AN5333

Safety application notes for MC24XS4 family

Rev. 3.0 — 26 January 2018 Application note

Document information

Information	Content
Keywords	AN5333
Abstract	This document discusses the safety requirements for the use of an NXP product and in functional safety relevant applications requiring high functional safety integrity levels.

1 Introduction

This document discusses the safety requirements for the use of an NXP product and in functional safety relevant applications requiring high functional safety integrity levels. This safety manual is provided to support the following MC24XS4 24 V eSwitches family. This family has five products:

- MC06XS4200
- MC10XS4200
- MC20XS4200
- MC22XS4200
- MC50XS4200

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

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

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

Example:

Assumption: The recommended operating conditions given in the data sheet are maintained.

This document also contains guidelines on configuring and operating the NXP device for functional-safety relevant applications requiring high functional safety integrity levels.

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

It is assumed that the user of this document is familiar with the NXP device, ISO 26262 and IEC 61508.

1.1 Related documents

This sections lists all the documentation mentioned in this Safety Manual.

The Safety Manual is to be used in combination with the data sheet.

Table 1. Related documents

Document Name	Description
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems, international standard, ed. 2.0, April 2010
ISO 26262:2011	Road vehicles – Functional safety, first edition
MC06XS4200, MC10XS4200, MC20XS4200, MC22XS4200, MC50XS4200	Data Sheet
MC24XS4ER	Errata

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

2 General information

This device is designed to be used in automotive or industrial applications, which needs to be integrated in a system that fulfills functional safety requirements, as defined by functional safety integrity levels, such as ASIL D of ISO 26262 or SIL 3 of IEC 61508.

2.1 Assumed conditions of operation

Assumption: The recommended operating conditions given in the device's NXP data sheet are maintained.

Assumption: The latest device errata is taken into account during system design, implementation and maintenance.

Assumption: All field failures of the devices are reported to the silicon supplier.

2.2 Safety function

Given the application independent nature of the NXP device, no general safety function can be specified. Therefore, this document specifies a safety function being application independent for the majority of applications. This application independent safety function has to be integrated into a complete (application dependent) system.

2.3 Safety goals

The safety goals at application level are:

- Prevent unintended turn-off and turn-on of the channel outputs
- Prevent application damage due to load misfunctioning

3 Assumptions of use

Figure 1 shows an example of a generic safety system architecture. The primary feature of the MC24XS4 family is to be the main switch to turn on and turn off lights in a vehicle. The device will also turn on and turn off other loads, such as DC motors, solenoids and power modules.

All devices have embedded internal fault-detection mechanisms and diagnostics. Several pins report fault and diagnostics back to the MCU.

MC24XS4 is also self protected against overload and overheating.

At the system level, the MC24XS4 family is compliant for integration in an ASIL B system.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

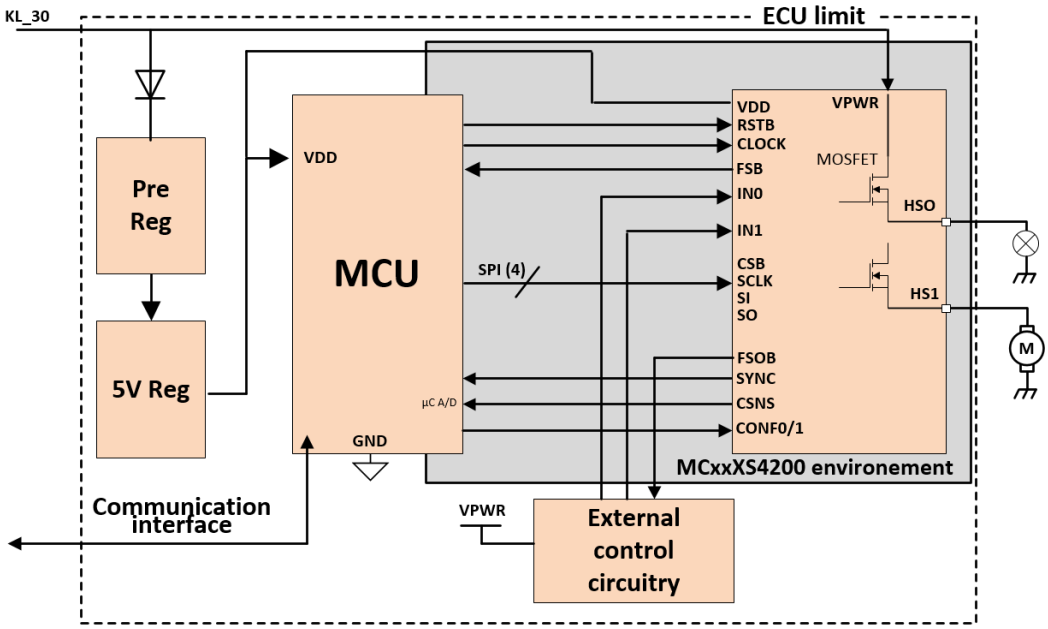


Figure 1. Generic safety system architecture example

Table 2. Pin descriptions

Pin	Description	Safety monitored
VDD	Digital core and interface supply	Yes
RSTB	Reset of device, active low to high	No
CLOCK	External PWM clock	Yes
FSB	Fault status output (fault reporting function)	No
IN0	Direct input drive	No
IN1	Direct input drive	No
SPI (4)	Serial peripheral interface between MCU and MCxxXS4200	Yes
FSOB	Fail safe output (fault reporting function)	No
SYNC	Current sense synchronization	No
CSNS	Current sense output	No
CONF0	Overcurrent profile mode	No
CONF1	Overcurrent profile mode	No
HS0	Power output	Yes
HS1	Power output	Yes

3.1 Targeted applications

The MC24XS4 family is developed to control different types of loads, including bulb lamps, solenoids, and DC motors with low RDSON in high-side drive mode. This family of devices is designed for truck, bus and industrial applications.

Applications:

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

- Lighting: High beam, low beam, turn indicators, side indicators, fog lamp, brake indicators, rear indicators
- Pump activation, Washer pump
- Wiper control
- Motor control
- Module power supply activation

Figure 2 shows an example of an application with external components.

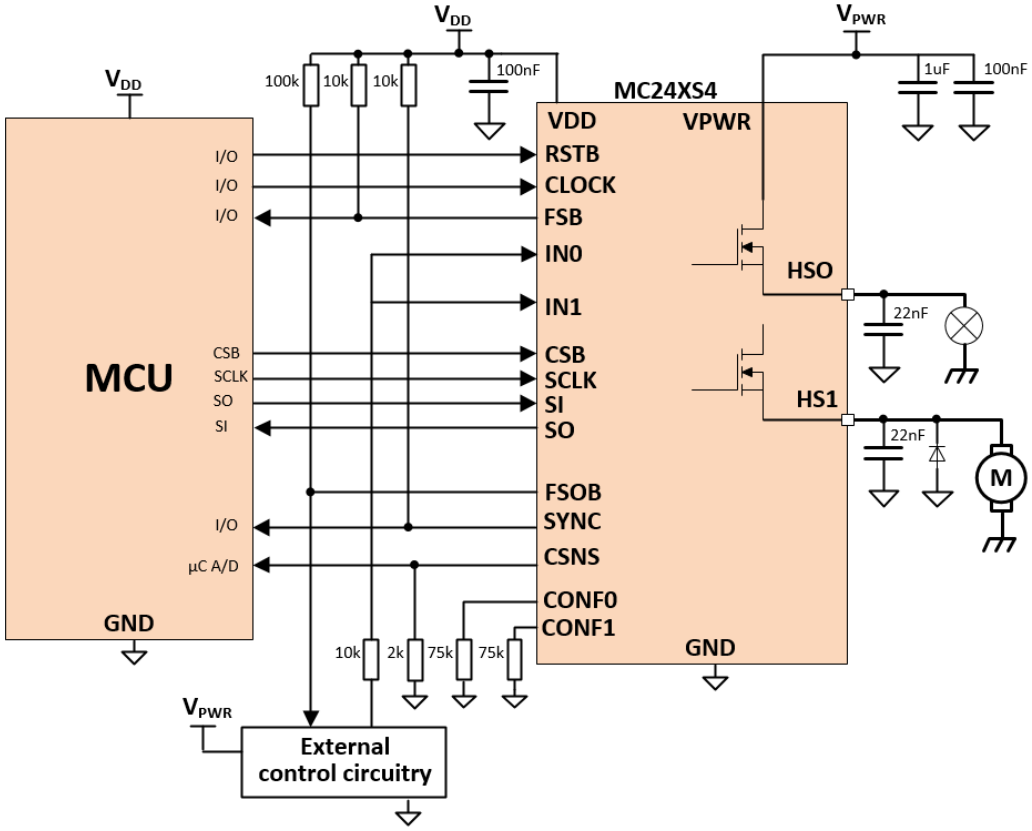


Figure 2. Example of application with external components

3.2 Main functions of the MC24XS4 family

The MC24XS4 family is a 24 V dual-high-side switch with integrated control and a high number of protective and diagnostic functions. It has been designed for truck, bus, and industrial applications. The low $R_{DS(ON)}$ channels can control different load types; bulbs, solenoids, or DC motors. Control, device configuration, and diagnostics are performed through a 16-bit Serial Peripheral Interface (SPI), allowing easy integration into existing applications. This device is powered by SMARTMOS technology.

Both channels can be controlled individually by external or internal clock signals, or by direct inputs. Using the internal clock allows fully autonomous device operation. Programmable output voltage slew rates (individually programmable) help improve Electromagnetic Compatibility (EMC) performance. To avoid shutting off the device upon inrush current, while still being able to closely track the load current, a dynamic overcurrent threshold profile is featured. The switching current of each channel can be sensed with a programmable sensing ratio. Whenever communication with the

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

external microcontroller is lost, the device enters a Fail-safe operation mode, but remains operational, controllable and protected.

Main functions:

- Turn OFF and ON the main power to the load
- Control of the turn-on/off with communication bus or direct inputs
- Control the slew rate when turning-on/off
- Control the duty cycle when in PWM mode
- Control delays between channels when turning-on/off
- Control the overcurrent profile, bulb or motor mode, with associated timing and current level windows
- Turn off the output when an overcurrent, over temperature, under voltage, or overvoltage is detected
- Control reactivation of the output when an overcurrent, over temperature, or under voltage is detected
- Control the output state when the external clock is out of range
- Control of both channels simultaneously when parallel mode is selected
- Report an image of the current in the power switch (MOSFET)
- Report the temperature on the device GND, pin 14

Embedded protections:

- Overload (OC)
- Severe short circuit (SC)
- VPWR Overvoltage (OV)
- VPWR Overvoltage over maximum ratings
- VPWR Under voltage (UV)
- Over temperature (OT)

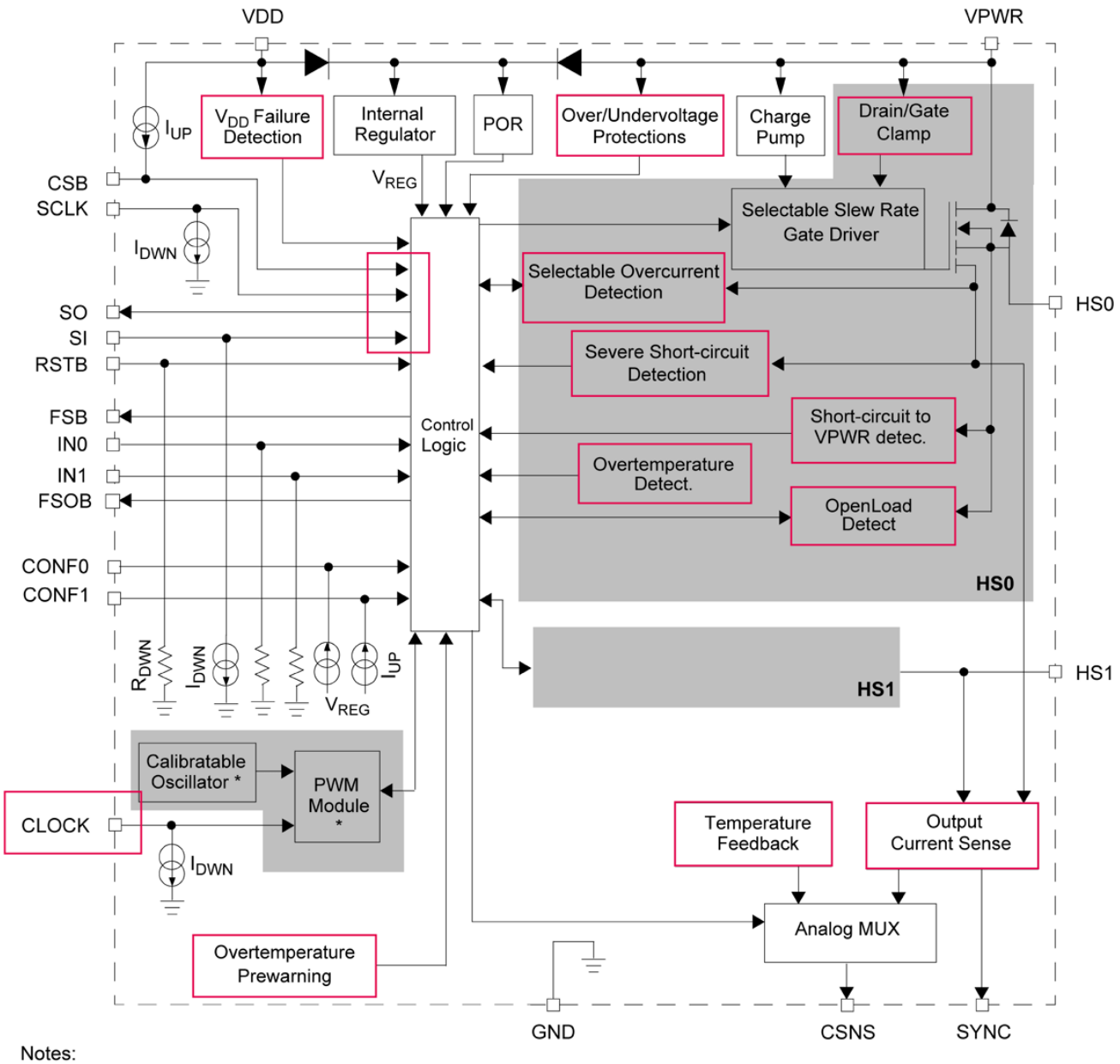
Embedded diagnostics:

- Open load detection when in ON mode
- Open load detection when in OFF mode
- Short to battery detection
- Warning on temperature level detection
- Output channel states
- Output current value
- Device temperature
- Direct input control state
- Register read

A block diagram of a device from the MC24XS4 family is shown in Figure 3. All devices in this family have the same block diagram.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.



Notes:
- Blocks marked in grey have been implemented independently for each of the two channels.
- Areas highlighted with a red rectangle are safety mechanisms.

Figure 3. Example of application with external components

4 Safety states

This section describes all the safe states of MC24XS4 that will be further identified in Section 6 "Device fault and diagnostics management".

In Figure 4, the states applied for the safe state mode are illustrated in red while unchanged states are illustrated in back.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

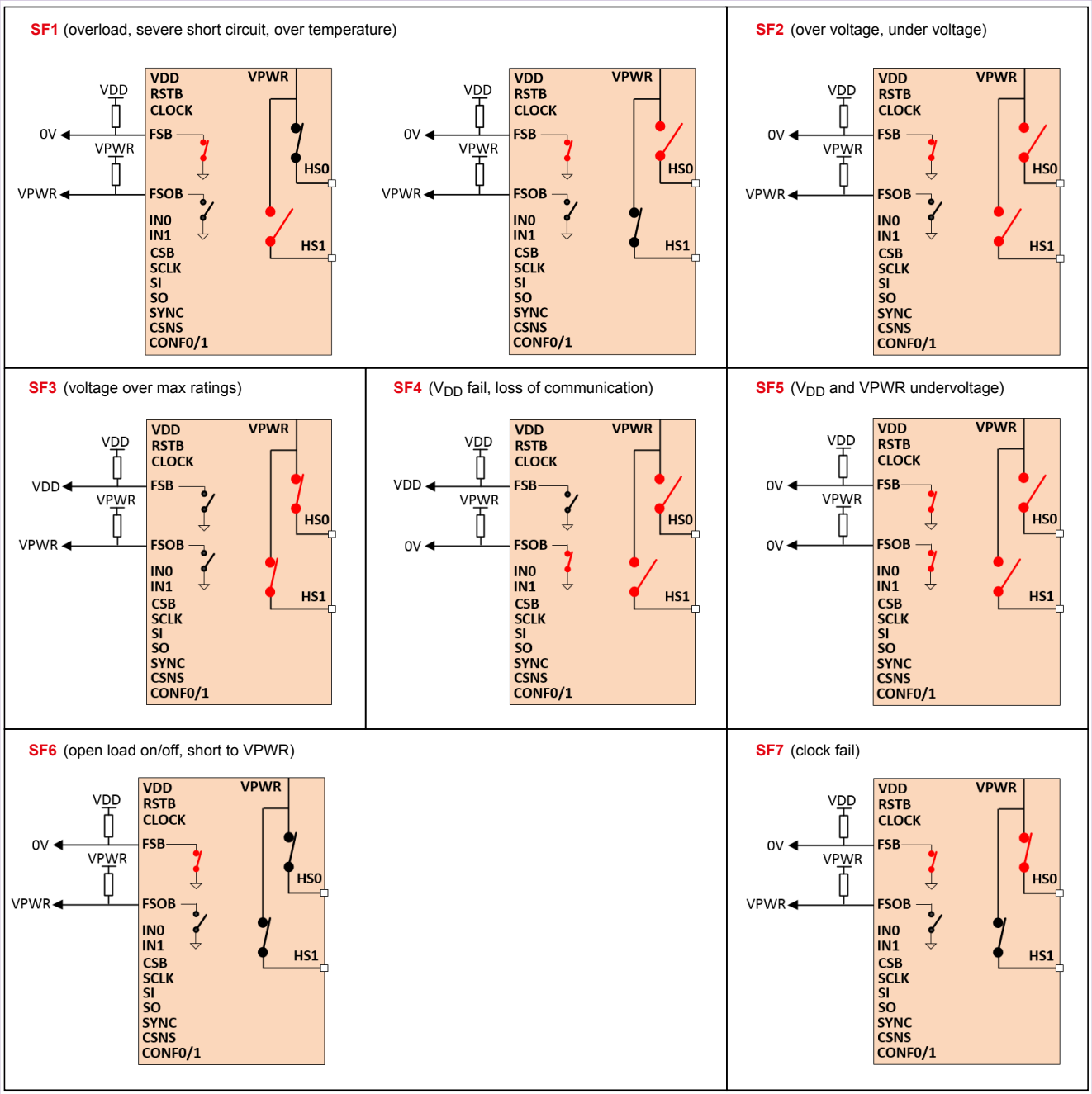


Figure 4. Safety states

5 Flags mapping relevant for diagnosis and faults

This section describes all flags of MC24XS4 that will be further identified in Section 6 "Device fault and diagnostics management". The register and labelling method use an "_s" extension to refer to each channel. A register name or bit name without the "_s" extension means the register or bit is common to both channels.

Example: The register name FAULTR_s means the register is same for both channels. FAULTR_0 refers to channel 0, FAULTR_1 refers to channel 1.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

Table 3, Table 4 and Table 5 refer to MCU SPI command to retrieve flags in the relevant device register.

Table 3. FAULT register and flags

READ	FAULTR_s register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	1	PF	0/1	0	0	0	0	0	0	0	0	0	0	0	0	1
MISO	WD	PF	SOA3	SOA2	SOA1	SOA0	NM	OTW	0	0	OLON_s	OLOFF_s	OS_s	OT_s	SC_s	OC_s
Flags								**FG7**			**FG6**	**FG5**	**FG4**	**FG3**	**FG2**	**FG1**

Table 4. STATR register and flags

READ	STATR register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	1	PF	0/1	0	0	0	0	0	0	0	0	0	0	0	0	0
MISO	WD	PF	SOA3	SOA2	SOA1	SOA0	NM	OV	UV	POR	RFULL1	RFULL0	FAULT1	FAULT0	OUT1	OUT0
Flags								**FG9**	**FG8**	**FG11**					**FG13**	**FG12**

Table 5. DIAGR register and flag

READ	DIAGR register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	1	PF	0/1	0	0	0	0	0	0	0	0	0	0	1	1	1
MISO	WD	PF	SOA3	SOA2	SOA1	SOA0	NM	CONF1	CONF0	ID1	ID0	IN1	IN0	CLOCK_fail	CAL_fail0	CAL_fail0
Flags												**FG15**	**FG14**	**FG10**		

Flag **FGALL** used later in the document refers to all bits of all the registers with default values.

6 Device fault and diagnostics management

The MC24XS4 family embeds internal fault detection leading to internal reactions on device operations.

In addition, the MC24XS4 family embeds internal diagnostics that do not lead to internal reaction on device operations, only reporting irregular operations. Both faults and diagnostics will be detailed separately.

6.1 Internal device faults detection

The MC24XS4 family embeds internal fault detection leading to internal reactions on device operations. The detected faults are:

- Overload (OC)
- Severe short circuit (SC)
- VPWR Overvoltage (OV)

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

- VPWR Overvoltage over maximum ratings
- VPWR Under voltage (UV)
- Over temperature (OT)

Two additional detections, not classified as faults in the device data sheets, have internal reactions and are similar to the previously mentioned faults. These detections are:

- V_{DD} out of range
- Loss of communication

Table 6. Summary table of device fault and device diagnostics management

ID	Name	Description	Module or function covered
SM1	Overload detection	On each channel, detect when the current in the load is over the specified range, either in the Lamp or DC Motor mode	Load fault, such as a short circuit at the end of a harness and over torque on motors
SM2	Severe short circuit detection	On each channel, detect a short circuit at the device output (on PCB)	Output channel pin shorted to GND , PCB fault, load fault if connected close to output channel
SM3	Overvoltage detection	On V_{PWR}, voltage is over the range specified AND OV bit is enabled	Battery line fault
SM4	Overvoltage over max ratings detection	On V_{PWR}, voltage is over the maximum specified between V_{PWR} and GND	Battery line fault
SM5	Under voltage detection	On V_{PWR}, voltage is under the specified range: $V_{PWR} < V_{PWR\ (UV)}$ $V_{DD} > V_{DD\ (FAIL)}$	Battery line fault
SM6	V_{DD} out of range detection	Monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD\_FAIL}$: enter in Fail safe mode provided $V_{DD\_FAIL\_EN}$ bit is set	Device or system V_{DD} fault
SM7	V_{DD} out of range detection	Monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD\_FAIL}$: does not enter in Fail safe provided $V_{DD\_FAIL\_EN}$ bit is not set	Device or system V_{DD} fault
SM8	V_{DD} out of range detection	Monitoring of V_{DD} low voltage threshold with conditions $V_{DD} > V_{DD\ (POR)}$ after $V_{DD} < V_{DD\ (POR)}$ AND $V_{PWR} < V_{PWR\ (POR)}$	Device or system V_{DD} fault
SM9	Lost of communication detection	Monitoring on the SPI frame integrity through Watchdog	SPI communication fault, MCU SPI pin fault
SM10	Over temperature detection	For each channel, detection of temperature is over 175°C (typ)	Module temperature, board overheating, power overload faults
SM11	Open load ON detection	On each channel, detection of current is below $I_{OLD(ON)}$ when channel is ON	Load disconnection, channel output pin disconnection
SM12	Open load OFF detection	On each channel, detection of current is below $I_{OLD(ON)}$ when the channel is OFF	Load disconnection, channel output pin disconnection
SM13	Short to V_{PWR} detection	On each channel, detection of channel output is short circuited to V_{PWR}, done only when channel is turned off	Load shorted to battery
SM14	External clock frequency range detection	When the external clock is used, detection whether the frequency of external clock in within $f < f_{CLOCK\ (LOW)}$ or $f > f_{CLOCK\ (HIGH)}$	MCU clock pin fault, MCU to device line fault, channel input clock disconnection

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

ID	Name	Description	Module or function covered
SM15	Over temperature warning detection	For each channel, detection of temperature is over T_{OTWAR} on GND, pin 14	Module temperature, board overheating, power overload faults
SM16	Output channel state detection	For each channel, detection of output channel state and reported into register	MCU to direct input connections or safety module control connection
SM17	Output current value & SYNC detection	For each channel, current recopy of output channel current	Output MOSFET malfunction or load disconnection
SM18	Device temperature detection	Die temperature is reported through CSNS pin	Overheating of device, malfunction of Power die temperature sensor
SM19	Direct input control state	For each channel, reporting of input state into register	MCU to direct input connections or safety module control connection
SM20	Register read	Register read reports data register and SO state	MCU SPI connection, device did not power up

6.1.1 Overcurrent (OC)

Overcurrent detection and conditions are depicted in the data sheet.

Table 7. Overload detection

Overload detection	Description of safety mechanism	On each channel, detect that the current in the load is over the specified range either in Lamp or DC Motor mode	SM1
	Device reaction	Turn off faulty channel	SF1
		FSB pin = 0 V	
		OC bit raised in FAULTR register	FG1
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, delatch sequence + FAULTR register read	

6.1.2 Severe short circuit (SC)

Table 8. Severe short circuit detection

Severe short circuit detection	Description of safety mechanism	On each channel, detect a short circuit at device output (on PCB)	SM2
	Device reaction	Turn off faulty channel	SF1
		FSB pin = 0 V	
		SC bit raised in FAULTR register	FG2
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, delatch sequence + FAULTR register read	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.1.3 Overvoltage (OV)

Table 9. Overvoltage detection

Overvoltage detection	Description of safety mechanism	On V_{PWR}, voltage is over the range specified AND OV bit is enabled	SM3
	Device reaction	Turn off the two channels	SF2
		FSB pin = 0 V	
		OV bit raised in STATR register	FG9
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, delatch sequence + STATR register read	

6.1.4 Overvoltage over maximum ratings

Table 10. Over voltage over maximum ratings

Overvoltage over max ratings detection	Description of safety mechanism	On V_{PWR}, voltage is over the maximum specified between V_{PWR} and GND	SM4
	Device reaction	Turn on the two channels	SF3
		FSB pin = 5 V (assume the OV_dis bit is disabled)	
		OV bit raised in STATR register	FG9
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, delatch sequence + STATR register read	

6.1.5 Under voltage (UV)

Table 11. Under voltage detection

Under voltage detection	Description of safety mechanism	On V_{PWR}, voltage is under the specified range: $V_{PWR} < V_{PWR(UV)}$ $V_{DD} > V_{DD\ (FAIL)}$	SM5
	Device reaction	Turn off the two channels	SF2
		FSB pin = 0 V	
		UV bit raised in STATR register	FG8
	MCU reaction	Integrator to decide action	
	Reset conditions	Under-voltage condition disappears, then: • If both internal commands are OFF, FSB returns to V_{DD}, UV bit is cleared upon a command to turn on one channel and read STATR register • If both internal commands are ON, the delatch sequence or POR needed and UV bit are cleared upon read STATR register • If one internal command is ON, the other is OFF. The channel with internal ON command needs the OFF then ON command to clear the fault (FSB = V_{DD}). The channel with ON internal command needs the ON command to clear the fault (FSB = V_{DD}). Then the UV bit is cleared upon a STATR register read.	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.1.6 V_{DD} out of range

Table 12. V_{DD} out of range detection1

V_{DD} out of range detection	Description of safety mechanism	Monitoring of V_{DD} low voltage threshold with conditions V_{DD} < V_{DD_FAIL} : enter in Fail safe mode provided $V_{DD\_FAIL\_EN}$ bit is set The SO data are not available	SM6
	Device reaction	Turn off the two channels	SF4
		FS0B pin = 0 V	
		All register contents are reset except POR and PARALLEL bits	FGALL
	MCU reaction	Integrator to decide action Channels can be turned ON by direct input IN0 and IN1 After V_{DD} is back to the specified range, reload the device configuration after the wake-up sequence	
	Reset conditions	None	

Table 13. V_{DD} out of range detection2

V_{DD} out of range detection	Description of safety mechanism	Monitoring of V_{DD} low voltage threshold with conditions V_{DD} < V_{DD_FAIL} : does not enter in Fail safe provided $V_{DD\_FAIL\_EN}$ bit is not set The SO data are not available	SM7
	Device reaction	None	None
		None	
	MCU reaction	Integrator to decide action Channels can be turned ON by direct input IN0 and IN1 or SPI	
	Reset conditions	None	

Table 14. V_{DD} out of range detection3

V_{DD} out of range detection	Description of safety mechanism	Monitoring of V_{DD} low voltage threshold with conditions V_{DD} > $V_{DD\ (POR)}$ after V_{DD} < $V_{DD\ (POR)}$ AND V_{PWR} < $V_{PWR\ (POR)}$ The SO data are not available	SM8
	Device reaction	POR generated	SF5
		Both channels are turned off	
		All registers are reset	
		POR bit raised in STATR register	FG11
	MCU reaction	Integrator to decide action After V_{DD} is back to the specified range, reload device configuration after wake-up sequence	
	Reset conditions	None	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.1.7 Loss of communication fault

Table 15. Loss of communication detection3

Loss of communication detection	Description of safety mechanism	Monitoring on the SPI frame integrity through Watchdog	SM9
	Device reaction	Both channels are turned off	SF4
		FSOB = 0 V	
		All register contents are reset except POR and PARALLEL bits	FGALL
	MCU reaction	Integrator to decide action Reload device configuration after wake-up sequence	
	Reset conditions	None	

6.1.8 Over temperature (OT)

Table 16. Over temperature detection

Over temperature detection	Description of safety mechanism	For each channel, detection of temperature over 175 °C (typ)	SM10
	Device reaction	If faulty channel is ON, channel is turned OFF	SF1
		FSB pin = 0 V	
		If both channels are OFF, FSB pin = 0 V until Tj < TSD and any channel is turned ON	SF1
		OT bit raised in FAULT register of faulty channel	FG3
	MCU reaction	Integrator to decide action	
	Reset conditions	After temperature < TSD , delatch sequence , read FAULTR register	

6.2 External fault diagnostics

The MC24XS4 family embeds internal diagnostics leading to noninternal reactions on device operations. Those diagnostics are:

- Open load in ON mode (OLON)
- Open load in OFF mode (OLOFF)
- Short to VPWR (OS)
- External clock fail (CLOCK_fail)
- Over temperature warning (OTW)
- Output channel states
- Output current value
- Device temperature
- Direct input control state
- Register read

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.2.1 Open load in ON mode (OLON)

Table 17. Open load ON detection

Open load ON detection	Description of safety mechanism	On each channel, detection of current below $I_{OLD(ON)}$ when channel is ON	SM11
	Device reaction	FSB pin = 0 V	SF6
		OLON bit raised in FAULTR register for faulty channel	FG6
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, FAULTR register read for OLON bit clearance	

6.2.2 Open load in OFF mode (OLOFF)

Table 18. Open load OFF detection

Open load OFF detection	Description of safety mechanism	On each channel, detection of current below $I_{OLD(ON)}$ when the channel is OFF	SM12
	Device reaction	FSB pin = 0 V	SF6
		OLOFF bit raised in FAULTR register for faulty channel	FG5
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, FAULTR register read for OLOFF bit clearance	

6.2.3 Short to VPWR (SC)

Table 19. Short to VPWR detection

Short to V_{PWR} detection	Description of safety mechanism	On each channel, detection of channel output is short circuited to V_{PWR}, done only when the channel is turned off	SM13
	Device reaction	FSB pin = 0 V	SF6
		OS bit raised in FAULTR register for faulty channel	FG4
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, FAULTR register read for SC bit clearance	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.2.4 External clock fail (CLOCK_Fail)

Table 20. Clock fail detection

External clock frequency range detection	Description of safety mechanism	When the external clock is used, frequency (f) is detected to be either: • $f < f_{CLOCK\ (LOW)}$ • $f > f_{CLOCK\ (HIGH)}$	SM14
	Device reaction	If state of bit ON in PWM register is selected for ON, channel output is ON	SF7
		FSB pin = 0 V	
		If state of bit ON in PWM register is selected for OFF, channel output is OFF	SF1
		FSB pin = 0 V	
		CLOCK_fail bit raised in DIAGR register	FG10
	MCU reaction	Integrator to decide action	
	Reset conditions	After fault disappears, DIAGR register read for CLOCK_fail bit clearance	

6.2.5 Over temperature warning (OTW)

Table 21. Over temperature warning detection

Over temperature warning detection	Description of safety mechanism	For each channel, detection of temperature is over T_{OTWAR} on GND, pin 14	SM15
	Device reaction	None	None
		OTW bit raised in FAULT register	FG7
	MCU reaction	Integrator to decide action	
	Reset conditions	After temperature < TOTWAR , FAULTR register read for OTW bit clearance	

6.2.6 Output channel state (OUT0, OUT1)

Table 22. Output channel state detection

Output channel state detection	Description of safety mechanism	For each channel, detection of output channel state and reported into register	SM16
	Device reaction	None	None
		OUT0 & OUT1 bit status in STATR register	FG12, FG13
	MCU reaction	Integrator to decide action	
	Reset conditions	None, output channel dependency	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.2.7 Output current value and SYNC

Table 23. Output current value & SYNC detection

Output current value & SYNC detection	Description of safety mechanism	For each channel, current recopy of output channel current and reflected on CSNS pin, SYNC pin is reflecting state of output when output is PWM'ed	SM17
	Device reaction	None	None
		None	None
	MCU reaction	Integrator to decide action	
	Reset conditions	None	

6.2.8 Device temperature

Table 24. Device temperature detection

Device temperature detection	Description of safety mechanism	Die temperature is reported through CSNS pin, this temperature is not Power die temperature, it is control die temperature	SM18
	Device reaction	None	None
		None	None
	MCU reaction	Integrator to decide action	
	Reset conditions	None	

6.2.9 Direct input control state (IN0, IN1)

Table 25. Direct input control detection

Direct input control state	Description of safety mechanism	For each channel, reporting of direct input state into register	SM19
	Device reaction	None	None
		IN0 & IN1 bit status in DIAGR register	FG14, FG15
	MCU reaction	Integrator to decide action	
	Reset conditions	None	

6.2.10 Register read

Table 26. Register read

Register read	Description of safety mechanism	Register read reports data register and SO state	SM20
	Device reaction	Reports on SO in register contents upon register read request	
	MCU reaction	Integrator to decide action	
	Reset conditions	None	

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.3 Fault detection time and fault reaction time

The fault detection time is the maximum time for detection of a fault and reporting the fault. This fault detection time is the same for all devices of the MC24XS4 family.

The fault reaction time is the maximum time needed to activate safety mechanisms, including internal processing time and external indication time.

6.3.1 Detection time and reaction time for over voltage, overload, short circuit, over temperature, and under voltage

The fault detection time is the time required for detection and to report the fault to the FSB pin.

The reaction time is time to turn off the channel output starting when the fault detection time is completed. The channel output is turned off only when over-voltage, over-temperature, overload, short circuit or under voltage are detected and when Fail safe mode is activated. This time is depicted as t_{DETECT} is 15 µs maximum. This time is specified under identified conditions as it is also load dependent.

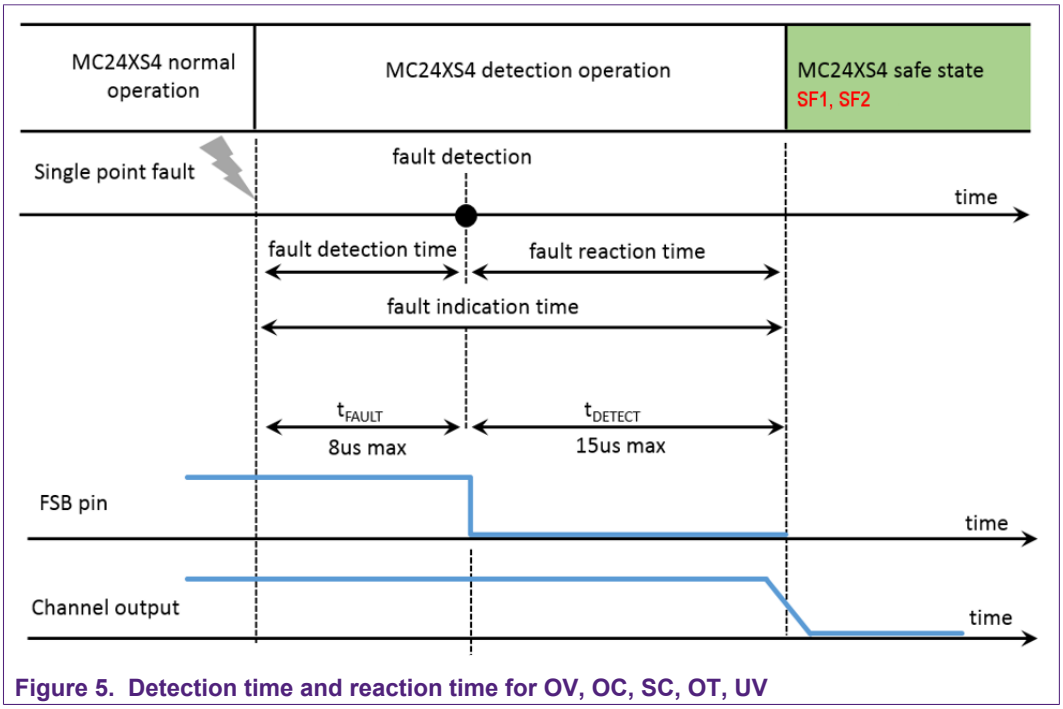


Figure 5. Detection time and reaction time for OV, OC, SC, OT, UV

6.3.2 Detection time and reaction time for open load on-off short circuit to VPWR

The fault detection time is the time required for detection and to report the diagnostic to the FSB pin. This time is depicted in the data sheet as t_{FAULT}, 8 µs maximum.

There is no reaction time for diagnostics.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

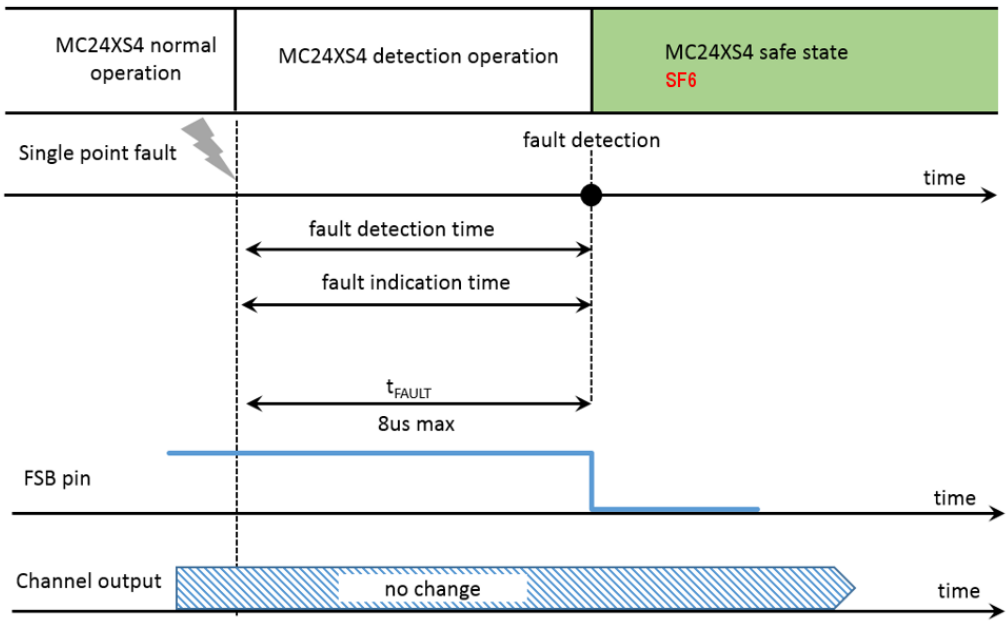


Figure 6. Detection time and reaction time for OLON, OLOFF, OS

6.3.3 Detection time and reaction time for V_{DD} out of range and loss of communication

The fault detection time is the time required for detection and to report the diagnostic to the FSOB pin. This time is not depicted in the data sheet; it is estimated as 8 µs maximum.

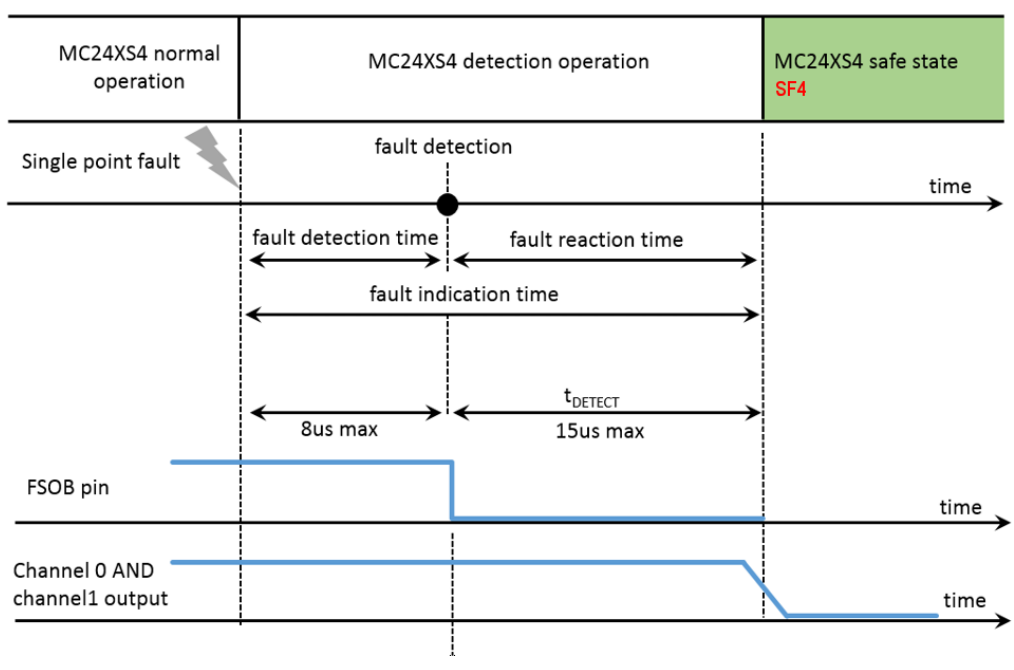


Figure 7. Detection time and reaction time for VDD out of range and loss of communication

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

6.3.4 Detection time and reaction time for external clock failure

The fault detection time is the time required for detection and to report the diagnostic to the FSB pin. This time is depicted in the data sheet as t_{FAULT}, 8 µs maximum.

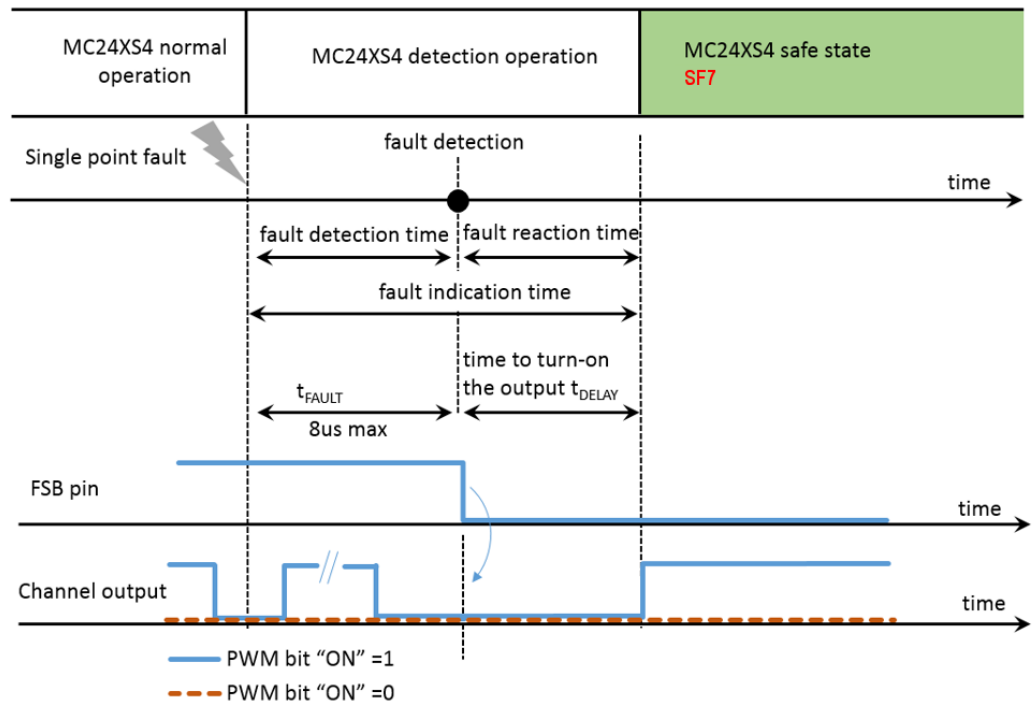


Figure 8. Detection time and reaction time for clock fail

7 Operation of use and mission profile

The MC24XS4 family is used in applications for which the mission profile is described in Table 27. This document is based on this mission profile, although use of MC24XS4 is not limited to these values. The mission profile may differ slightly from application to application. The mission profile shown is representative of a typical automotive profile.

Table 27. Mission profile

Mission parameters	Mission profile
Junction temperature	–40C to 150C
Lifetime	15 years
Total operation time (ON)	45000 hrs.
Total sleep time (Standby)	86400 hrs.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

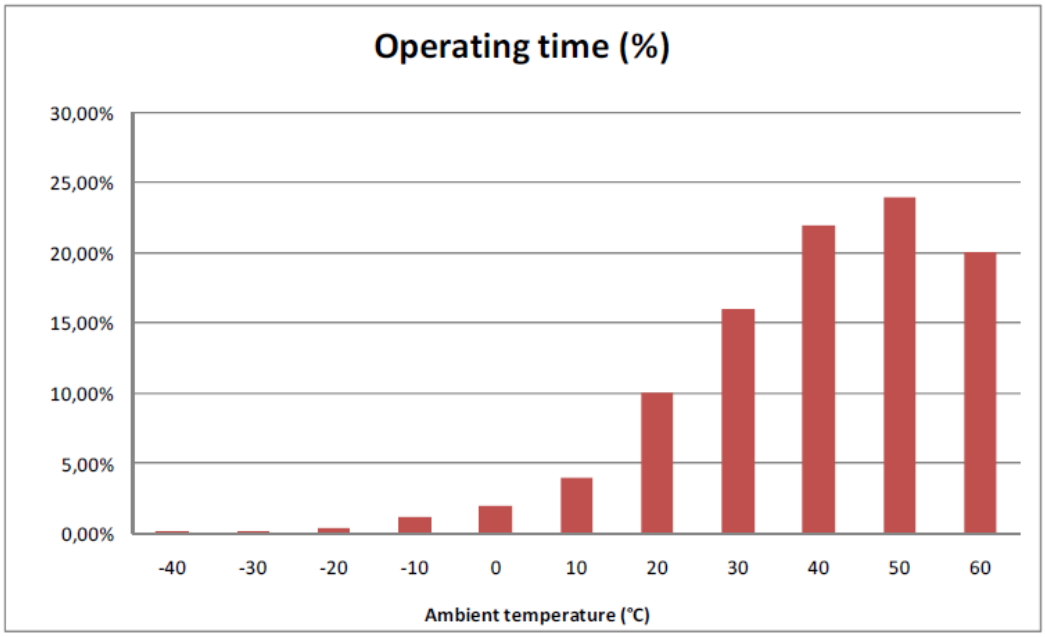


Figure 9. Temperature profile

Table 28. Thermal cycling

Mode	Cycle definition	Start temperature of the cycle (°C)	Number of cycles
Operating	Night	20	670
Operating	Day	25	1340
No-operating	Non used	10	30

Global Failures in Time (FIT) rate calculation for reference MC06XS4200, MC10XS4200, MC20XS4200 (PQFN package) and MC22XS4200, MC50XS4200 (eSOIC package):

The global FIT rate (λ) calculation is in accordance to the IEC/TR 62380. This standard considers the failure rate model for permanent faults in a semiconductor device to be the sum of three subcomponents:

- **Die** predictive failure rate
- **Package** predictive failure rate
- **Interface electrical overstress** predictive failure

Table 29. Global FIT rates

λ	FIT
λ component (PQFN package)	63.3
λ component (eSOIC package)	43.1

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

8 Safety analysis

This section reports the safety analysis of MC24XS4 family to compute Single Point Fault Metric (SPFM) and Latent Fault Metric (LFM) in accordance with ISO 26262-5-2011 standard.

SPFM and LFM were issued from FMEDA analysis in accordance with safety goals in a micro-controller based system.

The FMEDA has been constructed with device block sizes with device routing area being equally distributed over all device blocks. The digital block area was also distributed over other blocks except few analog blocks where digital was not considered.

8.1 Safety mechanisms

Here below table is all safety mechanism available and used for FMEDA construction.

Table 30. Safety mechanisms

Number	Safety mechanism	§ ISO 26262	Level of Diagnostic coverage	Used?	DC (%)
SM1	Overload detection	D.2.8.2	High	**Yes**	99%
SM2	Severe short circuit detection	D.2.8.2	High	**Yes**	99%
SM3	Over voltage detection	D.2.8.2	High	**Yes**	99%
SM4	Voltage over max ratings detection	D.2.8.1	Low	**Yes**	60%
SM5	Under voltage detection	D.2.8.2	High	**Yes**	99%
SM6	VDD out of range detection1	D.2.8.2	High	**Yes**	99%
SM7	VDD out of range detection2	D.2.8.2	High	**Yes**	99%
SM8	VDD out of range detection3	D.2.8.2	High	**Yes**	99%
SM9	Loss of communication detection	D.2.7.1, D.2.7.8, D.2.9.2	Medium	**Yes**	90%
SM10	Over temperature detection	D.2.1.1, D.2.10.1	Medium	**Yes**	90%
SM11	Open load ON mode detection	D.2.8.2	High	**Yes**	99%
SM12	Open load OFF mode detection	D.2.8.2	High	**Yes**	99%
SM13	Short to VPWR detection	D.2.8.2	High	**Yes**	99%
SM14	External clock frequency range detection	D.2.9.2	Medium	**Yes**	90%
SM15	Over temperature warning detection	D.2.1.1, D.2.10.1	Medium	**Yes**	90%
SM16	Output channel state	D.2.8.2	High	**Yes**	99%

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

Number	Safety mechanism	§ ISO 26262	Level of Diagnostic coverage	Used?	DC (%)
SM17	Output current value & SYNC	D.2.8.2	High	**Yes**	99%
SM18	Device temperature detection	D.2.1.1, D.2.10.1	Medium	**Yes**	90%
SM19	Direct input control state	D.2.8.2	High	**Yes**	99%
SM20	Register read	D.2.7.1, D.2.7.8, D.2.9.2	Medium	**Yes**	90%

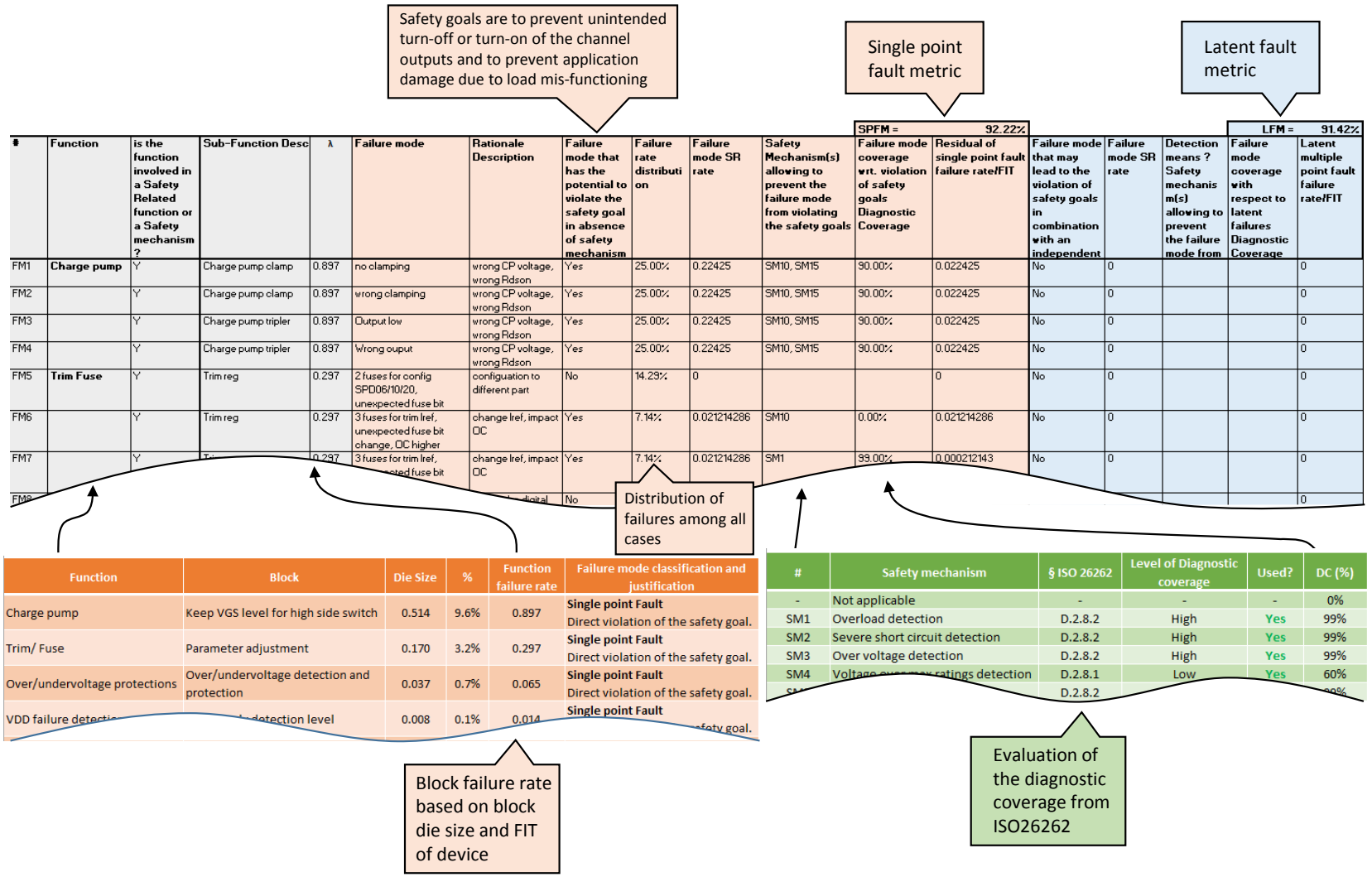
8.2 SPFM & LFM

The resulting SPFM is **92.2 %** and the resulting LFM is **91.4 %**.

Figure 10 is an extract of FMEDA along with different elements used for the construction.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.



#	Function	is the function involved in a Safety Related function or a Safety mechanism ?	Sub-Function Desc	λ	Failure mode	Rationale Description	Failure mode that has the potential to violate the safety goal in absence of safety mechanism	Failure rate distribution	Failure mode SR rate	Safety Mechanism(s) allowing to prevent the failure mode from violating the safety goals	Failure mode coverage wrt. violation of safety goals Diagnostic Coverage	Residual of single point fault failure rate/FIT	Failure mode that may lead to the violation of safety goals in combination with an independent	Failure mode SR rate	Detection means ? Safety mechanism(s) allowing to prevent the failure mode from	Failure mode coverage with respect to latent failures Diagnostic Coverage	Latent multiple point fault failure rate/FIT
FM1	**Charge pump**	Y	Charge pump clamp	0.897	no clamping	wrong CP voltage, wrong Rdson	Yes	25.00%	0.22425	SM10, SM15	90.00%	0.022425	No	0			0
FM2		Y	Charge pump clamp	0.897	wrong clamping	wrong CP voltage, wrong Rdson	Yes	25.00%	0.22425	SM10, SM15	90.00%	0.022425	No	0			0
FM3		Y	Charge pump tripler	0.897	Output low	wrong CP voltage, wrong Rdson	Yes	25.00%	0.22425	SM10, SM15	90.00%	0.022425	No	0			0
FM4		Y	Charge pump tripler	0.897	Wrong ouput	wrong CP voltage, wrong Rdson	Yes	25.00%	0.22425	SM10, SM15	90.00%	0.022425	No	0			0
FM5	**Trim Fuse**	Y	Trim reg	0.297	2 fuses for config SPD06/10/20, unexpected fuse bit	configuation to different part	No	14.29%	0			0	No	0			0
FM6		Y	Trim reg	0.297	3 fuses for trim Iref, unexpected fuse bit change, OC higher	change Iref, impact OC	Yes	7.14%	0.021214286	SM10	0.00%	0.021214286	No	0			0
FM7		Y		0.297	3 fuses for trim Iref,	change Iref, impact OC	Yes	7.14%	0.021214286	SM1	99.00%	0.000212143	No	0			0
FM8							No										0

Function	Block	Die Size	%	Function failure rate	Failure mode classification and justification
Charge pump	Keep VGS level for high side switch	0.514	9.6%	0.897	**Single point Fault** Direct violation of the safety goal.
Trim/ Fuse	Parameter adjustment	0.170	3.2%	0.297	**Single point Fault** Direct violation of the safety goal.
Over/undervoltage protections	Over/undervoltage detection and protection	0.037	0.7%	0.065	**Single point Fault** Direct violation of the safety goal.
VDD failure detecti	detection level	0.008	0.1%	0.014	**Single point Fault** afety goal.

#	Safety mechanism	§ ISO 26262	Level of Diagnostic coverage	Used?	DC (%)
-	Not applicable	-	-	-	0%
SM1	Overload detection	D.2.8.2	High	Yes	99%
SM2	Severe short circuit detection	D.2.8.2	High	Yes	99%
SM3	Over voltage detection	D.2.8.2	High	Yes	99%
SM4	Voltage ratings detection	D.2.8.1	Low	Yes	60%
		D.2.8.2			

Figure 10. FMEDA construction

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

9 Conclusion

In a micro-controller based system, the MC24XS06 family is **ASIL B** classified.

Table 31 identifies the ISO 26262 ASIL requirements for SPFM and LFM.

Table 31. ISO 26262 ASIL requirements for Single Point Fault and Latent Fault Metrics

Fault Metrics	ASIL B	ASIL C	ASILD
Single Point Fault Metrics	>= 90 %	>= 97 %	>= 99 %
Latent Fault Metrics	>= 60 %	>= 80 %	>= 90 %

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

10 Revision history

Revision	Date	Description of changes
3.0	1/2018	• Corrected minor typos • Replaced FG12 by FG11 in Table 14 • Replaced FG4 by FG10 in Table 20 • Replaced FG4 by FG7 in Table 21
2.0	1/2017	• Revised threee assumptions, removing "It is assumed that" from all three assumptions in Section 2.1. • Updated "Safety monitor" column in Table 2 for Pins FSB, FSOB, CONF0 and CONF1 to "No" in Section 3. • Added pins "HS0" and HS1" to Table 2 in Section 3. • Changed title of Section 3.1 from "HS0 and HS1 Power outputs (safety monitored)" to Section 3.1 • Updated first paragraph of Section 3.2. • Added five list items to the Embedded diagnostics list in Section 3.2 starting with "Output channel states." • Updated Figure 3, identifying the safety mechanisms "Temperature Feedback" and "Output Current Sense" in color. • Revised sentence before Figure 4 to read "In Figure 4, the states applied for the safe state mode are illustrated in red while unchanged states are illustrated in back." • Revised sentence before Table 3 to read "Table 3, Table 4 and Table 5 refer to MCU SPI command to retrieve flags in the relevant device register." • Updated Table 4, adding flags "FG13" and "FG12" to columns "D1" and "D0" respectively. • Updated Table 5, adding flags "FG15" and "FG14" to columns "D4" and "D3" respectively. • Added five new table rows to Table 6 for tables "SM16" through "SM20". • Performed minor formatting updates to the description column of Table 6 and the corresponding tables. • Added five new list items to the Embedded fault diagnostics list Section 6.2 "External fault diagnostics" starting with "Output channel states.". • Changed "OLON" to "OLOFF" in the Device reaction section of Table 18. • Added five sections/tables: Section 6.2.6/Table 22, Section 6.2.7/Table 23, Section 6.2.8/Table 24, Section 6.2.9/Table 25 and Section 6.2.10/Table 26. • Revised description of Global Failures in Time (FIT) rate calculation and Table 29 to incorporate PQFN and eSOIC packages. • Added Section 8 "Safety analysis", including Table 30 and Figure 10. • Added Section 9 "Conclusion", including Table 31.
1.0	10/2016	Initial release

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

11 Legal information

11.1 Definitions

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

11.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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

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

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

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

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

11.3 Trademarks

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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

Tables

Figures

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2018. All rights reserved.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 26 January 2018