

FUNCTIONAL SAFETY MANUAL (SIL)

SpeedSys® ODS

SpeedSys 200 and SpeedSys 300

GAME CHANGING
INNOVATION FOR SIL
RATED OVERSPEED
PROTECTION



COPYRIGHT

© 2021 Istec International BV | all rights reserved

Names of companies and products mentioned in this document may be trademarks of their respective owners.

For more information about this product and other ISTECS products, please visit www.istec.com.

This document is subject to change without notice. The latest version of this document can be downloaded from the ISTECS website.

Doc.-No.: MSSY00039 – revised in November 2025

IMPORTANT NOTICE

This product has been tested according to the listed standards. If the product is used in a manner not specified by manufacturer the degree of protection may be impaired. Therefore, this user manual must be read completely, carefully and all safety instructions must be followed.

ISTEC has made every effort to include all specific safety-related instructions and warnings in this manual, but the completeness and accuracy of this data cannot be guaranteed. Not all possibilities or situations are described in this manual. Before using this product, the user must evaluate it and determine its suitability to the intended application.

This manual is written for operators and integrators of the SpeedSys product. All operating personnel is expected to follow the specific safety related procedures and all applicable other (general) safety procedures. Operating personnel is assumed to have the necessary technical training and proven competence to enable them to install the product correctly and safely.

In case of unsafe, inexperienced or irregular use, ISTEC will decline any liability or warranty claims.

Table of contents

1	Safety Instructions	5
2	Specification of functionality and failure types	6
2.1	Interfaces	7
2.2	Assumptions and limitations	8
3	Safety characteristics and device configuration	9
4	Overall Safety Loop	10
4.1	SIL2 Relay Signaling	10
4.2	SIL3 Relay Signaling (SpeedSys 300 only)	11
4.3	SIL2 Analog Signaling	12
5	Installation and commissioning	12
6	Operation	13
6.1	Useful life time	13
7	Proof Test	14
7.1	Required Equipment	14
7.2	Proof Test Procedure	16
8	Maintenance	22

1 Safety Instructions

In addition to the present safety manual, the documentation also consists of the operating manual. This safety manual does not replace the operating manual!

MODELS

This functional safety manual applies to the following models: SpeedSys 200, SpeedSys 300 and SpeedSys 300. Where this manual refers to *SpeedSys*, it refers specifically to the models listed in this paragraph.

DISCLAIMER

The device is only approved for the intended use as defined in this safety manual. In case of violation, all manufacturer's responsibility and warranty will expire.

The user is responsible for planning, installation, commissioning, operation and maintenance.

Only qualified personnel may carry out installation, commissioning, operation and maintenance. The personnel must be familiar with the operating manual and safety manual.

QUALIFIED PERSONNEL

are persons who are familiar with the documentation of the device, as well as with the installation, commissioning, operation and maintenance of the device and have the appropriate qualifications for their work, e.g:

- Training, instruction or authorization to operate and maintain devices/systems in accordance with the standard of safety technology for electrical circuits, high pressures and aggressive and hazardous media.
- For devices with explosion protection: training, instruction or authorization to carry out work on electrical circuits for potentially explosive systems.
- Training or instruction in accordance with the standard of safety engineering in the maintenance and use of appropriate safety equipment.

2 Specification of functionality and failure types

Introduction

SpeedSys is an industrial and professional overspeed protection system intended for heavy and/or (semi-)critical machinery in the oil, gas and process industry, but can also be used on wind or hydro turbines or any similar application. This device was designed for indoor use only. Do not use in wet locations. It must only be operated in an altitude up to 2000 m. This device is for use in application within a pollution degree up to 2, overvoltage category II environment.

SpeedSys is a one channel transmitter and is designed to be compatible with the three most commonly used rotational speed probes; eddy current (proximity), Hall-effect and electromagnetic (VR/MPU). Only one of these three types can be connected per transmitter. For generating trip signals every transmitter has two fast-signaling energized-closed safety relays (SIL2). Additionally, for warning or status signals every transmitter has two status/alarm relays (non-safety) and one digital output (non-safety, SpeedSys 300 only). These outputs can all be individually configured. Moreover, SpeedSys allows for additional monitoring- and tailing equipment to use a SIL2 rated 4-20 mA analog output, a frequency output and/or a MODBUS RTU RS485 (SpeedSys 300 only) connection.

Analog output (current loop signal, 4...20 mA)

The analog output represents the measuring signal in the form of a 4 ... 20 mA current loop signal. The maximum load of 600Ω allows a current of 22 mA at an output voltage of 13.2 V.

In the **safe state** the current of the analog output is limited to <3.6mA.

Safety relay output 1 & 2

The relay switches state in response to an alarm, which may result from surpassing the configured thresholds or detecting a diagnostic error in the device. The maximum ratings are given in the operating manual.

In **safe state** the relay contact opens (NO contact, in safe state de-energized).

2.1 Interfaces

The device is equipped with the following **safety relevant interfaces**:

Table 1: safety relevant interfaces

Interface	Terminals	Comment
Measuring input,		dual-channel with comparison logic
2-wire-voltage input	B01, B02 (B03, B04 bridge)	Only one input can be used
3-wire-voltage input	B05, B06, B07	
2-wire-current input	B09, B10	
Analog output	A13, A14	Current loop, internally powered
Relay output 1 & 2	B17, B18 / B19, B20 and B21, B22 / B23, B24	Safety relays

The device is equipped with the following **non-safety relevant interfaces**:

Table 2: non-safety relevant interfaces

Interface	Terminals	Comment
Supply input	A17, A18 and A21, A22	redundant
Digital input	C13, C14	SpeedSys 300 only
USB configuration Interface		USB-B mini
Relay output 3 & 4	B13, B14 and B15, B16	Non-safety relays
Digital frequency output	A15, A16	Requires external pull-up resistor
Digital output	C15, C16	SpeedSys 300 only
RS485 interface	C17, C18, C19	SpeedSys 300 only

2.2 Assumptions and limitations

The FMEA was based on the following **assumptions**:

- The failure rates of the considered components are based on the Siemens standard SN 29500
- The analysis was based on average industrial environmental conditions:
 - average environmental temperature 40°C
 - The device is mounted stationary.
 - The failure rates are constant, attrition is not taken into account.
- The failure rates of the other components (other than the SpeedSys) in the safety loop are not included.

The following **restrictions** apply to the application:

- A single device of either SpeedSys 200 or SpeedSys 300 is SIL2 (1oo1). SIL3 can only be achieved with the SpeedSys 300 in a setup with a hardware fault tolerance (HFT) ≥ 1 .
- A single device may only be used in an application where the demand rate of the safety function is less than once a year (low demand).
- A setup with a HFT = 0 (1oo1, 2oo2, 3oo3), is always SIL2 for all devices.
- The device may only be used in an application where the allowable mean probability of failure on demand (PFDG) for the device is up to $17e-3$ (device claims 18% of the total failure rate of SIL2).

3 Safety characteristics and device configuration

Safety parameters	
SIL level	2
Systematic capability (SC)	3
Mode	Low demand / Demand mode
Device type	B
Hardware fault tolerance	0
Safety function reaction time	T _m + 8 ms (measuring time + HW response time)
Safety function response time including system diagnostics	5h (duration of RAM check)
Error rate (safe)	478 FIT
Error rate (dangerous, detected), 3-wire, 40°C	608 FIT
Error rate (dangerous, undetected), 3-wire, 40°C	28 FIT
SFF value (safe failure fraction), 40°C	97 %
Proof test interval, 40°C	10 years
PFDG (10y, 40°C, MTTR 72h)	1.73e-3

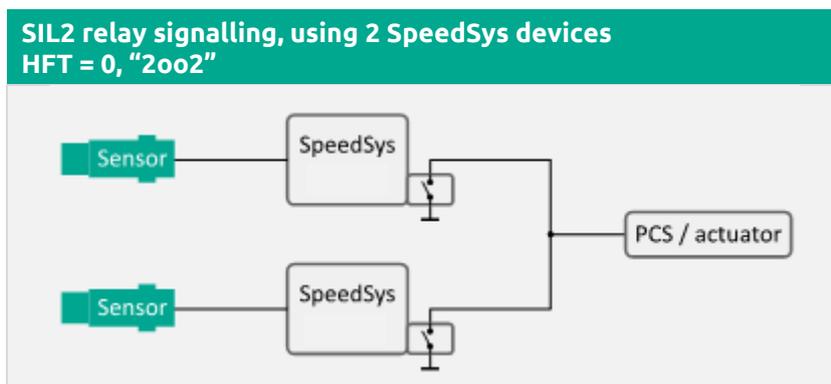
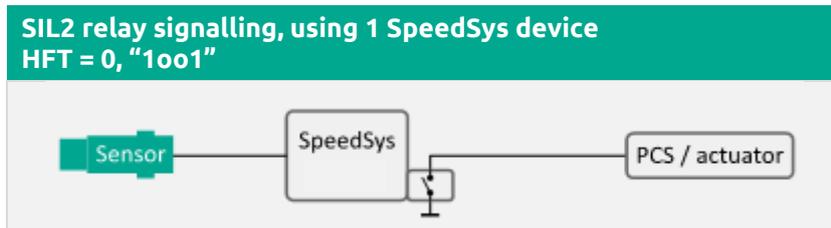
Device configuration	
Board designation	SpeedSys 200: (A), (B) SpeedSys 300 : (A), (B), (C)
Board revision	PCB A: 2020-12 PCB B: 2020-10 PCB C: 2020-10
Schematic revision	0.14.3
Firmware designation	SSY master, SSY slave
Firmware revision	1.20 (master), 1.0 (slave)

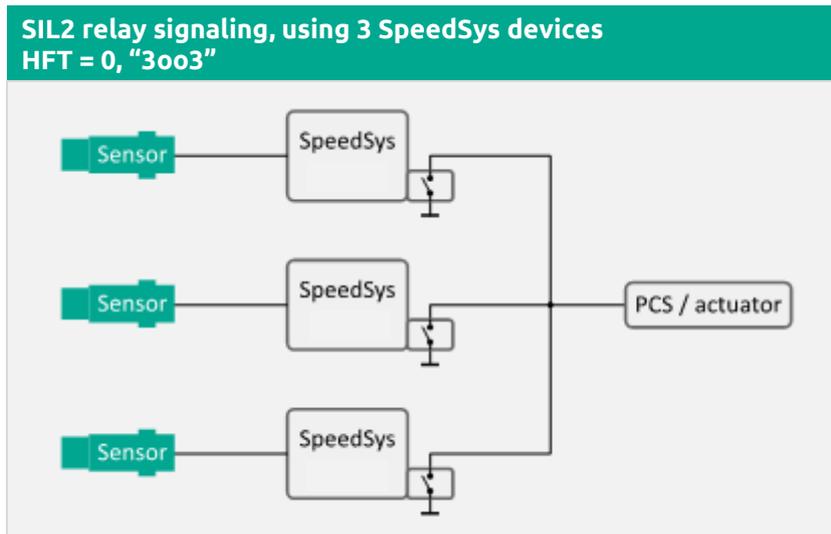
4 Overall Safety Loop

SpeedSys is to be used in a safety loop, sketched in the following figures, in which the safety function is to react to a limit-violation of the measured rotation frequency. In this context, the SpeedSys evaluates the measured frequency-value, as well as its derivation (acceleration) against configurable minimum- and maximum-limits. The outcome of the evaluation is signaled using two safe (SIL2 in standalone configuration, up to SIL3 (SpeedSys 300 only) in redundant configuration) relay outputs (relay1, relay2). Furthermore, the SpeedSys retransmits the measured value in the form of a calibratable, safe (SIL2) current-loop signal (mA-out) to a process control system (PCS). Errors, detected by self-diagnosis, leads to a switching to the safe state of the outputs.

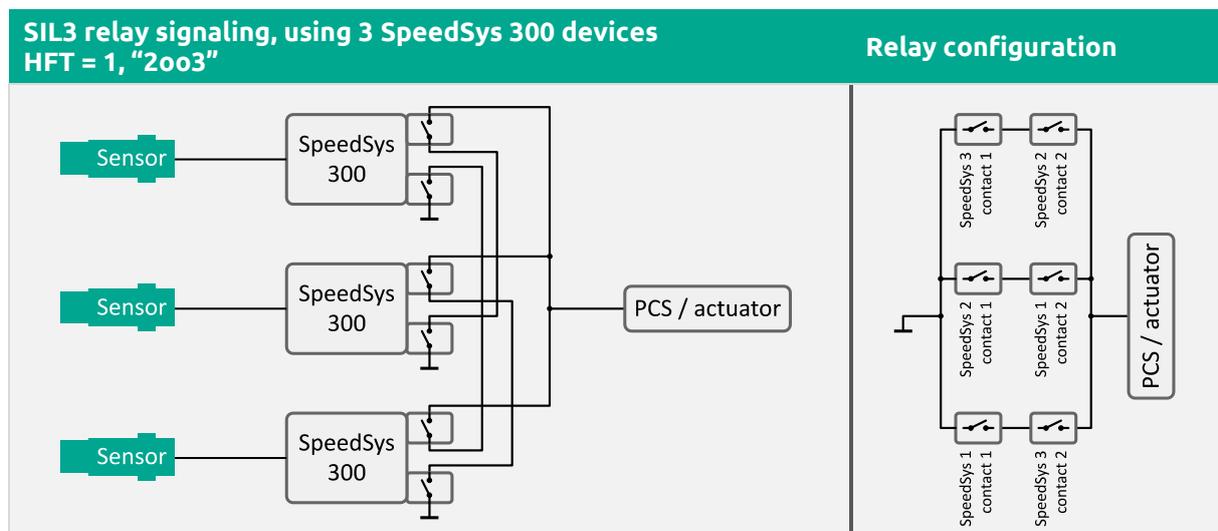
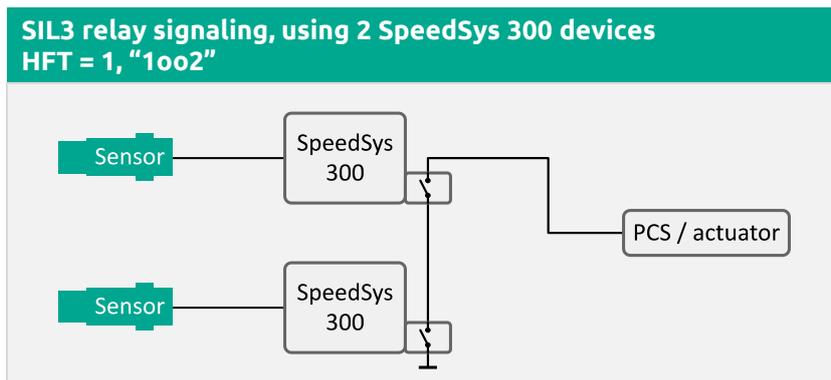
Depending on the setup, different SILs and different “availability HFTs” can be achieved. The different setups are exemplarily and show only one safety-relevant relay.

4.1 SIL2 Relay Signaling

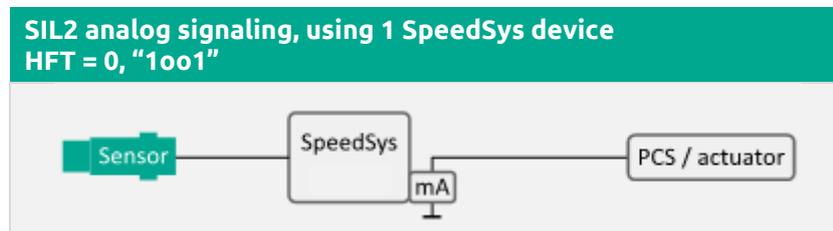




4.2 SIL3 Relay Signaling (SpeedSys 300 only)



4.3 SIL2 Analog Signaling



5 Installation and commissioning

The installation must be in accordance with the **operating manual** and this **safety manual**. This device may only be connected to devices that are suitable for safety applications.

To ensure the maximum current rating of the relay contacts, appropriate current limiting measures must be taken in the safety-relay loops.

The following steps must strictly be followed during the commissioning to ensure the expected behaviour of the safety function:

- Programming of the device parameters (values customized to the targeted safety purpose – See operating manual for description and procedure)
- Verification, of the programmed parameters (have the parameters been programmed correctly – This is carried out by the parametrization software)
- Validation of the intended safety function (does the setup fulfil the requirements to the safety loop)

6 Operation

Operation must be in accordance with the **operating manual** and this **safety manual**.



If the safety circuit is compromised, the safety function is no longer guaranteed!

- Do not manipulate the device !
- Do not repair the device !

6.1 Useful life time

The estimation of the useful life time is based on the assumption of constant failure rates of the components involved in the device. This assumption is based on the bathtub curve, which is typical for electronic components: the higher probability of early failures (for which it is assumed that they are already detected during manufacture and installation) is followed by the constant failure rate during the useful life time. Once the useful life time has been reached, the probability of failures typically increases significantly. Although the actual lifetime of the device may be higher than the operation life, the calculation of the safety characteristics is based on the assumption of constant failure probabilities and is therefore limited to the useful life time.

The useful life time of the individual components depends on the component itself, but also on its ambient conditions (especially the ambient temperature).

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years

The useful life time of the device may be longer under favorable ambient conditions, e.g. if the ambient temperature is significantly below 60 °C.

7 Proof Test

The purpose of the proof test is to detect potentially dangerous failures that were not detected by the internal diagnosis. The proof test must be performed according to the **proof test interval** given in the safety parameters and the **PFDG** value. The plant operator is responsible for planning and carrying out the proof tests.

The proof test procedure is focusing on the safety relay function. All other functions do not require testing during the life time of the SpeedSys.

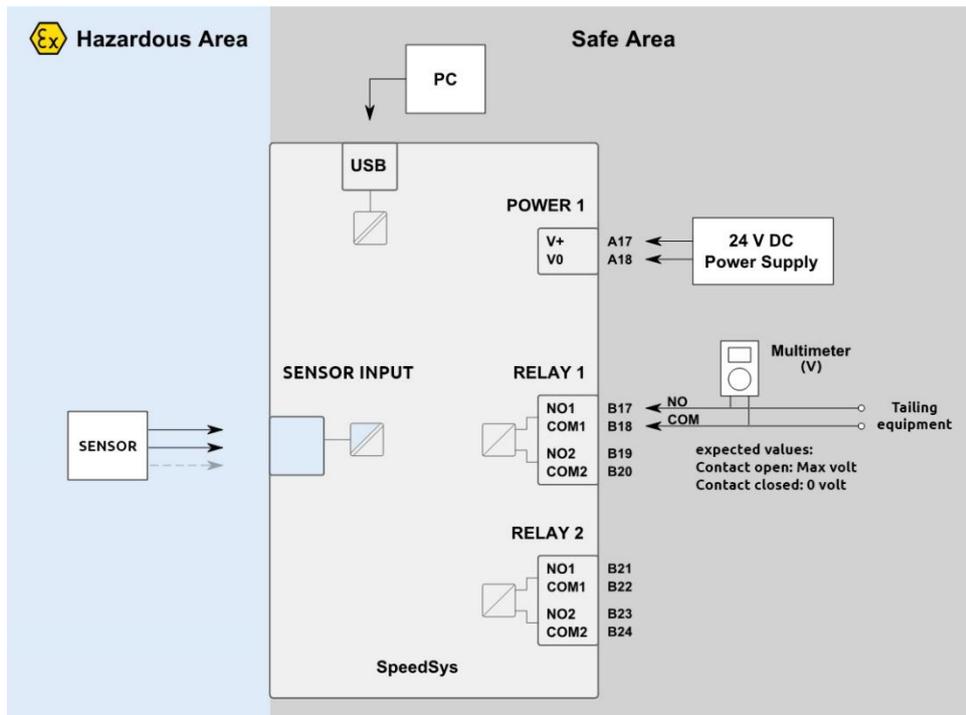
7.1 Required Equipment

- PC, USB cable and configuration software *SpeedSys200* or *SpeedSys 300*
- Digital voltmeter

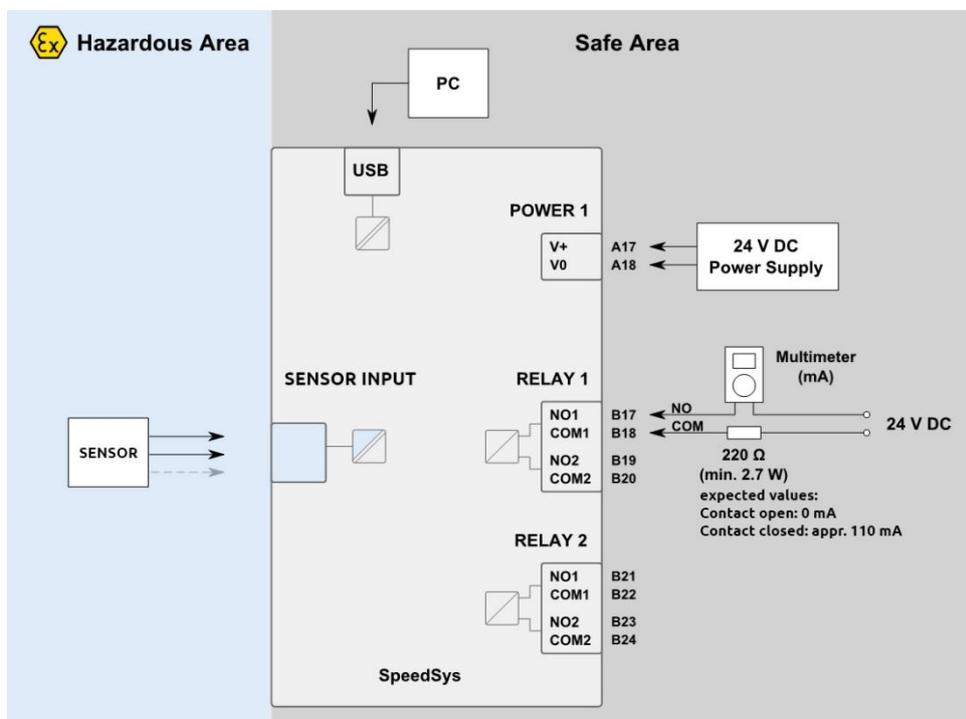
If the test is not performed in situ, additional equipment is required

- Power supply with a nominal voltage of 24 V DC, SELV
- Resistor of 220 Ω (min. 2.7 W)
- Speed sensor as used in the application

Prepare the test setup according to one of the figures below. Note that the test requires a sensor to be connected, in order to avoid sensor diagnostic errors. Please refer to the operation manual for sensor connections.



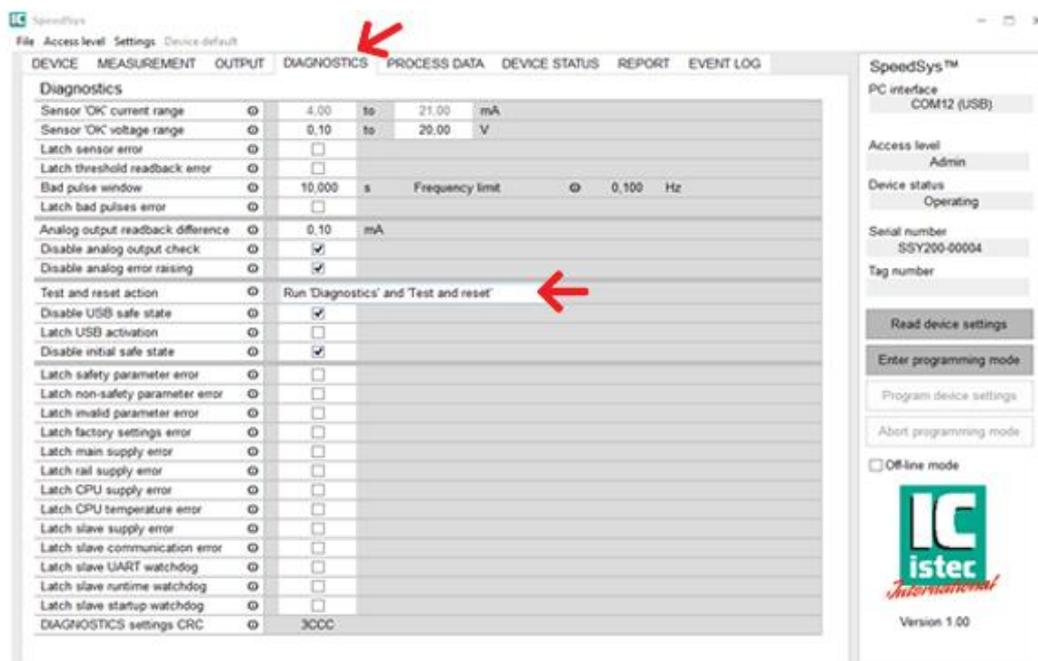
Test setup if performed in situ



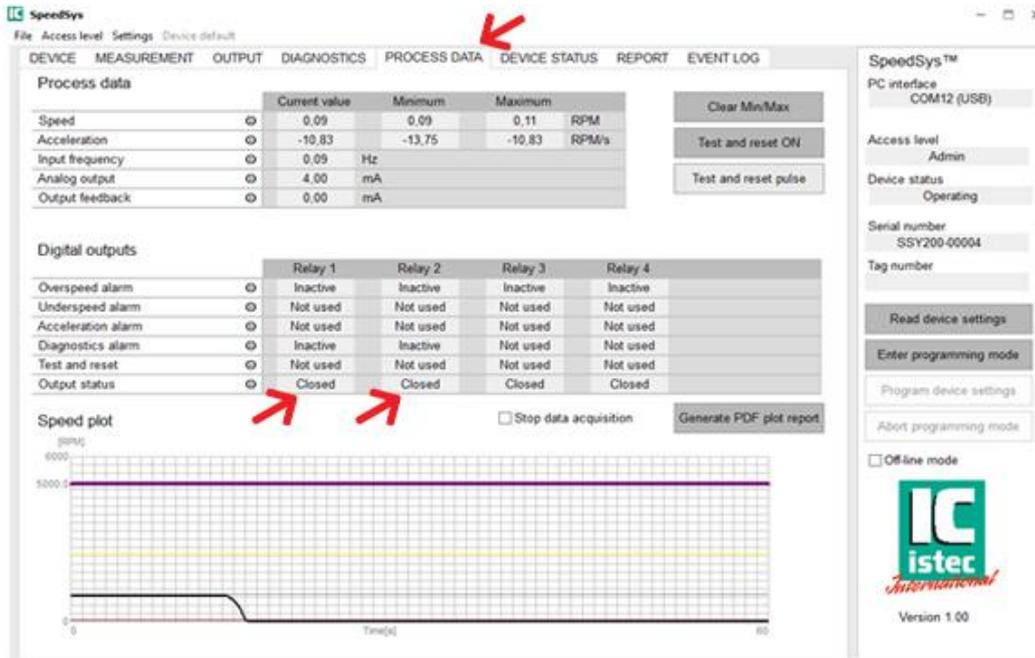
Test setup if not performed in situ

7.2 Proof Test Procedure

1. If tested in situ: Ensure that the unit under test is not affecting the safe operation.
 - a. It is preferred to perform the proof test during scheduled outage.
 - b. If applicable, a specific HAZOP has to be performed before executing the proof test.
 - c. If applicable, protect the application by means of other measures.
2. Connect a PC with the USB cable to the device and open the configuration software *SpeedSys200* or *SpeedSys 300* as described in the operation manual.
3. Select the *DIAGNOSTICS* menu and verify if the option *Test and measurement* is set to *Run Diagnostics and Test and reset*. If yes, continue to the next step. If no, refer to the operation manual to set this parameter.

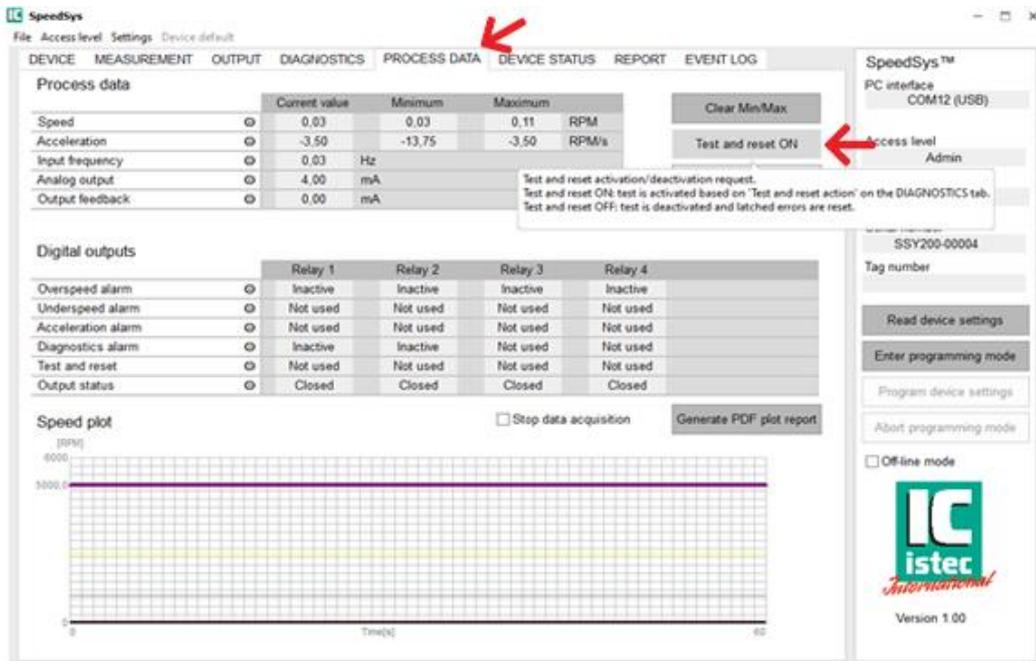


4. Select the *PROCESS DATA* menu and verify if the table *Process data* and the table *Digital outputs* are according to expectation.

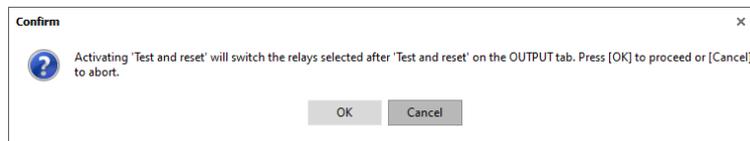


5. Use the multimeter to verify all relay outputs of the safety relays 1 and 2. Check that the relay contacts are closed. The yellow relay LEDs are ON.

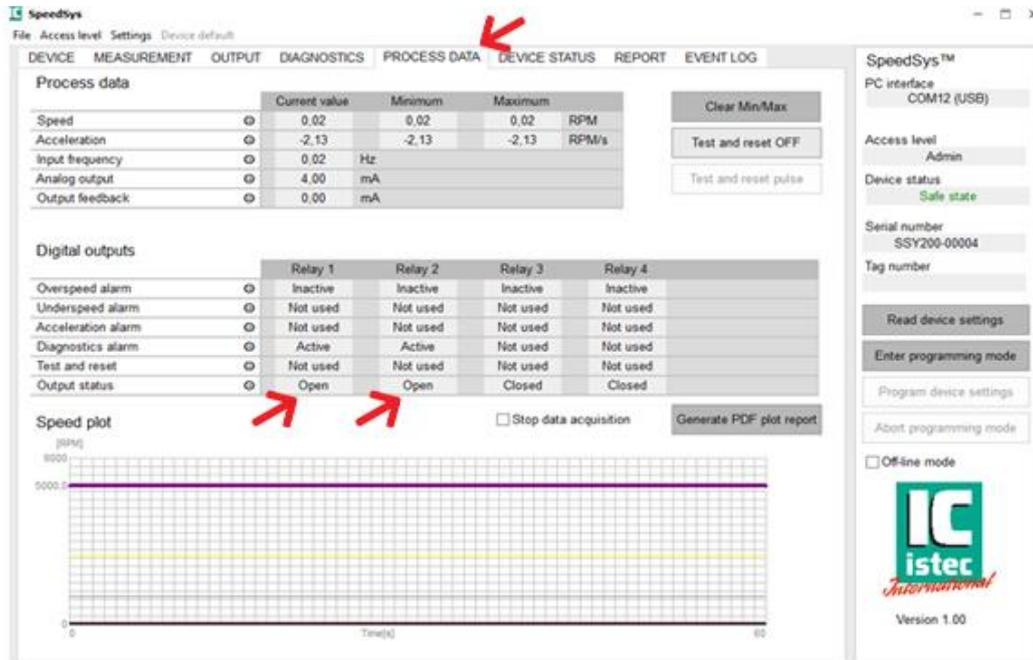
6. Press *Test and reset ON* button to activate the test signaling.



7. Press *OK* to confirm.



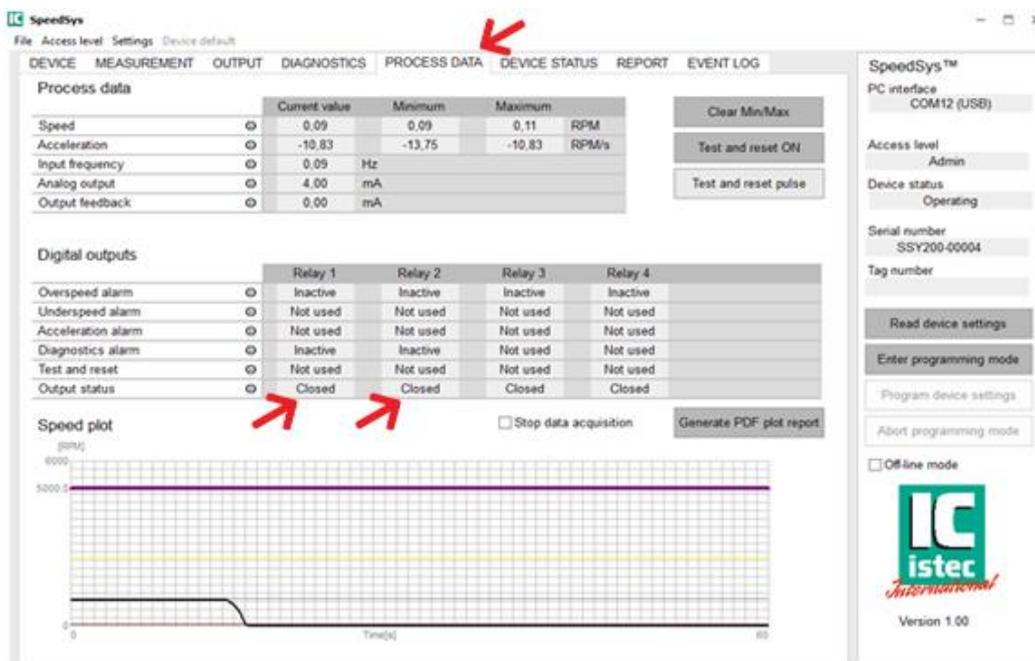
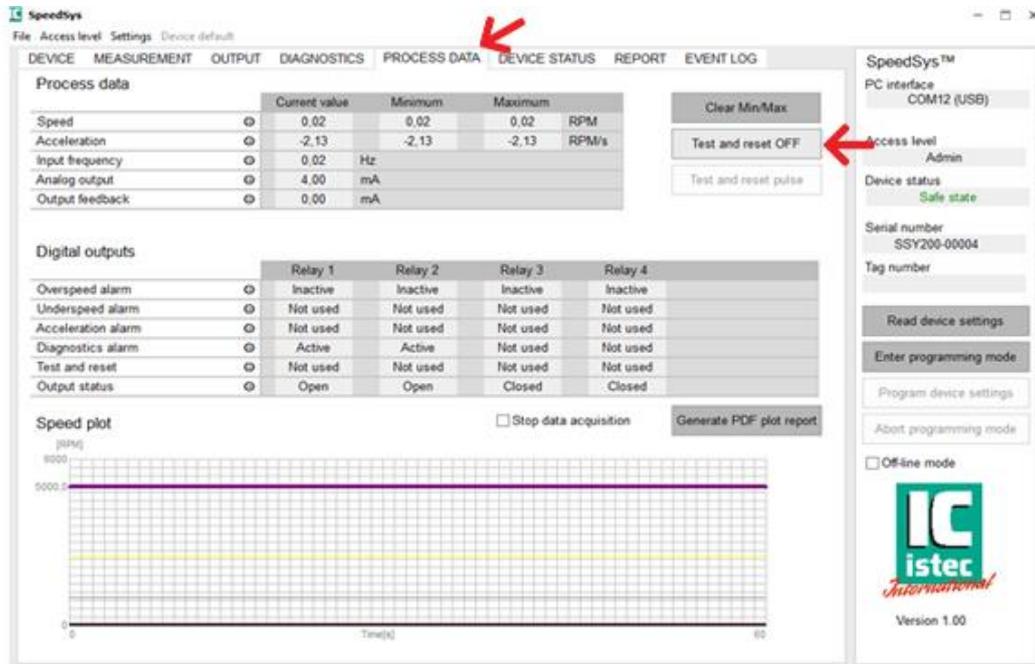
- Verify if the table *Output status* shows the required status of the safety relays.



- Use the multimeter to verify all relay outputs of the safety relays 1 and 2. Check that the relay contacts are open. The yellow relay LEDs are OFF.

- Optional tailing equipment verification (in situ test only): Verify the registration and feedback of tailing equipment (connected to safety relay 1 and 2).

11. After verification, press *Test and reset OFF* button to return to normal operating state.



12. Use the multimeter to verify all relay outputs of the safety relays 1 and 2. Check that the relay contacts are closed. The yellow relay LEDs are ON.

13. After successful performing the tests and documenting the results the unit under test can be restored to its original configuration. If it is not clear how to restore the original configuration, refer to the manual. **Before bringing the unit under test back to operation, verify if the unit operation is according to its intended safety function !**

8 Maintenance

With the exception of the proof test, the device is maintenance-free. Repairs to the device may only be carried out by the manufacturer.