Temposonics
AN AMPHENOL COMPANY

Safety Manual

MH-Series with CAN Safety

Magnetostrictive Linear Position Sensors

Table of Contents

1. Preamble

This document will list all information that will be included in the product's Safety manuals. The Safety manuals will take different forms for example as standalone versions, in-catalogue versions, or product announcement versions. Likewise, printed data sheets will differ from digital formats and languages will vary with geographic markets. All of those changes will be limited to graphical layout, supporting images, contact information etc. The technical data given will always adhere entirely to the content of this document.

2. Intended use of product

The product was designed to be used on off-highway machinery like it is common in construction, agriculture or municipal services. The machines typically feature wheeled or tracked drives, are powered electrically or by ICE, and have an on board DC supply.

The intended use also includes cranes and rolling stock on railroad or comparable urban systems.

The position target shall be a single Temposonics authorized magnet, placed in accordance with the sensor's active region specification and in accordance with the Temposonics guidelines for ferromagnetic material presence.[1]

The supply voltage shall be between 8.0 V and 32.0 V, the ambient temperature between –40 °C and +105 °C.

The CAN interface needs to be connected to a Safety capable control system through a data bus compliant with the CAN 2.0B specification and capable of communication using either the CAN Open protocol DS-304, or the J1939 protocol described in DJ1939-76_201811.

The person using the product to design a system with Safety Functions needs to have adequate knowledge in the field of Functional Safety and Machine Safety, as well as with CAN communication protocols.

This project is the successor to the "MH CAN SIL" sensor denoted by the protocol code "S01". There were no documented incidents during the years of service for that product.

Thus the reason for the new design is to provide compliance with newer standards, to add more mechanical form factors as well as the J1939 based CAN Safety protocol.

The MH variant denoted with the protocol code "S02" can be used in most applications where currently the "S01" design is applied. However, as diagnosis features and Safety Specifications are different, a thorough impact analysis needs to be done first.

1/ For details on those requirements see the respective product datasheet

3. Designators of variants covered by this document

The product comes in two form factors:

- Off-the-shelf offering for short and medium stroke mobile applications (Stroke ≤ 5 m)
- Off-the-shelf offering for FLEXible sensing elements for medium and long strokes (Stroke ≤ 11.5 m)

3.1 Off-the-shelf variant "MH"

This standard product can be configured for different pressure ratings (pipe wall thickness), various connection schemes and CAN factory settings.
The letters in red denote all variants that are covered by this Safety Manual, with the black letters being options that do not affect the Safety

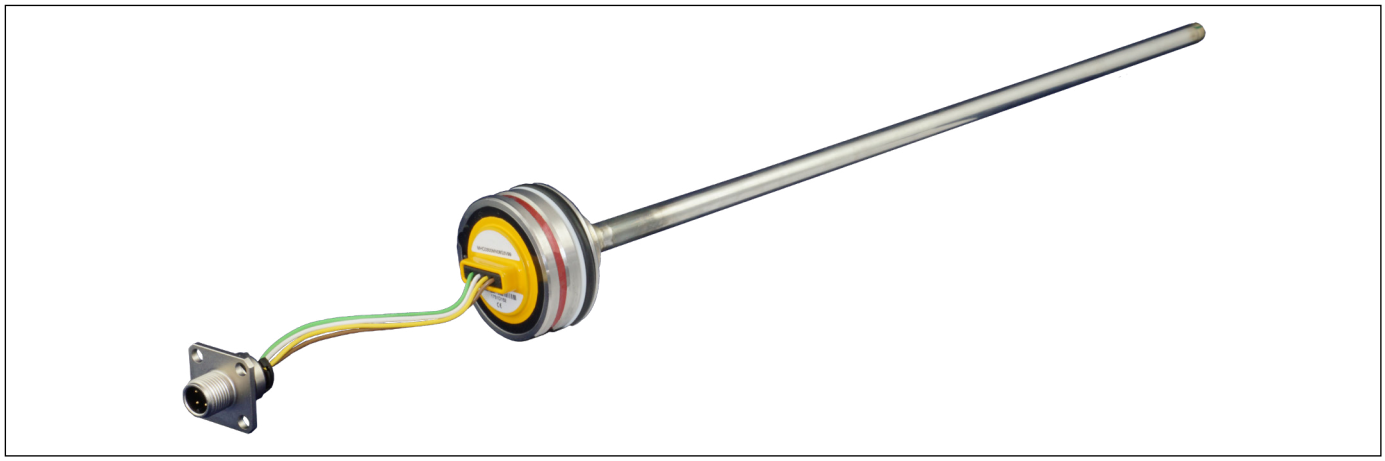

Fig. 1: MH-Series Safety

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Standard MH	M	H	F	L	L	L	L	M	C	C	C	C	3	S	0	2	B	A	A	0	0
	M	H	F	L	L	L	L	M	C	C	C	C	3	J	9	1	B	A	A	0	0

Function:

A = Address in CANBus (preset, that saves customer programming work)
B = Baud rate in CANBus (preset, that saves customer programming work)
C = Connection variations like pigtail length and connector type
F = Form factor
L = Stroke Length
O = Options not otherwise covered, for example "marked with customer's part number"

3.2 Off-the-shelf variant "FLEX MH"

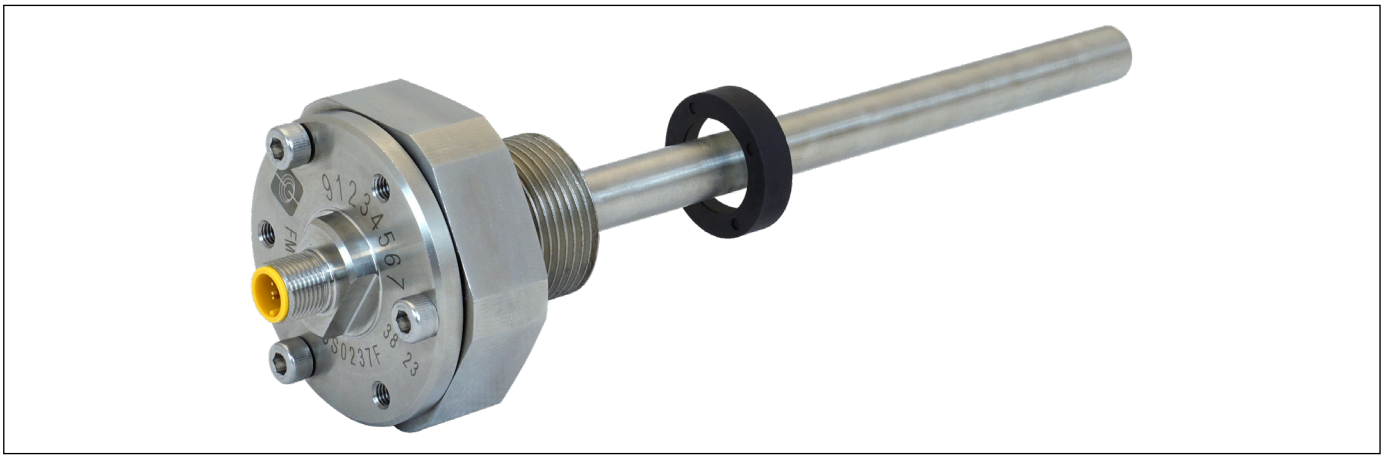

Fig. 2: MH-Series FLEX

This model targets longer stroke lengths. Replacing such sensors 'as a whole' can be cumbersome or outright impossible. Therefore, the MH FLEX allows the customer to separately replace the inner parts: the electronic puck and the core sensing element. Furthermore, the sensing element is FLEXible to aid easy handling.

Model Number Configurator:

FLEX MH style

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	F	M	1	F	F	L	L	L	L	L	M	C	C	C	C	3	S	0	2	B	A	A	U
	F	M	2	F	F	L	L	L	L	L	M	C	C	C	C	3	J	9	1	B	A	A	U

FLEX MH service parts

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	F	M	2	F	F	L	L	L	L	L	M	C	C			
	F	M	2	F	F	M	C	C	3	S	0	2	B	A	A	U
	F	M	2	F	F	M	C	C	3	J	9	1	B	A	A	U

The letters in red denote all variants that are covered by this Safety Manual, with the black letters being options that do not affect the Safety Function:

A = Address in CANbus (preset, that saves customer programming work)
B = Baud rate in CANbus (preset, that saves customer programming work)
C = Connection variations like pigtail length and connector type
F = Form factor
L = Stroke Length
U = Update rate in CANbus (preset, that saves customer programming work)

4. Maintenance and repair

The product does not require any maintenance.
The product cannot be repaired.
Failed units shall be returned to Temposonics for analysis of the root cause.

5. Definition of Safety Function and Safe State

The Safety Function of the product is to provide the position of the magnet with an accuracy better than ε = 17 mm + 1 % Full-Stroke.

It begins with a suitable magnet placed in the specified proximity along the measurement axis and ends with the sensor releasing position information on the CANBus. The core principle is magnetostrictive position sensing.

Safe State is maintained, as long as the sensor does not report a position with an error exceeding the range given above. The time for recognizing a failure and forcing the unit into the Safe State is 10 ms.

If the failure mode does not compromise microcontroller or CANBus hardware, the sensor will continue to communicate, setting the position to "0000" and raising error flags. Otherwise, it will seize to transmit on the CANBus. Similarly, it will recover from some failure modes automatically, require a power up on others and stay in safe mode indefinitely on the most serious failures.

Three layers of signal checking are employed to prevent the most common misuse from creating unsafe states:

- incorrect position magnet type
- incorrect position magnet distance
- interfering magnetic materials

6. Response times and Failure modes

The internal measurement rate depends on the electrical stroke length.
Devices with a stroke length up to 5 m have an internal measurement rate of TM = 2 ms.
Devices with a stroke length above 5 m have an internal measurement rate of TM = 5 ms.
For failures that are linked to the measurement cycle, TM becomes part of the response time.

Most errors are flagged by changing the position value to zero and setting error flags, or by aborting transmitting on the bus altogether.
For those errors, the CAN update period (TU) becomes part of the response time.

The following table lists all error modes with corresponding FIT rates and response times:

Name	Note	Dangerous undetected	FIT rate	Response time
Startup	Components, only needed on startup, failed	**NO**	49.225	N.A. will not start at power up
Don't Care	Component variations that do not harm performance	**NO**	0.040	N.A. continues unaffected
Controller Error	Various errors lead to raising that flag	**NO**	56.164	= TM + TU
No Magnet Error	Various errors lead to raising that flag	**NO**	112.446	= TM + TU
Shut Down 1	Errors flagged by absence of messages	**NO**	840.390	= TU
Shut Down 2	Errors flagged by absence of messages	**NO**	1.900	= 400 ms + TU
Shut Down 3	Errors flagged by absence of messages	**NO**	1070.343	= 1000 ms + TU
Shut Down 4	Errors flagged by absence of messages	**NO**	174.271	= 6000 ms + TU
Dangerous Undetected	Possibility for incorrect position	**YES**	0.182	N.A. undetected errors

7. Error codes

There are a few failure modes that have the potential to cause the sensor to put faulty communication on the CANBus. This in turn could lead to other Safety relevant functions to be impacted. Therefore, whenever the diagnostics routines detect such a possibility the sensor will refrain from communicating at all.

However, most of the failure modes do not fall in that category. Those then will lead to the sensor sending some information about the nature of the diagnosed malfunction.

The CANOpen Safety protocol and the J1939 Safety protocol both have a parameter called Error Code. However, the use of this parameter is restricted by protocol requirements and by constraints for maintaining backwards compatibility with prior products.

Therefore the information content of Error Code is limited. For details see the corresponding protocol descriptions.

For those reasons, the Status Byte has been arranged to give meaningful error information. The diagnosis processes handle close to 100 checks. Many failure modes trigger more than one of those checks.

The Status Byte contains two numerals. One made from the top 3-bits, pointing out the area in which area the problem occurred, the second one using the remaining 5 bits, designating the 'most offending check' that was triggered:

3 MSB			Numeral	Meaning
0	0	0	0	Microcontroller Health
0	0	1	1	Parameter Health
0	1	0	2	Voltage Health
0	1	1	3	Temperature Health
1	0	0	4	Measurement Health
1	0	1	5	reserved
1	1	0	6	reserved
1	1	1	7	reserved

The lower 5 bits, spanning 00..31 indicate which check failed, or in case of multiple violations, which one points most likely to the root cause.

Failed checks could either be transient, caused by an environmental parameter, or permanent, caused by a broken component. Some checks are more prone to the former one, others are more likely to be the later.

The Course Of Action depends on the application. If even the briefest unavailability of position data is critical, the application should shut down on the first occurrence.

On the other end of the spectrum, if position sensing can be interrupted for several seconds, the application could:

- wait 2 seconds, as many errors will revert automatically if the causing condition recedes
- initiate a power up, as that can clear another class of errors

If these measures do not clear the error, the sensor needs to be replaced.

For assistance with these topics, please contact Temposonics.

8. Failure probabilities

The product was designed in compliance with the SIL Level 2 requirements of IEC 61508:2010 as well as category 2 Performance Level d of ISO 13849-1:2006.

The product is intended for use in high demand mode of operation or continuous mode of operation. As the self-diagnosis routine is running parallel to the measurement function, this means there are no proof tests or checking intervals to observe.

Its internal structure is of 1001D type. The hardware fault tolerance is 0, with the element being of type A.

The failure modes are divided into those that can interfere with the Safety Function, the "Dangerous" failures, and those that will not directly impact the Safety Function, the "Safe" failures.

The Dangerous failures then are further divided depending on whether the diagnostics will detect them and force the device into the Safe State ("DD") or whether they stay undetected and thus can lead to an unsafe state ("DU").

The corresponding FIT rates are:

λS = 2287FIT λDD = 18.0FIT λDU = 0.182FIT

These ratings are valid for an ambient temperature of 55 °C. For profiles with a different ambient temperature, or a mix of ambient temperatures, correction factors can be calculated using the Arrhenius equation, applying 0.7 eV for the Activation Energy.

9. Fault Exclusions

The numbers given in chapter "Failure probabilities" where derived considering the impact of all electronics devices.

Failures in the connection part (e.g. harness ruptured) were not considered as they depend largely on the application environment. It is not conceiveable that they could create an unsafe state according to chapter "Definition of Safety Function and Safe State" but the will increase the likelihood of a safe error.

Communication faults on the CAN interface were also excluded.

The λDU caused by those should been extremely small as both standards, the CANOpen protocol DS-304 as well as the J1939 protocol described in DJ1939-76_201811 employ multiple layers of protection by message counters and CRC checksum procedures. In most cases any estimation will lead to numbers one or two magnitudes below the sensor's rating.

As for λDD and λDU, the electrical properties of the CANBus wiring as well as the number and kind of other participants have a large impact. As these things are the responsibility of the system designer, so are the estimations for the corresponding failure probabilities.

Temposonics
AN AMPHENOL COMPANY

UNITED STATES
Temposonics, LLC
Americas & APAC Region
3001 Sheldon Drive
Cary, N.C. 27513
Phone: +1 919 677-0100
E-mail: info.us@temposonics.com

GERMANY
Temposonics
GmbH & Co. KG
EMEA Region & India
Auf dem Schüffel 9
58513 Lüdenscheid
Phone: +49 2351 9587-0
E-mail: info.de@temposonics.com

ITALY
Branch Office
Phone: +39 030 988 3819
E-mail: info.it@temposonics.com

FRANCE
Branch Office
Phone: +33 6 14 060 728
E-mail: info.fr@temposonics.com

UK
Branch Office
Phone: +44 79 21 83 05 86
E-mail: info.uk@temposonics.com

SCANDINAVIA
Branch Office
Phone: +46 70 29 91 281
E-mail: info.sca@temposonics.com

CHINA
Branch Office
Phone: +86 21 3405 7850
E-mail: info.cn@temposonics.com

JAPAN
Branch Office
Phone: +81 3 6416 1063
E-mail: info.jp@temposonics.com

Document Part Number:
552177 Revision A (EN) 11/2024

UK CA CE ISO 9001 CERTIFIED

temposonics.com