_ERR_LIMIT[1:0] = 01, max value of WD error counter is set to 6 (intermediate value is 3)
- WD_RFR_LIMIT[1:0] = 01, max value of WD refresh counter is set to 4
- RSTB_DUR = 0, set to configure the RSTB low duration time to 10 ms

- FLT_ERR_CNT_LIMIT[1:0] = 01, to set the fault error counter intermediate value to 3 and its maximum to 6
- FLT_ERR_REACTION[1:0] = 1X, RSTB and FS0B are asserted LOW if FLT_ERR_CNT ≥ intermediate value
- FS1B_TDELAY[4:0] = 11001, FS1B_TDUR[4:0] = 11111, set FS1B in delay mode with T_{DELAY} = 1 s
- DFS_DIS_OTP = 0 by OTP (register CFG_OVUV_3_OTP), DFS function is enabled

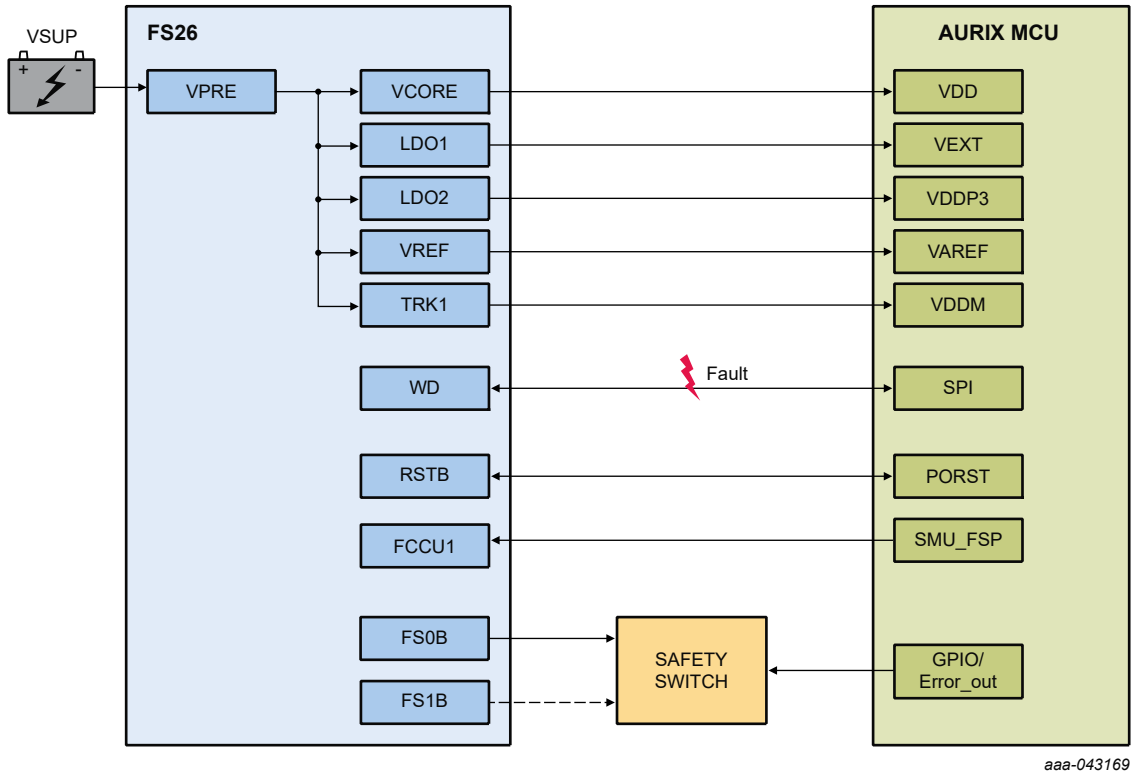


Figure 56. WD fault simple schematic

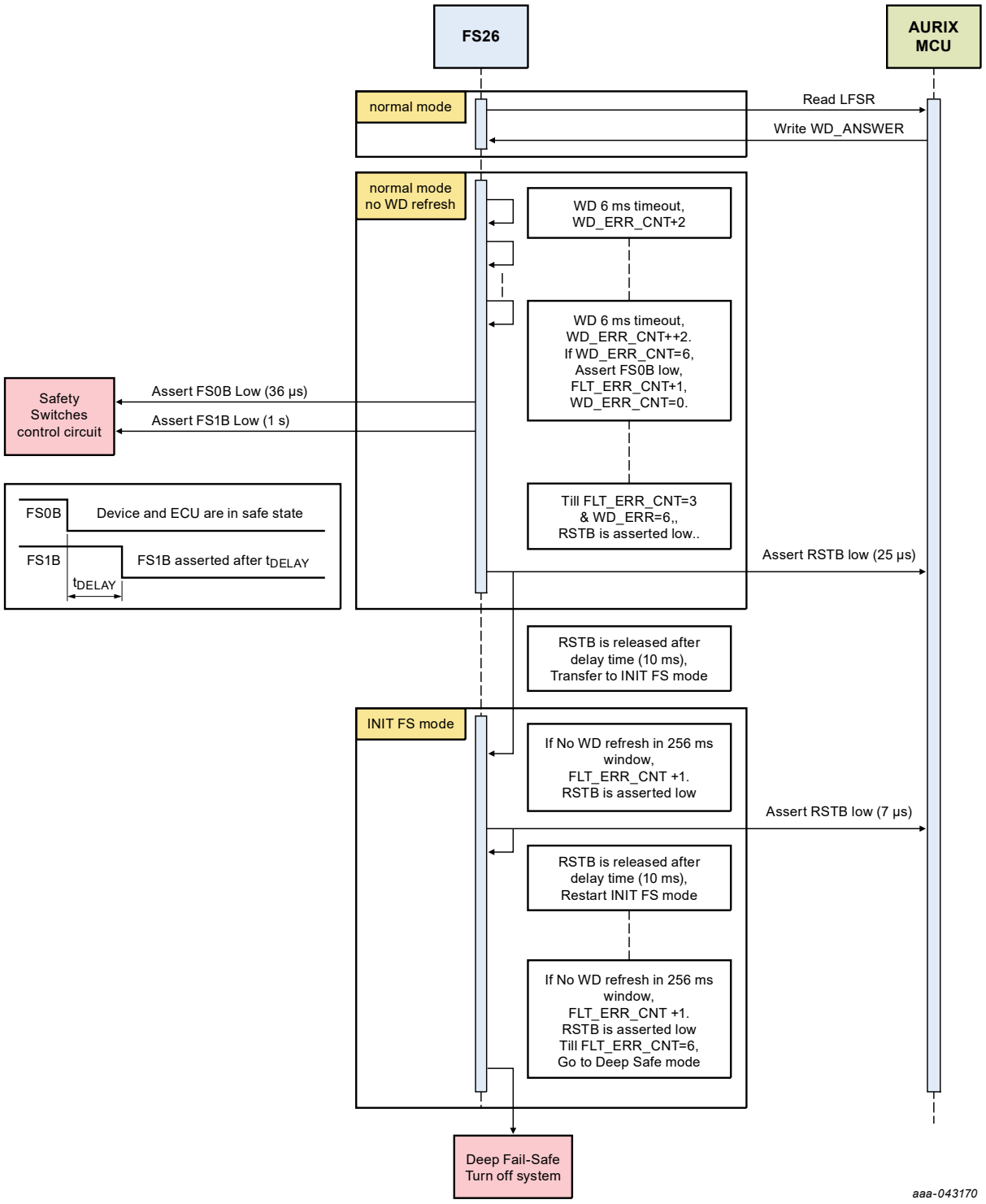


Figure 57. WD fault management sequence (to DFS)

1. FS26 window WD opens a 6 ms window with 50 % duty cycle in Normal mode.
2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2.
3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2.

4. When the WD_ERR_CNT = 6, FS0B is asserted LOW according to WD_FS_REACTION and WD_ERR_LIMIT configuration. The FLT_ERR_CNT increments to 1.
5. WD_ERR_CNT is set back to 0.
6. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_ERR_CNT = 6, RSTB and FS0B are asserted LOW.
7. FS26 asserts FS1B LOW following FS0B status after a 1 s delay.
8. AURIX MCU is reset.
9. After a 10 ms delay time, RSTB is released; FS26 transfers to INIT_FS mode, a 256 ms window opens and waits for a new WD refresh from the AURIX MCU.
10. In the absence of a good WD refresh, FLT_ERR_CNT is incremented and RSTB is asserted LOW again.
11. In the absence of a good WD refresh, the device loops from step 9 to step 10 until FLT_ERR_CNT = 6 (maximum value). FS26 then goes to DFS mode.

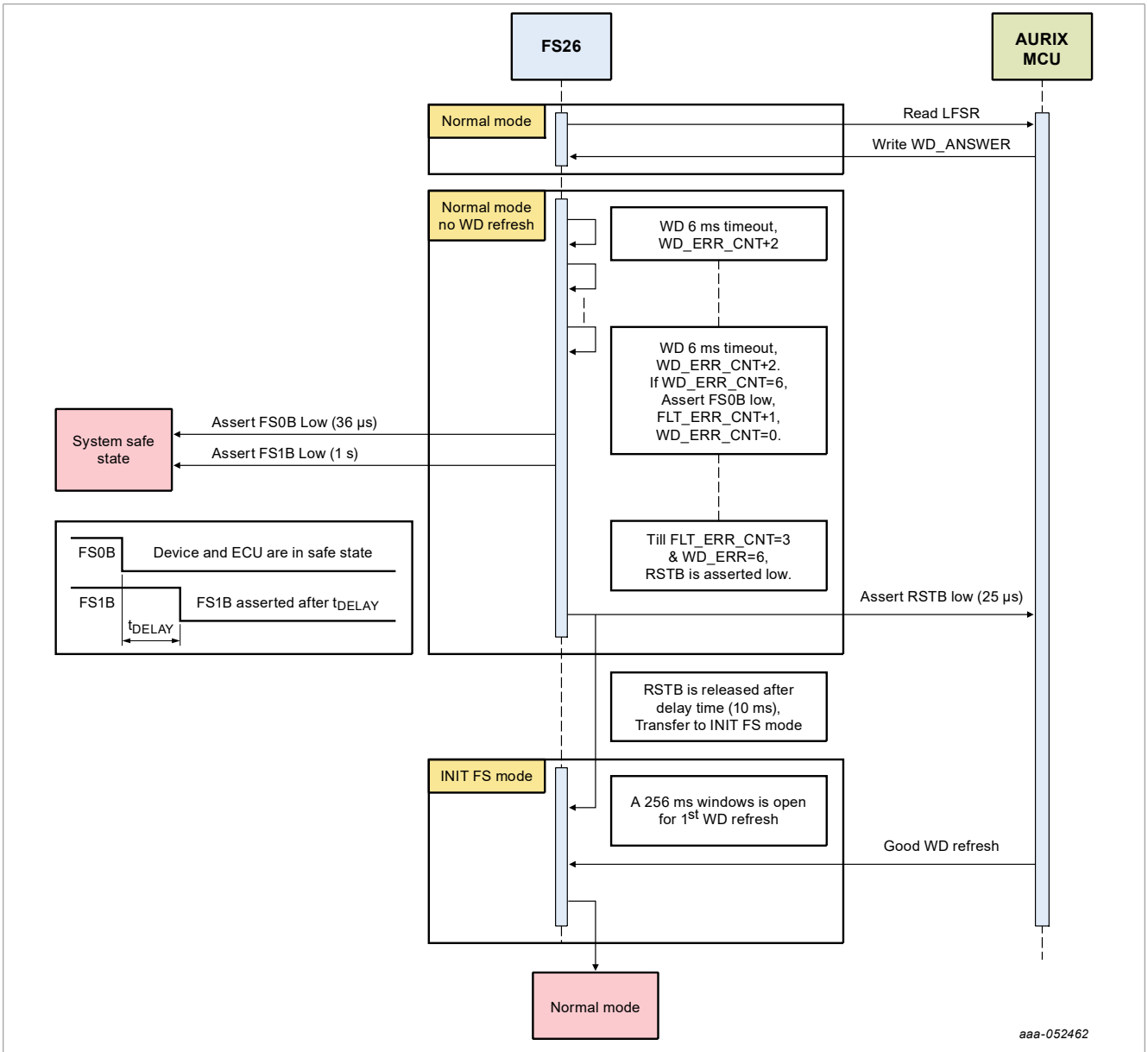


Figure 58. WD fault management sequence (to recovery)

1. FS26 Window WD opens a 6 ms window with 50% duty cycle in normal mode
2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2
3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2
4. When the WD_ERR_CNT = 6, FS0B is asserted LOW according to the WD_FS_REACTION and WD_ERR_LIMIT configuration; the FLT_ERR_CNT increments by 1
5. WD_ERR_CNT is set back to 0
6. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_ERR_CNT = 6, RSTB and FS0B are asserted LOW
7. FS26 asserts FS1B LOW to follow FS0B status after 1 s
8. AURIX MCU is reset
9. After a 10 ms delay time, RSTB is released; FS26 transfers to INIT_FS mode, a 256 ms window opens and waits for a new WD refresh from the AURIX MCU
10. The periodic WD handshake is recovered between the FS26 and the AURIX MCU; FS26 returns to Normal mode thanks to successive good WD refreshes, and as soon as the AURIX MCU releases FSxB safety outputs, FLT_ERR_CNT decrements to 0.

4.7.3 AURIX TC2xx/TC3xx FCCU fault

Use assumptions:

- System is running in Normal mode (RSTB and FSxB are released)
- FCCU_CFG[2:0] = 110, HIGH and LOW level timings are monitored on FCCU1 pin
- FCCU1_FS_REACTION = 0, FS0B only is asserted LOW when a fault is indicated on FCCU1
- FLT_RECOVERY_DIS_VOTP = 0, the fault recovery strategy feature is available
- WDW_RECOVERY[3:0] = 1011, set the WD window duration for MCU recovery to 64 ms
- RSTB_DUR = 0, set to configure the RSTB LOW duration time to 10 ms
- FLT_ERR_CNT_LIMIT = 01, to set the fault error counter intermediate value to 3 and its maximum to 6
- FLT_ERR_REACTION = 1X, RSTB and FS0B are asserted LOW if FLT_ERR_CNT ≥ intermediate value
- FS1B_TDELAY = 00000, FS1B_TDUR = 11111, set FS1B to react like FS0B
- DFS_DIS_OTP = 0x00 by OTP (register CFG_OVUV_3_OTP), DFS function is enabled

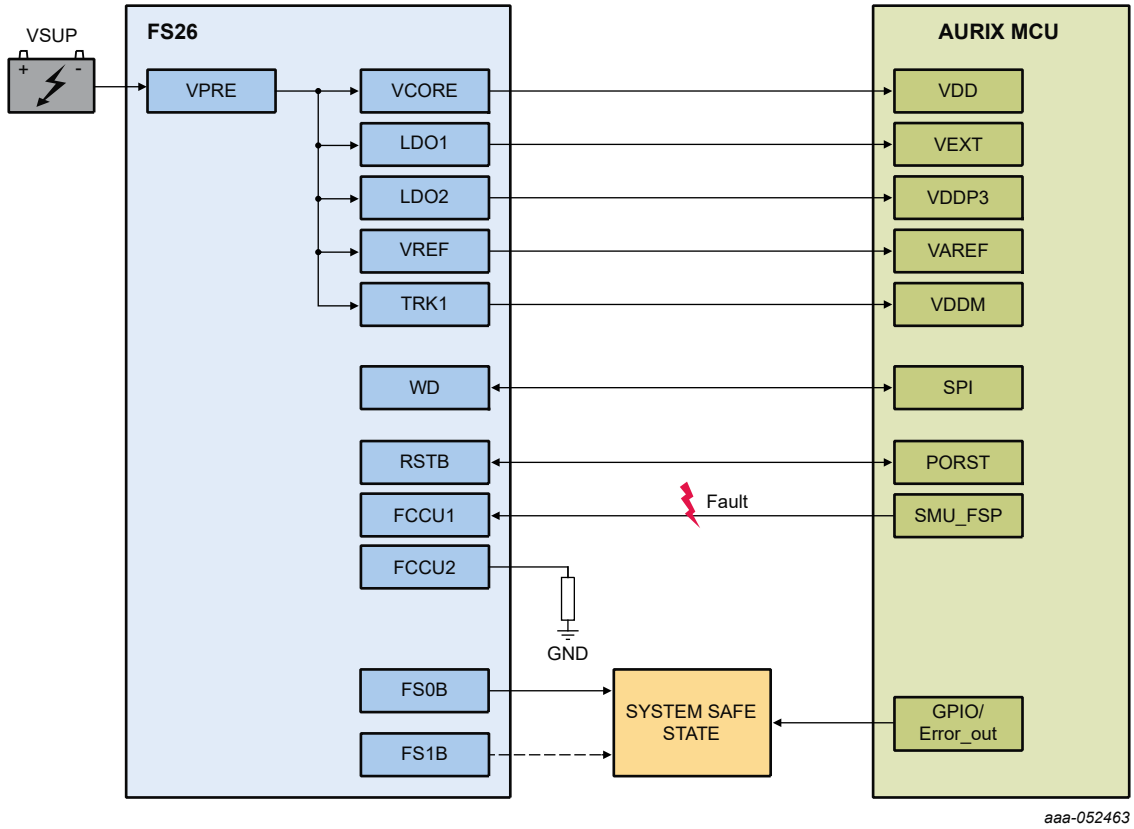


Figure 59. FCCU fault management simple schematic

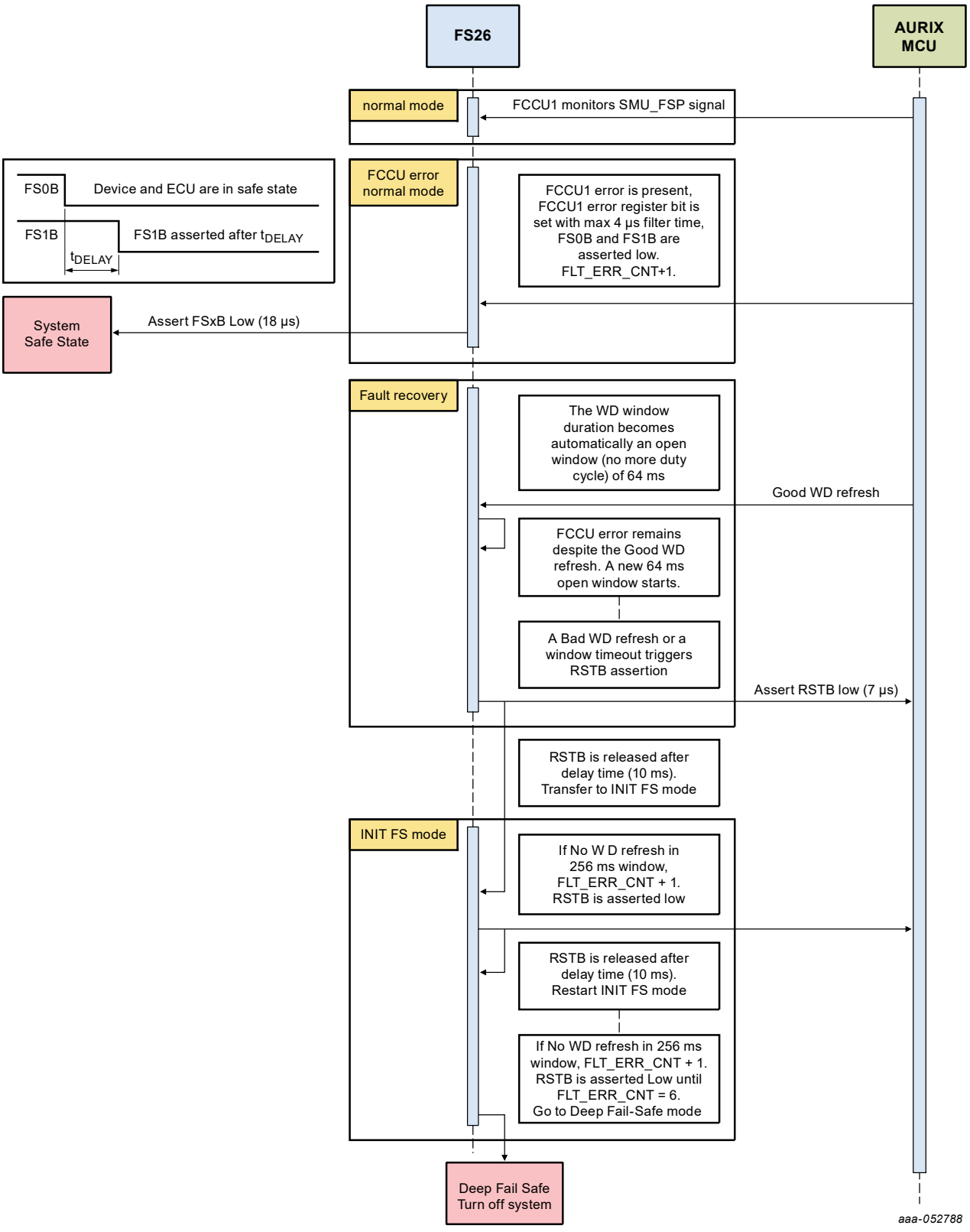


Figure 60. FCCU fault management sequence diagram (to DFS)

1. FS26 is continuously monitoring the AURIX SMU_FSP signal through its FCCU1 pin as soon as the INIT FS phase is closed
2. A hardware failure occurs on the AURIX MCU side; FS26 triggers an FCCU fault with maximum 1.2 µs filtering time (max $t_{FCCU\_ERR\_PWM}$) and FLT_ERR_CNT is incremented
3. FS26 asserts FS0B and FS1B LOW and a 64 ms open WD window starts to allow AURIX MCU to recover before RSTB is asserted
4. A good WD refresh is received from the AURIX MCU but the FCCU1 error remains; another 64 ms open WD window is created
5. FCCU error remains and a bad WD refresh or a timeout happens. RSTB pin is asserted LOW, bringing the AURIX MCU into reset
6. After a 10 ms delay time, RSTB is released; FS26 transfers to INIT_FS mode, a 256 ms window opens and waits for a new WD refresh from the AURIX MCU
7. In the absence of a good WD refresh, FLT_ERR_CNT is incremented and RSTB is asserted LOW again
8. In the absence of a good WD refresh, the device loops from step 6 to step 7 until FLT_ERR_CNT = 6 (maximum value); FS26 then goes to DFS mode

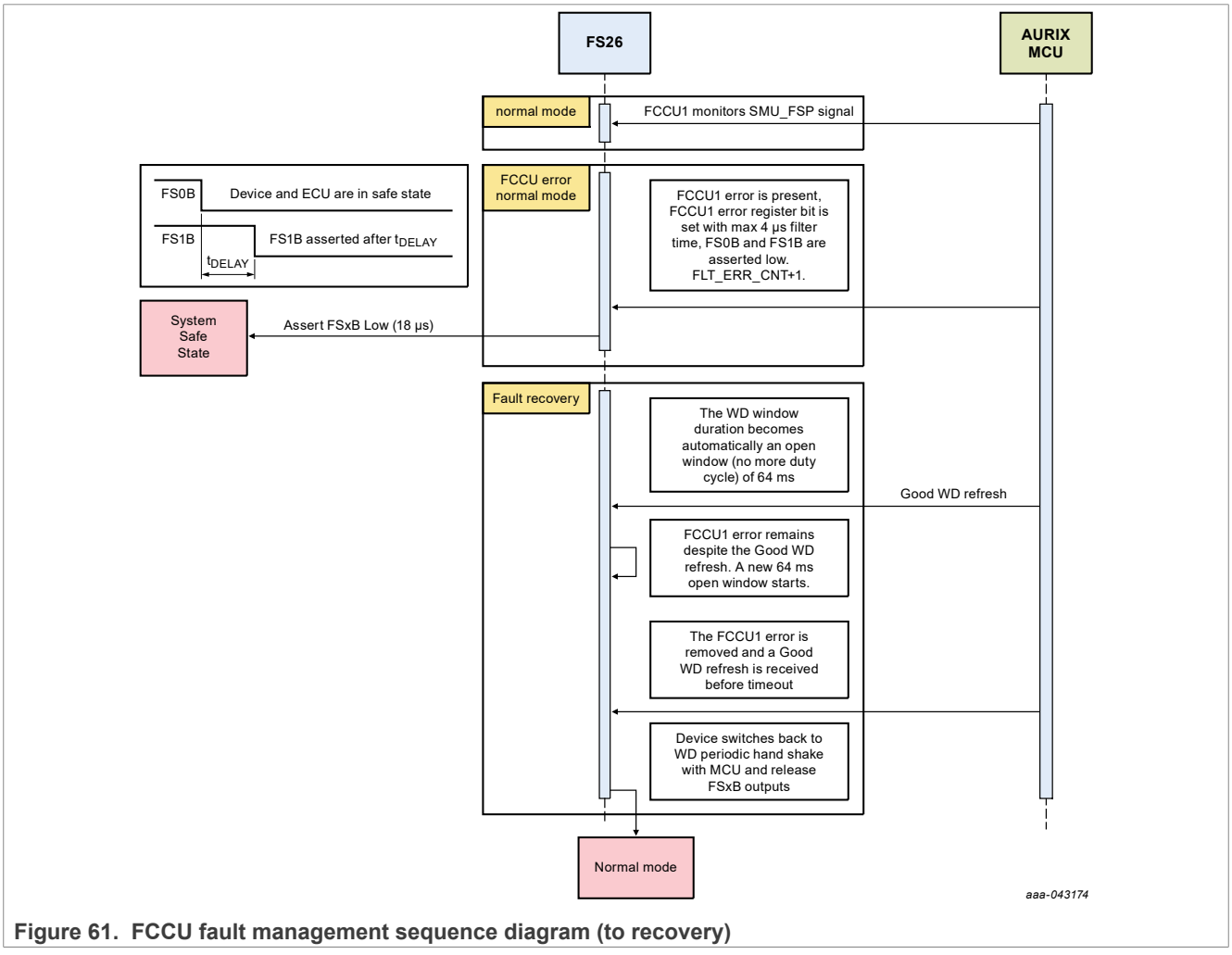


Figure 61. FCCU fault management sequence diagram (to recovery)

1. FS26 is continuously monitoring the AURIX SMU_FSP signal through its FCCU1 pin as soon as the INIT FS phase is closed
2. A hardware failure occurs on the AURIX MCU side; FS26 triggers a FCCU fault with max 1.2 µs (max $t_{FCCU\_ERR\_PWM}$) filtering time, and FLT_ERR_CNT is incremented

3. FS26 asserts FS0B and FS1B LOW and a 64 ms open WD window starts to allow AURIX MCU to recover before RSTB is asserted.
4. A good WD refresh is received from the AURIX MCU but the FCCU1 error remains; another 64 ms open WD window is created.
5. The FCCU error is removed and a good WD refresh is received; the AURIX MCU has recovered.
6. The periodic WD handshake is recovered between FS26 and AURIX MCU; the FS26 returns to Normal mode due to successive good WD refreshes, FLT_ERR_CNT decrements to 0, as soon as the AURIX MCU releases FSxB safety outputs.

4.7.4 Other recovery

When a fault occurs, both fail-safe outputs, FS0B and FS1B, are asserted LOW. Thereafter, some conditions must be fulfilled before allowing the device to release these pins again. These conditions are:

• ABIST1_PASS = 1

• Fault is removed

• Fault error counter must be cleared (= 0)

• RELEASE_FSxB command must be received and valid

When the device is in DFS, all the regulators are off and all safety outputs (RSTB, FS0B and FS1B) are asserted LOW. The FS26 device can either exit DFS thanks to WAKE1 pin toggled from LOW to HIGH level by the system, if enabled by OTP (WK1DFS_DIS_OTP = 0), or due to auto retry mode (infinite or limited tries) when enabled by OTP (RETRY_DIS_OTP = 0).

5 FS85/FS84 solution

5.1 Product overview

The FS85/FS84 family of SBCs integrates a battery-connected pre-regulator that generates an intermediate voltage, typically 3.3 V or 5.0 V. This intermediate voltage can be used as input voltage to: lower voltage DC-DC converters, VDDIO and LDO linear regulators. It can also be used as an input voltage to other PMICs due to its scalable current capability. Using I/Os and functional safety features built into the device, the system designer can maximize the safety level up to ASIL D.

5.1.1 Documentation references

- **FS85 Device Webpage**
- **FS84 Device Webpage**

The above links point to web pages that contain a variety of material related to the FS85/FS84 family. These web pages provide more detailed information about specific topics:

• **FS85/FS84 data sheet**: information such as features, functional description, parametric description, register mapping

• **F85/FS84 functional safety manual**: describes how to use the FS85/FS84 in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level

• **AN12333, FS85/FS84 product guidelines**: information such as application schematics, bill of material, placement and layout guidelines, application validation data [ISO/non-ISO pulses, EMC].

• **AN12807, Complete system power solution using FS85/FS84 and PF502x family**: application note with details on how to integrate an FS85/FS84 with a low voltage PMIC from the PF502x family.

5.1.2 Functional block diagram

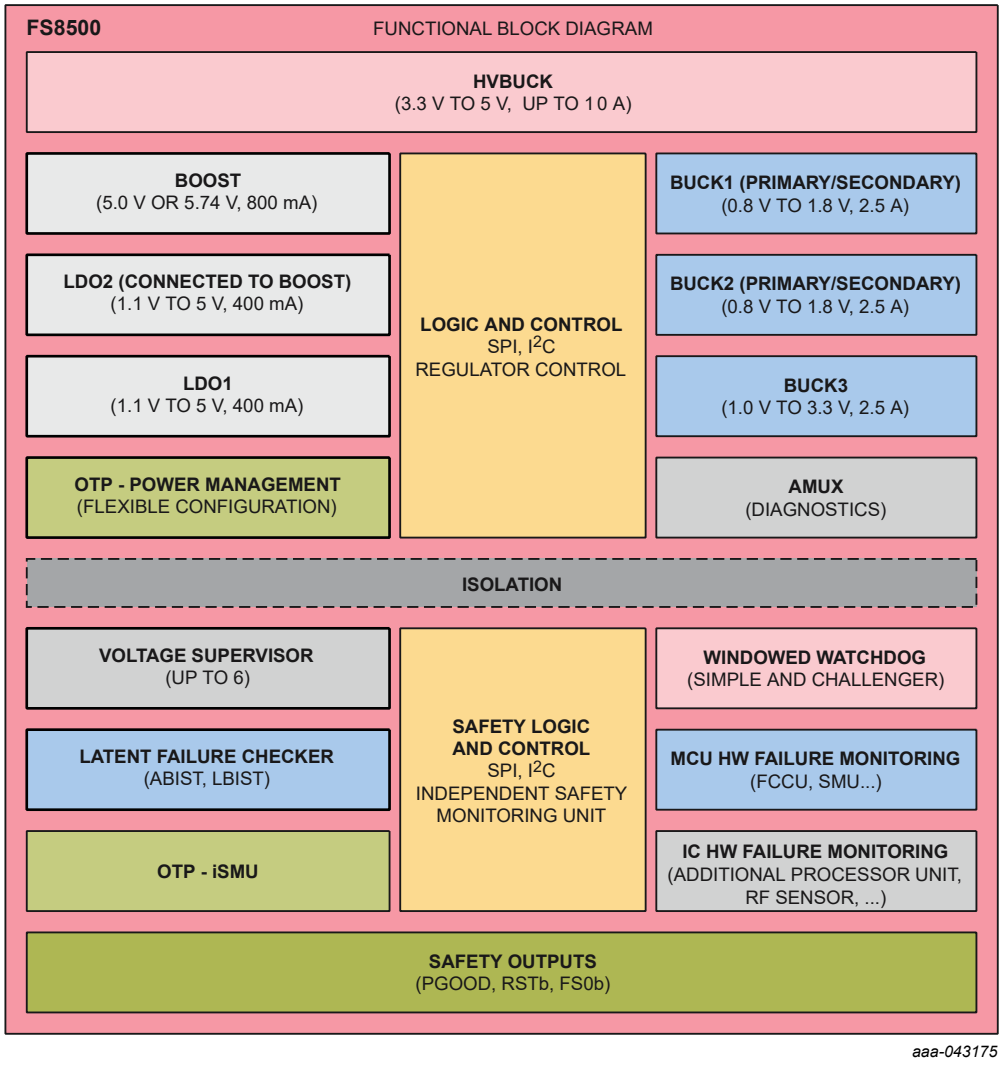


Figure 62. FS85 functional block diagram

5.1.3 Key features

The FS85/FS84 device presents different types of power management blocks, with an independent safety island for supporting ASIL B (FS84) or ASIL D (FS85) applications.

Below is a summary of the different power management blocks:

- Input supply up to 60 V for 12 V and 24 V systems
- HVBUCK (also named VPRE), synchronous buck with external MOSFET, programmable switching frequency 455 kHz or 2.22 MHz, programmable 3.3 V to 5 V, with scalable output current up to 10 A
- BUCK1/2, synchronous buck with internal MOSFET, programmable switching frequency up to 2.22 MHz, programmable 0.8 V to 1.8 V, with up to 2.5 A DC (3.6 A peak) can operate in dual phase, delivering 5 A DC. BUCK1/2, in dual phase and single phase, have static voltage scaling (SVS) capability
- BUCK3, synchronous buck with internal MOSFET, programmable switching frequency up to 2.22 MHz, programmable 1.0 V to 3.3 V, with up to 2.5 A DC (3.6 A peak)
- BOOST with internal MOSFET, 5 V or 5.74 V, up to 800 mA DC (1.5 A peak)

- LDO1/2, programmable 1.1 V to 5 V, up to 400 mA
- Synchronization signal for dual or multiple device operation / power good output
- Frequency synchronization Fin/Fout

The device presents also other safety and system features such as:

- Communication via 32-bit SPI and I^2C (including CRC)
- Standby mode (with supply off): 10 µA in LPOFF, wakeup via WAKE1/2 pins
- AMUX: Battery voltage monitoring, internal safety critical voltages, precise VREF and temperatures
- Emulation and programming capability offered in engineering mode only

But also provides functional safety:

- Independent safety monitoring unit: LBIST, ABIST, VMONx, ERRMON, FCCU, watchdog, safety outputs (PGOOD, RSTB and FS0B).

Compliance:

- EMC: spread spectrum, frequency synchronization, VPRE slew rate control, frequency tuning

5.2 Safety management with AURIX MCU

To fulfill the safety-critical applications, a dedicated Fail-safe machine (FSM) is provided. The FSM is composed of three main sub-blocks:

- Voltage supervisors
- Reset output;
- Two HW SoC monitoring pins (FCCU) inputs for NXP and non-NXP MCU monitoring
- Fail-safe output driver (FSO)
- Built-in self-test (BIST)

The FSM is independent from the rest of the circuitry to avoid common-cause failures. The FSM has its own voltage regulators (analog and digital), dedicated bandgap, and oscillator. This block is physically independent from the rest of the circuitry, due to dedicated layout placement and trench isolation.

5.2.1 Safety outputs

In normal operation, when FS0B and RSTB are released, the fault error counter is incremented when a fault is detected by the FS85/FS84 Fail-safe state machine.

Table 19 lists the faults and their impact on RSTB and FS0B pins according to the device configuration. The faults that are configured to not assert RSTB and FS0B will not increment the fault error counter. In that case, only the flags are available for MCU diagnostics. When FS0B is asserted, the fault error counter continues to be incremented by one each time the WD error counter reaches its maximum value. Refer to the safety manual for more details on the safety implementation.

Table 19. Application-related fail-safe fault list and reaction

Apps-related fail-safe faults	FLT_ ERR_CNT increment	FS0B assertion [1] [2]	RSTB assertion[1][2]	PGOOD assertion[1][2]
VCOREMON_ OV	+1	VCOREMON_OV_FS_ IMPACT[0]	VCOREMON_OV_FS_ IMPACT[1]	OTP_PGOOD_VCORE
VDDIO_OV	+1	VDDIO_OV_FS_IMPACT[0]	VDDIO_OV_FS_IMPACT[1]	OTP_PGOOD_VDDIO
VMONx_OV	+1	VMONx_OV_FS_IMPACT[0]	VMONx_OV_FS_IMPACT[1]	OTP_PGOOD_VMONx

Table 19. Application-related fail-safe fault list and reaction*...continued*

Apps-related fail-safe faults	FLT_ ERR_CNT increment	FS0B assertion [1] [2]	RSTB assertion[1][2]	PGOOD assertion[1][2]
VCOREMON_ UV	+1	VCOREMON_UV_FS_ IMPACT[0]	VCOREMON_UV_FS_ IMPACT[1]	OTP_PGOOD_VCORE
VDDIO_UV	+1	VDDIO_UV_FS_IMPACT[0]	VDDIO_UV_FS_IMPACT[1]	OTP_PGOOD_VDDIO
VMONx_UV	+1	VMONx_UV_FS_IMPACT[0]	VMONx_UV_FS_IMPACT[1]	OTP_PGOOD_VMONx
FCCU12 (pair)	+1	FCCU1_FS_IMPACT	FCCU1_FS_IMPACT	no
FCCU1 (single)	+1	FCCU12_FS_IMPACT	FCCU12_FS_IMPACT	no
FCCU2 (single)	+1	FCCU2_FS_IMPACT	FCCU2_FS_IMPACT	no
ERRMON	+1	ERRMON_FS_IMPACT	FCCU2_FS_IMPACT	no
WD error counter = max value	+1	WD_FS_IMPACT[0]	WD_FS_IMPACT[1]	no
fault error counter impact at intermediate value	no	FLT_ERR_IMPACT[0]	FLT_ERR_IMPACT[1]	no
wrong WD refresh in INIT_FS	+1	yes	yes	no
no WD refresh in INIT_FS	+1	yes	yes	no
external RESET (out of extended RSTB)	+1	no	yes (low externally)	OTP_PGOOD_RSTB
RSTB pulse request by MCU	no	no	yes	no
RSTB short to high	+1	yes	no (high externally)	no
FS0B short to high	+1	no (high externally)	FS0B_SC_HIGH_CFG	no
FS0B request by the MCU	no	yes	no	no
REG_ CORRUPT=1	+1	yes	no	no
OTP_ CORRUPT=1	+1	yes	no	no
GOTO_INITFS request by MCU	no	yes	no	no

[1] In orange, the reaction is not configurable.
[2] In green, the reaction is configurable by OTP for and by SPI only during the INIT_FS phase.

5.2.2 Voltage monitoring

VMON1/2/3/4 and VDDIO can be used to monitor FS85/FS84 supply rails, or even external regulators of the system. VCOREMON is used to monitor FS85/FS84 BUCK1. Depending on the system safety requirement, they can be used to monitor only FS85/FS84 device rails or also other peripherals voltage rails to reach an ASIL D safety level.

5.2.3 Watchdog

The FS85/FS84 acts as a supervisor of the application operation, and as a consequence, includes a windowed watchdog (temporal and logical monitoring) which must be refreshed periodically by the MCU. This means that the FS85/FS84 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 a safe-state system within the FTTI. Thus, either the MCU or the SBC can switch the system to a safe state.

The duration of the watchdog window is configurable, to allow different MCU handshake strategies. The configurable duty cycle of the window is fixed at 50 %. Therefore the first half of the window is said to be closed and the second half is said to be open. The watchdog must be refreshed during the open window (see Figure 63).

After a good or a bad watchdog refresh, a new window period starts immediately in order for the MCU to remain synchronized with the windowed watchdog. The first good watchdog refresh closes the INIT_FS. Then, the watchdog window is running, and the MCU must refresh the watchdog in the open window of the watchdog window period. The duration of the watchdog window is configurable from 1.0 ms to 1024 ms with the WDW_PERIOD[3:0] bits. The new watchdog window is effective after the next watchdog refresh. The watchdog window can be disabled during INIT_FS only. The watchdog disable is effective when the INIT_FS is closed.

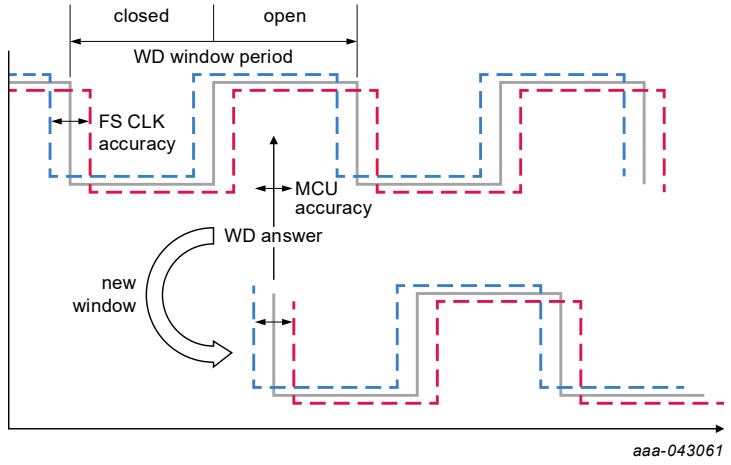


Figure 63. Windowed watchdog

5.2.4 HW SoC monitoring (FCCU)

FCCU monitoring is meant to detect any HW failures from the MCU. It is active as soon as the INIT_FS is closed by the first good WD refresh. In the FS85/FS84, FCCU_CFG bits must be configured by the MCU during the initialization phase to activate the FCCU monitoring. FCCU1 and FCCU2 pins monitor by pair in bistable protocol by default with NXP MCUs. They are also capable of monitoring non-NXP MCUs, however, such as AURIX TC2xx/TC3xx, due to independent monitoring configurations.

When connected to the AURIX MCU, the FCCU1 input pin can be configured as below to work with a single error-out pin from the AURIX SMU without connecting the FCCU2 pin.

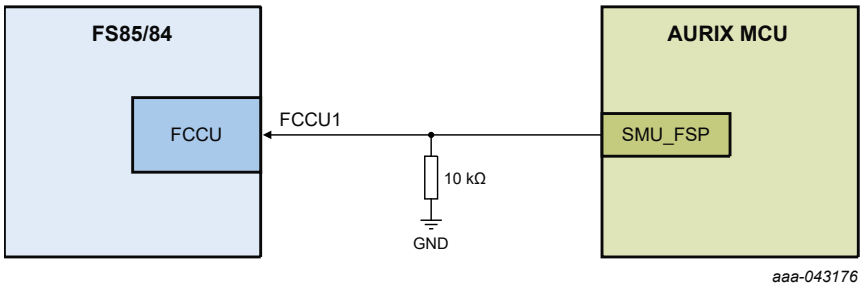


Figure 64. FS85/84 FCCU connection to AURIX SMU in single output fault mode

When using default polarity settings, internal pullups and pulldowns provide passive fault detection, in case the MCU does not drive its SMU_FSP (Fault Signaling Protocol) output pins. External pullup/pulldown must be used if using a reverse polarity configuration.

The FS84 and the FS85 are also capable of monitoring the AURIX MCU through the SMU_FSP signal in PWM mode (toggling signal). To make this possible, the system engineer has to take into account the following requirements:

- The PWM frequency indicates good MCU behavior, > 125 kHz. That corresponds to (1 / 4 us / 2) with a duty cycle = 50 %
- The steady state indicates an MCU error that is lLOW or HIGH for > 8 µs
- When FCCUx_FLT_POL = 0 (default), the FCCUx input must be HIGH before INIT_FS closure. When the PWM stops and FCCUx is stuck low for > 8 µs, the failure is detected
- When FCCUx_FLT_POL = 1, FCCUx input must be LOW before INIT_FS closure. When the PWM stops and the FCCUx is stuck HIGH for > 8 µs, the failure is detected
- The PWM starts after the INIT_FS is closed and before releasing the FS0B pin, within the FTTI of the safety goal
- When the failure is detected, the FS85/FS84 reacts with FS0B or FS0B + RSTB assertion, depending on the FCCUx_FS_IMPACT configuration

If FCCU1 happens to be shorted to ground, however, this event cannot be detected (see Figure 66) unless the MCU performs a latent failure check on this pin at initialization.

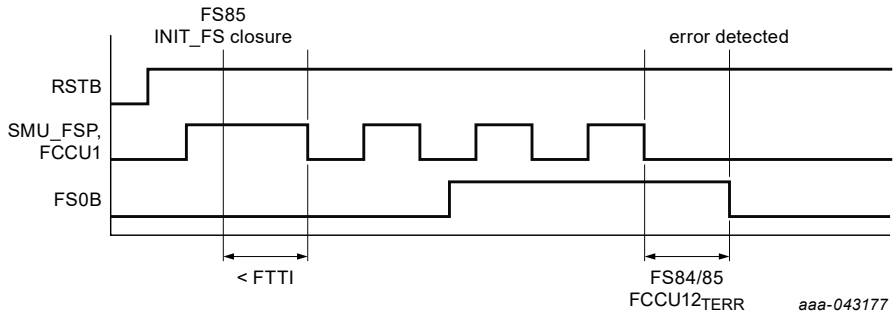


Figure 65. FS84/85 FCCU monitoring with AURIX PWM signal

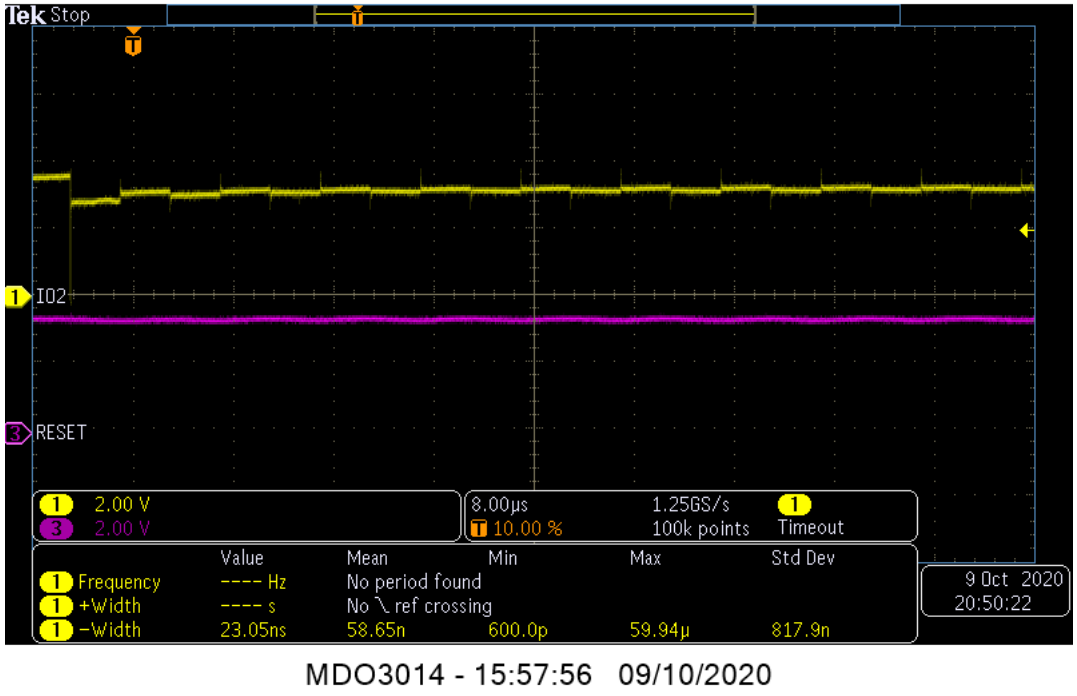


Figure 66. FCCU pin shorted to VDDIO - fault not detected and RESET not asserted

If the PWM frequency drifts lower, which is considered a MCU failure, the drift will be detected when dropping below 125 kHz.

If the PWM frequency drifts higher, though, the FS device cannot detect this failure event through FCCU monitoring alone (see Figure 67). In this situation T_{ON} and T_{OFF} timings will always be under the 4 µs filtering time, thus preventing the FS device from detecting the drift.

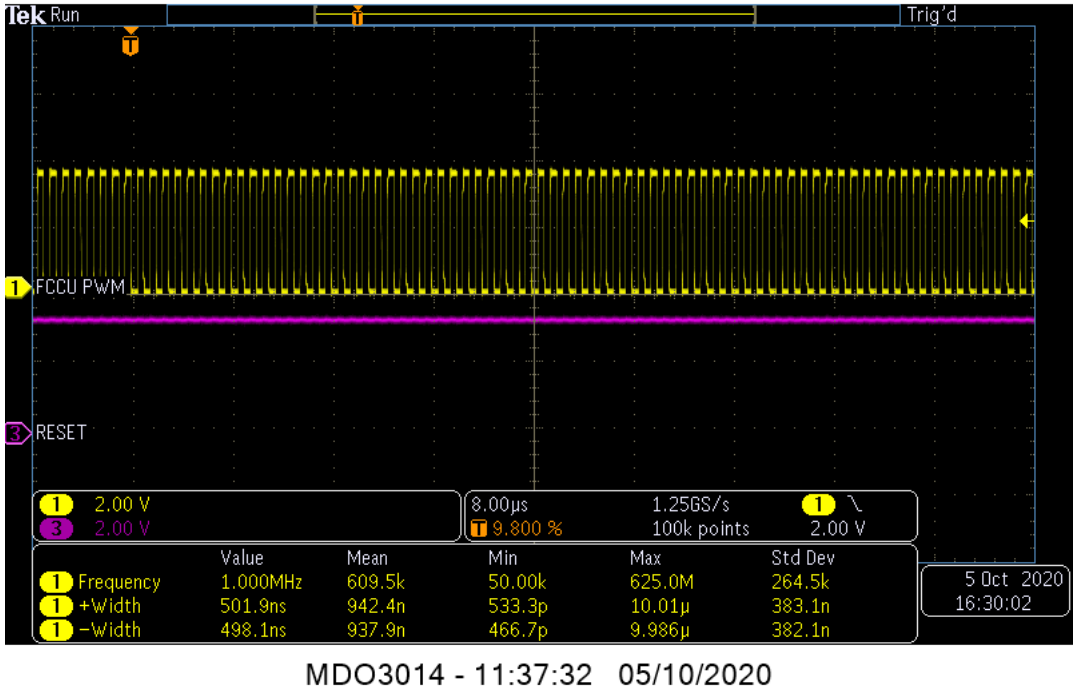


Figure 67. Frequency drift (up) fault not detected and RESET not asserted (f = 1 MHz / T_{ON} = 501.9 ns / T_{OFF} = 498.1 ns)

To be able to detect such an event, the windowed WD monitoring can be used in a variety of ways. An increasing drift in the MCU's clock frequency inevitably impacts its WD answer frequency and also leads to multiple WD errors.

The MCU must always trigger the WD in the open WD window, or an error is generated. Below are the steps followed during the handshake in the FS85 with challenger WD (FS84 is ASIL B and features simple WD only):

1. FS85 generates a pseudo random code (LFSR)
2. MCU reads the code
3. Both MCU and FS85 calculate the WD answer using the same formula
4. MCU sends its WD answer and FS85 compares with its own answer
5. If the WD answer is wrong or sent in the closed WD window, a WD error is generated If the good WD answer is sent in the open WD window, a new WD window opens and the handshake restarts

From here, there are two different ways to improve detectability:

- One can choose to reduce the WD window period, in order to capture as fast as possible the MCU frequency drift, taking into account the ±10 % accuracy of the FS85/FS84 clock but also the MCU accuracy.
- One can decide to have the MCU WD answer sent at the very beginning of the WD open window. This workaround is more severe and would allow detection to occur faster than any MCU frequency drift increase. Again, the MCU and the FS85/FS84 clock accuracies must be taken into the calculations, to prevent the occurrence of false WD answers.

Example: *Down to 1 ms, the WD period can be between 0.9 ms and 1.1 ms (1 ms ±10%). With 50 % duty cycle, the MCU WD answer should be sent between 0.55 ms (worst case is 60 % of 0.5 ms) and 0.9 ms (see Figure 63).*

Assuming the FCCU1 pin is connected as shown in Figure 64, follow the steps below to enable the FCCU with the AURIX SMU:

1. Configure the FS device: FCCU1 is the only active monitoring input.
2. Configure the AURIX SMU in PWM mode.
3. Proceed to a latent failure check to detect shorted pin: at INIT phase, toggle the pin and check the FCCU1 flag status. The flag must follow the pin status.
4. Set FCCU1 to its valid state (HIGH level in our use case) when closing the INIT_FS phase before entering Normal mode.
5. The FCCU/SMU function is checked and operational. AURIX can switch to PWM SMU_FSP signal.

5.3 Power management

5.3.1 FS8530 + TC29x/TC39x

The following diagrams and tables show all the power connections between FS85/FS84 and AURIX TC2xx/TC3xx.

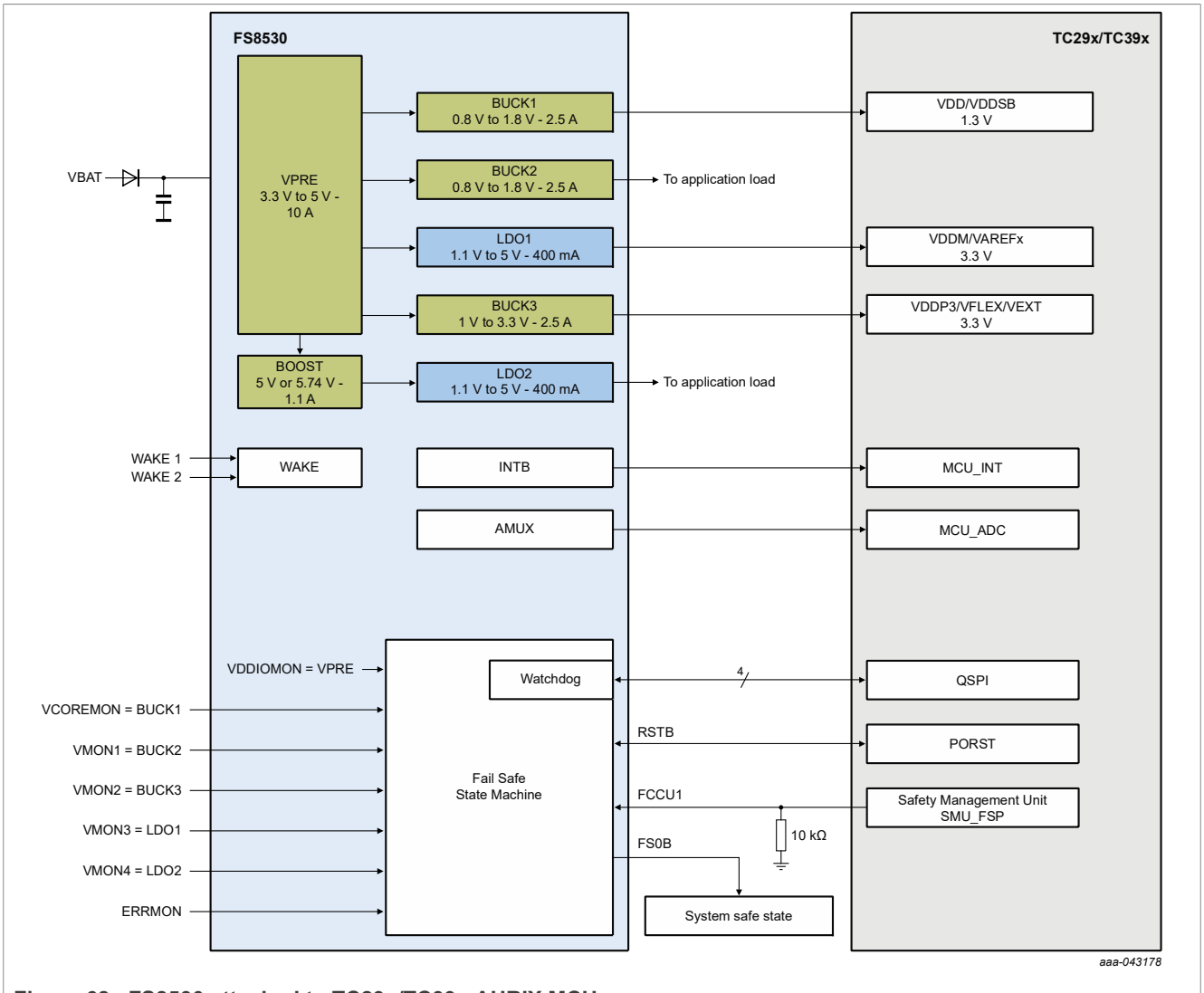


Figure 68. FS8530 attached to TC29x/TC39x AURIX MCU

The FS84 and FS85 family of products come with multiple variations. Depending on the safety level required, FS841x or FS843x (for ASIL B with up to 2 VMONx) and FS8510 or FS8530 (for ASIL D with up to 4 VMONx) are compatible part numbers to attach to AURIX TC2xx/TC3xx MCU families. They all feature the optional BUCK3 providing a 3.3 V power rail to supply AURIX 3.3 V rails.

Table 20. FS8530-TC29x/TC39x connections summary

FS8530 connection	TC29x/TC39x connection	description
BUCK1	VDD_1.3 V and VDDSB	BUCK1 provides 1.25 V voltage rail to VDD in TC29x/TC39x
BUCK3	VDDP3, VFLEX and VEXT	BUCK3 provides 3.3 V voltage rail to VDDP3, VFLEX and VEXT in TC29x/TC39x
LDO2	VDDM and VAREF1/2	LDO2 provides 3.3 V voltage rail to VDDM and VAREF1/2 with ±2 % accuracy in TC29x / TC39x
4 lines SPI	4 lines SPI	SPI connections between FS8530 to TC29x/TC39x
FCCU1	SMU_FSP	SMU connection with pulldown resistor
INTB	MCU_INT	interrupt signal connection
RSTB	PORST	RSTB bidirectional connection for internal/external reset
AMUX	MCU_ADC	monitor signal from AMUX to ADC input in TC29x

5.3.2 FS85/FS84 connections of other pins

Table 21. FS85/FS84 other system connections summary

FS85/FS84 connection	TC29x/TC39x connection	description
FS0B	connect to safety switch	active low (open drain structure); brings the application into a safe state
DBG	connect to resistor ladder in series of switch	for Debug mode enable/disable
FIN	connect to MCU clock	frequency synchronization input
PSYNC	connect to other PMIC	power synchronization input/output

5.4 Application schematic

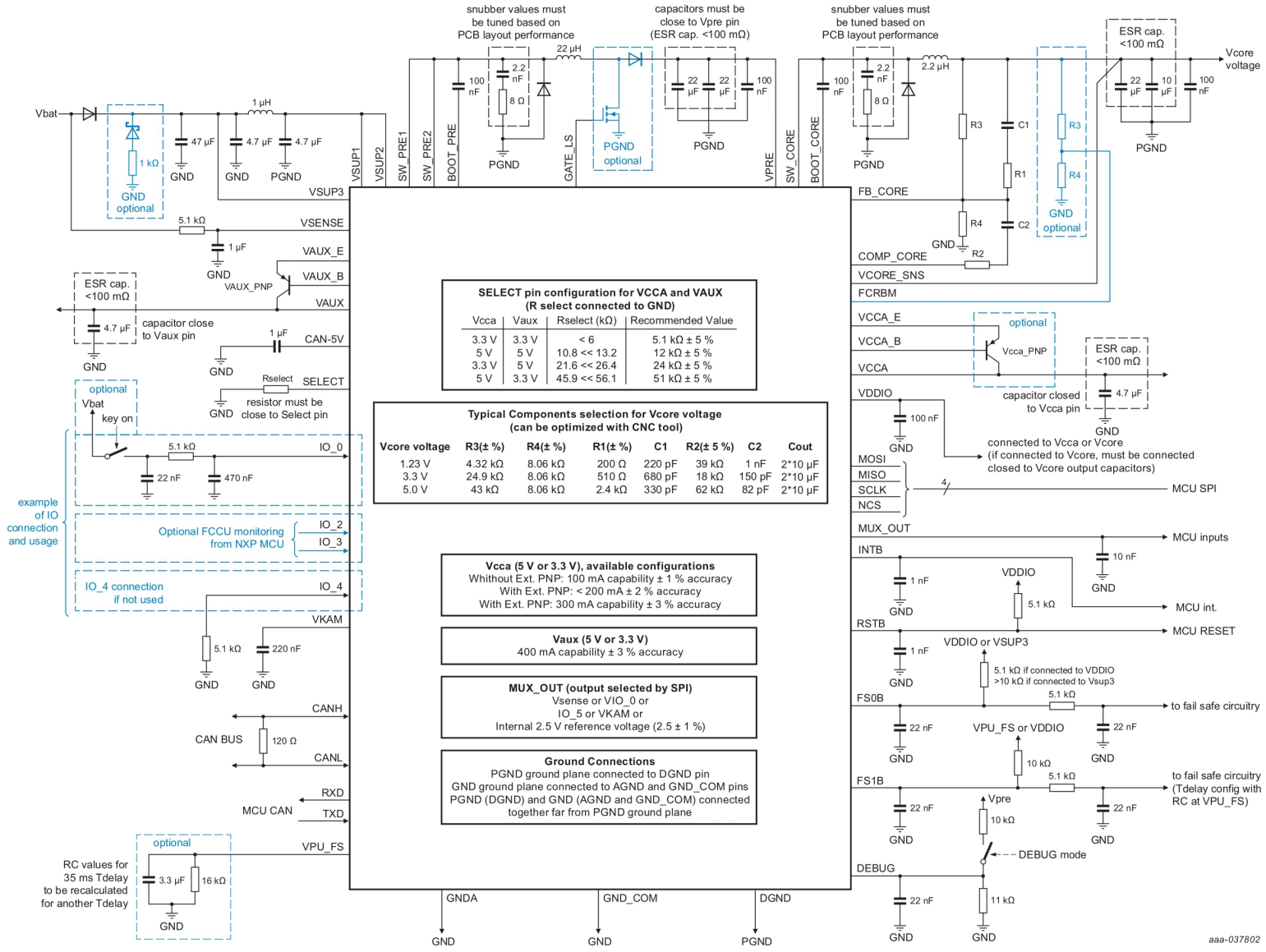


Figure 69. FS85/FS84 application schematic

5.5 BOM

Table 22. FS8530 BOM reference

Domain	item name	value	unit	description	optional
FCCU monitoring	FCCU_PU	5.1	kΩ	pullup resistor for FCCU2 to VDDIO	X
	FCCU_PD	10	kΩ	pulldown resistor for FCCU1	X
VSUP power supply	RP Diode	—		reverse battery protection diode	
	CBAT	47	µF	input crank capacitor	
	CPI1	10 + 0.1	µF	pi filter capacitor + input decoupling capacitor for conducted emission	
	LPI	1	µH	pi filter inductor	
	CPI2	10 + 0.1	µF	pi filter capacitor + input decoupling capacitor for conducted emission	
VBOS	COUT_VBOS	4.7	µF	best of supply decoupling output capacitor	
VPRE preregulator	NMOSFET	—		1 dual MOSFET or 2 single MOSFETs (refer to data sheet for recommended parts)	
	RG_MOSFET	2 x 1	MΩ	NMOSFET gate resistors	
	RSNS_VPRE	10 to 20	mΩ	shunt resistor for VPRE current sensing	
	R_SNUB	2.2	Ω	nubber resistor and capacitor	X
	C_SNUB	2.2	nF		X
	CBOOT_PRE	47	nF	bootstrap capacitor	
	L_VPRE	6.8 or 2.2	µH	power inductor	
	COUT_VPRE	44 to 66	µF	output capacitor	
	RCOMP_VPRE	X	Ω	compensation network	
	CCOMP_VPRE	X	F		
	CHF_VPRE	X	F		
BOOST regulator	LBOOST	4.7	µH	power inductor	
	DBOOST	—		diode	
	COUT_BOOST	44	µF	output capacitor	
BUCKx regulators	CIN_BUCKx	4.7 + 0.1	µF	input capacitor	
	L_BUCKx	1	µH	power inductor	
	COUT_BUCKx	44	µF	output capacitor	

Table 22. FS8530 BOM reference*...continued*

Domain	item name	value	unit	description	optional
LDO1 and LDO2 regulators	COUT1_LDOx	2 x 10	µF	output capacitors	
	COUT2_LDOx	2 x 1	µF		
VMONx (ext. resistor bridge)	R1_VMONx	X	kΩ	VMONx pullup resistor to monitored voltage regulator (must be calculated to deliver a middle point of 0.8 V)	
	R2_VMONx	22.1	kΩ	VMONx pulldown resistor to GND	
wake pins	CIN_WAKE	2 x 22	nF	input capacitors to damp ESD gun stress	
	R_WAKE	2 x 5.1	kΩ	resistors to limit the current	
	COUT_WAKE	2 x 10	nF	decoupling capacitors close to the pin for immunity	
VDDIO	COUT_VDDIO	100	nF	decoupling capacitor close to the pin for immunity	
VDDI2C	COUT_VDDI2C	100	nF	decoupling capacitor close to the pin for immunity	
SCL, SDA	PU_SCL, PU_SDA	5.1	kΩ	SCL, SDA pullup resistors to VDDIO	
AMUX	COUT_MUX	10	nF	resistor and capacitor required for buffer stability	
	R_MUX	220	Ω		
INTB	COUT_INTB	1	nF	decoupling capacitor close to the pin for immunity	
PGOOD	PU_PG	5.1	kΩ	PGOOD pullup resistor to VDDIO	
	PU_COUT	1	nF	PGOOD output capacitor	
reset and fail-safe outputs	COUT_RSTB	1	nF	RSTB decoupling capacitor	
	PU_RSTB	5.1	kΩ	RSTB pullup resistor to VDDIO	
	COUT_FS0B	22	nF	FS0B capacitor to damp ESD gun stress	
	CIN_FS0B	10	nF	FS0B decoupling capacitor close to the pin for immunity	
	PU_FS0B	5.1	kΩ	FS0B pullup resistor to VDDIO	
	R_FS0B	5.1	kΩ	FS0B resistor to limit the current, minimum 0805 size to avoid arcing with high dv/dt such as with ESD gun	

For more detailed information on product guidelines, refer to the dedicated application note: AN12333.

5.6 Timing sequence

5.6.1 Flowchart

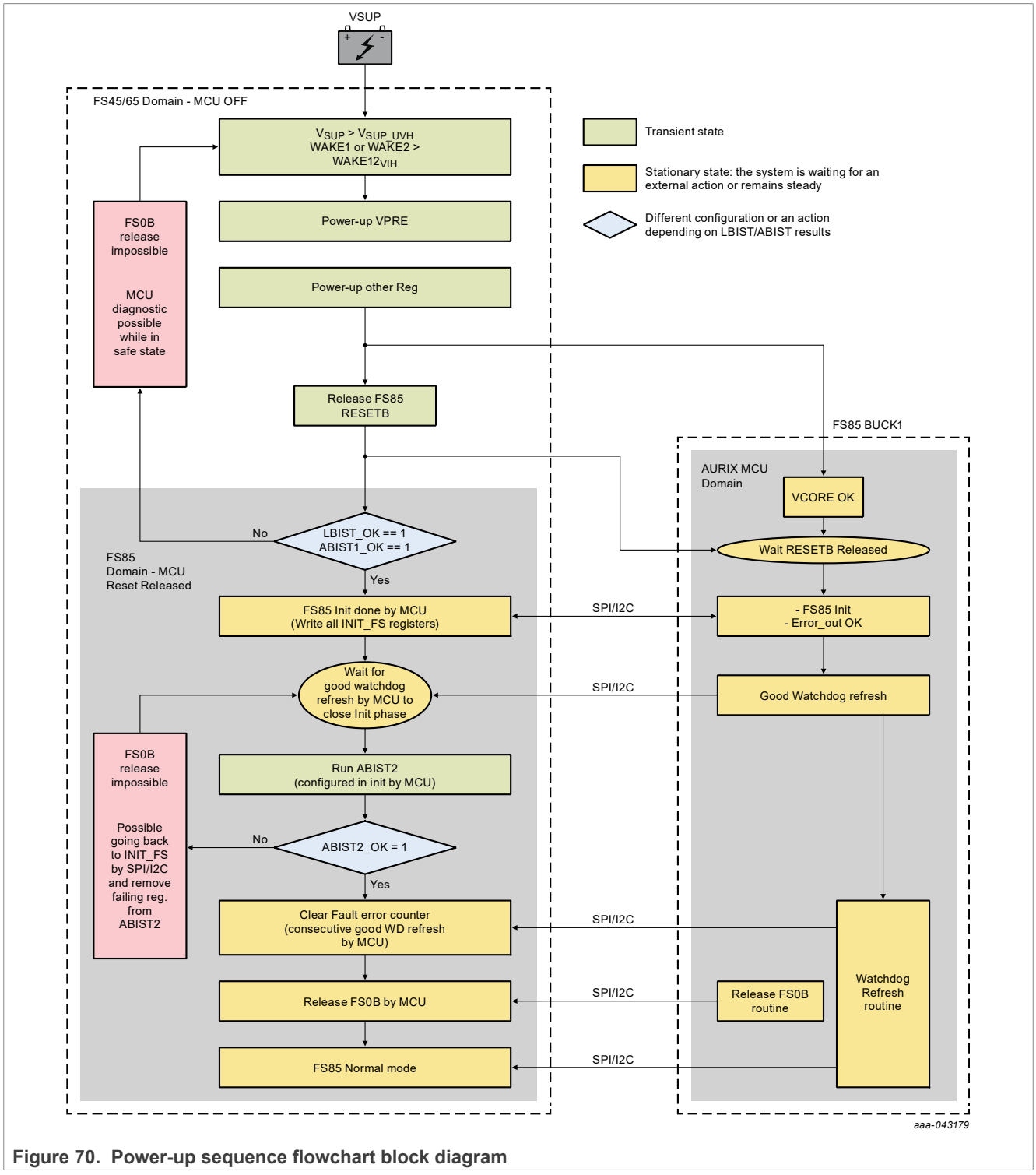


Figure 70. Power-up sequence flowchart block diagram

Below are more details concerning specific states in the flowchart.

FS85/FS84 domain:

- FS85/FS84 Init done by MCU: A window of 256 ms after the release of RSTB is available to configure the initialization register of the FS85/FS84. In this window the following must be configured
  - VMONX_FS_IMPACT[1:0]: defining whenever an overvoltage or undervoltage occurs on a monitored regulator, if RSTB and FS0B pins must be asserted LOW or not
  - VMONX_ABIST2: to decide if ABIST2 is performed on monitoring unit
  - Watchdog configuration, watchdog error counter, watchdog refresh counter, and fault error counter, limit and safety impact
  - FCCU configuration
  - ERRMON configuration

In order to close this window, the MCU must send a good watchdog refresh before the end of the window. Otherwise it will be considered a fault.

- FS85/FS84 Normal mode: In order to be in Normal mode for the FS85/FS84, the pin FS0B must be released. To do so, the error counter *must* be cleared by sending several good watchdog commands until it is back down to 0, and a SPI or I^2C command *must* be sent to finally release the FS0B.

AURIX TC2xx/TC3xx MCU domain:

- MCU VDD OK: Depending on the system architecture, VDD (equivalent for VCORE) from the MCU can be supplied by the FS85/FS84 or by an external source.
- MCU Wait for RSTB Released: The pin RSTB from the FS85/FS84 is chosen in this application note for releasing the RESET of the MCU.

Finally, in normal operation, FS85/FS84 power rails are turned on and the safety pins from the FS85/FS84 RSTB, PGOOD and FS0B are all released. If a fault occurs on the FS85/FS84, the device is ready to react depending on the initialization configuration done previously.

5.6.2 Power sequencing

VPRE is the first regulator to start automatically, followed by the BOOST, before the SLOT_0. The other regulators start based on the OTP power sequencing configuration. Seven slots are available to program the start-up sequence of BUCK1, BUCK2, BUCK3, LDO1 and LDO2 regulators. The delay between each slot is configurable to 250 µs or 1 ms by OTP using the OTP_TSLOT bit to accommodate the different ramp up speeds of BUCK1, BUCK2 and BUCK3.

The power-up sequence starts at SLOT_0 and ends at SLOT_7, while the power-down sequence follows the exact reverse order. All slots are executed, even if no regulators are assigned to a certain slot. Regulators enabled by OTP and assigned to SLOT_7 are not powered during the power-up sequence but it can be done in Normal mode using a SPI/I^2C command from the MCU.

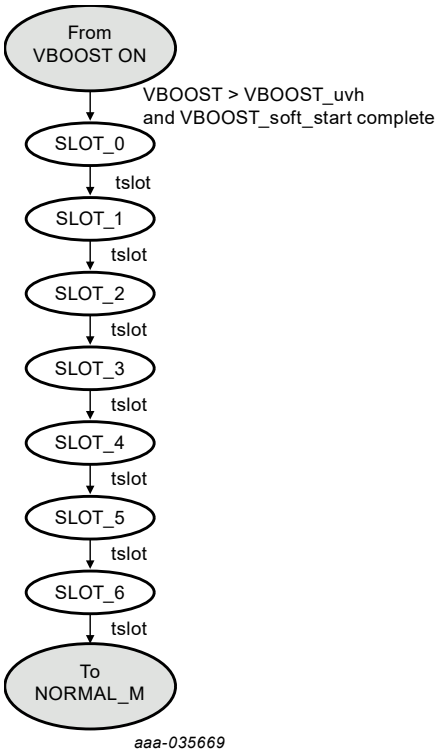


Figure 71. Power-up sequence flow

A system power-up sequence is shown below:

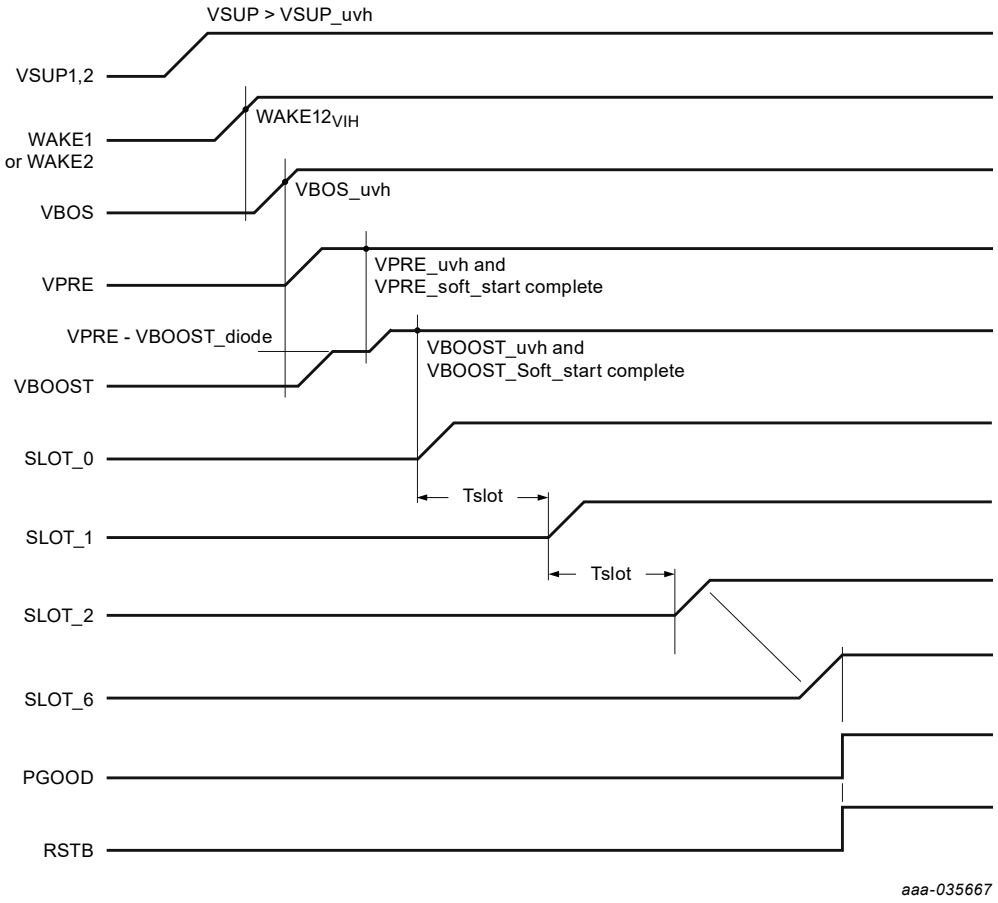


Figure 72. Power-up sequence timing

PGOOD and RSTB release depend on the combination of the power-up sequence and which regulator is assigned to PGOOD and ABIST1 through the voltage monitoring connection (VCOREMON, VDDIOMON and VMONx).

5.7 Fault management and recovery

When the system is operating in Normal mode, different types of faults can occur on the FS85/FS84, the MCU, or on external peripherals. This section explains several fault use cases that the system might encounter, and its reaction to each of them.

Two fault management use cases between FS85/FS84 and AURIX TC2xx/TC3xx are described below: VCORE overvoltage and LDO2 undervoltage. Other faults, such as watchdog and overtemperature follow the same sequence.

5.7.1 AURIX TC2xx/TC3xx VCORE overvoltage

When an overvoltage occurs on any of the voltage regulators assigned to VMONx_REG registers, the FS85/FS84 will:

- Increment its fault error counter
- Eventually assert its safety output FS0B to bring the system into a safe state
- Switch off the corresponding voltage regulator

In this use case, the FS85/FS84 is permanently monitoring the AURIX VDD power supply using its VCOREMON input pin.

Use assumptions:

- System is running in Normal mode (RSTB and FS0B are released)
- VCOREMON_OV_FS_IMPACT[1:0] = 1X (default) set in FS_I_OVUV during INIT_FS phase, BUCK1 OV asserts FS0B and RSTB
- OTP_VCORE_OV_DGLT = 0, set the overvoltage filtering time to 25 µs (typical)
- RSTB_DUR = 1 (default value), set to configure the RSTB LOW pulse duration time to 1 ms
- FLT_ERR_CNT_LIMIT 1:0] = 01 (default), set the maximum fault error counter value to 6

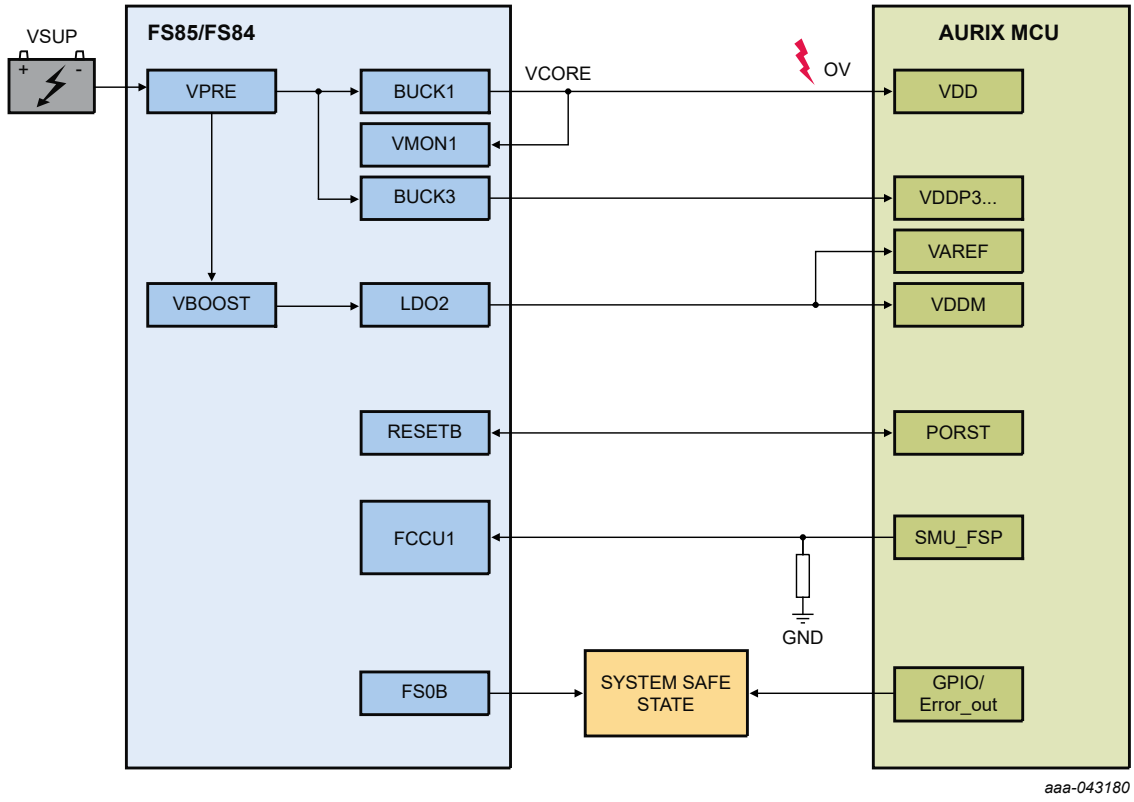


Figure 73. OV fault simplified schematic

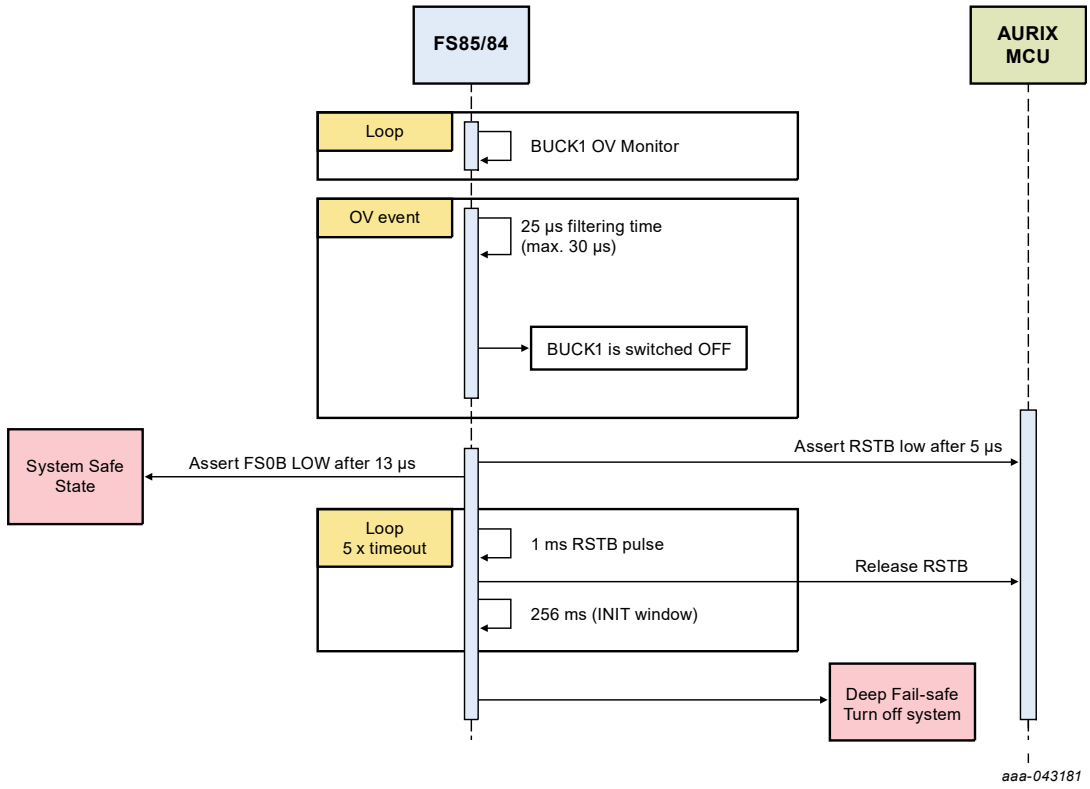


Figure 74. VCORE (BUCK1) OV fault management sequence diagram (to DFS)

1. AURIX MCU VCORE rail (VDD) is supplied by BUCK1, which is monitored by FS85/FS84 VCOREMON.
2. Overvoltage event occurs on VDD. FS85/FS84 triggers a fault after 25 µs (max 30 µs) filter time. BUCK1 is disabled. FS85/FS84 increments its fault error counter to 1.
3. FS85/FS84 asserts RSTB and FS0B low according to the VCOREMON_OV_FS_IMPACT configuration.
4. AURIX MCU is in RESET until the fault is cleared.
5. FS85/FS84 goes back to INIT_FS phase after 1 ms (RSTB_DUR) once the fault is cleared.
6. AURIX MCU did not recover. Hence there are consecutive INIT_FS phase timeouts (256 ms each) and resets until the fault error counter reaches its maximum value (6) and the device goes to DFS.

aaa-037403

Figure 75. Example of VCORE MCU overvoltage fault reaction

5.7.2 FS85/FS84 LDO2 undervoltage

Use assumptions:

- System is running in normal mode (RSTB and FS0B are released)
- VMON2_UV_FS_IMPACT 1:0] = 01 (default) set in FS_I_OVUV during INIT_FS phase, LDO2 UV asserts FS0B only
- OTP_VMON_UV_DGLT[1:0] = 0, set the undervoltage filtering time to 5 µs (typical)

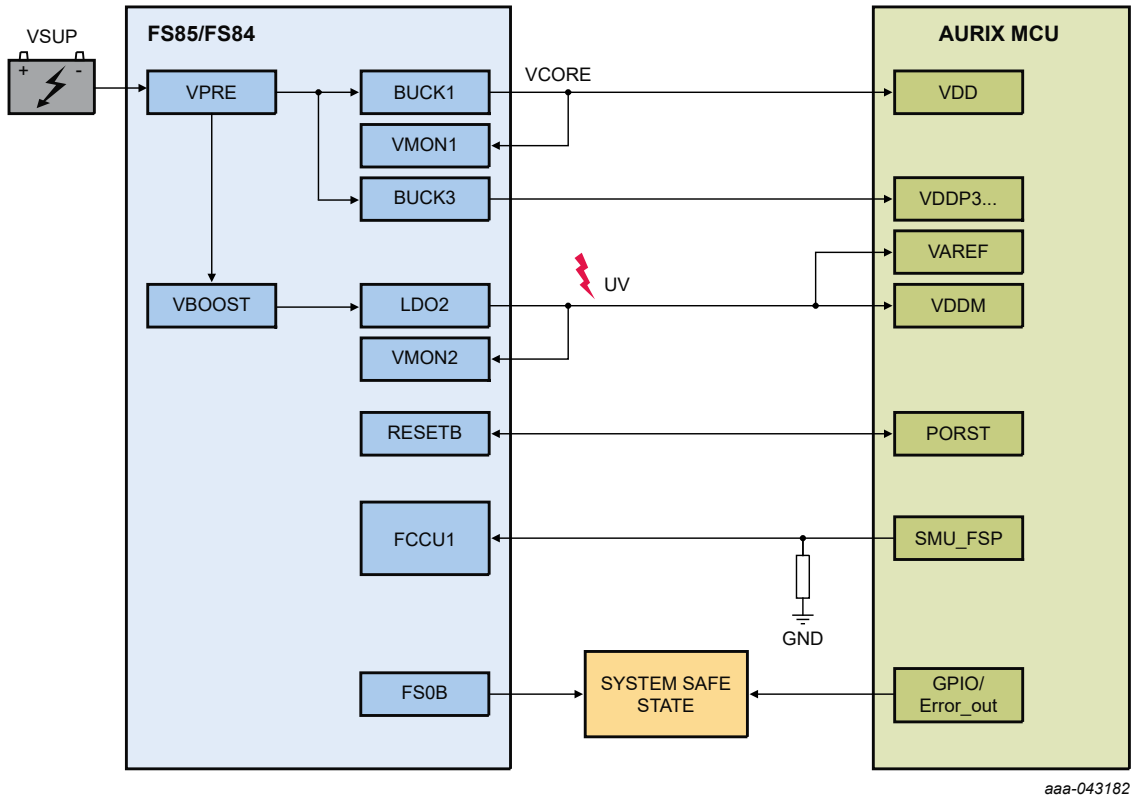


Figure 76. LDO2 UV fault simplified schematic

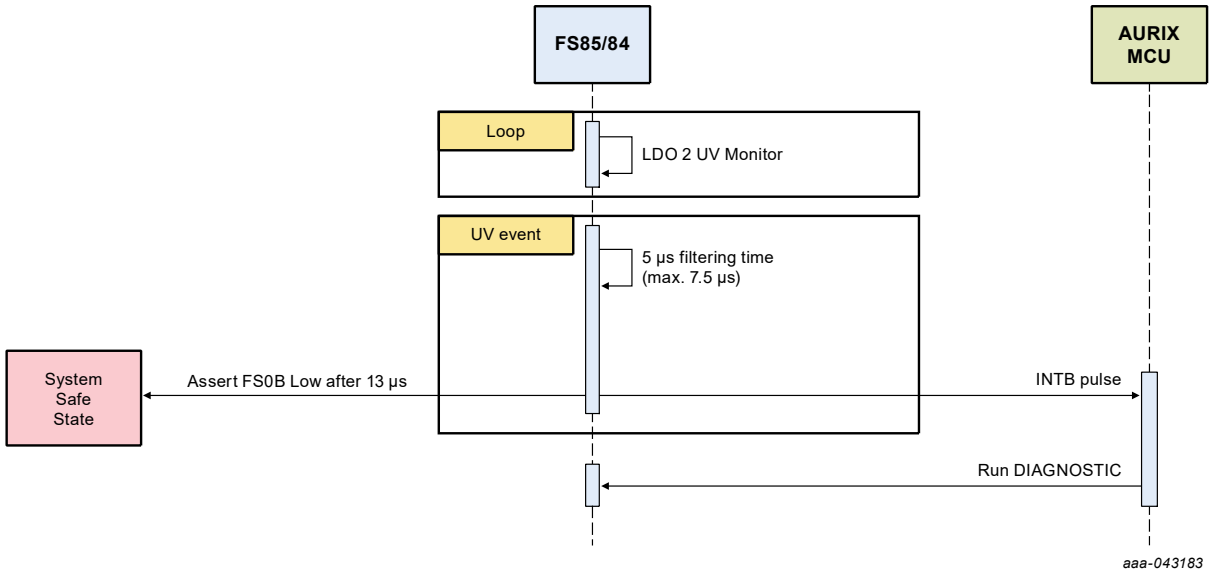


Figure 77. LDO2 UV fault management sequence diagram

1. AURIX MCU ADC rails (VAREFx/VDDM) are supplied by LDO2, which is monitored by FS85/FS84 VMON2.
2. Undervoltage event occurs on LDO2. FS85/FS84 triggers a fault after 5 µs (max 7.5 µs) filter time. LDO2 is still enabled. FS85/FS84 increments its fault error counter to 1.
3. FS85/FS84 asserts FS0B LOW only according to VMON2_UV_FS_IMPACT configuration and an interrupt pulse is generated.

4. AURIX MCU is informed of a problem and can run some diagnostics before eventually turning off LDO2 by SPI/I^{2}C.

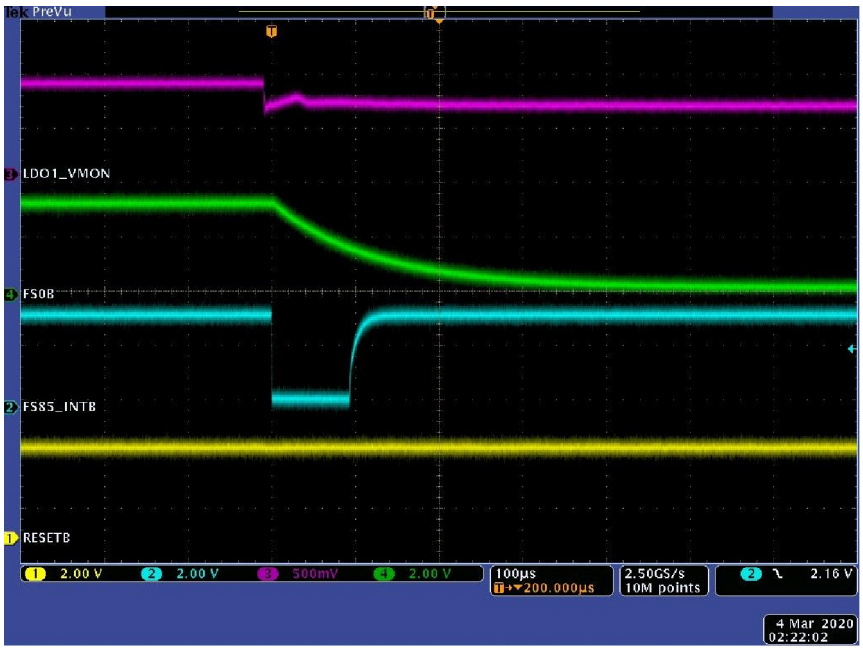


Figure 78. Example of FS85/FS84 LDO undervoltage fault reaction

Note: FS0B signal is measured after the C-R-C output filter (see Section 5.4) hence slower assertion.

6 FS23 solution

6.1 Product overview

FS23 is an automotive functionally safe multi-output power supply integrated circuit, with focus on body applications such as heating, ventilation and air conditioning (HVAC), door control module, and lighting. Its various functions and features include multiple voltage regulators, a system management state machine, SPI or I^2C for communication, controller area network bus (CAN) and local interconnect network bus (LIN) transceivers, as well as multiple configurable high-low voltage IOs with wake-up capability, and multiple high-side switches.

The FS23 is designed to optimize system EMC performance. It is developed in compliance with the ISO 26262:2018 standard, including enhanced safety features with fail-safe outputs, allowing creation of full safety-oriented systems supporting both QM and ASIL B safety integrity levels. FS23 is qualified in compliance with AEC-Q100 (Grade1, MSL3).

The FS23 family offers multiple device versions and configurable OTP settings for various use cases. Options include parts with added LIN communication and LDT (long duration timer) capability, using an HVBUCK for more power-demanding devices, and using the OTP settings to achieve different functionality. FS23 devices specific to either the QM or ASIL B safety levels are available.

6.1.1 Documentation references

- **FS23 Device Webpage**
- **DocStore Access**

Through the DocStore portal access under the “Power Management > Safety SBC > FS23” folder, various materials are available regarding the FS23 family that can be used to access more detailed information about specific topics:

- **FS23 data sheet**: information such as features, functional description, parametric description, register mapping
- **FS23 functional safety manual (ASIL B)**: describes how to use the FS23 in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level
- **FS23 Application notes**: describe how to use the FS23 and implement its features, how to implement the FS23 from the hardware point of view, and how to implement the FS23 as a companion for S32K3 and S32K1 microcontrollers
- **Recommended OTP configuration**: MFS2323BMBC7EP (Body Control System FS23 + S32K324 attach, FS23 + CYT2B attach, FS23 + TC21x/22x/23x, TC33x attach.

6.1.2 Typical block diagram

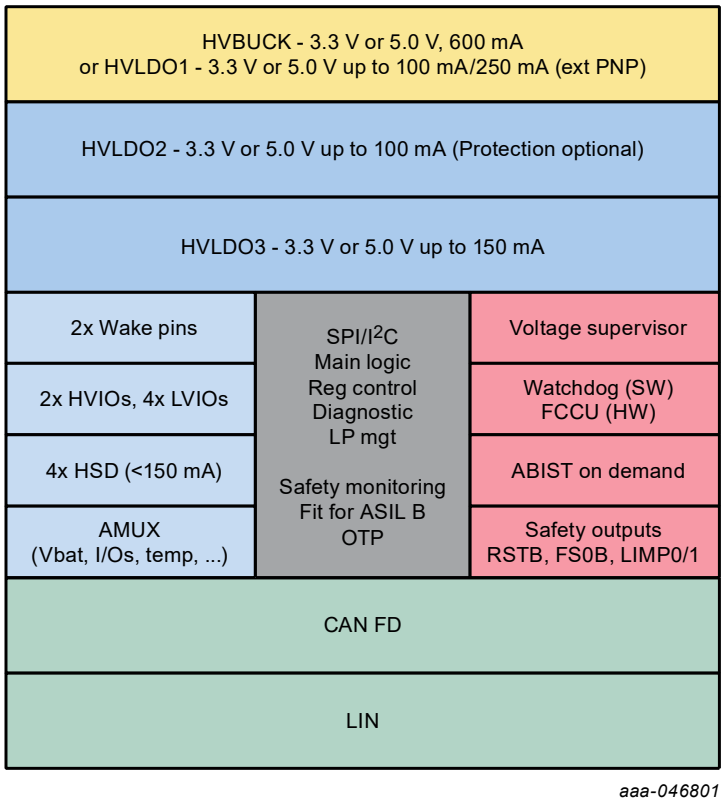


Figure 79. FS23 functional block diagram

6.1.3 Key features

Operating range

- 40 V DC maximum input voltage
- Low-power OFF mode with multiple wake-up sources
- Low-power ON mode with HVBUCK or HVLDO1 active and multiple wake-up sources

Power Supplies

- HVBUCK: synchronous buck converter with integrated FETs. Configurable output voltage (3.3 V or 5.5 V) and switching frequency, output DC current capability of 600 mA and PFM mode for Low-power ON mode operation.
- Or HVLDO1: high-voltage LDO instead of the HVBUCK for MCU supply with selectable output voltage (3.3 V or 5.5 V) and up to 100 mA current capability with internal PMOS and 250 mA with external PNP
- HVLDO2: high-voltage LDO regulator for system loads, with optional external protection for off-board sensors, selectable output voltage (3.3 V or 5.0 V) and up to 100 mA current capability in respect of thermal constraint
- HVLDO3: high voltage LDO regulator; can be used for CAN FD block supply or for other functionality with selectable output voltage (3.3 V or 5.0 V) and up to 150 mA current capability, in respect of thermal constraint

System support

- One CAN FD supporting up to 5 Mbps communication, following ISO 11898-2:2016 and SAE J2284 standards
- One LIN following LIN 2.2, ISO 17987-4 and SAE-J2602-2 standards
- Two wake-up inputs (40 V capable)

- Two high-voltage IOs with wake-up capability (40 V capable)
- Up to four low-voltage IOs with wake-up capability
- Four high-side drivers to supply LEDs, enable external devices (INH); cyclic sense capability
- Selectable wake-up sources from: WAKE pins, HVIO pins, LVIO pins, CAN FD and LIN-bus or SPI activity
- Device control via 32-bit SPI or via I^2C, with CRC
- Integrated LDT and analog multiplexer (AMUX)

Configuration and enablement

- QFN48EP: QFN, 48 pins with exposed pad for optimized thermal management, wettable flanks, 7 x 7 x 0.85 mm, 0.5 mm pitch, 48 pins
- OTP memory for device customization
- OTP emulation mode for system development and evaluation

6.2 Safety management with AURIX MCU

The FS23 includes multiple safety mechanisms to support the functional safety of the system up to the ASIL B level. Safety features are configurable, using either OTP or SPI/I^2C, allowing scalability depending on the application needs.

- Developed following ISO 26262:2018 standard to be fit for ASIL B applications
- Internal monitoring circuitry with its own reference
- Additional input for external voltage monitoring
- Window or timeout watchdog function to monitor the MCU for any software failure
- FCCU inputs to monitor the MCU for any hardware failure
- ABIST on demand
- Safety outputs (RSTB, FS0B, LIMPx)

6.2.1 Safety outputs

Three safety output pins, RSTB, FS0B and LIMP0, are implemented to ensure the safe state of the system. All those safety outputs are active LOW.

RSTB and FS0B are activated during power-up and can only be released when the device is in Normal mode. LIMP0, on the contrary, will be released at startup and will only be asserted when a fault occurs.

The three pins are managed independently, in parallel with the Main state machine.

Besides RSTB, FS0B and LIMP0, two additional pseudo-safety outputs can be used when configuring general purpose IOs as LIMP1 or LIMP2 functions. LIMP1 and LIMP2 follow LIMP0 assertion and release. They could work as asserted to a static level (HIGH or LOW), or as PWM (configurable polarity) when asserted.

Table 23. Application-related fail-safe fault list and reaction

Mode	fault source	FLT_ERR_CNT	RSTB assertion [1][2]	FS0B assertion [1][2]	LIMP0 assertion [1][2]
Slot 0 to Normal state	VxTSD and CONF_TSD_Vx_OTP	= max	yes	yes	yes
	VxMON OV	+1	VxMON_OV_RSTB_IMPACT	VxMON_OV_FS0B_IMPACT	VxMON_OV_LIMP0_IMPACT
	VxMON UV	+1	VxMON_UV_RSTB_IMPACT	VxMON_UV_FS0B_IMPACT	VxMON_UV_LIMP0_IMPACT
	FLT_ERR_CNT = mid value	no change	FLT_MID_RSTB_IMPACT	FLT_MID_FS0B_IMPACT	FLT_MID_LIMP0_IMPACT
	WD_ERR_CNT = WD_ERR_LIMIT	+1	WD_RSTB_IMPACT	WD_FS0B_IMPACT	WD_LIMP0_IMPACT
	FCCU1 single	+1	FCCU1_RSTB_IMPACT	FCCU1_FS0B_IMPACT	FCCU1_LIMP0_IMPACT
	FCCU2 single	+1	FCCU2_RSTB_IMPACT	FCCU2_FS0B_IMPACT	FCCU2_LIMP0_IMPACT
	FCCU12 pair	+1	FCCU1_RSTB_IMPACT	FCCU1_FS0B_IMPACT	FCCU1_LIMP0_IMPACT
	external reset (out of extended RSTB)	+1	no	EXTRSTB_FS0B_IMPACT	no
	RSTB short to High	no change	no	yes	yes
	RSTB short 8 seconds	= max	yes	yes	yes
	FS0B short to HIGH	no change	FS0B_SC_RSTB_IMPACT	no	no
	LIMP0 short to HIGH	no change	LIMP0_SC_RSTB_IMPACT	no	no
	INIT_CRC_NOK	+1	no	INIT_CRC_FS0B_IMPACT	INIT_CRC_LIMP0_IMPACT
	WD_NOK_RECOVERY	+1	yes	no	no
	1MHz_STUCK_AT	no change	yes	yes	yes
LPON state	V1_UVLP	no change	yes	yes by default	yes
	WD_ERR_CNT = WD_ERR_LIMIT	no change	WD_RSTB_IMPACT	yes by default	WD_LIMP0_IMPACT
	no Fault	= 1	no	yes by default	no
LPOFF state	no Fault	= 1	yes by default	yes by default	no
Fail-safe state	state machine in Fail-safe	= 1	yes by default	yes by default	yes by default

[1] In orange, the reaction is not configurable.
[2] In green, the reaction is configurable by OTP and by SPI and I^2C registers.

Table 2 shows the mapping between NXP Safety SBC and Aurix family for the use case when the VCORE regulator of the SBC is used to supply the VDD core voltage of the respective Aurix MCU directly, without using the EVR of the Aurix MCU.

For the use case where the EVR of the Aurix MCU is used (cf. Figures 1 and 2), an SBC with lower VCORE current capability can be used to supply the MCU with a 5 V or 3.3 V power supply. The system integrator is responsible for the correct sizing of the SBC, depending on MCU power consumption for the selected application use case, the additional loads on the VCORE rail and temperature conditions.

6.2.2 FS23 watchdog monitoring

The FS23 acts as a supervisor of the application operation, and as a consequence, includes a timeout or windowed watchdog (temporal and logical monitoring) that needs to be refreshed periodically by the MCU.

This means that the FS23 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 a safe state system within the FTTI. Thus, either the MCU or the SBC can switch the system to a safe state.

The duration of the watchdog window is configurable to allow different MCU handshake strategies.

In the case of a watchdog timeout, the watchdog must be refreshed before the end of the period.

In the windowed watchdog case, there is a duty cycle of 50 %. The first part of the window is said to be closed and the second is said to be open. The watchdog must be refreshed during the open window (see Figure 6).

After a good or a bad watchdog refresh, a new window period starts immediately in order for the MCU to remain synchronized with the windowed watchdog. The first good watchdog refresh closes the INIT phase.

Then the watchdog window is running and the MCU must refresh the watchdog before the end of the period or in the open window of the watchdog window period. The duration of the watchdog window is configurable from 1.0 ms to 1024 ms with the WDW_PERIOD[3:0] bits. The new watchdog window is effective after the next watchdog refresh. The watchdog window can be disabled either via OTP using the WD_INF_OTP bit, or only during INIT phase. In the second case, the watchdog disablement is effective when the INIT phase is closed.

6.2.3 HW SoC monitoring (FCCU)

The FS23 provides an FCCU monitoring feature, when it is enabled by the FCCU_EN_OTP bit. The FCCU input pins are in charge of monitoring HW failures from the MCU. The FS23 only provides one dedicated FCCU1 pin. Another input among HVIO1, HVIO2, LVIO3, LVIO4 and LVI5 can be configured as an FCCU2 pin, via the FCCU2_ASSIGN[2:0] bits, in the INIT phase.

When connected to the AURIX MCU, the FCCU input pins can be configured as shown below. This arrangement can work in PWM mode with the AURIX SMU. The frequency range in this case should be between 10 kHz and 45 kHz. The FCCU input pins should be set with the FCCU_CFG[2:0] bits in PWM mode, either using FCCU1 only, FCCU2 only, or both (when monitoring two AURIX MCUs, for instance):

- FCCU_CFG[2:0] = 101, PWM monitoring enabled on FCCU1 and FCCU2 pins
- FCCU_CFG[2:0] = 110, PWM monitoring enabled on FCCU1 pin and level monitoring only on FCCU2
- FCCU_CFG[2:0] = 111, PWM monitoring enabled on FCCU2 pin and level monitoring only on FCCU1

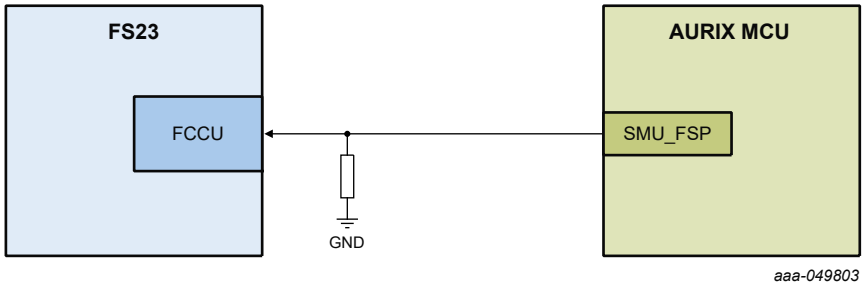


Figure 80. FCCU connection to AURIX SMU in PWM mode

6.3 Power management with AURIX MCU

The following diagrams and tables show the connections between the FS23 and AURIX TC2xx/TC3xx MCUs.

6.3.1 FS23xx + TC2xx/TC3xx

6.3.1.1 FS23xx - TC2xx/TC3xx connections

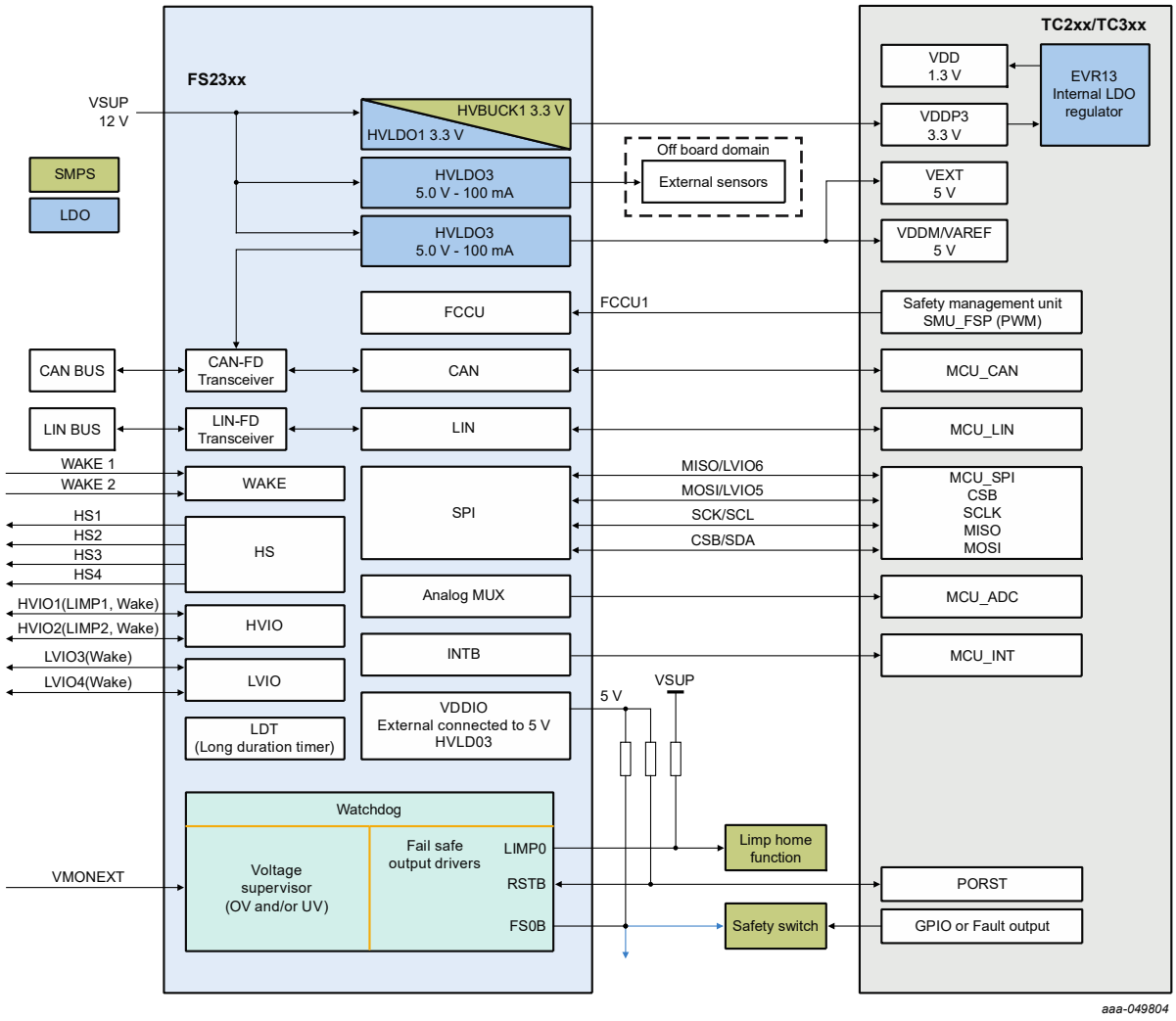


Figure 81. FS23xx attached to TC29x/TC38x AURIX MCU

Table 24. FS23xx - TC2xx/TC3xx connections summary

FS23xx connection	TC2xx/TC3xx connection	Description
HVBUCK \HVLDO1	VDDP3 and EVR13	V1 provides 3.3 V voltage rail to VDDP3 and EVR13
HVLDO2	external sensors	V2 provides 3.3 V or 5 V to external sensor with high voltage protection
HVLDO3	VEXT, VDDM and VAREF	V3 provides 3.3 V voltage rail to VEXT, VDDM and VAREF
RSTB	PORST	RSTB connection
FS0B	connect to safety switch	Works as a safety switch output to bring system into safe state. The connection may very based on customer requirements.

Table 24. FS23xx - TC2xx/TC3xx connections summary*...continued*

FS23xx connection	TC2xx/TC3xx connection	Description
LIMP0	connect to LIMP home function	Works as a LIMP home output when system is in safe state. The connection may very based on customer requirements.
AMUX	MCU_ADC	monitors signal from MUX_OUT to ADC input in TC2xx/TC3xx
INTB	MCU_INT	interrupt signal connection
FCCU1	SMU_FSP	SMU connection to FCCU monitoring
DEBUG	—	for Debug mode entry
VDDIO	connect to RSTB, and FS0B	pullup voltage source for RSTB, LIMP0 and FS0B with resistors
VMONEXT	connect to any external IC	monitors a voltage generated by another part in the application
4 lines SPI	4 lines SPI	SPI connections between FS23xx and TC2xx/TC3xx
CAN/LIN signal	CAN/LIN signal	CAN bus/LIN-bus communication signal

6.3.1.2 Application schematics

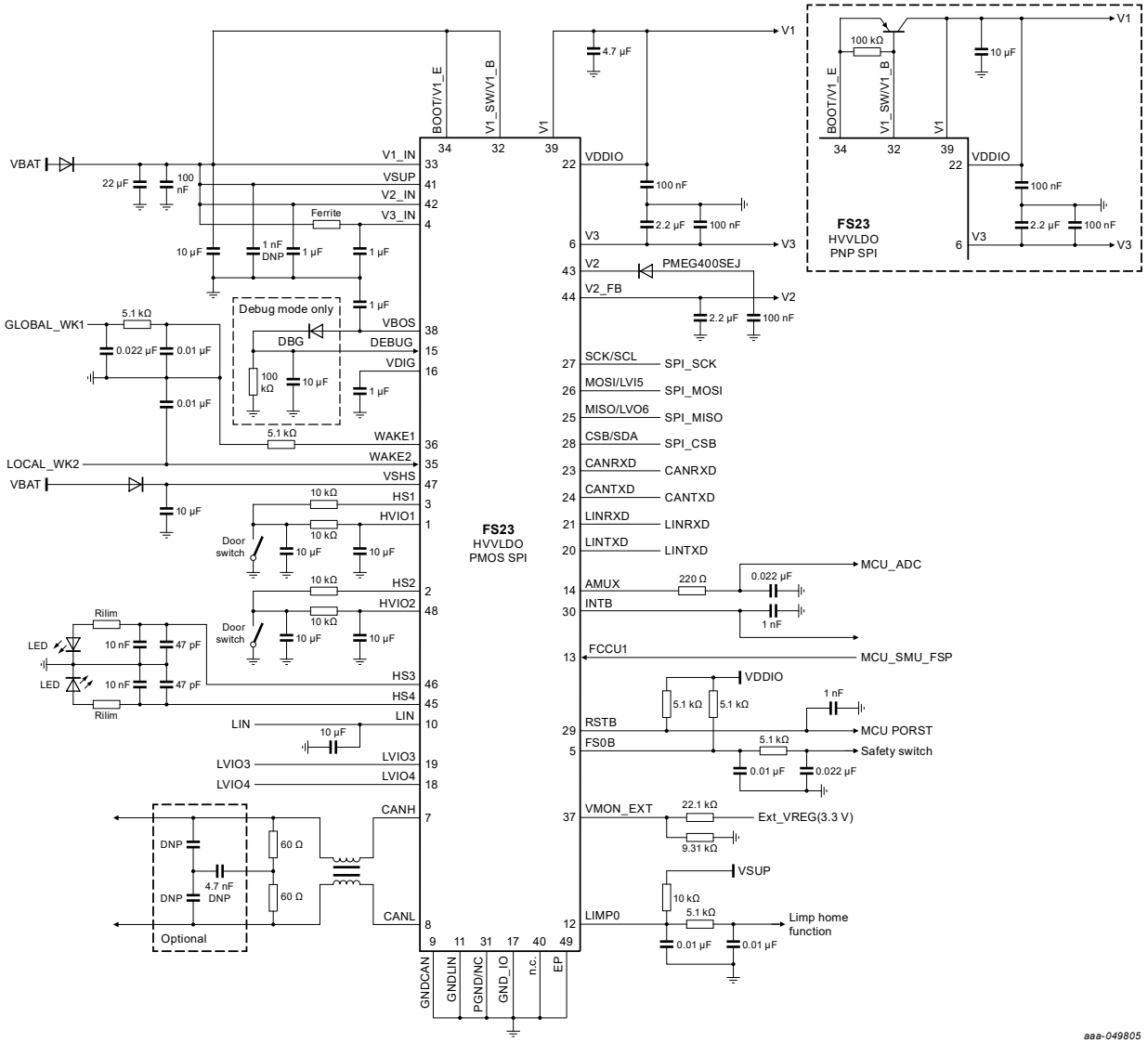


Figure 82. FS230x automotive schematic with FS230x version

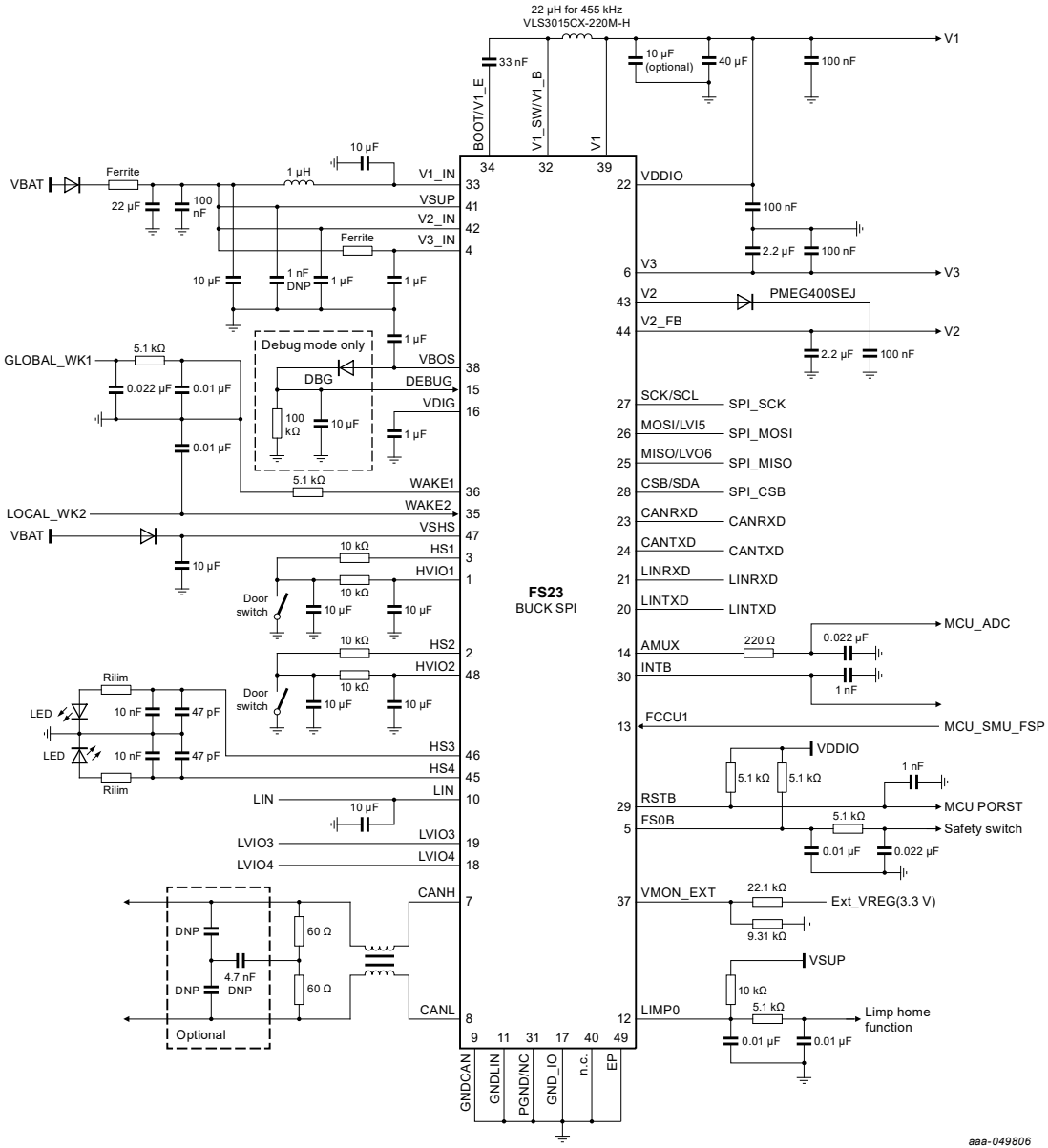


Figure 83. FS232x automotive schematic with FS232x

6.4 BOM

Table 25. FS23xx BOM reference

Domain	item name	value	unit	description	optional
FCCU monitoring	FCCU_RPU	5.1	kΩ	pullup resistor for FCCU1 to VDDIO	X
VSUP power supply	DBAT	—		reverse battery diode	
VSUP Power Supply HVBUCK1	CBAT	22	µF	decoupling capacitor	
	CSUP	10	µF	decoupling capacitor	
	LV1_BUCK (450 kHZ)	22	µH	inductor for Fswbuck = 450 KHz (± 30% tolerance)	
HVBUCK1 HVLDO1	LV1_BUCK (2.25 MHZ)	4.7	µH	inductor for Fswbuck = 2.25 MHz (± 30% tolerance)	
	C1_BUCK (450 kHZ)	10	µF	input capacitor Fswbuck = 450 KHz	
	C1_BUCK (2.25 MHz)	4.7	µF	input capacitor Fswbuck = 2.25 MHz	
	CBOOST_BUCK	33	nF	bootstrap capacitor	
	C1_OUT_BUCK (450 kHz)	25 to 100	µF	effective output capacitor for Fswbuck = 450 KHz	
	C1_OUT_BUCK (2.25 MHz)	6.5 to 40	µF	effective output capacitor for Fswbuck = 2.25 MHz	
	CIN_LDO1	1	µF	input capacitor (close to V1_IN pin)	
HVLDO1, HVLDO2, and HVLDO3	COUT_LDO1	2.2 to 4.7	µF	effective output capacitor	
	COUT_LDO1_PNP	10 to 22	µF	effective output capacitor, with external PNP	
	CIN_LDO2	1	µF	input capacitor (close to V2_IN pin)	
HVLDO2 and HVLDO3 AMUX	COUT_LDO2	2.2 to 4.7	µF	effective output capacitor	
	DLDO2	—		LDO2 protection (optional)	
	CIN_LDO3	1	µF	input capacitor (close to V3_IN pin)	
	COUT_LDO3	2.2 to 4.7	µF	effective output capacitor	
	CAMUX_OUT	2.2	nF	output capacitor	
AMUX	RAMUX_OUT	220	Ω	resistor and capacitor required for buffer stability	
WAKE1 and WAKE2	CIN_WAKE	2 x 22 + 2 x 10	nF	input capacitor	
WAKE1 and WAKE2	R_WAKE	2 x 5.1	kΩ	resistors to limit the current	
VDDIO	COUT_VDDIO	0.1	µF	decoupling capacitor close to the pin for immunity	
INTB	COUT_INTB	1	nF	decoupling capacitor close to the pin for immunity	

Table 25. FS23xx BOM reference*...continued*

Domain	item name	value	unit	description	optional
VMONEXT	R_VMONEXT	—	kΩ	resistor bridge for VMONEXT. R18 and R16 must satisfy: Vx * R18 / (R18 + R16) = 1.0 V (Vx is the monitored voltage)	X
LIMP0	LIMP0_RPU (VDDIO)	5.1	kΩ	external pull-up resistor to VDDIO (nominal)	
	LIMP0_RPU (VSUP)	10	kΩ	external pull-up resistor to VSUP (nominal)	
	LIMP0_RSER	5.1	kΩ	external serial resistor (optional, 0805 package size)	X
	LIMP0_COUT1	10	nF	external output capacitor (close to the pin)	
	LIMP0_COUT2	22	nF	external output capacitor (optional, after the serial resistor)	X
reset and fail-safe outputs	COUT_RSTB	1	nF	RSTB decoupling capacitor	
	PU_RSTB	5.1	kΩ	RSTB pullup resistor to VDDIO	
	COUT_FS0B	22	nF	FS0B capacitor to damp ESD gun stress	X
	CIN_FS0B	10	nF	FS0B decoupling capacitor close to the pin for immunity	X
	PU_FS0B	5.1	kΩ	FS0B pullup resistor to VDDIO	
	RFS0B	5.1	kΩ	FS0B resistor to limit current	

6.5 Flowchart

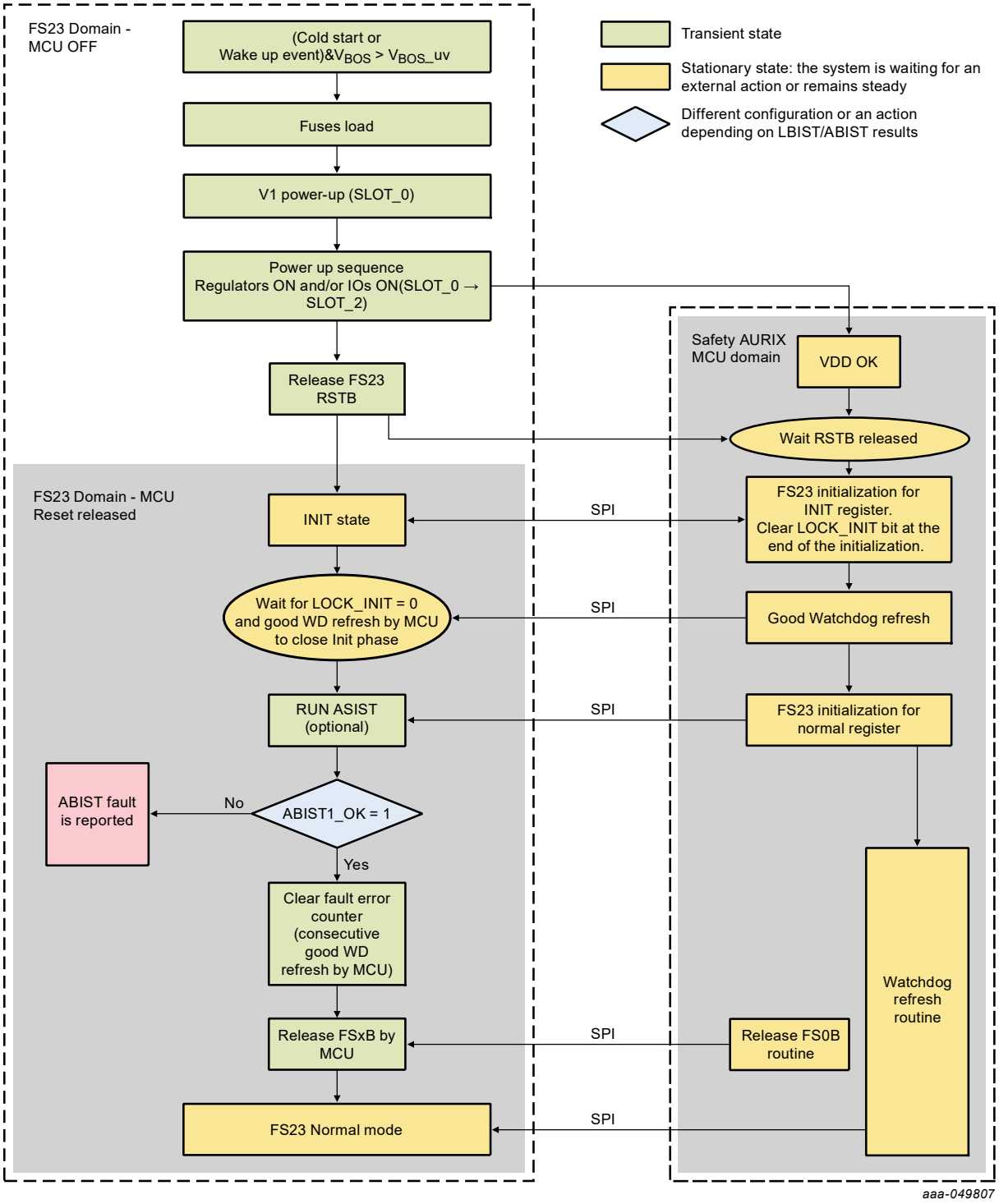


Figure 84. Power-up sequence flow chart block diagram

FS23 domains:

- Fuses load: FS23 loads its preset configuration through fuse memory (OTP).

- Normal mode: This is intended to be the fully functional mode, with all power supplies enabled as required by the system as well as availability to all the system functionality provided by the FS23 device. During the Normal mode, the fail-safe monitoring is available and provides full monitoring and operation of all the safety features in the device. To release the FS0B pins, send several consecutive good watchdog commands to clear the fault error counter down to 0. Finally, send a SPI command to release the FS0B safety outputs.

AURIX TC2xx/TC3xx MCU domains:

- MCU VDD OK: Depending on the system architecture, VDD (equivalent for VCORE) from the MCU can be supplied by the FS23 or by an external source.
- MCU waits for RESETB to be released: The pin RESETB from the FS23 is chosen in this application note for releasing the RESET of the MCU.

6.5.1 FS23 power sequencing

A system power-up sequence is shown in Figure 85:

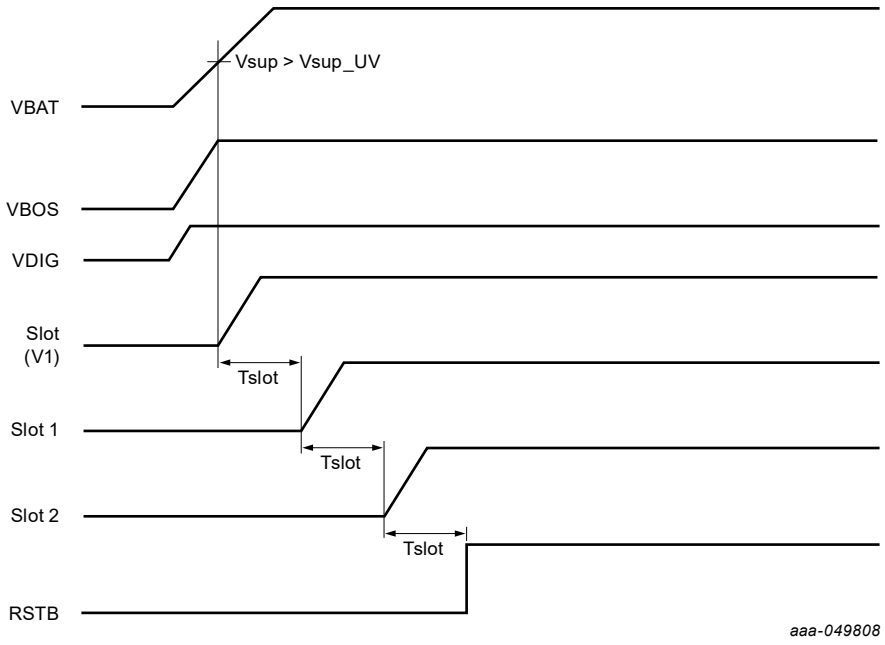


Figure 85. System power-up sequence

V1 is the first regulator to start automatically in SLOT_0, then the other regulators start, following the OTP power sequencing configuration. Three slots are available, from SLOT_0 to SLOT_2, to program the start-up sequence of V2 and V3 regulators, as well as release or assertion of IOs.

The power-up sequence starts at SLOT_0 and ends at SLOT_2, with a TSLOT_OTP delay between each slot. Regulators assigned off are not started during the power-up sequence but can be enabled later in Normal mode via an SPI command.

The power-up sequence starts at SLOT_0 towards SLOT_2. The power-down sequence is executed in reverse order, starting at SLOT_2 towards SLOT_0.

All regulators not assigned in any slot are not started during the power-up sequence. These regulators can be started (or not) later, when the Main state machine is in Normal mode, with an SPI/I^2C command written to the M_REG_CTRL register, if they were enabled by OTP.

6.6 Fault management and recovery

When the system is operating in Normal mode, various types of faults can occur on the FS23, the MCU, or on external peripherals.

Fault management use cases between the FS23 and the AURIX TC2xx/TC3xx are described in this section. Other faults, like overtemperature, follow the same sequence.

Table 26. Fault list

Fault number	Fault location	Fault type
1	FS23 AURIX V1 supply	overvoltage
2	FS23 AURIX SPI	watchdog fault
3	FS23 FCCU1	FCCU fault

6.6.1 AURIX TC2xx/TC3xx V1 overvoltage

Use assumptions:

- System is running in Normal mode (RSTB, FS0B and LIMP0 are released)
- V1MON_OVTH[3:0] OTP bits, set V1 monitoring overvoltage thresholds between +2.5 % to +10 % in increments of +0.5 %
- V1MON_OVDGLT_OTP bit, set V1 monitoring overvoltage filtering time (25 µs or 45 µs)
- V1MON_OV_RSTB/FS0B/LIMP0_IMPACT to 1, so that V1 OV will have an impact on RSTB, FS0B and LIMP0
- RSTB_DUR = 0, set to configure the RSTB LOW duration time to long pulse (10 ms)
- CONF_OV_V1_OTP = 1, V1 regulator is disabled and the device transitions to the Fail-safe state in case of OV

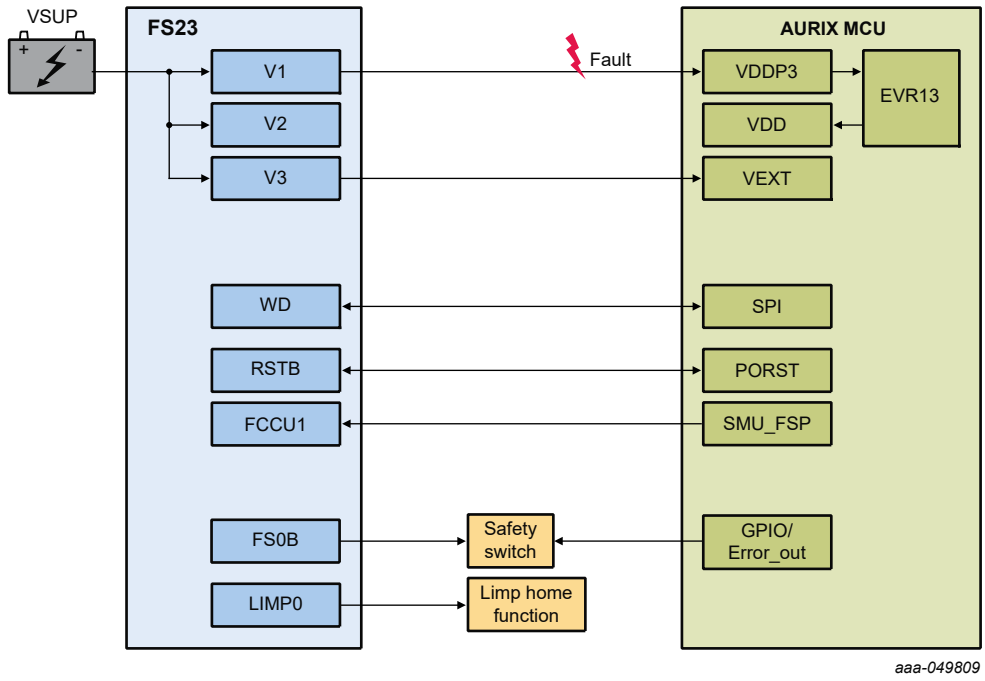


Figure 86. V1 OV fault simplified schematic

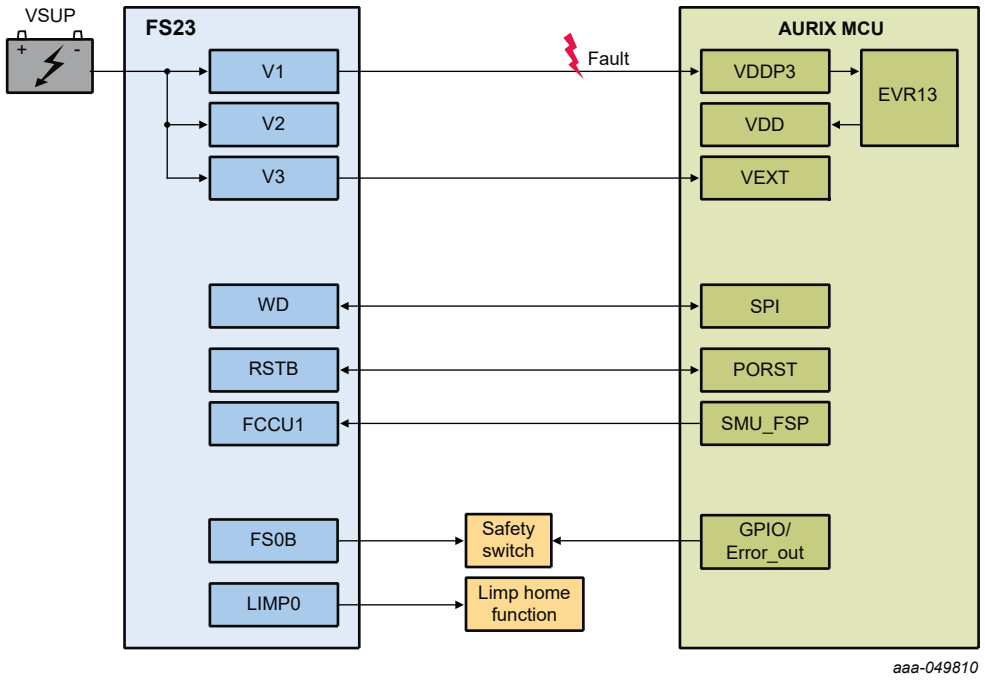


Figure 87. Figure V1 OV fault management sequence diagram (to Fail-safe)

1. FS23 V1 voltage is monitored internally.
2. OV event occurs on V1. FS23 triggers a fault after max 30 µs or 50 µs deglitch time. V1 regulator is disabled. FS23 increments FLT_ERR_CNT by one.
3. FS23 asserts RSTB, FS0B and LIMP0 LOW according to V1MON_ OV_ IMPACT configuration .
4. If the OV condition remains, RSTB stays LOW.
5. If RSTB stays LOW for 8 s, FS23 goes to Fail-safe mode (if the 8 s timer is enabled by OTP).

Note: *FS23 can also go directly to Fails-safe mode when OV is detected (step 2) if this behavior is configured by OTP.*

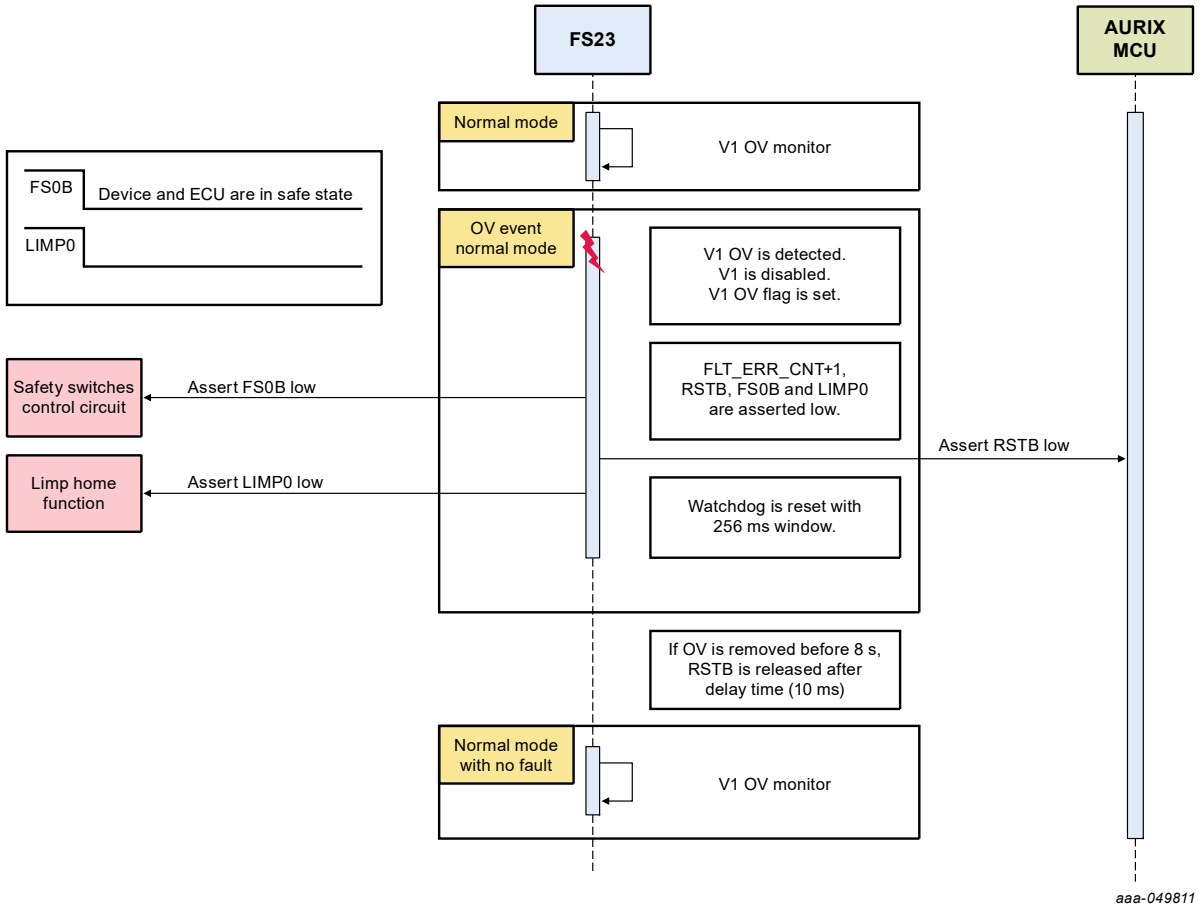


Figure 88. Figure V1 OV fault management sequence diagram (to recovery)

1. FS23 V1 voltage is monitored internally.
2. OV event occurs on V1. FS23 triggers a fault after max 30 µs or 50 µs deglitch time. V1 regulator is disabled. FS23 increments FLT_ERR_CNT by one.
3. FS23 asserts RSTB, FS0B and LIMP0 LOW according to V1MON_ OV_ IMPACT configuration.
4. If the OV condition is removed before 8 s, after 10 ms delay, RSTB is released. FS23 transfers to INIT mode, opens a 256 ms window and waits for LOCK_INIT = 0 and a new WD refresh from AURIX.
5. FS23 stays in Normal mode as a result of a good WD refresh. Due to successive good WD refresh, FLT_ERR_CNT decrements to 0.

6.6.2 AURIX TC2xx/TC3xx watchdog fault

Use assumptions:

- System is running in Normal mode (RSTB, FS0B, and LIMP0 are released)
- WDW_PERIOD[3:0] = 0101 and WDW_DC[2:0] = 010, WD window is set to 6 ms with 50 % duty cycle
- WD_ERR_LIMIT[1:0] = 01, max value of WD error counter is set to 6 (intermediate value is 3)
- WD_RFR_LIMIT[1:0] = 01, max value of WD refresh counter is set to 4
- WD_FS0B_IMPACT = 1, FS0B is asserted LOW if WD_ERR_CNT = WD_ERR_LIMIT
- WD_LIMP0_IMPACT = 1, LIMP0 is asserted LOW if WD_ERR_CNT = WD_ERR_LIMIT
- RSTB_DUR = 0, set to configure the RSTB LOW duration time to 10 ms
- FLT_ERR_CNT_LIMIT[1:0] = 01, to set the fault error counter intermediate value to 3 and its maximum to 6
- FLT_MID_RSTB_IMPACT = 1, RSTB will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.

- FLT_MID_FS0B_IMPACT = 1, FS0B will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.
- FLT_MID_LIMP0_IMPACT = 1, LIMP0 will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.

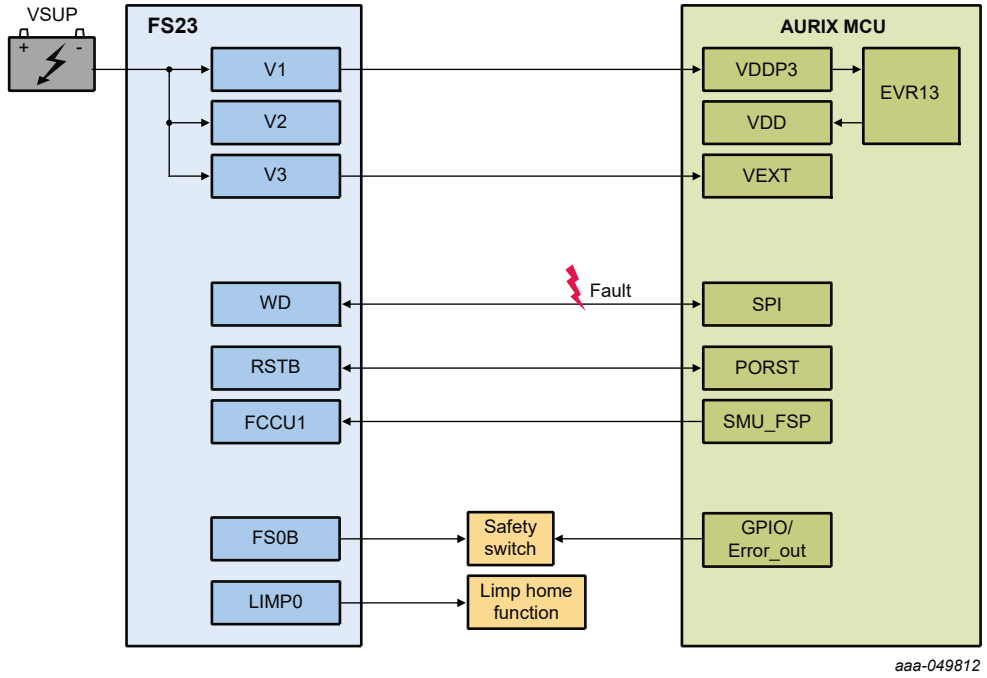


Figure 89. Watchdog fault simplified schematic

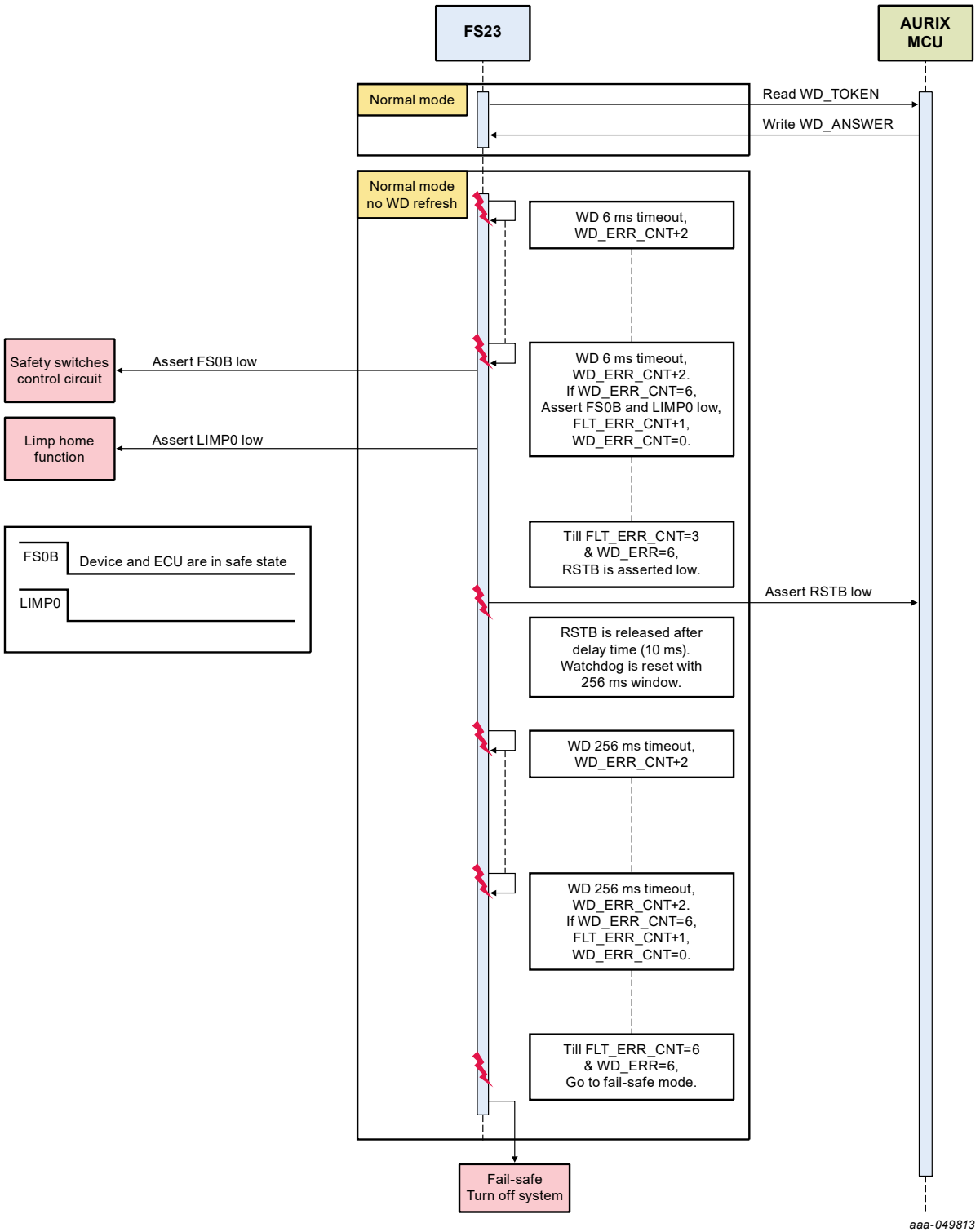


Figure 90. WD fault management sequence (to Fail-safe)

1. FS23 window WD opens a 6 ms window with 50 % duty cycle in Normal mode
2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2

3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2
4. When the WD_ERR_CNT = 6, FS0B and LIMP0 is asserted LOW according to WD_[FS0B/LIMP0]_IMPACT and WD_ERR_LIMIT configuration; FLT_ERR_CNT increments by 1
5. WD_ERR_CNT is set back to 0;
6. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_ERR_CNT = 6, RSTB is asserted LOW;
7. AURIX MCU is reset
8. After a 10 ms delay time, RSTB is released, watchdog is reset with 256 ms window opens and waits for a new WD refresh from the AURIX MCU
9. In the absence of a good WD refresh, FLT_ERR_CNT is incremented
10. In the absence of a good WD refresh until FLT_ERR_CNT = 6 (max value), FS23 goes to Fail-safe mode

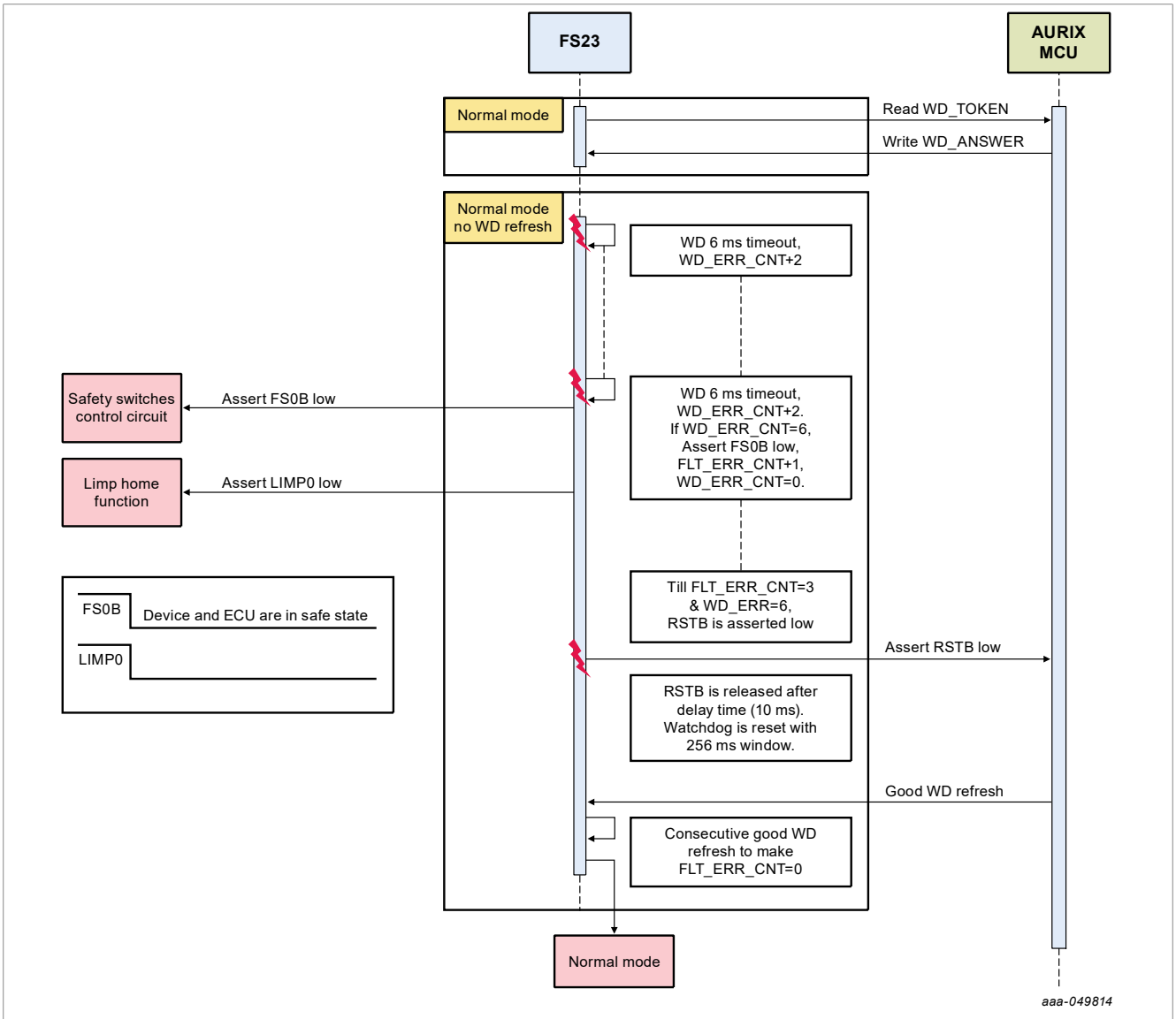


Figure 91. WD Fault management sequence (to recovery)

1. FS23 window WD opens a 6 ms window with 50 % duty cycle in Normal mode

2. In the absence of a good WD refresh in the open window, a WD timeout is triggered and the WD_ERR_CNT increments by 2
3. If a WD timeout is triggered continuously in the following WD windows, each time the WD_ERR_CNT keeps incrementing by 2;
4. When the WD_ERR_CNT = 6, FS0B and LIMP0 is asserted LOW according to WD_FS_REACTION and WD_ERR_LIMIT configuration. The FLT_ERR_CNT increments by 1.
5.
6. WD_ERR_CNT is set back to 0;
7. Loop from step 3 to step 6 until FLT_ERR_CNT ≥ 3 (intermediate value) and WD_ERR_CNT = 6, RSTB is asserted LOW
8. AURIX MCU is reset;
9. After a 10 ms delay time, RSTB is released, watchdog is reset with 256 ms window opens and waits for a new WD refresh from the AURIX MCU
10. The periodic WD handshake is recovered between FS23 and AURIX MCU. FLT_ERR_CNT decreases to 0 with consecutive good WD refreshes. Then AURIX MCU releases FS0B and LIMP0 safety outputs.

6.6.3 AURIX TC2xx/TC3xx FCCU fault

Use assumptions:

- System is running in Normal mode (RSTB, FS0B and LIMP0 are released)
- FCCU_CFG[2:0] = 011, HIGH and LOW level timings are monitored on FCCU1 pin
- FCCU1_RSTB_IMPACT= 1, RSTB is asserted LOW when a fault is indicated on FCCU1
- FCCU1_FS0B_IMPACT = 1, FS0B is asserted LOW when a fault is indicated on FCCU1
- FCCU1_LIMP0_IMPACT = 1, LIMP0 is asserted LOW when a fault is indicated on FCCU1
- WDW_RECOVERY[3:0] = 1011, set the WD window duration for MCU recovery to 64 ms
- WDW_REC_EN =1, enable fault recovery
- RSTB_DUR = 0, set to configure the RSTB LOW duration time to 10 ms;
- FLT_ERR_CNT_LIMIT = 01, to set the fault error counter intermediate value to 3 and its maximum to 6
- FLT_MID_RSTB_IMPACT = 1, RSTB will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.
- FLT_MID_FS0B_IMPACT = 1, FS0B will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.
- FLT_MID_LIMP0_IMPACT = 1, LIMP0 will be asserted LOW if FLT_ERR_CNT ≥ intermediate value.

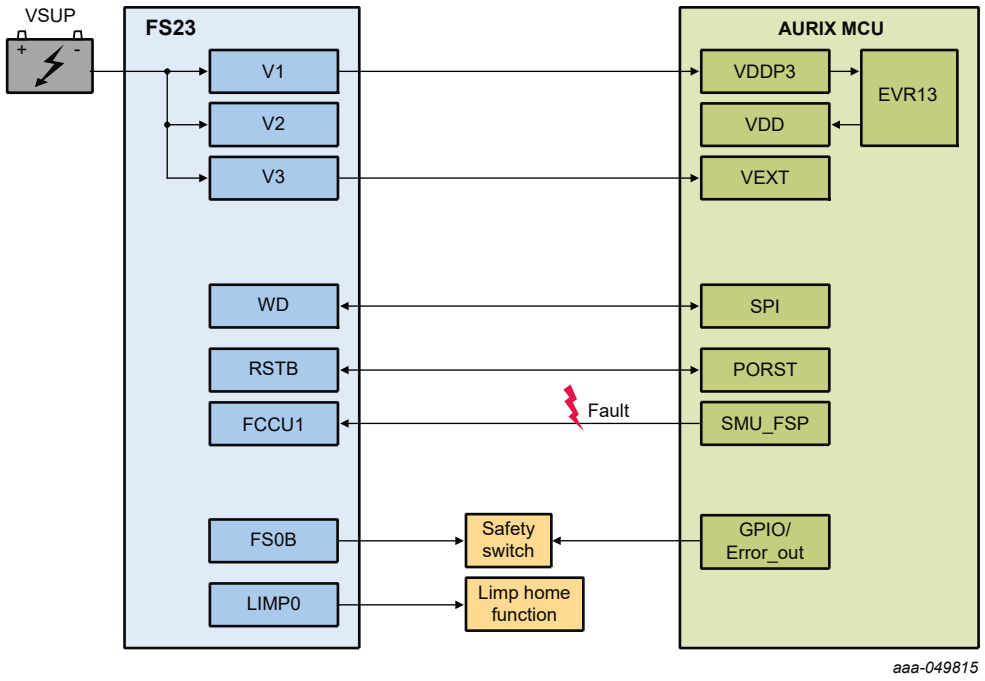


Figure 92. FCCU fault simplified schematic

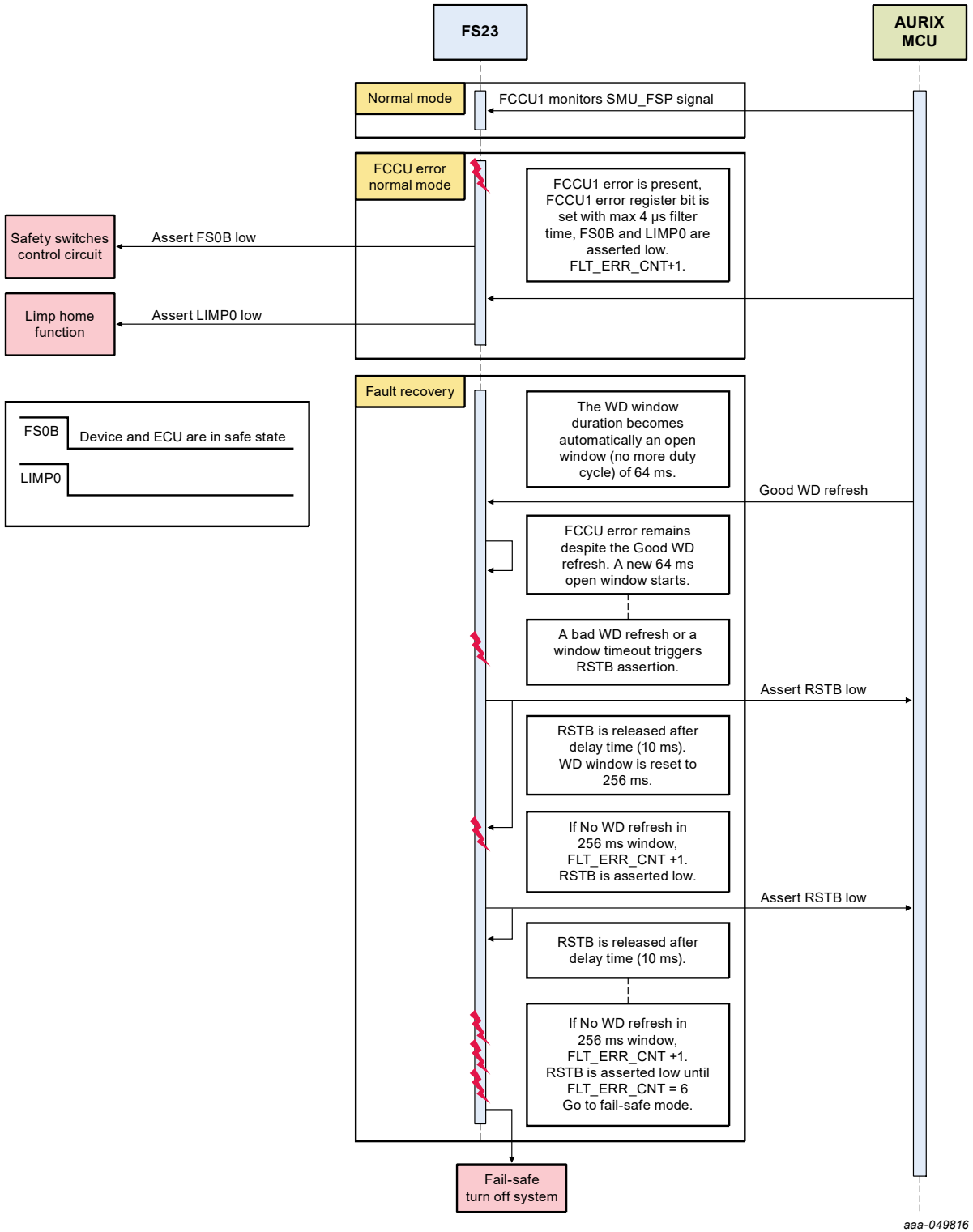


Figure 93. FCCU fault management sequence (to Fail-safe)

1. FS23 is continuously monitoring AURIX SMU_FSP signal through its FCCU1 pin in Normal mode.
2. A hardware failure occurs on the AURIX MCU side; FS23 triggers a FCCU fault and FLT_ERR_CNT is incremented .

3. FS23 asserts FS0B and LIMP0 LOW and a 64 ms open WD window starts to allow AURIX MCU to recover before RSTB is asserted.
4. A good WD refresh is received from AURIX MCU but FCCU1 error remains. Another 64 ms open WD window is created.
5. FCCU error remains and a bad WD refresh or a timeout happens. RSTB pin is asserted LOW bringing the AURIX MCU into reset.
6. After a 10 ms delay time, RSTB is released; a 256 ms window opens and waits for a new WD refresh from the AURIX MCU.
7. In the absence of a good WD refresh, FLT_ERR_CNT is incremented and RSTB is asserted LOW again.
8. In the absence of a good WD refresh, the device loops from step 6 to step 7 until FLT_ERR_CNT = 6 (max value). FS23 then goes to Fail-safe mode.

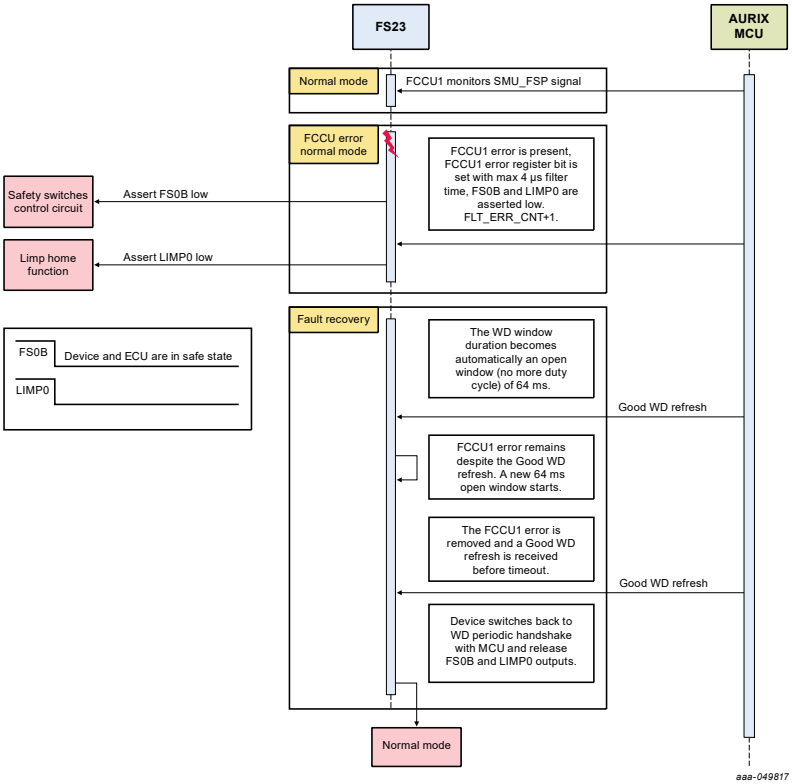


Figure 94. FCCU Fault management sequence (to recovery)

1. FS23 continuously monitors the AURIX SMU_FSP signal through its FCCU1 pin in Normal mode.
2. A hardware failure occurs on the AURIX MCU side; FS23 triggers a FCCU fault and FLT_ERR_CNT is incremented.
3. FS23 asserts FS0B and LIMP0 LOW and a 64 ms open WD window starts to allow AURIX MCU to recover before RSTB is asserted.
4. A good WD refresh is received from AURIX MCU but FCCU1 error remains. Another 64 ms open WD window is created.
5. FCCU error is removed and a good WD refresh is received. The AURIX MCU has recovered.
6. The periodic WD handshake is recovered between FS23 and AURIX MCU. FLT_ERR_CNT decreases to 0 with consecutive good WD refreshes. Then AURIX MCU releases FS0B and LIMP0 safety outputs.

6.6.4 Other recovery

When a fault occurs, both fail-safe outputs, FS0B and LIMP0, can be asserted LOW. Thereafter, some conditions must be fulfilled before allowing the device to release these pins again. These conditions are:

- No fault affecting FS0B or LIMP0 reported
- Fault error counter must be cleared (= 0)
- FS23 is in Normal mode
- FS23 is not in Debug mode and not in Init mode
- RELEASE_FS0B and RELEASE_LIMP0 command must be received and valid

When the device is in the Fail-safe state, all regulators are off and all safety outputs (RSTB, FS0B, and LIMP0) are asserted LOW; the device exits the Fail-safe state after T_{FS_DUR} time. If the FS_LPOFF_OTP bit is set to logic 1, the device exits the Fail-safe state and goes to LPOFF. Otherwise, it goes back to the power-up sequence.

7 AUTOSAR software drivers

In order to make their enablement as simple as possible, NXP safety SBCs come with dedicated software drivers developed in partnership with Vector Informatik GmbH (Vector). These fully Automotive Open System Architecture (AUTOSAR) compliant complex drivers allow the designer to define their application safety concept up to ASIL D.

- **FS65/FS45 and FS85/FS84 SW driver:**
  - Free demo code: Embedded software solution for FS65x/FS45x/FS8x family SBCs
  - Vector complex driver AUTOSAR 4.x drivers available (configurable with any AUTOSAR configuration editor)
- **FS26 SW driver:** NXP complex driver AUTOSAR ISO 26262 4.x available
- **FS23 SW driver:** NXP complex driver AUTOSAR ISO 26262 4.x available.

As part of the SW driver package, comprehensive technical reference documentation is available, detailing supported features such as:

- CAN/LIN function (FS65/FS45/FS23 specific)
- Watchdog function
- SPI access register function [raw application programming interface (API)]
- Event handling (OV/UV, OT, OC, WD/SPI error, wakeup, etc.)
- …

8 Revision history

Document ID	Date	Description
AN13322 v. 4.0	29 July 2026	• Changed security classification from confidential to public • Updated revision history format to match current standard • Revised Section 4.1.1 • Revised Section 6.1.1
3.0	07 July 2025	• Table 2: added **X**[2] to FS26x in TC39 column • Table 2: updated FS23xx (0.1 A/0.25 A/0.*4* A) to FS23xx (0.1 A/0.25 A/0.*6* A) • Section 4.3.2: updated FS262x/FS263x + TC29x/TC38x to FS262x/FS263x + TC29x/TC38x/*TC39x* • Figure 47: added TC39x • Table 14: added TC39x • Figure 48: added TC39x • Table 15: added TC39x
2	20240202	• Table 1: added FS23 • Revised Figure 28 • Section 2.1.5: rephrased second sentence for clarity • Section 3.2.3.2: changed *HIGH* to *stuck-HIGH* • Revised Table 3 • Section 3.2.1: added explanatory text under Table 3 • Revised Figure 14 • Revised Figure 19 • Revised Figure 22 • Revised the last step in Section 4.7.1 • Throughout: changed *increments FLT_ERR_CNT +1* to *increments FLT_ERR_CNT by one* • Revised Figure 23 • Revised Figure 24 • Section 3.7.2: corrected bit field names to *VCORE_FS_UV_1:0* and *FS1B_TIME_3:0* • Section 3.7.4: corrected bit field name formats to *FCCU_eaout_1:0*, *FLT_ERR_IMP_1:0*, and *FS1B_TIME_3:0* • Revised Figure 25 • Revised Figure 26 • Revised Figure 27 • Revised Figure 28 • Revised Figure 29: changed *Device and ECU is safe state* to *Device and ECU in safe state* • Revised Figure 30: changed *Device and ECU is safe state* to *Device and ECU in safe state* • Revised Figure 31 • Revised Figure 32 • Revised Figure 33: changed *Device and ECU is safe state* to *Device and ECU in safe state* • Updated Figure 34 • Revised Figure 36: fixed typo, changing *FS426* to *FS26* • Revised Figure 37 • Revised Table 17 • , changed *increments to 1* to *increments by 1* • Revised Figure 46

...continued

Document ID	Date	Description
		• Revised Figure 48 • Revised Figure 45: changed *CS* to *CSB* and *CLK* to *SCLK* • Revised Figure 46: changed *CS* to *CSB* and *CLK* to *SCLK*; in High Voltage Buck VPRE (green box), changed *3.2 V* to *3.7 V*; in blue VREF box, change *1%* to *.75%* • Revised Figure 47: In High Voltage Buck VPRE (green box), changed *3.2 V* to *3.7 V*. In VCORE green box, change second line of text; In blue VREF box, change *1%* to *.75%*; in SPI block, change top two items to *CSB* and *SCLK* • Revised Figure 48: In the green High Voltage Buck VPRE box, changed *3.2 V* to *3.7 V*; in the green VCORE box, changed *1.5 A* to *1.65 A*; in the SPI block, changed *CS* to *CSB* and *CLK* to *SCLK* • Revised Figure 49 • Revised Figure 50 • Revised Figure 51 • Revised Figure 53 • Section 4.7.2: changed *increments to 1* to *increments by 1* and revised List item for clarity • Revised Figure 56 • Revised Figure 60 • Revised Figure 61: changed *Device and ECU is safe state* to *Device and ECU in safe state* • Revised Section 4.7.1:clarified steps in in sequence *VCORE OV fault management sequence diagram (to recovery)* • Rephrased Section 4.7.3 final sequence, step List item, for clarity • Revised Figure 62 • Revised Figure 68 • Revised Figure 70 • Revised Figure 74 • Section 7: added FS23 information • Added FS23 power solution • Updated legal information
1	20210818	Initial version

Legal information

Definitions

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

Disclaimers

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

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

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

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

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

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

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

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

Suitability for use in automotive applications (functional safety) — This NXP product has been qualified for use in automotive applications. It has been developed in accordance with ISO 26262, and has been ASIL classified accordingly. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

AN13322

NXP SBC solution for Infineon AURIX TC2xx/TC3xx series MCU

For more information, please visit: https://www.nxp.com

Document feedback

Date of release: 31 July 2026
Document identifier: AN13322