AN11936

Safety application note for MC12XS3 family

Rev. 2.0 — 21 January 2019 Application note

Document information

Information	Content
Keywords	AN11936, safety, MC12XS3
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.

Revision history

Rev	Date	Description
2	20190121	Table 11: replaced FG8 by FG7
1	20170623	initial version

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 MC12XS3 12 V eXtreme switch family. This family has seven products:

- MC07XS3200
- MC09XS3400
- MC10XS3412
- MC10XS3425
- MC10XS3435
- MC15XS3400
- MC35XS3400

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 the design.

Example:

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

This document also contains guidelines on how to configure and operate 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 needs to use discretion in deciding whether these measures are appropriate for their applications.

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

1.1 Related documents

This section lists all the documentation mentioned in this application note.

The application note 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

Document name	Description
MC07XS3200, MC09XS3400, MC10XS3412, MC10XS3425, MC10XS3435, MC15XS3400, MC35XS3400	data sheet

1.2 Vocabulary

The following terms, defined in ISO 26262-1 and IEC 61508-4, apply to this document:

- **System:** Functional safety-related system, both implement the required functional safety goals necessary to achieve or maintain a safe state system for the equipment under control (control system), and is intended to achieve on its own or with other electrical/electronic/programmable electronic functional safety#related systems, and other risk reduction measures, the necessary functional safety integrity for the required safety functions.
- **System integrator:** The person who is responsible for the system integration.
- **Element:** Part of a subsystem comprising of a single component or any group of components (for example, hardware, software, hardware parts, software units) performing one or more element safety functions (functional safety requirements).

2 General information

These devices are used in automotive or industrial applications which must be integrated in a system that fulfills functional safety requirements, as defined by functional safety integrity levels, such as Automotive Safety Integrity Level (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 NXP data sheet are maintained.

Assumption: The latest device errata are considered during system design, implementation, and maintenance.

Assumption: All field failures of the devices are reported to 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 most applications. Integrate this application independent safety function into a complete (application-dependent) system.

2.3 Safety goals

The safety goals at application level are to:

- 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 a generic safety system architecture example. The primary feature of the MC12XS3 family is to be the main switch to turn on and turn off lights in a vehicle and other type of loads, such as DC motors, solenoids and power modules.

All devices embed internal fault-detection mechanisms and diagnostics. Serial peripheral interface (SPI) communication pins report fault and diagnostics back to the MCU.

MC12XS3 is also self-protected against overload and overheating.

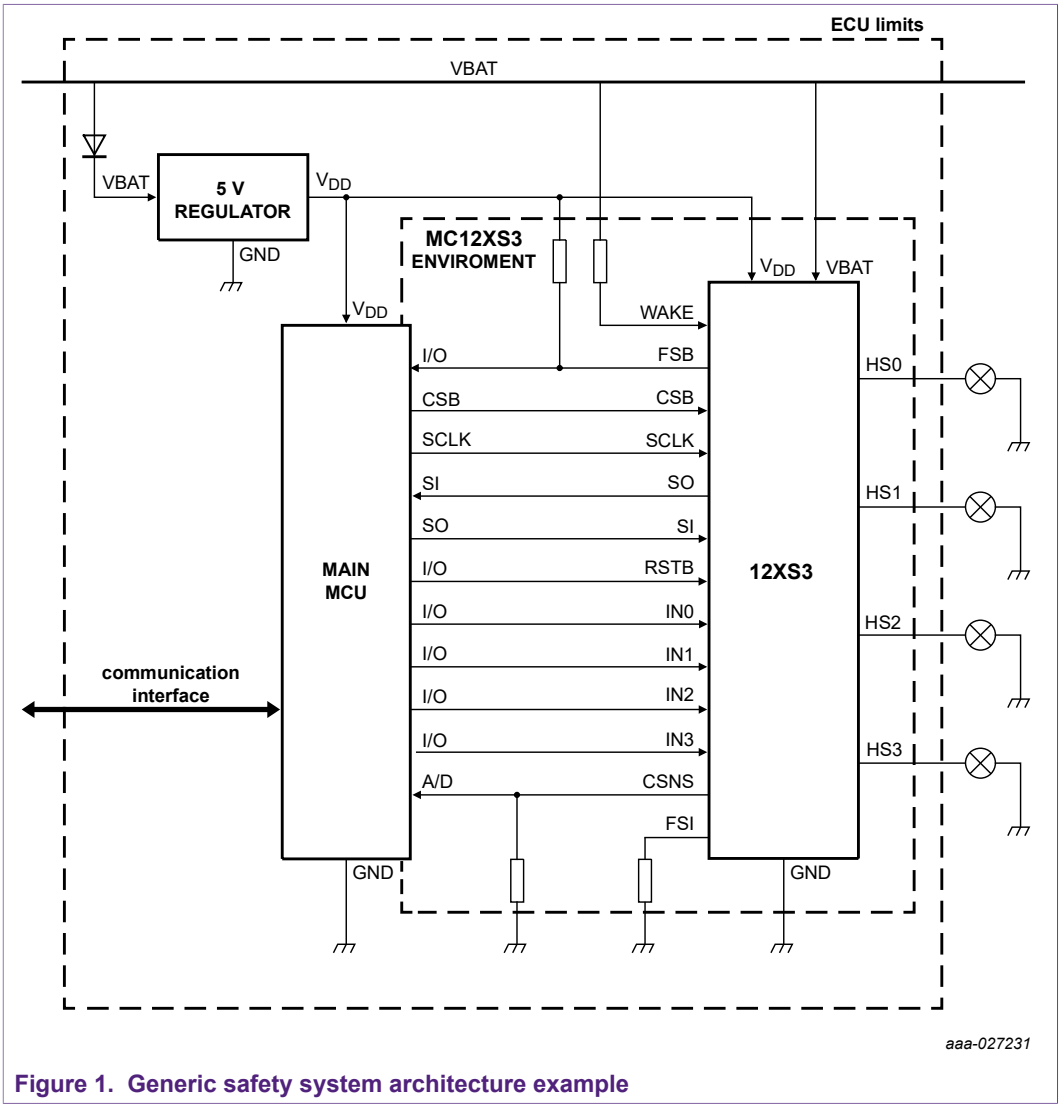

Figure 1. Generic safety system architecture example

Table 2. Pin descriptions

Pin	Description	Safety monitored
V_{DD}	digital core and interface supply	yes
V_{BAT}	power supply	yes
RSTB	reset of device, active LOW to HIGH	no
WAKE	wake-up input signal	no
FSB	fault status signal	yes
IN0 to IN3	direct input drive	no
SPI (4)	serial peripheral interface between MCU and MC12XS3 device	no
FSI	fail-safe input	no
CSNS	analog sense output	no
HS0 to HS3	power output	yes

3.1 Targeted applications

The MC12XS3 family is developed to control different type of loads (bulb lamps, HID ballast, xenon or LED modules) with low $R_{DS(on)}$ in high-side drive mode. It is designed for car, trailers and industrial applications.

Applications:

- Lighting: High beam, low beam, turn indicators, side indicators, fog lamp, brake indicators, rear indicators, parking lights
- Industrial: motor control, heaters, water pump, solenoids

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

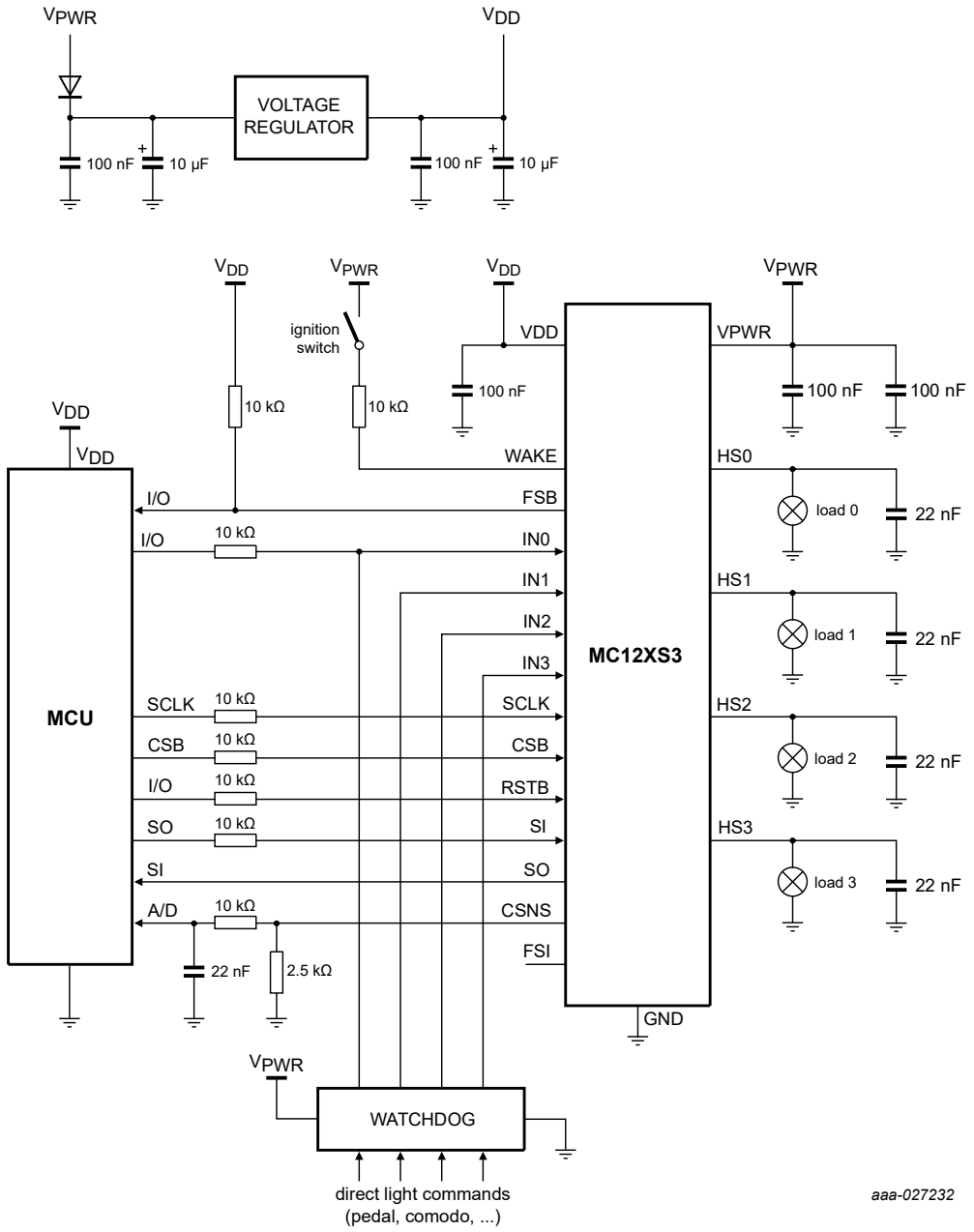

Figure 2. Example of an application with external components

3.2 Main functions of the MC12XS3 family

The MC12XS3 is a 12 V device family, composed by dual and quad high-side switches with integrated control, and a high number of protection and diagnostic functions. It has been designed especially for automotive 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 SPI, allowing easy integration into existing applications. This device is powered by SMARTMOS technology.

Power channels can be controlled individually by external or internal clock signals using SPI, or by direct inputs. Programmable output voltage slew rates (individually

programmable) such as setting the phasing between outputs helps to 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. Switching current of each channel can be sensed with a programmable sensing ratio. Whenever communication with the 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 (with duty cycle control)
- Control of the turn on/off either with communication bus and/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 and configure the transient overcurrent profile timing window and the continuous current level threshold
- Turn off the output when an overcurrent, overtemperature, undervoltage or overvoltage is detected
- Manage the bulb load inrush cooling time
- Control the number of reactivation of the output when overcurrent, overtemperature or undervoltage is detected
- Control output state when external clock is out of range
- Report an image of the current in the power switch (MOSFET)
- Report an image of the control die temperature

Embedded protections:

- Overload
- Severe short-circuit
- V_{PWR} over maximum voltage ratings
- V_{PWR} undervoltage
- V_{PWR} overvoltage
- Overtemperature

Embedded diagnostics:

- Open-load detection when in on mode (bulb or LED)
- Open-load detection when in off mode
- Short to battery detection or output channel states
- Warning on temperature level detection
- Output current value
- GND flag temperature value
- Clock failure
- Input logic state
- Register read
- Power-on reset of the device

All above mentioned protections are available in diagnostics.

A block diagram of a device from MC12XS3 family is shown in Figure 3. All devices in this family have the same block diagram. All safety mechanisms in Figure 3 are identified in red.

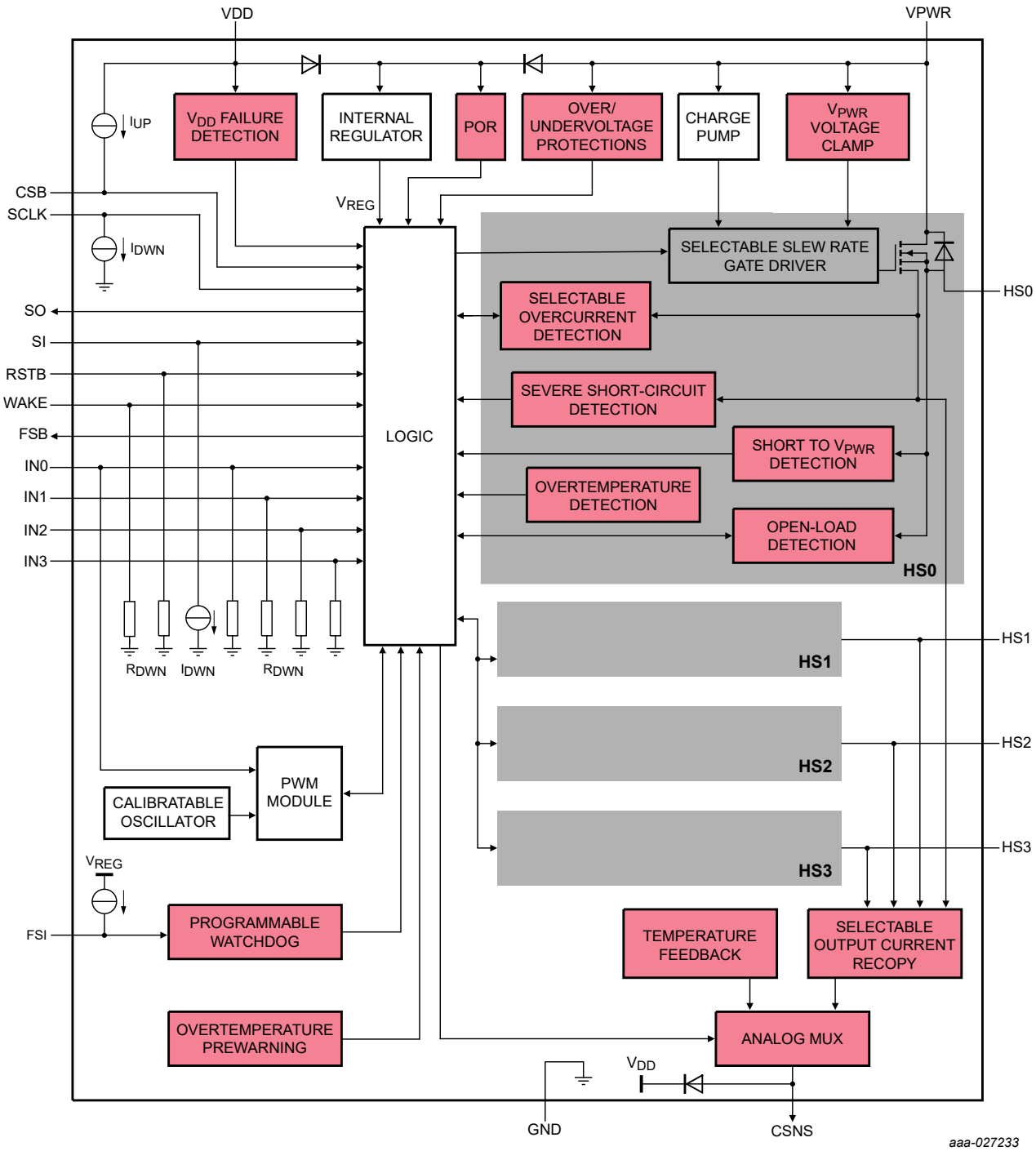

Figure 3. Internal block diagram

4 Safety states

This section describes all the safe states of MC12XS3 that are further identified in Section 6 "Device fault and device diagnostics management".

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

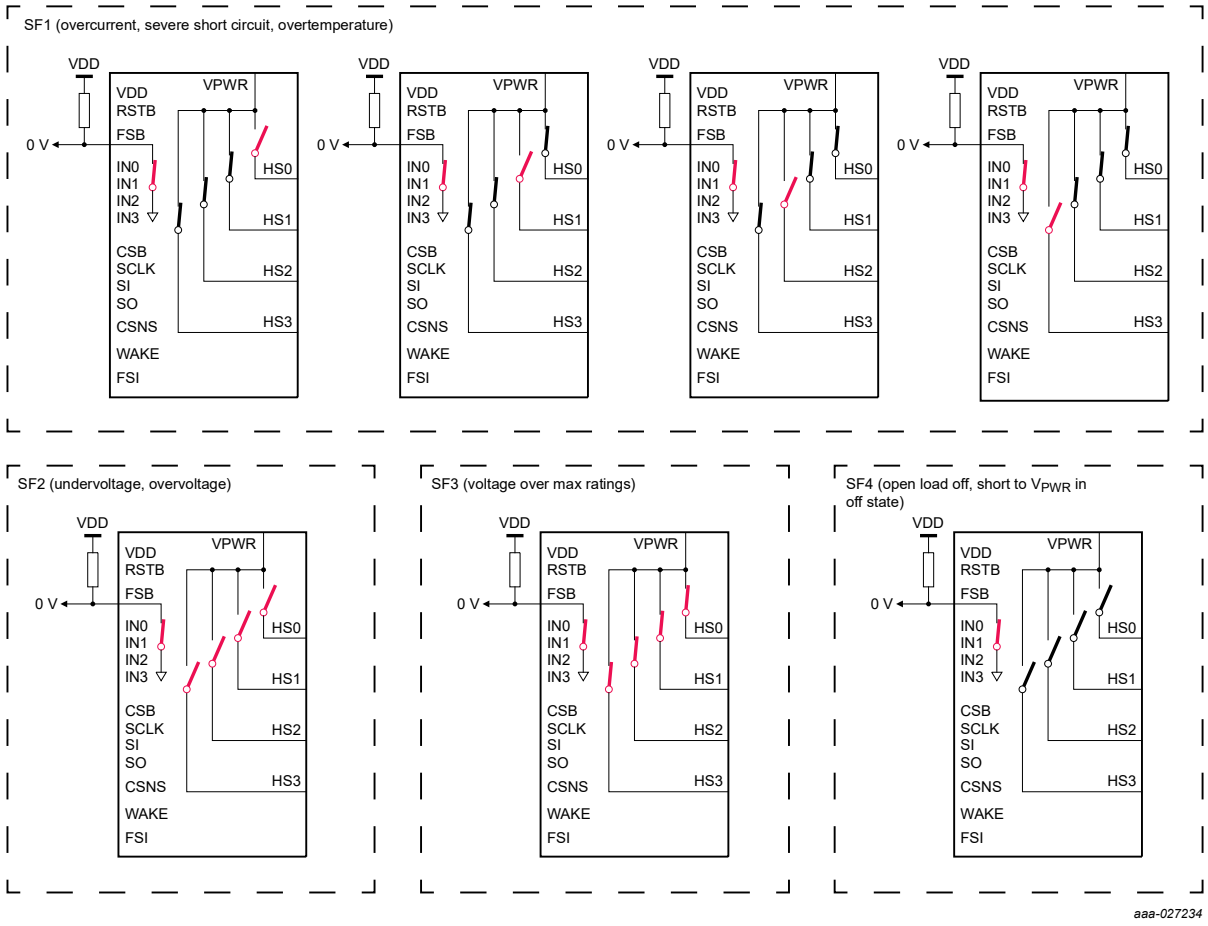

Figure 4. Safety states

5 Flags mapping relevant for diagnosis and faults

This section describes all flags of MC12XS3 that are further identified in Section 6 "Device fault and device diagnostics management". The labeling method uses an 's' extension to refer to each channel. A register name or bit name without the 's' extension means the register (or the bit) is common to all channels.

The following tables relate to MCU SPI commands to retrieve flags in the relevant device register.

Table 3. Status register and flags

Read	Status register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	WDIN	–	–	0	0	0	0	0	0	0	0	A1[1]	A0[1]	0	0	0
MISO	WDIN	A1[1]	A0[1]	0	0	0	NM	POR	UV	OV	OLON_s	OLOFF_s	OS_s	OT_s	SC_s	OC_s
Flags	**FG11**						**FG10**	**FG9**	**FG8**	**FG7**	**FG6**	**FG5**	**FG4**	**FG3**	**FG2**	**FG1**

[1] Output selection with A0/A1 bits.

Table 4. DIAGR0 register and flags

Read	DIAGR0 register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	WDIN	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
MISO	WDIN	0	1	1	1	1	NM	–	–	–	–	–	–	CLK_FAIL	CAL_FAIL	OTW
Flags	**FG11**						**FG10**							**FG13**		**FG12**

Table 5. DIAGR1 register and flags

Read	DIAGR1 register read command															
	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
MOSI	WDIN	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
MISO	WDIN	0	1	1	1	1	NM	–	–	–	–	IN3	IN2	IN1	IN0	WD_EN
Flags	**FG11**						**FG10**					**FG14**				

6 Device fault and device diagnostics management

MC12XS3 family embeds internal fault detection leading to internal reactions on device operations.

In addition, MC12XS3 family embeds internal diagnostics that do not lead to internal reaction on device operations, only reporting nonregular operations. Both faults and diagnostics are detailed separately.

6.1 Internal device faults detection

MC12XS3 family embeds internal fault detection leading to internal reactions on device operations. The detected faults are:

- Overcurrent (OC)
- Severe short-circuit (SC)
- V_{PWR} over maximum voltage ratings
- V_{PWR} undervoltage (UV)
- V_{PWR} overvoltage (OV)
- Overtemperature (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:

- Power-on reset (POR)
- External clock failure (CLOCK_FAIL)

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

ID	Name	Description	Module or function covered
SM1	overcurrent detection	on each channel, detect the current in the load is over specified range either in transit or in DC operation	load fault (short-circuit at end of harness, overloaded channel…)
SM2	severe short#circuit detection	on each channel, detect the short-circuit at device output (on PCB)	output channel pin shorted to GND, PCB fault, if connected close to output channel load fault
SM3	voltage over maximum ratings detection	on V_{PWR}, voltage is over the maximum specified between V_{PWR} and GND	battery line fault
SM4	undervoltage detection	on V_{PWR}, voltage is under the specified range: $V_{PWR} < V_{PWR(UV)}$ and $V_{DD} > V_{DD(FAIL)}$	battery line fault
SM5	overvoltage detection	on V_{PWR}, voltage is over the specified range: $V_{PWR\#GND} > V_{PWR(OV)}$	battery line fault
SM6	overtemperature detection	for each channel, detection of temperature is over 175 °C (typ)	module temperature, board overheating, power overload faults
SM7	V_{DD} out of range detection; case 1	monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD(FAIL)}$ and VDD_FAIL_EN = 1 in normal mode	system VDD fault
SM8	V_{DD} out of range detection; case 2	monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD(FAIL)}$ and VDD_FAIL_EN = 0 in normal mode	system VDD fault
SM9	loss of communication detection	monitoring of the SPI frame integrity through Watchdog	SPI communication fault, MCU SPI pin fault
SM10	open-load on mode detection	on each channel, detection of current below $I_{OLD(ON)}$ or $I_{OLD(ON\_LED)}$ (if LED mode activated) when the channel is on and feature enabled	load disconnection, filament cut, channel output pin disconnection
SM11	open-load off mode detection	on each channel, detection of current below $I_{OLD(OFF)}$ when the channel is off and feature enabled	load disconnection, filament cut, channel output pin disconnection

ID	Name	Description	Module or function covered
SM13	clock fail detection	if external clock is disconnected or out of the f_{CLK} frequency range, when the device operates in PWM	MCU clock pin fault, MCU to device line fault, channel input clock disconnection
SM14	overtemperature warning detection	for each channel, detection of temperature over T_{OTWAR}	module temperature, board overheating, power overload faults
SM15	short to V_{PWR} detection	on each channel, detection of channel output state and report into register; allows diagnosis if channel is short-circuited to V_{PWR} when channel is off state	load or output short to battery
SM16	input channel state detection	each device input state (INx) is monitored and reported into register	monitor a possible wrong GPIO event on master/slave MCU
SM17	output current value	for each channel, current recopy of output channel current can be multiplexed on CSNS pin	load dysfunction, degradation or partial disconnection detection
SM18	device temperature detection	control die temperature (not power die temperature) is reported through the CSNS pin	module temperature monitoring, board overheating
SM20	register read	register read reports data register and SO state	MCU SPI connection, device did not power up

6.1.1 Overcurrent

Overcurrent detection and conditions are depicted in data sheet.

Table 7. Overcurrent detection

Overcurrent detection	description of safety mechanism	on each channel, detect the current in the load is over specified range either in transit or in DC operation	SM1
	device reaction	turn-off faulty channel and if enabled make auto-retries (by default) or if device is in fail-safe mode; FSB pin = 0 V	SF1
	MCU reaction	OC bit raised on STATR register for corresponding output (s); integrator to decide action	FG1
	reset conditions	after fault disappeared, de-latch sequence	

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 the short-circuit at device output (on PCB)	SM2
	device reaction	turn-off faulty channel; FSB pin = 0 V	SF1
		SC bit raised on STATR register for corresponding output (s)	FG2
	MCU reaction	integrator to decide action	
	reset conditions	after fault disappeared, de-latch sequence	

6.1.3 Voltage over maximum ratings

Table 9. Voltage over maximum ratings

Voltage over maximum ratings detection	description of safety mechanism	on V_{PWR}, voltage is over the maximum value, specified between V_{PWR} and GND [1]	SM3
	device reaction	turn-on all channels	SF3
		if overload is enabled (by default) FSB pin = 0 V; OV bit raised in STATR register	FG7
	MCU reaction	integrator to decide action	
	reset conditions	after fault disappeared, flag is removed	

[1] This condition applies when outputs are open in the application.

6.1.4 Undervoltage (UV) with $V_{DD} > V_{DD(FAIL)}$

Table 10. Undervoltage detection without $V_{DD(FAIL)}$

Undervoltage detection	description of safety mechanism	on V_{PWR}, voltage is under the specified range: $V_{PWR} < V_{PWR(UV)}$ and $V_{DD} > V_{DD(FAIL)}$	SM4
	device reaction	turn-off all channels	SF2
		FSB pin = 0 V; UV bit raised in STATR register; if retry is enabled when $V_{PWR} > V_{PWR(UV)}$ (or if device is in fail-safe mode) the on/off of the outputs is kept in logic and outputs are restarted	FG8
	MCU reaction	integrator to decide action	
	reset conditions	undervoltage condition disappeared, then UV bit is cleared upon a reading of STATR register	

6.1.5 Overvoltage (OV) with $V_{DD} > V_{DD(FAIL)}$ and OV_DIS = 0 (by default)

Table 11. Overvoltage detection in fail mode

Overvoltage detection	description of safety mechanism	on V_{PWR}, voltage is over the specified range: $V_{PWR} > V_{PWR(OV)}$ with $V_{DD} > V_{DD(FAIL)}$ and OV_DIS = 0 (by default)	SM5
	device reaction	turn-off all channels as long as $V_{PWR} > V_{PWR(OV)}$	SF2
		FSB pin = 0 V	FG7
	MCU reaction	integrator to decide action	
	reset conditions	overvoltage condition disappeared and read of STATR register; the restart of the outputs is done automatically	

6.1.6 Overtemperature (OT)

Table 12. Overtemperature detection

Overtemperature detection	description of safety mechanism	for each channel, detection of temperature is over 175 °C (typ)	SM6
	device reaction	if faulty channel is on, channel is turned off; if channels are off and $T_j > T_{sd}$ there is no way to turn on; FSB pin = 0 V	SF1
		OT bit raised in STATR register of faulty channel; if faulty channel was on before the event, it restarts when $T_j < T_{sd}$ if retry is enabled (by default) or if device is in fail-safe mode	FG3
	MCU reaction	integrator to decide action	
	reset conditions	after temperature < T_{sd}, de-latch sequence, read STATR register	

6.1.7 V_{DD} out of range with VDD_FAIL_EN = 1

Table 13. V_{DD} out of range detection case 1

V_{DD} out of range detection case 1	description of safety mechanism	monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD(FAIL)}$ and VDD_FAIL_EN = 1 in normal mode	SM7
	device reaction	turn off all channels	SF2
		device goes in fail-safe mode operation and SO data are no longer available	n/a
	MCU reaction	all register contents are reset; integrator to decide action; channels can be turned on by direct input pins	
	reset conditions	none	

6.1.8 V_{DD} out of range with VDD_FAIL_EN = 0

Table 14. V_{DD} out of range detection case 2

V_{DD} out of range detection case 2	description of safety mechanism	monitoring of V_{DD} low voltage threshold with conditions $V_{DD} < V_{DD(FAIL)}$ and VDD_FAIL_EN = 0 in normal mode	SM8
	device reaction	device transit to fail mode after WD window period	none
	MCU reaction	integrator to decide action	
	reset conditions	none	

6.1.9 Loss of communication detection

Table 15. Loss of communication detection

Loss of communication detection	description of safety mechanism	monitoring of the SPI frame integrity through Watchdog	SM9
	device reaction	device is truned into fail-safe mode; channels are turned off; all register contents are reset	SF2
	MCU reaction	possibility to activate outputs with direct inputs INs; integrator to decide action; reload device configuration after wake-up sequence	
	reset conditions	none	

6.2 External fault diagnostics

MC12XS3 family does embed internal diagnostics leading to non-internal reactions on device operations. Those diagnostics are:

- Open load in on mode for incandescent and LED (OLON)
- Open load in off mode (OLOFF)
- External clock fail (CLOCK_FAIL)
- Overtemperature warning (OTW)
- Output shorted to V_{PWR} (OS)
- Direct input state (IN0 to IN3)
- Output current value (CSNS)
- Device temperature value (CSNS)

6.2.1 Open load in on mode (OLON)

Table 16. Open load on detection

Open load on mode detection	description of safety mechanism	on each channel, detection of current below $I_{OLD(ON)}$ or $I_{OLD(ON\_LED)}$ (if LED mode activated) when channel is on	SM10
	device reaction	OLON_s is raised into STATR register	FG6
	MCU reaction	integrator to decide action	
	reset conditions	after fault disappeared, channel status must be read to clear the fault	

6.2.2 Open load in off mode (OLOFF)

Table 17. Open load off detection

Open load off mode detection	description of safety mechanism	on each channel, detection of current below $I_{OLD(OFF)}$ when the channel is off; feature is enabled (by default)	SM11
	device reaction	OLOFF_s is raised into STATR register; FSB pin = 0 V	FG5
	MCU reaction	integrator to decide action	
	reset conditions	after fault disappeared, FAULTR register read for OLOFF bit clearance	

6.2.3 External clock fail (CLOCK_FAIL)

Table 18. Clock fail detection

Clock fail detection	description of safety mechanism	when the external clock is disconnected or out of the f_{CLK} frequency range	SM13
	device reaction	if output channel on bit is set to logic 1, the output is turned on 100 %; if output channel on bit is set to logic 0, the output is kept off; CLK_FAIL bit raised in DIAGR0 register	FG13
	MCU reaction	integrator to decide action	
	reset conditions	after fault disappeared, read DIAGR0 register for CLK_FAIL bit clearance	

6.2.4 Overtemperature warning (OTW)

Table 19. Overtemperature warning detection

Overtemperature warning detection	description of safety mechanism	when the GND flag temperature is over T_{OTWAR}	SM14
	device reaction	OTW raised in DIAGR0 register	FG12
	MCU reaction	integrator to decide action	
	reset conditions	after temperature < T_{OTWAR}; channel status read for bit clearance	

6.2.5 Output channel state

Table 20. Output channel state detection

Output channel state detection	description of safety mechanism	on each channel, detection of channel output state and report into register; allows diagnosis if channel is short#circuited to V_{PWR} when channel is off state	SM15
	device reaction	OS_s bit raised into STATR register	FG4
	MCU reaction	integrator to decide action	
	reset conditions	none	

6.2.6 Input channel state

Table 21. Input channel state detection

Input channel state detection	description of safety mechanism	each device input pin is monitored, its logic state is reported into register	SM16
	device reaction	IN0 to IN3 bit raised in DIAGR1 register	FG14
	MCU reaction	integrator to decide action	
	reset conditions	none	

6.2.7 Output current value

Table 22. Output current value detection

Output current value detection	description of safety mechanism	for each channel, current recopy of output channel current can be multiplexed on CSNS pin	SM17
	device reaction	none	none
	MCU reaction	integrator to decide action	
	reset conditions	none	

6.2.8 Device temperature

Table 23. Device temperature detection

Device temperature detection	description of safety mechanism	control die temperature (not power die temperature) is reported through the CSNS pin	SM18
	device reaction	none	none
	MCU reaction	integrator to decide action	
	reset conditions	none	

6.2.9 Register read

Table 24. Register read description

Register read description	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	

6.3 Detection time and reaction time

The *fault detection time* is the maximum time for detection of a fault or a diagnostic and the reporting of the fault (through SPI and/or on FSB pin). After this timing, the device activates the reaction.

The *fault reaction time* is the maximum time to put the device in a safe configuration with outputs turned off.

6.3.1 Detection and shutdown time along with the different fault types

Figure 5 shows the total maximum time to get the MC12XS3 part into a safe condition after a fault occurs.

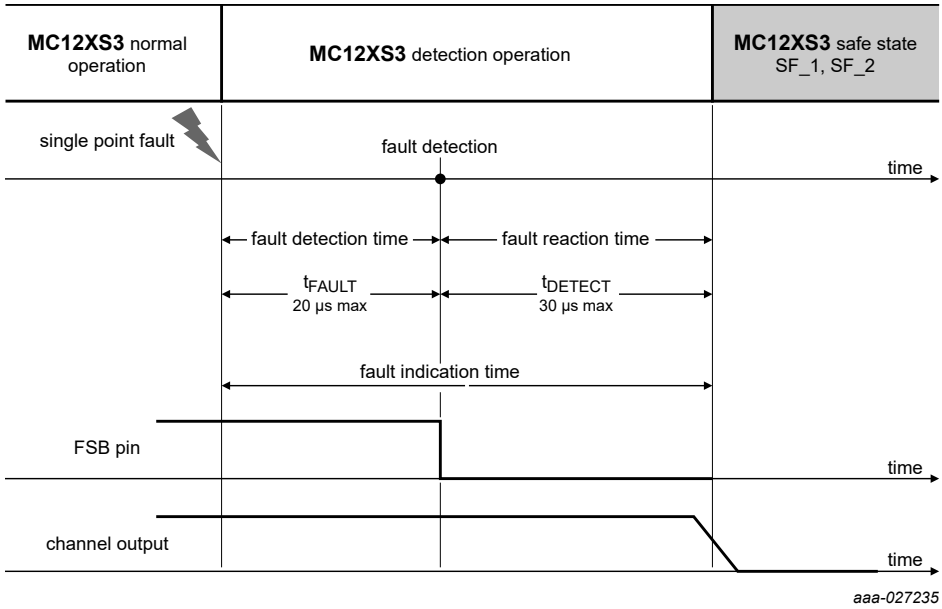

Figure 5. Reaction time to get IC in safe condition after a fault occurs

7 Operation of use and mission profile

The MC12XS3 family is used in application for which the mission profile is described in Table 25. This document is based on this mission profile, although use of MC12XS3 is not limited to these values. Mission profile may slightly differ application to application but the one used is representative of a typical automotive profile.

Table 25. Mission profile

Mission parameters	Mission profile
Junction temperature	−40 °C to +150 °C
Lifetime	15 years
Total operation time (on)	12000 h
Total sleep time (standby)	119400 h

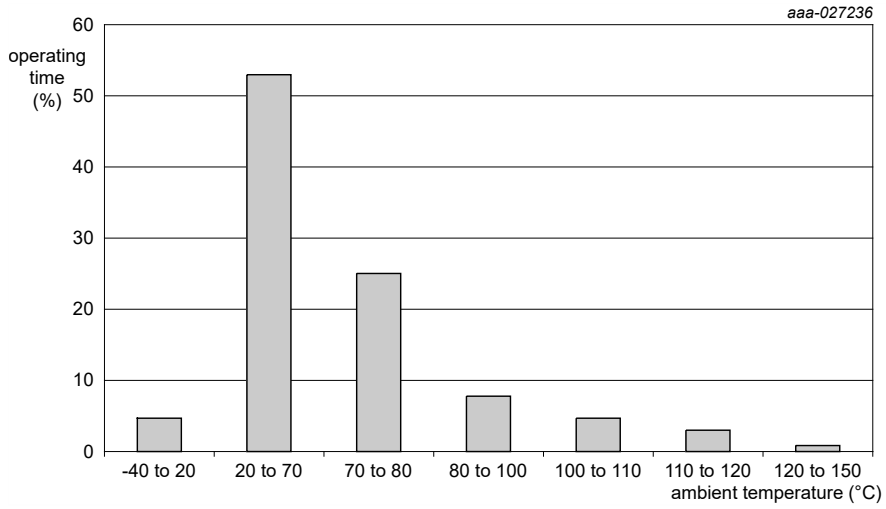

Figure 6. Temperature profile

8 Legal information

8.1 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.

8.2 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.

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.

Suitability for use in automotive applications — This NXP Semiconductors product has been qualified for use in automotive applications. Unless otherwise agreed in writing, the product is 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.

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.

8.3 Trademarks

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

NXP — is a trademark of NXP B.V.

POR — is a trademark of NXP B.V.

SMARTMOS — is a trademark of NXP B.V.

Tables

Tab. 1. Related documents 3
Tab. 2. Pin descriptions 6
Tab. 3. Status register and flags 11
Tab. 4. DIAGR0 register and flags 11
Tab. 5. DIAGR1 register and flags 11
Tab. 6. Summary table of device fault and device diagnostics management 12
Tab. 7. Overcurrent detection 13
Tab. 8. Severe short-circuit detection 13
Tab. 9. Voltage over maximum ratings 14
Tab. 10. Undervoltage detection without VDD(FAIL) 14
Tab. 11. Overvoltage detection in fail mode 14
Tab. 12. Overtemperature detection 15
Tab. 13. VDD out of range detection case 1 15
Tab. 14. VDD out of range detection case 2 15
Tab. 15. Loss of communication detection 16
Tab. 16. Open load on detection 16
Tab. 17. Open load off detection 16
Tab. 18. Clock fail detection 17
Tab. 19. Overtemperature warning detection 17
Tab. 20. Output channel state detection 17
Tab. 21. Input channel state detection 17
Tab. 22. Output current value detection 18
Tab. 23. Device temperature detection 18
Tab. 24. Register read description 18
Tab. 25. Mission profile 19

Figures

Fig. 1. Generic safety system architecture example 5
Fig. 2. Example of an application with external components 7
Fig. 3. Internal block diagram 9
Fig. 4. Safety states 10
Fig. 5. Reaction time to get IC in safe condition after a fault occurs 19
Fig. 6. Temperature profile 20

Contents

1 Introduction 3
1.1 Related documents 3
1.2 Vocabulary 4
2 General information 4
2.1 Assumed conditions of operation 4
2.2 Safety function 4
2.3 Safety goals 5
3 Assumptions of use 5
3.1 Targeted applications 6
3.2 Main functions of the MC12XS3 family 7
4 Safety states 10
5 Flags mapping relevant for diagnosis and faults 11
6 Device fault and device diagnostics management 11
6.1 Internal device faults detection 12
6.1.1 Overcurrent 13
6.1.2 Severe short-circuit (SC) 13
6.1.3 Voltage over maximum ratings 14
6.1.4 Undervoltage (UV) with VDD > VDD(FAIL) 14
6.1.5 Overvoltage (OV) with VDD > VDD(FAIL) and OV_DIS = 0 (by default) 14
6.1.6 Overtemperature (OT) 15
6.1.7 VDD out of range with VDD_FAIL_EN = 1 15
6.1.8 VDD out of range with VDD_FAIL_EN = 0 15
6.1.9 Loss of communication detection 16
6.2 External fault diagnostics 16
6.2.1 Open load in on mode (OLON) 16
6.2.2 Open load in off mode (OLOFF) 16
6.2.3 External clock fail (CLOCK_FAIL) 17
6.2.4 Overtemperature warning (OTW) 17
6.2.5 Output channel state 17
6.2.6 Input channel state 17
6.2.7 Output current value 18
6.2.8 Device temperature 18
6.2.9 Register read 18
6.3 Detection time and reaction time 18
6.3.1 Detection and shutdown time along with the different fault types 19
7 Operation of use and mission profile 19
8 Legal information 21

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

Date of release: 21 January 2019
Document identifier: AN11936