



C520S/C520XS R520S/R520XS

Safety manual SIL

HART Temperature Transmitter for up to SIL 2 applications



INOR

1	Introduction	3
1.1	Field of application	3
1.2	User benefits	3
1.3	Manufacturer's safety instructions	3
1.3.1	Notes about the documentation	3
1.4	Relevant standards / Literature	4
2	Terms and definitions	5
2.1	Terms and definitions	5
3	Functional principle	6
3.1	Functional principle	6
4	Safety function	8
4.1	Description of the failure categories	8
4.2	The specification of the safety function.....	8
4.3	Redundancy.....	10
4.3.1	Sensor Drift	10
4.3.2	Sensor Backup	10
5	Project planning	11
5.1	Applicable device documents	11
5.2	Project planning, behavior 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	Assumption	14
7.2	Specific safety-related characteristics C520S / C520XS / R520S / R520XS....	14
8	FMEDA summary	18
8.1	FMEDA summary / Exida report.....	18
9	Annex 1: Return form, requested maintenance of devices	21
10	Declaration of conformity for Functional Safety (SIL)	22

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 is the rail mounted version of C520.

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

The 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 61508-2.

1.2 User benefits

- This intelligent HART temperature transmitter is designed to perform temperature measurements of solids, fluids and gases up to SIL 2 according special safety requirements of IEC 61508-2 (see exida FMEDA report INOR 08-11-47 R002 V2R1).
- 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 INOR Software ConSoft and INOR USB-kit ICON must be used.
- Continuous measurement
- Easy commissioning

SIL 2 requirements are based on the standard IEC 61508-2 current at the time of certification.

The C520S/C520XS/R520S/R520XS certification involves the HW assessment of the products with an FMEDA.

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.

1.3.1 Notes about the documentation

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 part 2	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	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 60079-0:2006	Electrical apparatus for explosive gas atmospheres – Part 0: General requirements
EN 60079-11:2007	Explosive atmospheres – Part 11: Equipment protection by intrinsic safety “i”
EN 60079-15:2005	Electrical apparatus for explosive gas atmospheres – Part 15: Construction, test and marking of type of protection “n” electrical apparatus
EN 60079-26:2007	Explosive atmospheres – Part 26: Equipment with equipment protection level (EPL) Ga

Table 1 Supported standards during the development of C520/R520

2.1 Terms and definitions

Acronym	Description
DC _D	Diagnostic Coverage of dangerous failure. Diagnostic coverage is the ratio of the detected failure rate to the total failure rate
FIT	Failure In Time (1×10^{-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 demands 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 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
Type A component	"Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	"Complex" subsystem (at least one failure mode are not well defined); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

Table 2 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 transmitters is based on the analog to digital and back to analog signal conditioning. The temperature sensor used is either a Resistance Temperature Device (RTD) or a thermocouple (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.

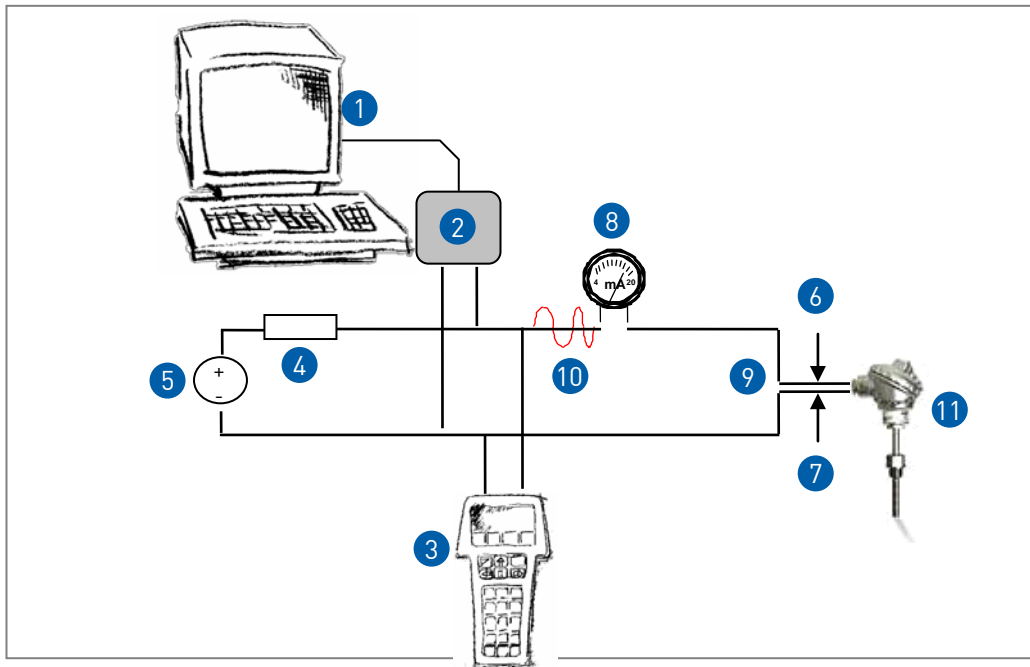


Figure 1: The functional principle of C520

- 1 Primary Master
- 2 HART modem
- 3 Secondary master
- 4 Load $\geq 250\Omega$
- 5 DC power supply
- 6 Terminal 6 (+ on C520/C520X)
- 7 Terminal 7 (- on C520/C520X)
- 8 Milliampere-meter Load $\geq 250\Omega$
- 9 4...20 mA
- 10 HART
- 11 C520/C520X connected with sensor in the sensor head

The low level analog 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 analog 4-20 mA output signal.

The C520/R520 are smart temperature transmitters 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 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	Failure of a component which is not part of the safety function but part of the circuit diagram

Table 3 Definitions of the failure rate during the diagnostic calculations for C520

4.2 The 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 NE43.

The failure information is defined by two selectable alarm levels: Fail Low (Downscale $\leq 3,6$ 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 then 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 also password-protected. It can also be changed by HART communication, still password-protected.

When the SIL-switch is activated the following limitations to configuration apply:

Function	Active/Not Active	Output	Alarm level *
Sensor Break	Active	4-20 mA / 20-4 mA	$\leq 3,6$ mA / $\geq 21,0$ mA
Sensor Short	Active	4-20 mA / 20-4 mA	$\leq 3,6$ mA / $\geq 21,0$ mA
Low isolation	Not active		
System error **	Active	4-20 mA / 20-4 mA	$\leq 3,6$ mA / $\geq 21,0$ mA
Sensor Drift (Dual sensors needed) ***	Active / Not Active selectable	4-20 mA / 20-4 mA	$\leq 3,6$ mA / $\geq 21,0$ mA

* : For some system failures the alarm output will toggle between a high alarm level ($\geq 21,0$ mA) and a low alarm level ($\leq 3,6$ 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").

** : System errors = failures in the software or hardware detected by the diagnostics in the transmitter.

*** : The Sensor Drift function is valid from SW-versions; IPM-SW 01.01.03 and OPM-SW 01.01.04 and HW-versions 5 and later, implemented in transmitters with Serial No 1006.xxxxxx or later. Serial No 1006.xxxxxx means manufactured week 6 in 2010 and this information is found on the label or it can be read from the transmitter via ConSoft. The SW-versions and HW-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 Thermocouple sensors
- 1x Thermocouple sensor and 1x 3W RTD sensor
- 1x Thermocouple sensor and 1x 4W RTD sensor (only valid for R520/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.

NOTE! 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.

OBSERVE! 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 documents

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

Document name	Description and application
86DC520001	Data sheet C520
86B5200001	Handbook (User instructions)
INOR 08/11-47 R002 V2R1	Exida FMEDA report

Table 4 Applicable user documentation useful for C520S/R520S

5.2 Project planning, behavior during operation and malfunction

- Under normal conditions the useful operating lifetime is 10 years (8-12 years).
- Requirements in the Handbook (User instructions) have to be kept.
- Repair and inspection intervals are based on safety calculation.
- For repairs or recalibration of the C520S/R520S, use the original or a suitable secure packing, include a properly filled out return form (see attachment) and send the device to INOR for service. **NOTE!** It is of vital importance that all type of failures of the equipment are reported to INOR Process AB 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 at Inor Process AB 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

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 C520S / R520S
- 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 C520S/R520S.

Proof test of the transmitter C520S/R520S should be made based on the required PFD depending on the used sensor, see tables in chapter 7. 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 C520S/R520S transmitter
- Replacement of the old connected temperature sensor by new ones
- Reconfiguration of the C520S /R520S device
- At need of the C520S/R520S relocation

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 transmitter C520S/R520S is simulated and tested for the internal errors in the hardware and the firmware.

How to run the proof test manually.

Step	Description
1.	Connect C520S / R520S to the PC via USB interface
2.	Start ConSoft (Check version Help menu->About)
3.	Identify C520S / R520S by clicking on "Read from transmitter" button
4.	Decide the choice of the SIL password (default value is '0000')
5.	Configure the C520S / R520S by selecting "Sensors" tab in the C520 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 C520 / R520 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 k Ω
7.3.	Select check box for sensor backup
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 5 Proof test configuration

Simulate and check for following

Step	Description:	Yes	No	Comments
1.	Connect the selected Sensors on Ch 1 and Ch2, 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 Proof test check points

Repeat configurations points 7. to 8.2 in the Table 5 and change to Down scale error value ($\leq 3,6$ mA). Repeat all check points in the Table 6. (to be sure the transmitter is not stuck in some of conditions).

7.1 Assumption

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

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- External power failures 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.

7.2 Specific safety-related characteristics C520S / C520XS / R520S / R520XS

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 PFDavg and PFH values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFDavg value is caused by the sensor part (including the transmitter). For a SIL 2 application operating in low demand mode the total PFDavg value of the SIF should be smaller than $1,00E-02$, hence the maximum allowable PFDavg 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.

The boxes marked in yellow (■) in the following tables mean that the calculated PFDavg 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 green (■) mean that the calculated PFDavg 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 red boxes (■) indicates that the PFDavg respectively the PFH values do not fulfill the requirements for SIL 2 of table 2 / 3 of IEC 61508-1.

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.

Under the assumptions described in 7.1 and the definitions given in section 4.1 the following tables show the failure rates according to IEC 61508-1/-2:

Sensor Type	Failure category [FIT] (5)				SFF	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		SFF (1)	1 year	2 years	5 years		
Single RTD 2/3w sensor											
Close coupled low stress	0	146	427	49	92,1 %	2,44 E-04	4,57 E-04	1,09 E-03	2,16 E-03	4,90 E-08	SIL 2
Close coupled high stress	0	146	1175	213	86,1 %	1,05 E-03	1,97 E-03	4,74 E-03	9,36 E-03	2,13 E-07	(SIL 2)
Extension wires low stress	0	146	768	135	87,1 %	6,63 E-04	1,25 E-03	3,00 E-03	5,93 E-03	1,35 E-07	(SIL 2)
Extension wires high stress	0	146	7988	1940	80,7 %	9,45 E-03	1,79 E-02	4,31 E-02	8,52 E-02	1,94 E-06	(SIL 1)

λ_{SD} = Fail safe detected

λ_{SU} = Fail safe undetected

λ_{DD} = Fail dangerous detected

λ_{DU} = Fail dangerous undetected

(1) The numbers listed are for reference only. The SFF, PFDavg and PFH must be determined for the complete Safety Instrumented Function (SIF)

(2) SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL level

(3) It is assumed that proof testing is performed with a proof test coverage of 99%.

(4) The PFDavg was calculated for profile 2 using Markov modeling. The results must be considered in combination with PFDavg 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 PFDavg value needs to be $< 10^{-1}$ for the SIF

For SIL 2 applications, the PFDavg value needs to be $< 10^{-2}$ for the SIF

(5) FIT: Failure rate [1/h]

(6) PFH = λ_{DU} (Fail dangerous undetected)

Sensor Type	Failure category [FIT] (5)				SFF	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		SFF (1)	1 year	2 years	5 years		
Dual RTD 3w sensor (*)											
Close coupled low stress	0	146	483	41	93,9 %	2,07 E-04	3,85 E-04	9,18 E-04	1,81 E-03	4,10 E-08	SIL 2
Close coupled high stress	0	146	2291	57	97,7 %	3,27 E-04	5,74 E-04	1,35 E-03	2,55 E-03	5,70 E-08	SIL 2
Extension wires low stress	0	146	1329	50	96,7 %	2,71 E-04	4,87 E-04	1,14 E-03	2,22 E-03	5,00 E-08	SIL 2
Extension wires high stress	0	146	19198	230	98,8 %	1,56 E-03	2,56 E-03	5,55 E-03	1,05 E-02	2,30 E-07	(SIL 1)

(*): Sensor drift monitoring is activated

Sensor Type	Failure category [FIT] (5)				SFE	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Single RTD 4w sensor					SFF (1)					PFH (6)	
Close coupled low stress	0	146	436	43	93,1 %	2,16 E-04	4,02 E-04	9,62 E-04	1,89 E-03	4,30 E-08	SIL 2
Close coupled high stress	0	146	1338	90	94,2 %	4,62 E-04	8,52 E-04	2,02 E-03	3,97 E-03	9,00 E-08	(SIL 2)
Extension wires low stress	0	146	883	45	95,8 %	2,36 E-04	4,31 E-04	1,02 E-03	1,99 E-03	4,50 E-08	SIL 2
Extension wires high stress	0	146	10288	140	98,6 %	9,15 E-04	1,52 E-03	3,34 E-03	6,38 E-03	1,40 E-07	(SIL 2)

Sensor Type	Failure category [FIT] (5)				SFE	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Dual RTD 4w sensor (**)					SFF (1)					PFH (6)	
Close coupled low stress	0										
Close coupled high stress	0										
Extension wires low stress	0										
Extension wires high stress	0										

** : Sensor drift monitoring is activated; Only for IPAQ R520S / R520XS; In preparation

Sensor Type	Failure category [FIT] (5)				SFE	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Single TC sensor					SFF (1)					PFH (6)	
Close coupled low stress	0	146	483	45	93,3 %	2,26 E-04	4,22 E-04	1,01 E-03	1,98 E-03	4,50 E-08	SIL 2
Close coupled high stress	0	146	2288	140	94,5 %	7,325 E-04	1,33 E-03	3,15 E-03	6,19 E-03	1,40 E-07	(SIL 2)
Extension wires low stress	0	146	1288	140	91,1 %	6,99 E-04	1,31 E-03	3,13 E-03	6,16 E-03	1,40 E-07	(SIL 2)
Extension wires high stress	0	146	18388	2040	90,0 %	1,02 E-02	1,90 E-02	4,56 E-02	8,98 E-02	2,04 E-06	(SIL 1)

Sensor Type	Failure category [FIT] (5)				SFF	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Dual TC sensors					SFF (1)					PFH (6)	
Close coupled low stress	0	146	588	41	94,7 %	2,10 E-04	3,88 E-04	9,21 E-04	1,81 E-03	4,10 E-08	SIL 2
Close coupled high stress	0	146	4378	50	98,9	3,44 E-04	5,61 E-04	1,21 E-03	2,30 E-03	5,00 E-08	SIL 2
Extension wires low stress	0	146	2378	50	98,0%	2,96 E-04	5,13 E-04	1,16 E-03	2,25 E-03	5,00 E-08	(SIL 2)
Extension wires high stress	0	146	40188	240	99,4 %	2,11 E-03	3,15 E-03	6,27 E-03	1,15 E-02	2,40 E-07	(SIL 1)

Sensor Type	Failure category [FIT] (5)				SFF	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Single TC + Single RTD 2/3W					SFF (1)					PFH (6)	
Close coupled low stress	0	146	535	41	94,3 %	2,09 E-04	3,86 E-04	9,20 E-04	1,81 E-03	4,10 E-08	SIL 2
Close coupled high stress	0	146	3334	54	98,4 %	3,38 E-04	5,72 E-04	1,27 E-03	2,45 E-03	5,40 E-08	SIL 2
Extension wires low stress	0	146	1853	50	97,5 %	2,83 E-04	5,00 E-04	1,15 E-04	2,23 E-03	5,00 E-08	SIL 2
Extension wires high stress	0	146	29693	235	99,2 %	1,83 E-03	2,85 E-03	5,93 E-03	1,10 E-02	2,35 E-07	(SIL 1)

Sensor Type	Failure category [FIT] (5)				SFF	PFDavg (4) @ Tproof (3) =				PFH	SIL AC (2)
	λ_{SD} [FIT]	λ_{SU} [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]		1 year	2 years	5 years	10 years		
Single TC + Single RTD 4W					SFF (1)					PFH (6)	
Close coupled low stress	0	146	538	40	94,4 %	2,04 E-04	3,77 E-04	8,98 E-04	1,76 E-03	4,00 E-08	SIL 2
Close coupled high stress	0	146	3381	48	98,6 %	3,10 E-04	5,18 E-04	1,14 E-03	2,18 E-03	4,80 E-08	SIL 2
Extension wires low stress	0	146	1883	45	97,8 %	2,60 E-04	4,55 E-04	1,04 E-03	2,02 E-03	4,50 E-08	SIL 2
Extension wires high stress	0	146	30283	145	99,5 %	1,42 E-03	2,05 E-03	3,93 E-03	7,08 E-03	1,45 E-07	(SIL 2)

8.1 FMEDA summary / Exida report

**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 V2, Revision R1; March 2010

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights on the format of this technical report reserved.



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 5 and software versions OPM-SW 01.01.04 and IPM-SW 01.01.03. 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 B¹ subsystems with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF has to be $\geq 90\%$ for SIL 2 subsystems according to table 2 of IEC 61508-2.

It is important to realize that the "no effect" failures are included in the "safe" failure category according to IEC 61508:2000. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

A user of the universal dual-input 2-wire transmitters IPAQ C520* and IPAQ R520* can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.3.1 along with all assumptions.

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 $\leq 3,6\text{mA}$ or $\geq 21\text{mA}$. 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 subsystem: "Complex" subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.



Table 2: Summary – IEC 61508 failure rates

<i>exida</i> Profile 2 ²	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	146
Fail safe undetected	0
No effect	145
Annunciation undetected (95%)	1
Fail Dangerous Detected (λ_{DD})	388
Fail detected (detected by internal diagnostics)	294
Fail high (detected by safety logic solver)	65
Fail low (detected by safety logic solver)	29
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	40³
Fail dangerous undetected	40
Annunciation undetected (5%)	0
No part	44
Total failure rate (safety function)	574 FIT
SFF⁴	92.9%
DC_o	91%
MTBF	185 years
SIL AC⁵	SIL2

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 4.02E-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 The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵ 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.

Return / Maintenance Form

Customer details:

Customer:	Description
Company:	
Address:	
Contact person:	
Telephone:	
Fax:	
Mail:	

Device details:

Device details:	Description
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 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, therefore to Upscale value.

Select even Sensor backup.

Step	Description:	Yes	No	Comments
1.	Connect the selected Sensors on Ch 1 and Ch2, check for the output range value is within measuring range.			
2.	Simulate sensor break for each single wire (on terminals 1-5), check the output value (≥ 21 mA) / ($\leq 3,6$ mA)			
3.	Simulate sensor short between 1-5 terminals and check the output value (≥ 21 mA) / ($\leq 3,6$ 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 gods including this document to:

INOR Process AB, Service, Slipstengatan 6, SE-213 76 Malmö, SWEDEN

 www.inor.com Member of the KROHNE Group	DECLARATION OF CONFORMITY Konformitätserklärung Déclaration de Conformité Försäkran om Överensstämmelse	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

INOR Process AB, Slipstengatan 6, P.O. Box 9125, SE-20039 Malmö, SWEDEN

declares in sole responsibility, that the product
 erklärt in alleiner 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 61508-2:2000 provided that the safety instructions are observed (see Safety Manual). 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 61508-2:2000 geeignet. Die Untersuchung der sicherheitsrelevanten und gefährlichen, zufälligen Fehler führt zu folgenden Kenndaten:

peuvent être utilisés pour des applications de sécurité fonctionnelle jusqu'à SIL 2 selon IEC 61508-2 :2000 en respectant les consignes de sécurité spécifiées dans le Safety Manual. L'évaluation des défaillances aléatoires et dangereuses pour la sécurité donne les valeurs suivantes :

är användbara för säkerhetsapplikationer upp till SIL 2 enligt IEC 61508-2:2000 förutsatt att säkerhetsföreskrifterna följs (se Safety Manual). Bedömningen av kritiska och slumpmässiga farliga fel har lett fram till följande parametrar:

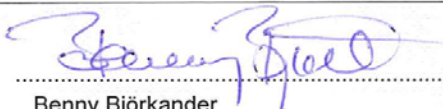
Type B device, Hardware Fault Tolerance HFT = 0

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 (2)	146 FIT	388 FIT	40 FIT	92,9 %	2,00E-04	4,02E-08 1/h

(1) Reference : *exida* FMEDA report "INOR 08/11-47 R002 V2R1"

(2) FIT = Failure rate [1/h]

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, 2010-03-29	Managing Director Geschäftsführer Directeur Général Verkställande Direktör	 Benny Björkander
----------------------	-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------