IPAQ C520/R520 Supplementary Instructions

HART® Temperature Transmitter
for up to SIL 2 applications

Safety manual SIL

SIL 2
Safety Integrity Level

INOR

CONTENTS

1 Introduction 3

1.1 Field of application ... 3
1.2 User benefits ... 3
1.3 Manufacturer's safety instructions ... 3
1.4 Relevant standards / Literature ... 4

2 Terms and definitions 5

3 Description of the subsystem 6

3.1 Functional principle ... 6

4 Safety function 8

4.1 Description of the failure categories ... 8
4.2 Specification of the safety function ... 8
4.3 Redundancy ... 9
4.3.1 Sensor drift ... 10
4.3.2 Sensor backup ... 10

5 Project planning 11

5.1 Applicable device documentation ... 11
5.2 Project planning, behaviour during operation and malfunction ... 11
5.2.1 SIL data ... 11

6 Periodic checks / Proof tests 12

6.1 Periodic checks ... 12
6.2 Proof tests ... 12

7 Safety-related characteristics 14

7.1 Assumptions ... 14
7.2 Specific safety-related characteristics ... 15

8 Appendix 20

8.1 Declaration of conformity for Functional Safety (SIL) ... 20
8.2 exida / FMEDA management summary ... 21
8.3 Type Examination Certificate ... 24
8.4 Return / maintenance form ... 26

9 Notes 27

1.1 Field of application

The IPAQ C520 (hereafter referred to as C520) is a universal, isolated, dual-input temperature transmitter for RTD and thermocouple sensors. It's primarily intended to be mounted in a DIN-B housing.

IPAQ R520 (hereafter referred to as R520) is the rail mounted version of the IPAQ C520.

IPAQ C520X and R520X are the intrinsically safe versions of the IPAQ C520 and R520.
An S is added for the SIL versions, e.g. C520S and C520XS.

The IPAQ C520/R520 temperature transmitter utilizes a modular design in hardware as well as in software to ensure the quality and reliability of the transmitter signal output to meet the special safety requirements according to IEC 61508:2010 part 1 to part 3 for use in SIL2 applications.

1.2 User benefits

- This intelligent HART® temperature transmitter is designed to perform temperature measurements of solids, fluids and gases up to SIL2 according to special safety requirements of IEC 61508:2010 (see Certificate No. SC0266-13 issued by RISE Research Institute of Sweden AB (former SP Technical Research Institute of Sweden).
- Remote configuration with process control system, PC or HART® hand terminal is **not** possible in combination with SIL activation to prevent unintended changes, only read-out of parameters from the unit is possible via HART®. To change settings or deactivate the SIL function the INOR software ConSoft and INOR USB-kit ICON must be used.
- Continuous measurement
- Easy commissioning

SIL 2 requirements are based on the standard IEC 61508:2010.

The C520S/C520XS/R520S/R520XS certification involves the HW assessment of the products with an FMEDA plus a full assessment made by RISE Research Institute of Sweden AB.

1.3 Manufacturer's safety instructions

The measuring device has been built and tested in accordance with the current state of the art, and complies with the relevant safety standards
However, dangers may arise from improper use or use for other than intended purpose.
For this reason, observe all the safety instructions in this document and in the Handbook carefully.

Hardware	Production order no.	IPM	OPM	ConSoft	Handbook	Safety Manual
≤ 9	≤ 571029873	01.01.03xxx	01.01.04xxx	≥ 2.0.0.8	86B5200001 ≤ 2	86B520S001 ≤ R1.2
≥ 11	≥ 571030029	01.02.02xxx	01.02.02xxx 01.02.03xxx 01.02.04xxx	≥ 2.0.0.8	86B5200001 ≥ 4	86B520S001 ≥ R1.3

This "Safety manual" is a complement to the regular Handbook(User Instructions) for IPAQ C520 and R520.
In addition to the safety rules in this documentation, national and regional safety rules and industrial safety regulations must also be observed.

1.4 Relevant standards / Literature

Standard	Designation
IEC 61508:2010 all parts	Functional safety of electrical/electronic/programmable electronic safety related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61326-3-1:2008 EN 61326-3-1:2008	Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)- General industrial applications
Namur NE 21	Electromagnetic compatibility of industrial process and laboratory control equipment
Namur NE 32	Data retention in the event of a power failure in field and control instruments with microprocessors
Namur NE 43	Standardization of the signal level for the failure information of digital transmitters
Namur NE 53	Software of field devices and signal processing devices with digital electronics
Namur NE 79	Microprocessor equipped devices for safety instrumented systems
Namur NE 89	Temperature transmitter with digital signal processing
Namur NE 107	Self-monitoring and diagnosis of field devices
EN 60079-0:2009 EN 60079-0:2012	Electrical apparatus for explosive gas atmospheres - Part 0: General requirements
EN 60079-11:2007 EN 60079-11:2012	Explosive atmospheres - Equipment protection by intrinsic safety "i"
EN 60079-26:2007 EN 60079-26:2015	Explosive atmospheres - Part 26: Equipment with equipment protection level (EPL) Ga

Table 1-1: Supported standards during the development of C520/R520

Used abbreviations

Acronym	Description
DC_D	Diagnostic Coverage of dangerous failures. Diagnostic coverage is the ratio of the detected failure rate to the total failure rate.
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEA	Failure Modes Effects Analysis is a structured qualitative analysis of a system, subsystem, process, design or function to identify potential failure modes, their causes and their effects on (system) operation.
FMEDA	Failure Modes Effects and Diagnostic Analysis adds a qualitative failure data for all components being analyzed and ability of the system to detect internal failures via automatic on-line diagnostics parts to FMEA.
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demand for operation made on a safety-related system is not greater than one per year and not greater than twice the proof-test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year and greater than twice the proof-check frequency.
MTBF	Mean Time Between Failure is average time between failure occurrences.
MTTR	Mean Time To Restoration is average time needed to restore normal operation after a failure has occurred.
PFD_{AVG}	Probability of Failure on Demand is the average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour is the probability of a system to have a dangerous failure occur per hour.
SFF	Safe Failure Fraction summarizes the fraction of failure, 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
Type A component / Type A element	"Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2:2000 / 7.4.4.1.2 of IEC 61508-2:2010.
Type B component / Type B element	"Complex" subsystem (at least one failure mode are not well defined); for details see 7.4.3.1.3 of IEC 61508:2000 / 7.4.4.1.3 of IEC 61508-2:2010.
T[Proof]	Proof Test Interval

Table 2-1: Used abbreviations during the development of C520/R520

3.1 Functional principle

The C520/R520 supports up to two sensor channels with general input circuits that may be configured for RTD and/or thermocouple temperature sensors.

All safety related calculations are based on these connections.

Functional principle of the C520/R520 is based on the analog to digital and back to analog signal conditioning. The temperature sensors used are either Resistance Temperature Device(s) (RTD) or thermocouple(s) (T/C). The RTD has a temperature dependent, non-linear, variable resistance while the T/C generates a low level, highly non-linear, EMF (voltage) that depends on the temperature difference between opposite ends of the T/C wire pair. Hence the connection end of the T/C (cold junction) constitutes a temperature reference or base value that has to be measured in order to determine the temperature at the critical spot (hot junction). This action is referred to as cold junction compensation (CJC). One or two sensors of the same or different types may be connected.

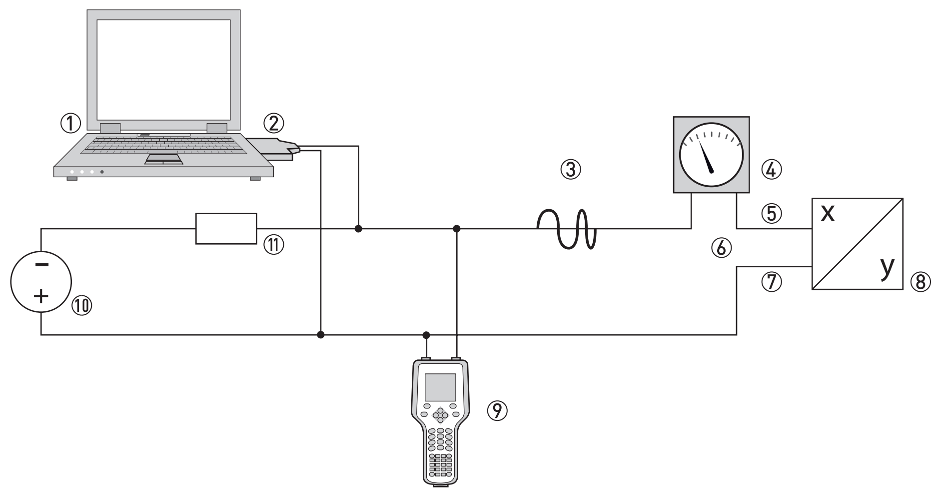

Figure 3-1: The functional principle of C520

① Primary Master
② HART modem
③ HART
④ Milliampere-meter Load ≥ 250Ω
⑤ Terminal 7 (- on C520)
⑥ 4...20 mA
⑦ Terminal 6 (+ on C520)
⑧ C520 connected with sensor in the sensor head
⑨ Secondary master
⑩ DC power supply
⑪ Load ≥ 250Ω

The low level analogue signal from temperature sensors is amplified and filtered before converting it to a digital signal. The digital signal is less prone to electromagnetic interference. Digital signal processing like sensor linearization, calculation, temperature drift compensation etc. is controlled by processors, isolated and converted back to analogue 4...20 mA output signal.

The C520/R520 are smart temperature transmitter which improves predicting problems within the industrial safety instrumented systems – SIS, reducing the manual testing.

The C520/R520 is a modular and configurable system with the ability to pre-configure inputs for measuring sensor(s) and outputs to fault conditions. Configuration of the transmitter is protected by password.

4.1 Description of the failure categories

The following definitions of the failure are used during diagnostic calculations:

State definition	Description
Fail-Safe State	The fail-safe state is defined as the output reaching the user defined threshold value.
Fail - Safe	A safe failure (S) is defined as a failure that causes the module/(sub)system to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	A dangerous failure is defined as a failure of the temperature transmitter C520/R520 not responding to a demand from the process, i.e. being unable to go to the defined fail-safe state, and the output current deviates by more than 2% of measuring span of the actual temperature measurement value.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics and causes the output signal to go to the predefined alarm state (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (≥ 21 mA) acc. to NAMUR NE 43.
Fail Low	Failure that causes the output signal to go to the minimum output current (≤ 3.6 mA) acc. to NAMUR NE 43.
Fail No Effect	Failure of a component that is part of the safety function but is neither a safe failure nor a dangerous failure and has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which is not part of the safety function but part of the circuit diagram.

Table 4-1: Definitions of the failure rate during the diagnostic calculations for C520/R520.

4.2 Specification of the safety function

The safety function of the C520/R520 transmitter is the quality and reliability of the transmitter signal output, i.e. measurement performance, error detection and error indication in the signal-processing path of the transmitter.

The valid range of the output signal is between 3.8 mA and 20.5 acc. to NE 43.

The failure information is defined by two selectable alarm levels: Fail Low (Downscale ≤ 3.6 mA) and Fail High (Upscale ≥ 21 mA).

The configuration of the transmitter is protected by a password set via the software ConSoft. The password is stored in the transmitter.

The C520S/C520XS/R520S/R520XS checks sensor errors (sensor break or sensor short) for both channels if it is configured in this manner.

A software SIL-switch is available in the transmitter, handled by the PC-configuration software ConSoft. It is password-protected by the same password that protects from change of configuration. The SIL-switch can also be changed by HART communication, still password-protected. The password may be changed either via ConSoft or via HART communications. It is stored in the transmitter and it has to be accurate in order to download any changes to the transmitter configuration. When the transmitter is shipped, the password default value is "0000". **For SIL applications the password must be changed** to a user specific password in order to prevent unintended change of configuration.

The following definitions of the failure are used during diagnostic calculations:

Function	Active/Not Active	Output	Alarm level ①
Sensor break	Active	4...20 mA / 20...4 mA	≤3.6 mA / ≥21.0 mA
Sensor short	Active	4...20 mA / 20...4 mA	≤3.6 mA / ≥21.0 mA
Low isolation	Not active	-	-
Transmitter error ②	Active	4...20 mA / 20...4 mA	≥21.0 mA
Sensor drift (dual sensor needed) ③	Active/Not Active selectable	4...20 mA / 20...4 mA	≤3.6 mA / ≥21.0 mA

① For some system failures the alarm output will toggle between a high alarm level (≥21.0 mA) and a low alarm level (≤3.6 mA). For some HW failures the alarm level will be high even though a low level is configured and for some other HW failures the alarm will go low even though a high level has been selected.

To prevent a safety system from restart due to the toggling output the system should be setup so that once an alarm signal has occurred from the safety loop the system shouldn't go back to normal run automatically but only manual ("Restart Interlock").

② Transmitter errors = failures in the software or hardware detected by the diagnostics in the transmitter.

③ The sensor drift function is valid from SW-versions; IPM-SW 01.01.03 and OPM-SW 01.01.04 and hardware versions 5 and later, implemented in transmitters with serial number 1006.xxxxxx or later. Serial number 1006.xxxxxx means manufactured week 6 in 2010 and this information is found on the nameplate or it can be read from the transmitter via ConSoft. The software and hardware versions can be read from the ConSoft software, tab "Device Information".

4.3 Redundancy

For the following configurations:

- 2 x 2w RTD sensors
- 2 x 3w RTD sensors
- 2 x 4W RTD sensors (only valid for R520S/R520XS)
- 2 x Thermocouple sensors
- 1x Thermocouple sensor and 1 x 3w RTD sensor
- 1x Thermocouple sensor and 1 x 4w RTD sensor (only valid for R520S/R520XS)

are either "Sensor drift monitoring" function or "Sensor backup" function selectable at a time.

4.3.1 Sensor drift

If the function "Sensor drift" monitoring is selected, a difference between the sensors of more or equal to the value stated in the configuration will cause the output to go either "Downscale" or "Upscale" depending on the user configuration. Maximum temperature difference has to be specified in °C via ConSoft.

4.3.2 Sensor backup

If "Sensor backup" function is activated the sensor chosen as output measuring in the configuration will reflect the actual measuring value as long as it's working properly. A sensor break or a sensor short cause the transmitter to switch over to the other sensor and the output signal will reflect the measured value of that sensor. A diagnostic message is transmitted via HART® to the PLC.

If the "Average" function is activated in the configuration, the output value will reflect the actual mean measuring value as long as the sensors are working properly. A sensor break or a sensor short cause the transmitter to switch over to the non-broken sensor and the output signal will reflect the measured value of that sensor. A diagnostic message is transmitted via HART® to the PLC.

The functions "Sensor backup" and "Average" doesn't give any extra safety according to SIL and are not used for calculating the system (transmitter + sensor) safety figures.

CAUTION!
The possibility to select the function for sensor drift monitoring is implemented in software revision IPM-SW 01.01.03 and OPM-SW 01.01.04, from serial number 1006.xxxxxx.

5.1 Applicable device documentation

Please see the following documents for additional information about the product:

Document name	Description and application
86DPQ00013/86DPQ00014	Data sheet C520/R520
86B5200001	Handbook (User instructions) C520/R520

Table 5-1: Applicable user documentation

5.2 Project planning, behaviour during operation and malfunction

- Under normal conditions the useful operating lifetime is 10 years (8...12 years).
- Requirements made in the handbook have to be kept.
- Repair and inspection intervals are based on safety calculation.
- For repairs or recalibration of the SIL transmitter, use the original or a suitable secure packing, include a properly filled out return form (see Appendix) and send the device to the manufacturer for service.
  Note: It is of vital importance that all type of failures of the equipment are reported to the manufacturer in order to make it possible for the company to make corrective actions and prevent systematic errors.
- The owner of hazardous waste is responsible for disposal of it. However all transmitter produced by the manufacturer are free from any hazardous materials.
- Modifications made without specifically authorization of the manufacturer are strictly prohibited.

5.2.1 SIL data

- Measurement accuracy in SIL mode: a hardware error influencing the measured value will result in a system error signal if the measured signal deviates more than 2% of selected input span
- System Error Detection Time: < 5 min (for a complete software check running in background when SIL is activated)
- Update times for input signals change, with filter set to default value 4 and SIL-switch on: 1 input channel: < 2 s
- Update times for input signals change, with filter set to default value 4 and SIL-switch on: 2 input channels: < 3 s
- Minimum supply needed for system safety functions to work properly: ≥ 15 VDC
- To avoid unintended change of the configuration of the transmitter it is recommended that the default password (0000) is changed to a safe password. **For SIL applications the password must be changed**. Please note that it is necessary for the user to save and protect his password.
  The password is the key that unlocks the transmitter for configuration and if forgotten, there is NO WAY to get it back other than to return the transmitter to the factory.

6.1 Periodic checks

The user of the C520S/R520S transmitter is responsible for:

- The set-up, SIL rating and validation of any sensors connected to the SIL transmitter
- Project management and functional testing
- Configuration of the transmitter according to the description in the following chapters.

It is recommended that the user performs regularly proof tests of the sensors used with the SIL transmitters.

Proof test of the SIL transmitter should be made based on the required PFD depending on the used sensor. For detailed information refer to *Safety-related characteristics* on page 14.

For PFH figures a proof test interval of one year is recommended. The needed frequency of proof tests necessary for the safety-related system must be found by the customer.

The proof tests should be done by the user at following measures:

- At commissioning of the SIL transmitter
- Replacement of the old connected temperature sensor by new ones
- Reconfiguration of the SIL device
- If a relocation of the SIL transmitter is needed

6.2 Proof tests

The proof tests shall cover SIL safety test requirements. Up to 99% of the internal failures shall be detected via the proof tests. The input to the SIL transmitter is simulated and tested for the internal errors in the hardware and the firmware.

Proof test configuration

Step	Description
1	Connect transmitter to the PC via USB interface.
2	Start ConSoft (Check version: "Help menu → About").
3	Identify transmitter by clicking on "Read from transmitter" button.
4	Enter the SIL chosen password (default value is "0000").
5	Configure the transmitter by selecting sensors tab in the transmitter window.
5.1	The sensor for Channel 1 and the connection for Channel 1.
5.2	The sensor for Channel 2 and the connection for Channel 2.
6	Choose measuring range for process value by selecting "Function" tab in the transmitter window
6.1	Select measuring output mapping (Channel 1; Channel 2; Ch 1 minus Ch 2; Ch 2 minus Ch 1; minimum of Ch 1 and Ch 2; maximum of Ch 1 and Ch 2; Average of Ch 1 and Ch 2).
6.2	Select output values in mA which correspond to the chosen measuring range.
6.3	Select filtering level and line frequency rejection.
7	In the error monitoring tab select check box for sensor break. Select upscale (≥21 mA) value.
7.1	Select check box for sensor short circuit. Select upscale (≥21 mA) value.
7.2	Select check box for sensor low isolation. Select upscale (≥21 mA) value. Select desired resistance limit; default: 300 kΩ
7.3	Select check box for sensor backup.

Step	Description
8	Select device information tab. Specify a mounting date in tag field.
8.1	Describe the proof test in the description field and date of the test.
8.2	Specify any other information in the message field.

Table 6-1: Proof test configuration for the SIL transmitters

Proof test check points

Step	Description	Yes	No	Comments
1	Connect the selected sensors on Ch 1 and Ch 2 and check for the output range values.			
2	Simulate sensor break for each single wire and check the output value (≥21 mA).			
3	Simulate sensor short between 1...5 terminals and check the output value (≥21 mA).			
4	Simulate sensor break or sensor short (one error at a time) for sensor connected on Ch 1. Check if the transmitter will switch automatically over to measuring on Ch 2.			

Table 6-2: Proof test check points

- Repeat configurations points 7...8.2 of the proof test configuration and change to down scale error value (≤3.6 mA).
- Repeat all check points (to be sure the transmitter is not stuck in some of conditions).

7.1 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the HART® temperature transmitter C520S/R520S.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- External power failure rates are not included.
- The mean time to restoration (MTTR) after safe failure is 24 hours.
- For safety applications only the 4..20 mA output was considered. The HART® protocol at C520/R520 is only used for setup and diagnostic purpose, not during safety operation mode.
- The failure rates of the electronic components used in this analysis are obtained from a collection of industrial databases.
- The temperature transmitters IPAQ C520S/C520XS/R520S/R520XS with 4..20 mA output are considered to be type B subsystems with a hardware fault tolerance of 0.
- The failure rates do not include failures resulting from incorrect use of the equipment.
- The HART® protocol is only used for setup, calibration and diagnostics purpose, not during safety operation mode.

7.2 Specific safety-related characteristics

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $\leq 10^{-2}$ for SIL 2 Safety Instrumented Functions (SIFs). For systems operating in high demand mode of operation the PFH value has to be $\geq 10^{-7}$ to $\leq 10^{-6}$ for SIL 2 SIFs according to table 3 of IEC 61508-1. A generally accepted distribution of PFD_{avg} and PFH values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{avg} value is caused by the sensor part (including the transmitter).

For a SIL 2 application operating in **low demand** mode the total PFD_{avg} value of the SIF should be smaller than 1.00E-02, hence the maximum allowable PFD_{avg} value for the sensor part would then be 3.50E-03.

For a SIL 2 application operating in **high demand** mode the total PFH value for the SIF should be smaller than 1.00E-06 1/h, hence the maximum allowable PFH value for the sensor part would be 3.50E-07 1/h.

For type B components with a hardware fault tolerance of 0 the SFF shall be > 90% for SIL 2 SIFs according to table 3 of IEC 61508-2.

λ_{SD}:	Fail safe detected
λ_{SU}:	Fail safe undetected
λ_{DD}:	Fail dangerous detected
λ_{DU}:	Fail dangerous undetected
FIT:	Failure rate [1/h]
SFF:	The number listed is for reference only. The SFF, PFD_{avg} and PFH must be determined for the complete **Safety Instrumented Function (SIF)**.
PFD_{avg}:	The PFD_{avg} was calculated for profile 2 using Markov modeling. The results must be considered in combination with PFD_{avg} values of other devices of the Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL) For SIL 1 applications, the PFD_{avg} value needs to be < 10^{-1} for the SIF. For SIL 2 applications, the PFD_{avg} value needs to be < 10^{-2} for the SIF.
T[Proof]:	It is assumed that proof testing is performed with a proof test coverage of 99%.
PFH:	= λ_{DU} (Fail dangerous undetected)
SIL AC:	SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL level

Table 7-1: Explanation of table headers for the tables showing failure rates on upcoming pages.

Under the assumptions described in the chapter before and the definitions given in chapter "Desription of the failure categories" the following table show the failure rates according to IEC 61508.

The boxes marked in light grey in the following tables mean that the calculated PFD_{avg} and/or PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in medium grey mean that the calculated PFD_{avg} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in dark grey indicate that the PFD_{avg} respectively the PFH values do not fulfill the requirements for SIL 2 of table 2 / 3 of IEC 61508-1.

Single RTD 2-/3-wire sensor

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	436	49	89.9	2.44E-04	4.57E-04	1.09E-03	2.16E-03	4.90E-08	(SIL 2)
Close coupled high stress	0	0	1184	213	84.8	1.05E-03	1.97E-03	4.74E-03	9.36E-03	2.13E-07	(SIL 2)
Extension wires low stress	0	0	777	135	85.2	6.63E-04	1.25E-03	3.00E-03	5.93E-03	1.35E-07	(SIL 2)
Extension wires high stress	0	0	7997	1940	80.5	9.45E-03	1.79E-02	4.31E-02	8.52E-02	1.94E-06	(SIL 1)

Dual RTD 3-wire sensor with activated sensor drift monitoring

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	492	41	92.3	2.08E-04	3.85E-04	9.19E-04	1.81E-03	4.10E-08	SIL 2
Close coupled high stress	0	0	2300	57	97.6	3.27E-04	5.75E-04	1.32E-03	2.55E-03	5.70E-08	SIL 2
Extension wires low stress	0	0	1338	50	96.4	2.71E-04	4.88E-04	1.14E-03	2.22E-03	5.00E-08	SIL 2
Extension wires high stress	0	0	19207	230	98.8	1.56E-03	2.56E-03	5.55E-03	1.05E-02	2.30E-07	(SIL 1)

The boxes marked in light grey in the following tables mean that the calculated PFD_{avg} and/or PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in medium grey mean that the calculated PFD_{avg} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in dark grey indicate that the PFD_{avg} respectively the PFH values do not fulfill the requirements for SIL 2 of table 2 / 3 of IEC 61508-1.

Single RTD 4-wire sensor

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	445	43	91.2	2.16E-04	4.02E-04	9.62E-04	1.89E-03	4.30E-08	SIL 2
Close coupled high stress	0	0	1347	90	93.7	4.62E-04	8.52E-04	2.02E-03	3.97E-03	9.00E-08	(SIL 2)
Extension wires low stress	0	0	892	45	95.2	2.36E-04	4.31E-04	1.02E-03	1.99E-03	4.50E-08	SIL 2
Extension wires high stress	0	0	10297	140	98.7	9.16E-04	1.52E-03	3.34E-03	6.38E-03	1.40E-07	(SIL 2)

Dual RTD 4-wire sensor with activated sensor drift monitoring. Only valid for IPAQ R520S/R520XS

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	497	40	92.6	2.03 E-04	3.76 E-04	8.97 E-04	1.76 E-03	4.00 E-08	SIL 2
Close coupled high stress	0	0	2392	45	98.2	2.72 E-04	4.67 E-04	1.05 E-03	2.03 E-03	4.50 E-08	SIL 2
Extension wires low stress	0	0	1397	41	97.1	2.29 E-04	4.07 E-04	9.40 E-04	1.83 E-03	4.10 E-08	SIL 2
Extension wires high stress	0	0	20387	50	99.8	7.28 E-04	9.45 E-04	1.60 E-03	2.68 E-03	5.00 E-08	SIL 2

The boxes marked in light grey in the following tables mean that the calculated PFD_{avg} and/or PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in medium grey mean that the calculated PFD_{avg} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in dark grey indicate that the PFD_{avg} respectively the PFH values do not fulfill the requirements for SIL 2 of table 2 / 3 of IEC 61508-1.

Single TC sensor

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	492	45	91.6	2.27E-04	4.22E-04	1.01E-03	1.98E-03	4.50E-08	SIL 2
Close coupled high stress	0	0	2297	140	94.3	7.24E-04	1.33E-03	3.15E-03	6.19E-03	1.40E-07	(SIL 2)
Extension wires low stress	0	0	1297	140	90.3	7.00E-04	1.31E-03	3.13E-03	6.16E-03	1.40E-07	(SIL 2)
Extension wires high stress	0	0	18397	2040	90.0	1.02E-02	1.90E-02	4.56E-02	8.98E-02	2.04E-06	(SIL 1)

Dual TC sensor with activated sensor drift monitoring

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	597	41	93.6	2.10E-04	3.88E-04	9.21E-04	1.81E-03	4.10E-08	SIL 2
Close coupled high stress	0	0	4387	50	98.9	3.44E-04	5.61E-04	1.21E-03	2.30E-03	5.00E-08	SIL 2
Extension wires low stress	0	0	2387	50	97.9	2.96E-04	5.13E-04	1.16E-03	2.25E-03	5.00E-08	(SIL 2)
Extension wires high stress	0	0	40197	240	99.4	2.11E-03	3.15E-03	6.27E-03	1.15E-02	2.40E-07	(SIL 1)

The boxes marked in light grey in the following tables mean that the calculated PFD_{avg} and/or PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in medium grey mean that the calculated PFD_{avg} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03 respectively 3.50E-07 1/h.

The boxes marked in dark grey indicate that the PFD_{avg} respectively the PFH values do not fulfill the requirements for SIL 2 of table 2 / 3 of IEC 61508-1.

Single TC + Single RTD 3-wire with activated sensor drift monitoring

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	544	41	93.0	2.09E-04	3.87E-04	9.20E-04	1.81E-03	4.10E-08	SIL 2
Close coupled high stress	0	0	3343	54	98.4	3.38E-04	5.72E-04	1.27E-03	2.45E-03	5.40E-08	SIL 2
Extension wires low stress	0	0	1862	50	97.4	2.83E-04	5.00E-04	1.15E-04	2.23E-03	5.00E-08	SIL 2
Extension wires high stress	0	0	29702	235	99.2	1.83E-03	2.85E-03	5.91E-03	1.10E-02	2.35E-07	(SIL 1)

Single TC + Single RTD 4-wire with activated sensor drift monitoring. Only valid for IPAQ R520S/R520XS

	Failure category				SFF	PFD_{avg} at T_{proof} =				PFH	SIL AC
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}							
	[FIT]				[%]	1 year	2 years	5 years	10 years		
Close coupled low stress	0	0	547	40	93.2	2.04E-04	3.78E-04	8.98E-04	1.77E-03	4.00E-08	SIL 2
Close coupled high stress	0	0	3390	48	98.6	3.11E-04	5.19E-04	1.14E-03	2.18E-03	4.80E-08	SIL 2
Extension wires low stress	0	0	1892	45	97.7	2.60E-04	4.55E-04	1.04E-03	2.02E-03	4.50E-08	SIL 2
Extension wires high stress	0	0	30292	145	99.5	1.42E-03	2.05E-03	3.93E-03	7.08E-03	1.45E-07	(SIL 2)

8.1 Declaration of conformity for Functional Safety (SIL)

KROHNE INOR www.inor.com	DECLARATION OF CONFORMITY Konformitätserklärung Déclaration de Conformité Försäkran om Överensstämmelse	SIL 2

INOR Process AB, P.O. Box 9125, SE-20039 Malmö, SWEDEN

declares in sole responsibility, that the product
erklärt in alleinger Verantwortung, dass das Produkt
déclare sous sa seule responsabilité que le produit
försäkrar härmed, att produkten

2-Wire Temperature Transmitters	**IPAQ C520S and IPAQ R520S** Including the following options: Einschliesslich der Optionen: Incluant en option: Inklusive följande optioner: C520XS and R520XS (X = Ex-approved version)

is suitable for the use in a safety-related application up to SIL 2 according to IEC 61508:2010 provided that the safety instructions are observed (see Safety Manual). *A consideration according to SIL 3 has not been conducted.*

An application in a higher SIL level (up to SIL 3) is in principle possible by suitable proof of operational reliability according to IEC 61511-1 - 2017 Chap. 11.5.4. The end user is solely accountable for providing the required proof, he holds ultimate responsibility.

The assessment of the safety critical and dangerous random errors lead to the following parameters:

sind unter Beachtung der Sicherheitshinweise im Sicherheitshandbuch für den Einsatz in sicherheitsgerichteten Applikationen bis SIL 2 nach IEC 61508:2010 geeignet. Eine Betrachtung nach SIL 3 hat nicht stattgefunden.

Ein Einsatz in einem höherwertigen SIL Level (bis SIL 3) ist prinzipiell durch einen geeigneten Nachweis der Betriebsbewährung gem. IEC 61511-1 – 2017 Kap. 11.5.4 möglich. Die erforderlichen Nachweise sowie die Verantwortung liegt hierbei in alleiniger Verantwortung des Betreibers. Die Untersuchung der sicherheitsrelevanten und gefährlichen, zufälligen Fehler führt zu folgenden Kenndaten:

peuvent être utilisés pour des applications de sécurité fonctionelle jusqu'à SIL 2 selon IEC 61508 :2010 en respectant les consignes de sécurité spécificées dans le Safety Manual. La prise en comte des exigences SIL 3 n'ont pas été prises en compte.

Une utilisation dans une application de niveau SIL supérieur (jusqu'à SIL 3) est en principe possible en prouvant la fiabilité opérationnelle selon les exigences IEC 61511-1 - 2017 Chap. 11.5.4. L'utilisateur final est le seul responsable pour foumir les justifications demandées. Il est le seul responsable final.

L'évaluation des défaillances aléatoires et dangereuses pour la sécurité donne les valeurs suivantes :

är användbara för säkerhetsapplikationer upp till SIL 2 enligt IEC 61508:2010 förutsatt att säkerhetsföreskrifterna följs (se Safety Manual). Någon bedömning enligt SIL 3 krav har inte gjorts.

Bedömningen av kritiska och slumpmässiga farliga fel har lett fram till följande parametrar:

Type B device, Hardware Fault Tolerance HFT = 0

IPAQ C/R 520(X)S with 4 ... 20 mA output signal

Only Electronic	Fail safe detected λ_{SD}	Fail safe undetected λ_{SU}	Fail dangerous detected λ_{DD}	Fail dangerous undetected λ_{DU}	SFF (1)	PFDavg T[proof] 1 year	PFH
Worst-case configuration	0 FIT	0 FIT	397 FIT	40 FIT	90,0 %	2,02E-04	4,04E-08 1/h

(1) Reference: *exida* FMEDA report "INOR 08/11-47 R002 V4R4"
(2) FIT = Failure rate [1/h]
(3) RISE full assessment report "Functional safety assessment of IPAQ C520*/R520* according to IEC 61508:2010".

For a complete set of figures we refer to the: Für eine komplette Reihe von Zahlen, die wir auf: Pour un ensemble complet de chiffres que nous référer à : För en komplett sammanställning av parametrar, se:	C520S, C520XS, R520S and R520XS SIL Safety Manual, 86B520S001.

Malmö, 2023-03-21	Managing Director Geschäftsführer Directeur Général Verkställande Direktör	Tobias Schulten

Inor Process AB, Mailing address: P.O. Box 9125, 200 39 Malmö, Sweden, Visiting address: Travbanegatan 10, 213 77 Malmö, Sweden
Tel.: +46 40 312 560, Fax: +46 40 312 570, www.inor.com

Dokumentnummer: DOC10.074.013

8.2 exida / FMEDA management summary

Failure Modes, Effects and Diagnostic Analysis

Project:
Universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520*

Customer:
INOR Process AB
Malmö
Sweden

Contract No.: INOR 08/11-47
Report No.: INOR 08/11-47 R002
Version V4, Revision R4; November 2018
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* in hardware version 11 and software versions IPM-SW 01.02.02 and OPM-SW 01.02.03. Table 1 gives an overview of the different configurations that belong to the considered universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520*.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Configuration overview

IPAQ C520S	Head mounted, dual input 2-wire temperature transmitter, SIL suitable
IPAQ C520XS	Head mounted, dual input 2-wire temperature transmitter, SIL suitable and intrinsically safe
IPAQ R520S	Rail mounted, dual input 2-wire temperature transmitter, SIL suitable
IPAQ R520XS	Rail mounted, dual input 2-wire temperature transmitter, SIL suitable and intrinsically safe

For safety applications only the described versions were considered. All other possible output variants or electronics are not covered by this report.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook (see [N2]) for Profile 2.

The failure rates for the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* do not include failures resulting from incorrect use of the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520*, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* are considered to be Type B[1] elements with a hardware fault tolerance of 0. For Type B elements with a hardware fault tolerance of 0 the SFF has to be ≥ 90% for SIL 2 elements according to table 2 of IEC 61508-2.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* communicate detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled for the worst case configuration of the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520*.

[1] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

Table 2: Summary – IEC 61508:2010 failure rates

	exida Profile 2 [2]
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**397**
Fail detected (detected by internal diagnostics)	309
Fail high (detected by safety logic solver)	65
Fail low (detected by safety logic solver)	23
Annunciation detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**40** [3]
Annunciation undetected (λ_{AU})	1
No effect	152
No part	46
Total failure rate (safety function)	**437 FIT**
SFF	**90%**
DC_D	**90%**
MTBF	**179 years**
SIL AC [4]	**SIL 2**

The failure rates are valid for the useful life of the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* (see Appendix 2).

[2] For details see Appendix 3.

[3] This value corresponds to a PFH of 4.04E-08 1/h. A fault reaction time of 5 minutes requires also that a connected device can detect the output state within a time that allows reacting within the process safety time.

[4] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

8.3 Type Examination Certificate

RI.
SE

TYPE EXAMINATION
CERTIFICATE
SC0266-13

Temperature transmitter "IPAQ C520*/R520* "

Issued to

INOR Process AB
Box 9125, SE-200 39 MALMÖ, Sweden
Reg.number 556346-9385
VAT.number SE556346938501

Product name

IPAQ C520*/R520*

Product description

The IPAQ C520*/R520* are programmable transmitters designed primarily for temperature measurements in the process industry. They are two-wire, 4-20 mA current loop transmitters with power supply via the current loop.
IPAQ C520*/R520* have dual sensor input channels to make elaborate supervision and diagnostics possible.

IPAQ C520*/R520* temperature transmitter	Description
IPAQ C520S	SIL
IPAQ C520XS	Ex i and SIL
IPAQ R520S	SIL
IPAQ R520XS	Ex i and SIL

Certificate

The product(s) described in this certificate have been type-examined by RISE and found to fulfil the requirements for SIL 2 of the standard IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems, part 1-3 for the following element safety function:

- Provide measurement values of the measured unit (typically temperature) with a maximum deviation from specified accuracy on 2%

The certification is based on a functional safety assessment according to IEC 61508 described in RISE report P116607:A dated 2022-12-06 and safety manual for IPAQ C520*/R520*in the currently valid revision.
Note: The SIL (Safety Integrity Level) reached for the complete safety function must be determined by the end user.

Certificate SC0266-13 | issue 4 | 2022-12-12

RISE Research Institutes of Sweden AB | Certification
Box 857, SE-50115 Borås, Sweden
+46 10 516 50 00 | certifiering@ri.se | www.ri.se

1153963

Page 1 (2)

RI.SE

TYPE EXAMINATION CERTIFICATE

Marking

Each product that conforms in all respects with the original item type-examined may display the text 'Type examined by RISE'. When this marking is applied the marking shall also contain reference to the standard IEC 61508:2010, the reached SIL (Safety Integrity Level) of the item, the number of this certificate and the serial number or equivalent of the item.

Validity

This certificate is valid until not later than 2027-12-12. The validity of this certificate can be verified by RISE.

Miscellaneous

Other terms and conditions are set out in RISE certification rules for type-examination, SPCR 123. This issue replaces all earlier issues.

Martin Tillander

Certificate SC0266-13 | issue 4 | 2022-12-12

RISE Research Institutes of Sweden AB | Certification

8.4 Return / maintenance form

Customer details

Company:	
Address:	
Contact person:	
Telephone:	
Fax:	
Email:	

Device details

Product ID:	
Serial no.:	
Reason for the return / maintenance:	

Have you performed the proof test on the product? Yes No

If yes please fill out the table with following check points.

Before you begin, configure the C520/R520 for RTD measurement 3-wire connection on both channels. Select measuring range 0...+100°C, output – dedicated dynamic variable Ch1 select sensor break and sensor short circuit to downscale, thereafter to upscale value.

Also check the Sensor backup function by selecting Sensor backup. This is done in step 4.

Proof test check points

Step	Description	Yes	No	Comments
1	Connect the selected sensors on Ch 1 and Ch2 and check for the output range value is within measuring range.			
2	Simulate sensor break for each single wire (on terminals 1...5) and check the output value (≥21 mA) / (≤3.6 mA).			
3	Simulate sensor short between 1...5 terminals and check the output value (≥21 mA) / (≤3.6 mA).			
4	Simulate sensor break or sensor short (one error at a time) for sensor connected on Ch 1. Check if the transmitter will switch automatically over to measuring on Ch 2.			

Send goods including this document to

Inor Process AB
PO Box 9125
SE-200 39 Malmö
Sweden
Phone: +46-(0)40-312 560
Fax: +46-(0)40-312 570
E-mail: support@inor.se

Subsidiaries

Inor Transmitter Oy
Unikkotie 13
FI-01300 Vantaa
Finland
Phone: +358-(0)10-4217900
Fax: +358-(0)10-4217901
E-mail: myynti@inor.fi
Web: www.krohne-inor.fi

Inor Transmitter GmbH
Am See 24
D-47279 Duisburg
Germany
Phone: +49-(0)203 7382 762 0
Fax: +49-(0)203 7382 762 2
E-mail: info@inor-gmbh.de
Web: www.inor-gmbh.de

Inor North America
55 Cherry Hill Road
Beverly, MA 01915
United States
Phone: +1 978 826 6900
Fax: +1 978 535 1720
E-mail: inor-info@krohne.com
Web: www.inor.com

The current list of all INOR contacts and addresses can be found at:
www.inor.com

11/2022 - 86B520S001 - AD 520 SIL R1.5 en