MTS SENSORS

Temposonics®

Magnetostrictive Linear Position Sensors

SAFETY MANUAL
TH – SIL 2 Capable

The Measurable Difference

Table of contents

1. Introduction

This manual provides to the user electrical installation and operation guidelines for the Temposonics® T-Series models with analog output in safety related applications. The T-Series model is SIL (Safety Integrity Level) 2 certified according to IEC 61508.

IEC 61508	Functional safety of electrical / electronic / programmable electronic safety-related systems

2. Risk analysis

IEC 61508 SIL	$MTTF_d$	High Demand Mode PFH
3	high, 30 < 100 years	$\geq 10^{-8}$ to $< 10^{-7}$
2	med, 10 < 30 years	$\geq 10^{-7}$ to $< 10^{-6}$
1	low, 3 < 10 years	$\geq 10^{-6}$ to $< 10^{-5}$
No special requirements	-x–x-	$\geq 10^{-5}$ to $< 10^{-4}$

Fig. 1: Probability of dangerous failure

3. System design

3.1 Redundant design without internal diagnostic

A redundant design is one in which two sensors, each with an independent output (reverse output operation) are put into place. The validation of the function is performed by a cross-comparison where the correct output of 2 signals of one sensor is defined as:

Z = CH (A) + CH (–B) = 0
with: Z = result of cross comparison
CH (A) = output of position signal
CH (–B) = output of inverted position signal

If this necessary result is not received, the controller interprets a system fault and places the system into the emergency stop.

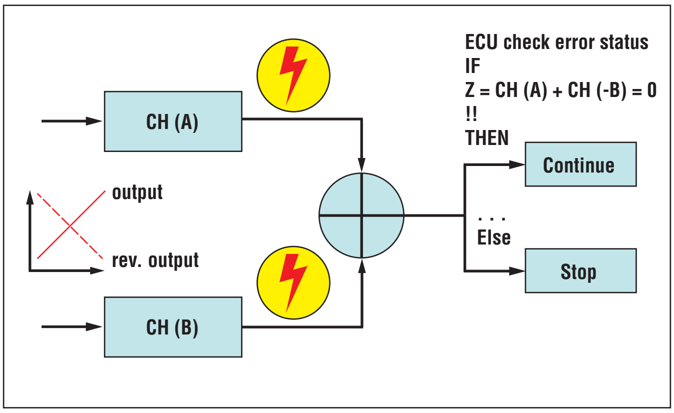

Fig. 2: Redundant design without diagnostic

Without internal diagnostics of the channels, the system is not able to detect which channel has failed. The controller is busy with the comparison algorithm and its processing capacity will be reduced.

3.2 Redundant design with internal diagnostic

Sensors with internal self-diagnostic capability enable a failure message independent from the controller processing loop. The sensor itself will place itself into the fail safe state.

In this case the controller is able to separate the channels and the system can enter into a safe operational mode, where the machine is able to continue performing the function with one channel operation until the failed sensor gets replaced.

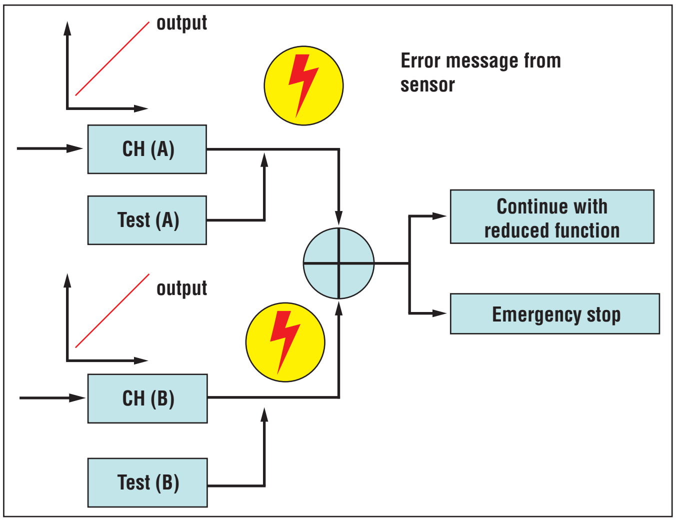

Fig. 3: Redundant design with diagnostic

3.3 The safety function

The T-Series Safety sensor will continuously output a position signal proportional to the magnet position, and the internal diagnostic function will check safety relevant parameters within the hardware.
The sensor will report an output error signal in the event of a failure. The control unit (ECU) receives the provided signals. In the event of a failure the ECU must react in an appropriate manner in order to manage the emergency function. The system will shut off or operate in emergency mode.

T-Series Analog Safety	
Current output	4…20 mA
Error output	< 3.6 mA

Fig. 4: T-Series output function

Failure types

1. Safe Failures (λ_{SD} and λ_{SU}) detected and undetected
2. Dangerous Failures (λ_{DD} and λ_{DU}) detected and undetected
   IEC 60079-14 and local regulations.

Type of failures (λ) within safety related systems		
Fail State	**Detected**	**Undetected**
Fail Safe	λ_{SD} Safe Detected	λ_{SU} Safe Undetected
	The sensor will run without any command from the controller into the safe state.	
Dangerous Fail	λ_{DD} Dangerous Detected: The sensor runs into a dangerous state (= inoperative function)	λ_{DU} Dangerous Undetected: The sensor is not able to run into a safe state.

Fig. 5: Failure types

4. Device specific notes

4.1 Determination and intended use / certification

The T-Series Safety model is a magnetostrictive linear-position sensor certified according to IEC 61508 for single input in low demand mode and high demand mode, SIL 2 safety instrumented systems. The sensor measures the relative position of a travelling magnet relative to its NULL position. The output signal is transmitted to an external controller (ECU) and processed according to its requirements.

4.2 Mechanical and electrical installation

No special or additional sensor installation requirements exist beyond the standard installation practices documented in the actual T-Series operation manual. Environmental operating specifications are applicable as published in the specifications section in the T-Series operation manual (document no. 551513).

4.3 Operating and offline proof tests

For complete information regarding performance, installation, operation, and specifications of T-Series Safety models, refer to our operation manual (document no. 551513). All normal installation recommendations as documented in the operation manual for T-Series analog sensors are applicable. All configurations are allowed for the T-Series Safety models. Functional tests of safety relevant circuits will give a reliable statement about all components in use (sensor, controller and acting device). The user is responsible for applying proof test (check interval is 1 year).

4.4 Maintenance and repair

The T-Series Safety models are not field repairable; device repairs must be performed by MTS. All terminal faults which are not followed by 10 consecutive startups without terminal faults must be reported. In the event of a failure contact MTS Sensors.

4.5 Illegal and safety critical operation modes

All operating modes outside given specifications are not allowed. The specific limits are valid and they shall not be exceeded. Especially the operation manual needs to be considered. No firmware changes are permitted nor authorized. The sensor should be replaced if a storage temperature of 93 °C is ever exceeded. In order to assure the safety values in fig. 7, the sensor should be replaced if the operating temperature exceeds the indicated value.

4.6 Common Cause Failure (CCF)

The following CCF issues have been considered in the design of the T-Series sensor models and can be used in overall system CCF analysis:

1. The sensor is protected against overvoltage, up to max. voltage rating, and miswiring (VDC – GND).
2. The FMEDA is available and the results of the FMEDA were taken into account for CCF analysis.
3. The designers of this sensor have been trained to understand the causes and consequences of common cause failure.
4. The sensor has been tested for: EMC (emission and immunity), mechanical loads (e.g. vibration, pressure), environmental influences like fluid ingress and temperature. The sensor is compatible within these environments and is intended to be used in these conditions provided it remains sealed against contamination from these environments.

4.7 Measures against foreseeable misuse

The measures that have been taken against the foreseeable misuse of the T-Series Safety are:

1. Full protection against miswiring of the sensor.
2. Detailed instructions in the operation manual on methods to prevent damage to the sensor during installation.
3. Checking the function of the sensor after installation will mitigate the possibility of undetected damage to the sensor during the installation process.

4.8 Fault failure action plan

In the event the sensor exhibits a terminal fault response, the sensor must operate without a subsequent terminal fault (i.e. the sensor does not output a current less than 3.6 mA) for 10 consecutive starts following the initial fault response. Otherwise, the sensor must be returned to MTS Sensors for inspection.

4.9 Product identification

The T-Series sensor is offered in numerous configurations that vary in length, flange type, connection type, explosion protection and output. The model number of the sensor includes the character “S” in position 14 to indicate approval for SIL 2. All versions with the “S” option for functional safety are SIL 2 capable.

Example T-Series: TxxxxxxxxxxxxSxxxx

5. T-Series Analog Safety

5.1 Functional description

The T-Series Analog Safety position sensor is classified according to IEC 61508 type B having a hardware fault tolerance of 0. The sensor performs self-diagnostics and enters a fail-safe state upon the detection of a failure, indicating the safety function cannot be performed. For the sensor output to be considered valid, value must be in the range 3.8…20.5 mA for 10 consecutive milliseconds. If the sensor output value ever lies outside of 3.6…21 mA, and therefore in a fault condition, the fault condition shall be considered present until the output is in the valid range for 10 consecutive milliseconds. The active measurement range is 4…20 mA (for the defined stroke of sensor).

Online proof test

The conditions that will trigger a fault are:

- Missing or damaged position magnet
- Invalid checksum of parameter memory
- Invalid checksum of program memory
- Internal hardware failure
- Magnet position is outside the valid measuring range

5.2 Offline proof test-method for checking the safety function

The offline proof test can be applied in order to check the safety function of the sensor.

Within the offline proof test recommended functional tests:

The safety function of the T-Series Safety sensor is internally checked but the diagnostic coverage of the sensor can be increased by checking the function of the sensor externally.

The recommended method for checking the function of a T-Series Analog Safety is:

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Set the T-Series to its zero position.
3. Move the T-Series sensor’s position magnet through its full stroke length to its full-scale position to confirm full range of motion.
4. Return the T-Series to its zero position.
5. Perform a 3 point calibration verification of the T-Series over the full working range.
6. Remove the bypass and restore normal operation.

All applied methods and results of the proof test have to be written in a test report. When the functional test is negative, the device and the system need to be shut down. The process has to be kept in a safe mode due to appropriate actions. Please pay attention to the valid technical literature: operation manual (electrical operation and installation, document no. 551513).

5.3 Safety tolerance

Review the T-Series operation manual (document no. 551513) for the operating accuracy of the sensor. The safety accuracy of the T-Series analog sensor is 1 % of full stroke. An example of the calculations necessary for determining the maximum safe position of the sensor magnet is as follows:

Full stroke: 80 mm
Magnet speed: 100 mm/sec
Worst-case response time: 10 ms

Safety tolerance
= 1 % × 80 mm
= 0.8 mm

Response time tolerance (if moving)
= 100 mm/sec × 10 ms
= 1.0 mm

5.4 Certification and failure rate data

The failure rates are from the FMEDA generated following IEC 61508. The following assumptions are valid:

– The sensor operates in low demand mode and high demand mode.
– Failure rates of external power supplies are not considered.
– Refer to FMEDA-report for mentioned SFF and PFD_{avg} values.
– The T-Series analog sensor will enter a fail-safe state in the event of a failure.
– The controller device needs to interpret the failure signal in the correct manner.
– The ambient conditions follow the specifications out of the valid operation manual (document no. 551513)
– PFD value is calculated assuming a 1-year proof test interval.

Failure rates assume useful lifetime of components are not exceeded. The useful lifetime is defined as an operational time interval where failure rate is relatively constant.

T-Series (SIL 2: Analog Safety)	IEC 61508
Safety level	SIL 2
Device type	B
$MTTF_d$	100 years @ 60 °C; 44 years @ 80 °C
PFD_{avg}	3.49E-04 @ 60 °C; 9.85E-04 @ 80 °C
Diagnostic response time (Fail Detection Time)	25 ms (max) 1 sec for CRC fault detection
% of SIL 2 range for PFD	3.5 % @ 60 °C; 9.9 % @ 80 °C
Hardware fault tolerance (HFT)	0
Useful lifetime	50 years @ 60 °C; 18 years @ 80 °C

Fig. 6: T-Series parameters

Device @ 1 % accuracy	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
T-Series @ 60 °C	0	100	802	62	93.6 %
T-Series @ 80 °C	0	283	2266	175	93.6 %
T-Series @ 85 °C	0	400	3205	248	93.6 %

Fig. 7: Safety values for maximum operating temperature

6. Terms and abbreviations

Term	Specifications
Cat.	Safety category according to EN 954-1
E/E/PE	Electrical / Electronic / Programmable Electronic
FIT	Failure In Time (1×10-9 failures per hour)
FMEDA	Failure Mode, Effects and Diagnostic Analysis (analytical method for determining failure modes and failure rates)
FSM	Functional Safety Management
HFT	Hardware Fault Tolerance, HFT=x where x is the number of faults that the design can tolerate without losing its safety function.
High Demand Mode	High demand or continuous mode is where the frequency of demands for operation made on a safety-related system is greater than one per year.
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
$MTTF_d$	Mean Time to Dangerous Failure
PFD_{avg}	Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of device(s), logic solver(s) and final element(s).
SLC	Safety Lifecycle
Type A component	"Non-Complex" component (using discrete elements); for details see 7.4.4.1.2 of IEC 61508-2
Type B component	"Complex" component (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
V&V	Verification and Validation
Verification	The demonstration for each phase of the life-cycle that the (output) deliverables of the phase meet the objectives and requirements specified by the inputs to the phase. The verification is usually executed by analysis and/or testing.
Validation	The demonstration that the safety-related system(s) or the combination of safety-related system(s) and external risk reduction facilities meet, in all respects, the Safety Integrity Requirements Specification. The validation is usually executed by testing.

Notes

MTS SENSORS

Document Part Number:
551504 Revision A (EU.EN) 01/2015

LOCATIONS

GERMANY
MTS Sensor Technologie GmbH & Co. KG
Auf dem Schüffel 9
58513 Lüdenscheid, Germany
Tel. +49 2351 9587-0
Fax +49 2351 56491
info.de@mtssensors.com
www.mtssensors.com

FRANCE
MTS Systems SAS
Zone EUROPARC Bâtiment EXA 16
16/18, rue Eugène Dupuis
94046 Creteil, France
Tel. +33 1 58 4390-28
Fax +33 1 58 4390-03
info.fr@mtssensors.com
www.mtssensors.com

USA
MTS Systems Corporation Sensors Division
3001 Sheldon Drive
Cary, N.C. 27513, USA
Tel. +1 919 677-0100
Fax +1 919 677-0200
info.us@mtssensors.com
www.mtssensors.com

ITALY
MTS Systems Srl.Sensor Division
Via Diaz,4
25050 Provaglio d'Iseo (BS), Italy
Tel. +39 030 988 3819
Fax +39 030 982 3359
info.it@mtssensors.com
www.mtssensors.com

JAPAN
MTS Sensors Technology Corp.
737 Aihara-machi,
Machida-shi,
Tokyo 194-0211, Japan
Tel. +81 42 775-3838
Fax +81 42 775-5512
info.jp@mtssensors.com
www.mtssensors.com

CHINA
MTS Sensors
Room 504, Huajing Commercial Center,
No. 188, North Qinzhou Road
200233 Shanghai, China
Tel. +86 21 6485 5800
Fax +86 21 6495 6329
info.cn@mtssensors.com
www.mtssensors.com

LEGAL NOTICES

ISO 9001 CERTIFIED

Reg.-No. 003095-QN

SIL 2 Safety Integrity Level IEC 61508

CE