![TDK InvenSense]

IAM-20685 Safety Manual

Automotive 6-axis MotionTracking® MEMS Device for ADAS and Autonomous Driving Applications

SCOPE

This Safety Manual describes how functional safety (ISO-26262) is achieved on IAM-20685, providing the necessary information to enable its integration when used in systems designed under ISO-26262.

This manual is intended be used in conjunction with datasheet DS-000182.

PRODUCT OVERVIEW

The IAM-20685 is a 6-axis MotionTracking device that combines a 3-axis gyroscope and a 3-axis accelerometer in a small 4.5x4.5x1.1 mm (24-pin DQFN).

The IAM-20685 features:

- Gyroscope full scale range up to ±1966 dps with accuracy guaranteed up to ±300 dps
- Accelerometer with programmable full-scale range from ±2g to ±65g with accuracy guaranteed up to ±36g
- Two temperature sensors
- 10 MHz Serial Peripheral Interface (SPI)
- ISO-26262 ASIL-B
- Automotive-qualified
- Reliability testing performed according to Automotive Electronics Council AEC – Q100 grade 2 (-40°C to 105°C) qualification

IAM-20685 includes on-chip 16-bit ADCs, programmable digital filters, and embedded temperature sensors. The device features an operating voltage range from 5.5V down to 3.0V.

ORDERING INFORMATION

PART NUMBER	TEMPERATURE	PACKAGE	MSL*
IAM-20685†	−40°C to +105°C	24-Pin DQFN	3

†Denotes RoHS and Green-compliant package

* Moisture sensitivity level of the package

APPLICATIONS

- Navigation
- Telematics
- Autonomous Driving
- ADAS
- Dead Reckoning

TYPICAL OPERATING CIRCUIT

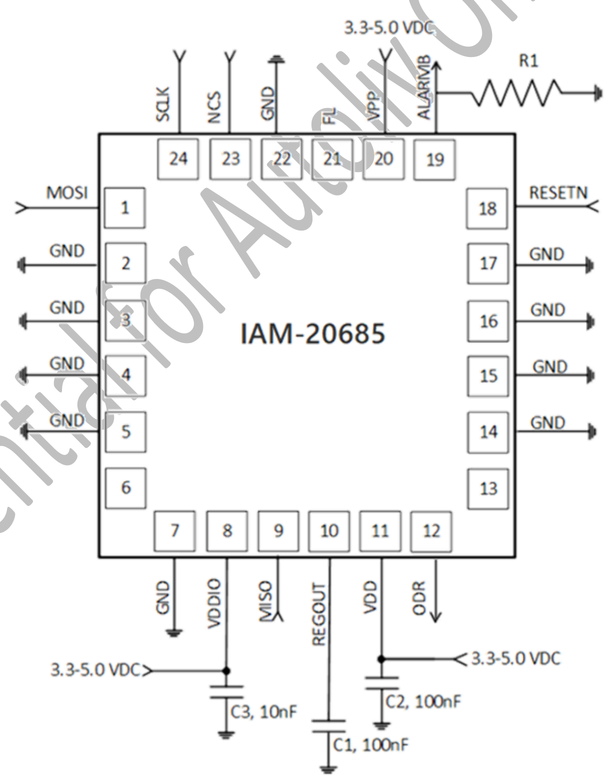

TABLE OF CONTENTS

1 Introduction 4

1.1 Purpose and Scope 4

1.2 Product Overview 4

1.3 Applications 4

1.4 Features 4

2 Features 5

2.1 Gyroscope Features 5

2.2 Accelerometer Features 5

2.3 Additional Features 5

2.4 PINOUT AND Typical Operating Circuit 6

2.5 Block Diagram 7

3 SAFETY CONCEPT 8

3.1 Functional Safety REquirements 8

3.2 embedded safety mechanisms 9

3.3 fault handling and safe state 10

3.4 Functional safety requirements VS MAIN BLOCKS 11

3.5 Functional safety requirements VS safety mechanisms 12

3.6 safety mechanisms VS MAIN BLOCKS 13

4 ASSUMPTION OF USE 15

4.1 REQUIRED EXTERNAL COMPONENTS 15

4.2 USAGE CONSTRAINTS 15

4.3 KNOWN LIMITATIONS 15

4.4 TASKS IN CHARGE OF HOST SYSTEMS (SM101) 16

5 ISO-26262 METRICS 17

6 Document Information 18

6.1 Revision History 18

Table of Abbreviations

ABBREVIATION	MEANING
ADC	Analog to Digital Converter
MEMS	Micro Electro-Mechanical System
SPI	Serial Peripheral Interface
MISO	Master Input Slave Output (SPI)
MOSI	Master Output Slave Input (SPI)
ASIL	Automotive Safety Integrity Level
SEooC	Safety Element out of Context
SM	Safety Mechanism
FSR	Functional Safety Requirement
TSR	Technical Safety Requirement
CRC	Cyclic Redundancy Check
FIT	Failure In Time (1 FIT corresponds to 1 random failure every 1e9 hours)
SPF	Single Point Failure
LF	Latent Failure
MPF,L	Multi Point Failure, Latent
MPF,DP	Multi Point Failure, Detected
DPLF	Digital Low Pass Filter

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document is a safety manual, providing information on how functional safety is achieved according to ISO-26262.

This manual is intended to be used in conjunction with datasheet DS-000182, providing the additional necessary details to integrate IAM-20685 in systems under ISO-26262.

1.2 PRODUCT OVERVIEW

The IAM-20685 is a 6-axis MotionTracking device that combines a 3-axis gyroscope and a 3-axis accelerometer in a small 4.5x4.5x1.1 mm (24-pin QFN) package. The IAM-20685, with its 6-axis integration, enables manufacturers to eliminate the costly and complex selection, qualification, and system level integration of discrete devices, guaranteeing optimal motion performance.

1.3 APPLICATIONS

- Autonomous Driving
- Advanced Driver Assistance Systems (ADAS)
- Navigation
- Telematics
- Dead Reckoning

1.4 FEATURES

- Low accelerometer and gyroscope offset
- On-Chip 16-bit ADCs and Programmable Filters
- Digital-output temperature sensors
- VDD operating range of 3.0 V to 5.5 V
- MEMS structure hermetically sealed and bonded at wafer level
- RoHS and Green compliant
- Automotive-qualified
- Reliability testing performed according to AEC-Q100 grade 2
- ISO-26262 ASIL level B

2 FEATURES

2.1 GYROSCOPE FEATURES

- Digital-output X-, Y-, and Z-axis angular rate sensors (gyroscopes) with a programmable full-scale range from ±41 dps to ±1966 dps and integrated 16-bit ADCs
- Digitally programmable low-pass filter
- Factory calibrated sensitivity scale factor
- Self-test

2.2 ACCELEROMETER FEATURES

- Digital-output X-, Y-, and Z-axis accelerometer with a programmable full-scale range from ±2*g* to ±65*g* and integrated 16-bit ADCs
- Self-test

2.3 ADDITIONAL FEATURES

- Smallest and thinnest package in the industry: 24-pin DQFN 4.5x4.5x1.1 mm
- Minimal cross-axis sensitivity between the accelerometer and gyroscope axes
- Digital-output temperature sensor
- User-programmable digital filters for gyroscope and accelerometer
- 10,000*g* shock tolerant
- 10 MHz SPI interface for communicating with all registers
- MEMS structure hermetically sealed and bonded at wafer level

2.4 PINOUT AND TYPICAL OPERATING CIRCUIT

PIN NUMBER	PIN NAME	PIN DESCRIPTION
1	MOSI	Connect to host SPI MOSI pin
7	GND	Ground pin
8	VDDIO	VDDIO rail (3.3V or 5V)
9	MISO	Connect to host SPI MISO pin
10	REGOUT	Connect to ground through a 100 nF capacitor
11	VDD	Connect to 5V or 3.3V supply voltage and decouple with a 100 nF capacitor
12	ODR	Output Data-ready for synchronous sensor data readings (optional), leave floating when not used
18	RESETN	Connect to host reset signal (active low) or to VDDIO
19	ALARMB	Connect to host alarm monitoring pin
20	VPP	Connect to VDDIO
23	NCS	Connect to host CS pin
24	SCLK	Connect to host SPI SCLK pin
6, 13, 21	FL	Leave floating
2, 3, 4, 5, 14, 15, 16, 17, 22	GND	Connect to ground

Table 1. Pin Descriptions

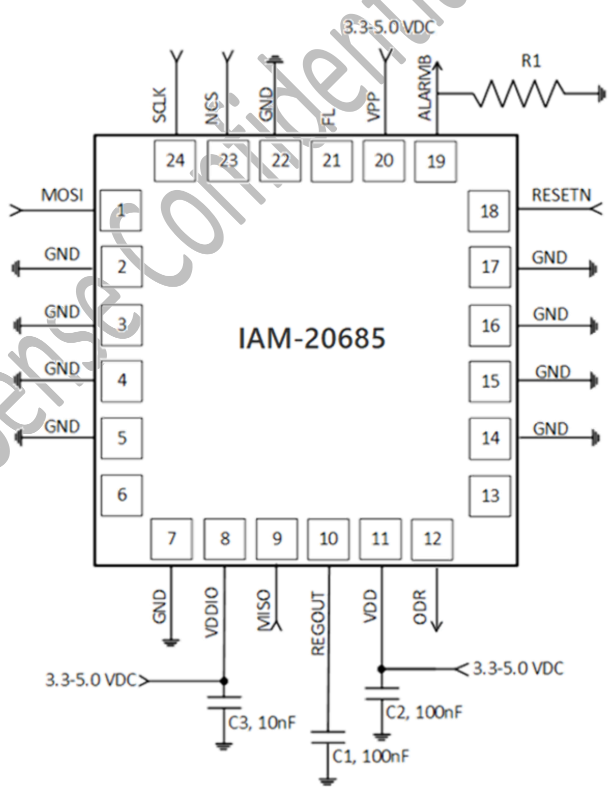

Figure 1. Application Schematic

2.5 BLOCK DIAGRAM

Main functional blocks are shown in the following diagram:

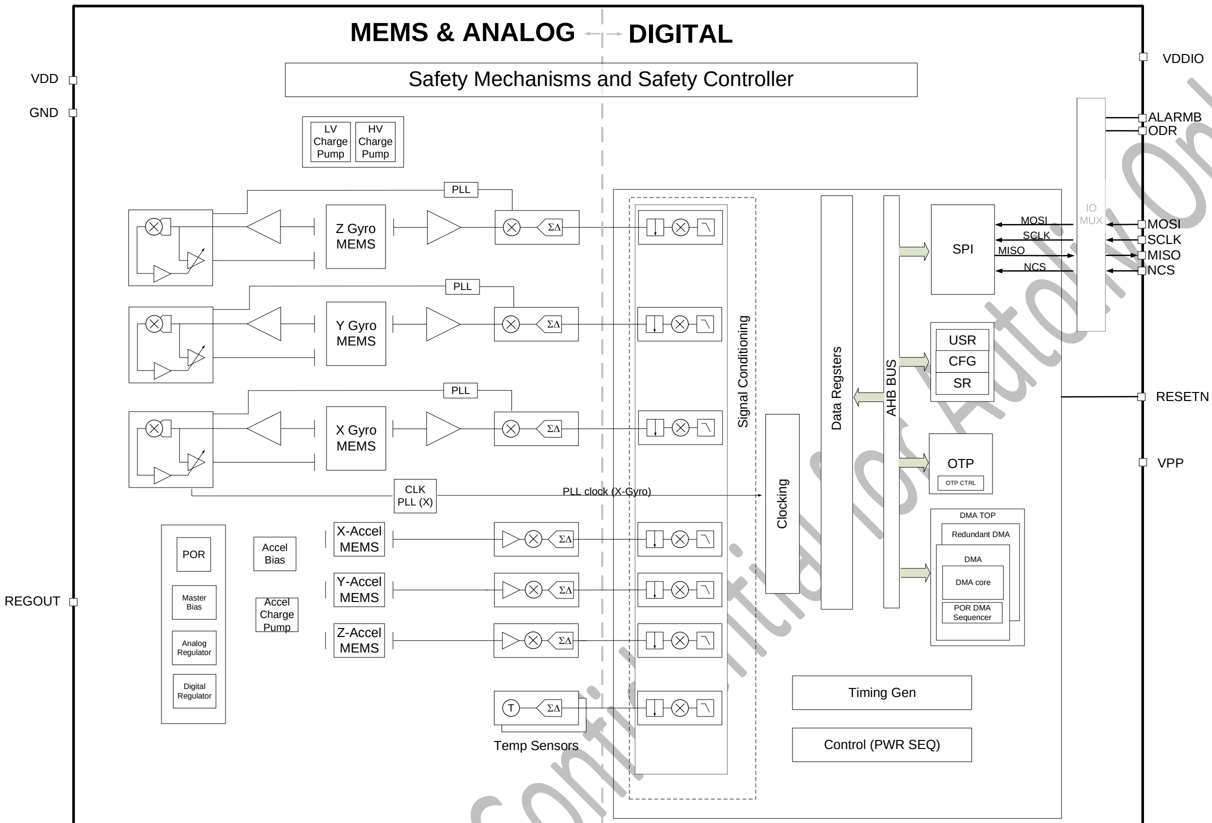

Figure 2. IAM-20685 Block Diagram

3 SAFETY CONCEPT

3.1 TECHNICAL SAFETY REQUIREMENTS

The IAM-20685 has been developed according to ISO-26262:2011 targeting the automotive safety integrity level ASIL-B.

IAM-20685 shall be considered as a Safety Element out of Context (SEooC) based on the following Functional Safety Requirements:

TECHNICAL SAFETY REQUIREMENT	DESCRIPTION	ASIL	MIN FAULT TOLERANT TIME
TSR-101	It is required to detect the Gyro output failures which could lead to a Full Scale Measurement Range of less than ±300 °/s.	B	10ms
TSR-102	It is required to detect the Gyro output failures which could lead to a Total Sensitivity error of more than ±5%.	B	10ms
TSR-103	It is required to detect thel Gyro output failures which could lead to a Total Offset error of more than ±3°/s.	B	10ms
TSR-104	It is required to detect the Gyro output failures which could lead to a Sensitivity Nonlinearity Error of more than 1 % FSO (Full Scale Output).	B	10ms
TSR-105	It is required to detect the Gyro output failures which could lead to a self test response of more than 150 °/s.	B	10ms
TSR-106	It is required to detect the Gyro output failures which could lead to a self test response of less than 75 °/s.	B	10ms
TSR-110	It is required to detect the failures which could lead to Gyro fixed value, as well as absence of signal (no-signal through SPI).	B	10ms
TSR-201	It is required to detect the Acc output failures which could lead to a Full Scale Measurement Range of less than ±7.4 g.	B	10ms
TSR-202	It is required to detect the Acc output failures which could lead to a Total Sensitivity error of more than ±4%.	B	10ms
TSR-203	To detect the Acc output failures which could lead to a Total Offset error of more than ±0.1G.	B	10ms
TSR-204	It is required to detect the Acc output failures which could lead to a Sensitivity Nonlinearity Error of more than ±2 % FSO (Full Scale Output).	B	10ms
TSR-205	It is required to detect the Acc output failures which could lead to to a self test response of more than 50% of TSR. (Self test response should be meet in range of 25-50% of total TSR).	B	10ms
TSR-206	It is required to detect the Acc output failures which could lead to to a self test response of less than 25% of TSR. (Self test response should be meet in range of 25-50% of total TSR).	B	10ms

TSR-209	It is required to detect the failures which could lead to Acc fixed value (stuck to any value), as well as absence of signal (no-signal through SPI).	B	10ms
TSR-403	It is required to detect SPI communication error.	B	0.75ms
TSR-701	To detect failure causing more than 20ms group delay (e.g. filter).	B	10ms

Table 2. List of Technical Safety Requirements

Min Fault Tolerant Time is an indication for the application, meaning that at system level Fault Tolerant Time shall be greater than what is indicated in the table above.

3.2 EMBEDDED SAFETY MECHANISMS

Random fault detection over lifetime is achieved by a set of safety mechanisms (SMs) executed either in at startup, upon command, or in a continuous manner. The typical handling time (detection+signaling) is <=0.75 ms.

The safety mechanisms are listed in Table .

SM #	SM NAME	TYPE	HW/SW	FAULT HANDLING TIME DETECTION + SIGNALING
3	SM03 – Clocks Check	Continuous	Sensor Hardware	<0.75ms
4	SM04 – Gyroscopes Quadrature Check	Continuous	Sensor Hardware	<10ms
7	SM07 – Gyroscopes Drive Signal Integrity Check	Continuous	Sensor Hardware	<0.75ms
8	SM08 – Temperature Check	Continuous	Sensor Hardware	<0.75ms
9	SM09 – Reset Check	Continuous	Sensor Hardware	<0.75ms
10	SM10 – Master Regulator Check	Continuous	Sensor Hardware	<0.75ms
11	SM11 – Analog VDD Regulator Check	Continuous	Sensor Hardware	<0.75ms
12	SM12 – Digital VDD Regulator Check	Continuous	Sensor Hardware	<0.75ms
13	SM13 – External Regulators Check	Continuous	Sensor Hardware	<0.75ms
14	SM14 – Voltage References Check	Continuous	Sensor Hardware	<0.75ms
16	SM16 – Accelerometers Self Test	Startup + On Demand	Sensor Hardware	<10ms
17	SM17 – Shield Voltage Reference Check	Continuous	Sensor Hardware	<0.75ms
18	SM18 – Accelerometer Drive Voltage Check	Continuous	Sensor Hardware	<0.75ms
22	SM22 – Data Integrity Check	Continuous	Sensor Hardware	<0.75ms
26	SM26 – Correct Register Loading From OTP Check	Startup	Sensor Hardware	<0.75ms
29	SM29 – AHB Matrix Check	Startup	Sensor Hardware	<0.75ms
30	SM30 – SPI Integrity Check	Continuous	Sensor Hardware	<0.75ms
33	SM33 – Continuous Register Check	Continuous	Sensor Hardware	<0.75ms
34	SM34 – Bandgaps Check	Continuous	Sensor Hardware	<0.75ms
36	SM36 – Gyroscope DC Self Test	Startup + On Demand	Sensor Hardware	<40ms
101	SM101 – Host SPI Check	Continuous	Host Software	<10ms

Table 3. List of Safety Mechanisms

Most of the Safety Mechanisms operate indirectly, working on the causes potentially jeopardizing the specific Functional Safety Requirement. Some others operate more directly on the parameter addressed in the specific Functional Safety Requirement.

Each safety mechanism can trigger one or more alarms. An alarm is a bit in the register space. Each alarm will in turn trigger the pin ALARMB, unless it is masked by its corresponding mask bit. The pin ALARMB can also be masked by using msk_alarmpin. Many alarms can be latched by their corresponding latch enable bits. When an alarm is latched, the corresponding alarm register will clear only when read, even if the alarm signal ceases to be active.

Some safety mechanisms run continuoulsy, while others run only at startup and/or upon command by the host. “Host SPI Check” is executed by the host micro-controller. Safety mechanisms can be enabled and disabled by their corresponding enable bits.

Please note that when enabling/disabling and masking/unmasking safety mechanisms, before writing a bit into the enable and mask registers, to preserve the chip configuration, the register must be read and only the desired bits must be changed, while all other bits must be left at the existing value.

SM101 provides the coverage for what can’t be diagnosed internally by IAM-20685, requiring the active role of the external host system (refer to 4.4).

Further details of Safety Mechanisms are described within datasheet DS-000182.

3.3 FAULT HANDLING AND SAFE STATE

Safe State for this Sensor is defined as the signalling of internal issues (Single Point Faults or Latent Faults) by means of three channels:

1. Sensor - Internal registers accessible through SPI
2. Sensor - ALARMB pin activation (alarm on low level)
3. Host - System capability to detect malfunctions, refer to SM101

Safe State is achieved when the first one of these 3 channels detects and communicates a functional safety issue.
Note that in case of intermittent alarm activation the sensor can transit back from the safe state, meaning the alarm signal is de-asserted.
Intermittent alarms are expected to be driven by analogue safety mechanisms, when the root cause is not steadily above threshold. Basic assumption is that real sensor issues are expected to be present with monitored parameters steadily above thresholds, causing stable alarms. While intermittent alarms are typically caused by external causes like power supply drops or EMC, or environmental conditions out of specs.
In any case, as long as alarm condition persists sensor data shall not be considered valid.

Summarizing, alarms are confirmed when:

- ALARMB=Low confirmed by internal alarm registers
- ALARMB is steadily inconsistent respect to internal alarm registers

Most of Safety Mechanisms operate indirectly respect to Safety Requirements, monitoring key parameters influencing Safety Requirements. Alarms might be conservatively signalled even when safety requirements are not yet violated but monitored parameters are out of specs.

3.4 FUNCTIONAL SAFETY REQUIREMENTS VS MAIN BLOCKS

The following table shows whether each functional block / pin may influence Functional Safety Requirements.

	TSR-101	TSR-102	TSR-103	TSR-104	TSR-105	TSR-106	TSR-110	TSR-201	TSR-202	TSR-203	TSR-204	TSR-205	TSR-206	TSR-209	TSR-403	TSR-701
DriveBlock	X	X	X	X	X	X	X								X	X
DriveSenseBlock	X	X	X	X	X	X	X								X	X
CoriolisSenseBlock	X	X	X	X	X	X	X								X	X
XY-AccelReadOut								X	X	X	X	X	X	X	X	
Z-AccelReadOut								X	X	X	X	X	X	X	X	
Accel Bias								X	X	X	X		X	X	X	
Accel CP								X	X	X	X	X	X	X	X	
DemodADC	X	X	X	X	X	X	X								X	X
PLL (Y-Z)	X	X	X	X	X	X	X								X	X
CP25V5V	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Bias	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Areg+Dreg	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Master Reg	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Temp1 (Main)	X	X	X		X	X		X	X	X		X	X			X
POR	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RC Oscillator1 (Main)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
MOSI/TDI	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
VSS	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
VDDIO	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
MISO/TDO	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
REGOUT	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
VDD	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
RESETN	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
TP0/TSRT/ALARMB	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DVDDSCAN	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
NCS/TCK	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
SCK/SCN_CK	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
AccelDEC								X	X	X	X	X	X	X	X	
AccelGOS								X	X	X	X	X	X	X	X	
AccelDLPF+FS								X	X	X	X			X	X	
GyroDEC	X	X	X	X	X	X	X								X	X
GyroGOS	X	X	X	X	X	X	X								X	X
GyroDLPF+FS	X	X	X	X			X								X	X
Clock/Power Management Unit	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Registers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
OtpTop	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
AHB BUS Matrix	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SPI	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DMA	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
MEMS Accel	X	X	X		X	X		X	X	X	X	X	X	X	X	X
MEMS Gyro	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PLL (X)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Quad/DriveRatio Demod			X	X												
Package		X	X		X	X		X	X	X	X	X	X	X	X	

3.5 FUNCTIONAL SAFETY REQUIREMENTS VS SAFETY MECHANISMS

The following table shows whether each Safety Mechanis covers main functional blocks / pins, for the considered failure modes. Only Safety Mechanisms considered for ISO-26262 metrics are shown in this table.

	TSR-101	TSR-102	TSR-103	TSR-104	TSR-105	TSR-106	TSR-110	TSR-201	TSR-202	TSR-203	TSR-204	TSR-205	TSR-206	TSR-209	TSR-701
SM3	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM4	X	X	X	X	X	X	X								X
SM7	X	X	X			X	X								
SM8	X	X	X		X	X		X	X	X		X	X		
SM9	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
SM10	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM12	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM13	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
SM14	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM17	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM18								X	X	X			X	X	
SM22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM26	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM30	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
SM33	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM34	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SM101	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Safety Mechanisms SM16/SM29/SM36 are not considered effective for ISO-26262 metrics because they are executed at start-up only, therefore they do not respect fault tolerant time of technical safety requirements.

3.6 SAFETY MECHANISMS VS MAIN BLOCKS

The following table shows whether each Safety Mechanis covers main functional blocks / pins, for the considered failure modes.

	SM3	SM4	SM7	SM8	SM9	SM10	SM11	SM12	SM13	SM14	SM16	SM17	SM18	SM22	SM26	SM29	SM30	SM33	SM34	SM36	SM101
DriveBlock	X	X	X																	X	
DriveSenseBlock	X	X	X							X											
CoriolisSenseBlock		X																			
XY-AccelReadOut											X		X								X
Z-AccelReadOut											X		X								X
Accel Bias												X									
Accel CP													X								
DemodADC																				X	X
PLL (Y-Z)	X	X																		X	
CP25V5V	X	X																		X	
Bias										X		X							X		
Areg+Dreg							X	X													X
Master Reg					X	X															
Temp1 (Main)				X																	
POR					X			X													X
RC Oscillator1 (Main)	X																				
MOSI/TDI																	X				
TP3/ASIC																					X
VSS																					X
VDDIO									X												X
MISO/TDO																					X
REGOUT							X														X
VDD							X		X												X
TP1/TMS																					X
TP2/GSIC																					X
RESETN																					X
TP0/TSRT/ALARMB																					X
VPP																					X
DVDDSCAN								X													X
NCS/TCK																					X
SCK/SCN_CK																	X				
AccelDEC											X										
AccelGOS											X										
AccelDLPF+FS											X										
GyroDEC																				X	

GyroGOS																				X	
GyroDLPF+FS																				X	
Clock/Power Management Unit	X										X										
Registers														X				X			
OtpTop															X						
AHB BUS Matrix															X						X
SPI																	X				X
DMA															X						
MEMS Accel		X									X										
MEMS Gyro	X	X																		X	
PLL (X)	X																				
Quad/DriveRatio Demod		X							X												
Package		X																			

4 ASSUMPTION OF USE

Functional Safety performances decribed in this manual can be achieved provided that also the following instructions in this chapter are followed.

4.1 REQUIRED EXTERNAL COMPONENTS

COMPONENT	LABEL	SPECIFICATION	QUANTITY
REGOUT Capacitor	C1	X7R, 100 nF ±10%	1
VDD Bypass Capacitors	C2	X7R, 100 nF ±10%	1
VDDIO Bypass Capacitor	C3	X7R, 10 nF ±10%	1
ALARMB Pull-down Resistor	R1	47 kΩ ± 10%	1

Table 4. Required external components

4.2 USAGE CONSTRAINTS

Functional safety performances are guarateed provided that all the indications provided within datasheet DS-000182 are followed.

4.3 KNOWN LIMITATIONS

1. Gyro is particularly sensitive to vibrations in some ranges, see “Table 1. Gyroscope Specifications” in DS-000182 (20-036, 02-037, 02-038). No Alarm is guaranteed in those ranges.

4.4 TASKS IN CHARGE OF HOST SYSTEMS (SM101)

The Host System has an active role to fully achieve Functional Safety; it's expected to implement the following tasks:

1. In order to check potential stuck-at-1/0 on ALARMB, the host shall verify that the intended start-up sequence on ALARMB is correctly executed:
   - Rising Edge at T=0 (some hundreds of us after power-on, depending on power-up ramp)
   - Falling Edge at T=10.8ms (10.3ms-11.3ms)
   - Rising Edge at T=79.4ms (75.6ms-83.2ms)

   Any deviation from that sequence of edges means an issue is present, to be considered as an Alarm.
2. Recommended error injection at start-up by Host by transmitting with wrong CRC first, and with wrong Clock Count after and checking SM30 alarm.
3. The host processor shall check the consistency between the non-masked alarm registers and the ALARMB pin and the correctness of the received CRC values. Any SPI reply with RS=11 corresponds to an internal error, like wrong CRC or wrong Clock cycles. To guarantee proper access to registers, the following actions are recommended:
   - every 500us the content of one known register shall be checked (e.g. fixed value [15:0], bank 0, offset 0x0B, "0xAA55")
   - after each write operation the written register shall be read back for check
4. In order to cover the unexpected activation of commanded safety mechanisms, the host shall periodically read the safety mechanisms manual trigger bits.
5. In order to check for accelerometer saturation (should no other alarms be active), the host shall execute SM16 commanded self-test, to check whether an axis is stuck or not.
6. SM16 is start-up / commanded self-test sensitive to Vibrations. In order to avoid false alarms during its execution the host shall make sure no vibrations above 0.6g-pk are present (limit based on tests on 6 samples).
7. Every time alarm registers are checked by the host, it's suggested to check also reg_eccdone_warn, otp_eccdone_warn, ahb_eccdone_warn (SM22). Those registers are set when a single error is corrected by ECC (Error Correction Code). A single error is automatically corrected, and it does not represent a dangerous fault (e.g. bit flip due to radiations). The double error is detected; thus, the relevant alarm register is set and ALARMB pin is asserted.
8. The last 30 Gyro/Accel samples shall be compared. 30 consecutive identical values represent an anomaly causing an alarm.
9. In case TP1 pin is configured as ODR clock, then the host shall check the period of the signal considering it acceptable when it is 125us±10%.
10. In order to minimize the delay between internal issue signaling on alarm registers and the relevant SPI reading, the host should read internal alarm registers with a refresh rate compatible with required TSR fault tolerant time.
11. **Register_Write_Lock** bit (BANK0 Addr=0x16 bit 19) shall be set as last action of sensor initialization, after start-up. As consequence of this action register bank switch is no more effective, therefore only BANK 0 is accessible afterwards. That means that Alarms shall be checked by reading registers:
    - SUMMARY STATUS Addr 0Eh (i_s_ok_c , i_s_ok_a , i_s_ok_r)
    - GYRO_ST_STATUS_1 Addr 10h
    - GYRO_ST_STATUS_2 Addr 11h
    - ACCEL_ST_STATUS_1 Addr 12h
    - ACCEL_ST_STATUS_2 Addr 13h
    - COMMON_ST_STATUS_1 Addr 14h
    - COMMON_ST_STATUS_2 Addr 15h

5 ISO-26262 METRICS

Based on a Failure Mode Effect and Diagnostic Analysis it was possible to analyze 600+ failure modes potentially jeopardizing target Functional Safety Requirements, and the safety mechanisms able to detect them.
Only permanent faults are considered for metric calculations, even if also some transient faults are handled by some safety mechanisms.
Assessment was based on failure rate prediction associated to the following mission profile over 15 years:

Temperature range	Time (%)	Hours	
-40C – 23C	6%	1670	30000h operating
23C – 60C	80%	24000	
60C – 85C	10%	3000	
85C – 90C	4%	1170	
90C – 105C	1%	160	
20C – 35C		101400	non operating

Assessment has been done on the Sensor + the 3 external capacitors:

CMOS die + MEMS die + Package	15.86 FIT
Each external Capacitor (x3)	0.89 FIT (2.68 FIT)
Total	**18.54 FIT**

Calculated ISO-26262 metrics and FIT are reported in the following table:

TechnicalSafety Requirement	ASIL	min Fault Tolerant Time	SPF Metric	LF Metric	Lamda SPF (FIT)	Lamda RF (FIT)	Lamda MPF,L (FIT)	Lamda MPF,DP (FIT)	Lamda Safe (FIT)
TSR-101	B	10ms	94.2%	92.2%	0.38	0.57	1.21	8.72	7.66
TSR-102	B	10ms	93.3%	92.1%	0.50	0.59	1.21	8.74	7.50
TSR-103	B	10ms	91.7%	92.1%	0.77	0.59	1.21	8.75	7.22
TSR-104	B	10ms	94.1%	91.9%	0.42	0.51	1.21	8.46	7.95
TSR-105	B	10ms	96.7%	92.2%	0.20	0.32	1.21	8.19	8.62
TSR-106	B	10ms	94.4%	92.2%	0.33	0.58	1.21	8.74	7.69
TSR-110	B	10ms	94.4%	92.0%	0.33	0.54	1.18	8.68	7.81
TSR-201	B	10ms	94.9%	91.6%	0.63	0.14	1.21	7.80	8.77
TSR-202	B	10ms	94.8%	91.6%	0.66	0.14	1.21	7.80	8.74
TSR-203	B	10ms	92.7%	91.4%	0.97	0.15	1.21	7.82	8.40
TSR-204	B	10ms	96.1%	91.7%	0.46	0.13	1.21	7.76	8.98
TSR-205	B	10ms	95.8%	91.6%	0.52	0.11	1.21	7.77	8.93
TSR-206	B	10ms	94.8%	91.6%	0.63	0.15	1.21	7.81	8.74
TSR-209	B	10ms	95.6%	91.9%	0.52	0.14	1.18	7.78	8.92
TSR-403	B	0.75ms	99.3%	90.4%	0.02	0.07	1.18	7.22	10.05
TSR-701	B	10ms	94.3%	97.7%	0.74	0.23	0.36	1.10	16.12

Table 3. ISO-26262 metrics

6 DOCUMENT INFORMATION

6.1 REVISION HISTORY

REVISION DATE	REVISION	DESCRIPTION
09/27/2019	0.1	First draft release
10/24/2019	1.0	First draft controlled revision
11/26/2019	1.1	• Improved description of Safe State • Fixed typo in SM101
06/25/2020	1.2	• Specified that ISO-26262:2011 is applicable • Revised Fault Tolerant Time to indicate the min allowed Fault Tolerant Time • General revision for SM101 • General revision for all the tables based on assessed safety analysis • Introduced the setting of Register_Write_Lock bit to protect configuration registers from unintentional writings
11/03/2020	1.3	• Figure 2: Changed block diagram • Chapter 5: Added Failure Rate breakdown • Table 4: Fixed failure rates for FSR-201 • Table 4: Updated Lamda Safe failure rates
11/06/2020	1.4	Table 2: Updated SM36, now able to be automatically executed at start-up
03/04/2021	1.5	• Figure 2: added ALARMB pin in block diagram • Reduced SM04 and SM101 fault handling time as consequence of the delay of Digital Low Pass Filter; as consequence also Min Fault Tolerant Time for the affected Technical Safety Requirements are reduced • Renamed Functional Safety Requirements (FSR) to Technical Safety Requirements (TSR) • Updated failure rates and ISO-26262 metrics based on new reliability data
04/08/2021	1.6	Revised failure rates based on a more conservative approach
04/20/2021	1.7	Revised SM101.1 and SM101.8