JUMO Safety Manual

for pressure transmitter and
Differential pressure transmitter

Typ 403022 Typ 403023 Typ 403026

Typ 403025

Safety Manual

40302202T99Z001K000

JUMO

Contents

Contents

1 Safety Manual

1.1 General information

The JUMO dTRANS p20 device family consists of the following types:

- Type 403022 JUMO dTRANS p20 DELTA
- Type 403023 JUMO dTRANS p20 DELTA Ex d
- Type 403025 JUMO dTRANS p20
- Type 403026 JUMO dTRANS p20 Ex d

1.2 Intended use

The pressure transmitters JUMO dTRANS p20 (type 403025) and JUMO dTRANS p20 Ex d (type: 403026) and the differential pressure transmitter JUMO dTRANS p20 DELTA (type 403022) and JUMO dTRANS p20 DELTA Ex d (type 403023) are devices for pressure/differential pressure measurement in gases and fluids without solids content.
They are deployed in safety technology systems for minimum, maximum and range monitoring in compliance with the requirements of the IEC 61508:2010 series of standards.
Types 403025/403026 and types 403022/403023 are identical in terms of electronics and software; they differ only in terms of the mechanical layout. The precise functionality and the design type (e.g. the measuring ranges or the process connections) are driven by the respective operating conditions.

The safety function of the stated JUMO dTRANS p20 series relates exclusively to measuring pressures. The transducer generates a process-related measured pressure value, which is transmitted to the automation system as a 4 - 20 mA output signal. The current output is the only safety-related signal of the transmitter.
The HART® protocol is only used to configured the pressure transmitter.

The user is responsible for the correct choice of material required for the process, and for complying with the specifications stated in the data sheet (e.g. the process and ambient temperature, positive pressure ranges, pressure surges).

Unprofessional or unintended use of the device can lead to application-related risks (e.g. corrosion due to selecting the wrong

material, or product spills due to incorrectly mounting or adjusting the device).

JUMO shall not be held liable for damage resulting from unprofessional or unintended use.

The safety function applies exclusively to the linear output function (classical pressure measurement).

1.3 Validity of the Safety Manual

The functional safety assessment in this Safety Manual and the representations of the certificates relate exclusively to devices with the basic type extension "2" and the software versions 236.02.01 or 236.03.01.

1.4 Other applicable device documentation

The steps, values, and requirements specified in the Operating Manuals also supplied, relating to installation, the electrical connection, operation, and maintenance, must be observed.

1.5 Pertinent standards

Failure of the devices can affect the safety of persons and/or the safety of the environment.

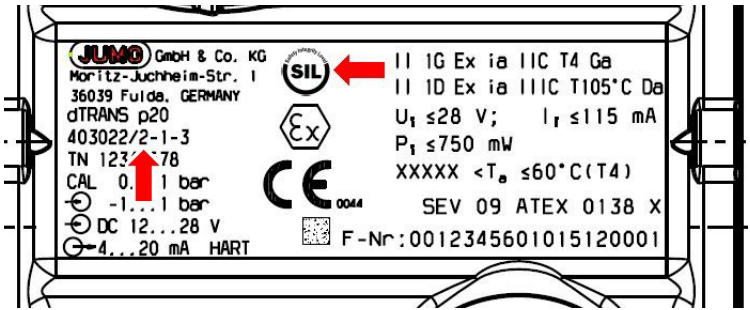
To assess the device in terms of functional safety, certification according to IEC 61508 part 1-3 has been performed.

The pressure transmitters type 403022, -23, -25, and -26 with the basic type extension "2" and the software versions 236.02.01 or 236.03.01 meet these requirements.

- For the safety function up to SIL 2 according to IEC 61508 part 1-3: Functional safety of electrical/electronic/programmable electronic safety-related systems

1.6 Nameplate

The SIL identification marking and the correct basic type extension must be stated on the nameplate as follows (see arrows)!



1.7 Safety function

The safety function relates exclusively to measuring pressures. The pressure transmitter generates a process-related measured pressure value, which is transmitted to the logic unit as a 4 - 20 mA output signal.

The current output is the only safety-related signal of the transmitter; it delivers:

- The valid output signal between 3.8 mA and 20.5 mA in the sense of the NAMUR recommendation NE 43
- An output signal in case of malfunction of ≤ 3.6 mA or ≥ 21.0 in the sense of the NAMUR recommendation NE 43
- A safety accuracy of: 2% plus the accuracy specifications stated in the data sheet
- Safety response time: A watchdog timeout of 2.0 s has been incorporated into the programming to safeguard against uncontrolled software behavior. During a reset phase triggered by this, a minimum error current is always output independently of the configured error current!
- **Note:** After 3 device resets, an error must be assumed.

For reliable error detection, the logic unit must be able to detect and evaluate HI alarms (≥ 21.0 mA) and LO alarms (≤ 3.6 mA).

Important information:

- Parameter P2 (current start of measurement) must be configured to 4 mA and P3 (current end of measurement) must be configured to 20 mA.
- Parameter P11 ("Characteristic") must be set to **LIN = linear**.

Important information:

The pressure transmitter's output does not fulfill any safety function during the following activities:

- During changes in the configuration level
- During simulation ("P8 current generator")
- When HART® Multidrop is used

- The safety relevant parameters/settings were entered prior to safety relevant operation via the local controls or using setup communication.
  Check the parameters/settings on the device's display.

⇨ Operating manual, chapter 7 "Operation"

Important information:

The device does not implement any "network and system security measures" according to the IEC 62443 series of standards. This means that only the "safety" aspect is considered.

- The interfaces (JUMO setup or HART® protocol) and local operation may only be used to read/validate data during safety operation. Safe parameterization is not possible during operation.
- Parameterization must be locked following startup

⇨ Operating Manual, chapter 7 (Parameters P10 Key)

- Parameter P9 Err must NOT be set to **LASt=last value**, as error detection by the downstream logic unit is not possible with this setting. The following may be used: ErLo = 3.6 mA or ErHi = 21.6 mA
- On startup, a complete functional test must be performed.

⇨ Chapter 1.9.2 "Testing the safety function"

1.7.1 Set requirements for the test facility

The following requirements are mandatory:

1.) For the layout of the plant according to IEC 61508 the operator must make sure that the entire plant meets the qualitative and quantitative requirements of the respective standard.

2.) Generally, for the redundant use of the system (HFT > 0), the subsequent logic has to carry out an evaluation of the measuring signals 4 to 20 mA (e.g. through cross comparison).

3.) The provisions in the user documentation are mandatory.

4.) After the installation of the pressure transmitter into the plant, a validation of the safety function must take place.

1.8 Safety-relevant parameters

The following parameters were calculated by means of a component FMEDA under the following conditions:

- Error models corresponding to requirements of IEC 61508 for conformity with SIL1 or SIL2
- Path 2_H and 2_S were selected for the certification.

Assumption: The mean temperature, which is observed over an extended period of time, is 40 °C.

1.8.1 Failure rates and SSF for type 403022, -23, -25, and -26

Type	Architecture	λ_{sd} [Fit]	λ_{su} [Fit]	λ_{dd} [Fit]	λ_{du} [Fit]	SFF	DC	$MTTF_d$ in years	MTBF in years	PTC	PFD_{avg}	PFH
403022 403023	1oo1	54.78	264.62	265.32	123.92	82.51%	68.16%	293.27	95.07	58.36%	$2.60 \bullet 10^{-3}$	$1.24 \bullet 10^{-7}$
403025 403026	1oo1	69.25	276.58	310.64	193.16	77.27%	61.66%	226.59	85.52	73.83%	$2.87 \bullet 10^{-3}$	$1.93 \bullet 10^{-7}$

MTTR = MRT = 72 h

Lifetime: 87600 h (10 years)

Interval for regular inspection (T1):
The values for PFD_{avg} in the table were computed for T1 = 8760 h (1 year).

1.8.2 Calculation of PFD_{avg}

- Regular inspection is required for a SIL 2-certified system.
- The operator defines the test interval; this must be taken into consideration when evaluating the probability of a hazardous failure PFD_{avg} of the sensor system.
  In the case of a single-channel system architecture, the mean probability of a hazardous failure PFD_{avg} of the transmitter is a function of the inspection interval T1, the failure rate of hazardous, undetectable errors, λ_{du}, the **P**roof **T**est **C**overage PTC and the assumed lifetime can be approximated as:

$$PFD_{avg} = \lambda_{dd} \cdot MTTR + PTC \cdot \lambda_{du} \cdot \left(\frac{T1}{2} + MRT \right) + (1 - PTC) \cdot \lambda_{du} \cdot \frac{Lifetime}{2}$$

MTTR = MRT = 72 h

Lifetime: Maximum of 87600 h (10 years)

Interval for regular inspection (T1) (the operator can define this itself):
The values for PFD_{avg} in the table were computed for T1 = 8760 h (1 year).

1.8.3 Performing regular inspection

During regular inspection, the output signal of the transmitter must be checked for compliance with the required accuracy at two different points (e.g. start and end value of the pressure measuring range).

- If the device exhibits anomalies during regular inspection, such as deviations in accuracy or error messages, then the device must be replaced.
- After the lifetime of 10 years expires, the systems no longer meet the requirements according to their SIL certification and must be replaced.

1.8.4 Safety-relevant system properties

Safety feature	Requirement / comment
SIL	SIL 1 or SIL 2 ⇨ Chapter 1.8.5
Operating mode in terms of safety function	Operating mode with lower and higher demand rate possible on a customer-specific basis
Safety function	Measuring of pressures via the standard signal 4..20 mA current loop
Nominal measuring range	See accuracy data in the data sheet
Safety accuracy	2% plus the accuracy specifications stated in the data sheet
Subsystem type	Type B
Safety architecture	1oo1
Systematic Capability	SC = 2
Hardware error tolerance	HFT = 0
Average failure probability of a safety function on demand (overall system)	SIL 2: Low demand: $PFD_{avg} < 10^{-2}$ High-demand: $PFH < 10^{-6}$
Interval for regular inspection (T1)	1 year (the operation can define this interval itself.) ⇨ Chapter 1.8.2
Lifetime	Maximum of 10 years

Only devices with the following features have these properties:

- Software versions 236.02.01 or 236.03.01
- Basic type extension "2"
- Temperature range -40 to +85 °C
- Voltage supply range: DC 12 to 36 V (ATEX Ex ia: DC 12 V to 28 V)

1.8.5 Determining the SIL Level

Due to the architecture (1oo1) of the pressure transmitter categorized as type B, the hardware fault tolerance = 0.
This results in the following in line with architecture path 2H of IEC 61508-2:

- The pressure transmitters can be deployed in single-channel mode (i.e. HFT = 0) for low-demand applications (PFD) up to SIL 2
- The pressure transmitters can be deployed in single-channel mode (i.e. HFT = 0) for high-demand applications (PFD) up to SIL 1, and redundantly (i.e. HFT ≥ 1) up to SIL2.

Important information:

The devices use a single-channel design (1oo1 architecture) and thus have a HFT = 0.

Two pressure transmitters whose output signals are evaluated by a safety-technology logic unit must be provided for a HFT = 1.

1.8.6 Example of calculating the overall accuracy of the safety function

To determine the overall accuracy of the safety function, add a safety accuracy of 2% of the nominal measuring range to the accuracy data from the data sheet.

The safety accuracy describes the maximum impact of a random single error on the measured value that is still classified as non-critical.
The resulting overall accuracy is used to add a safety reserve for process monitoring.
Such that the plant is still safely shut down if a random, single error occurs.
Overall accuracy of the safety function = ± [accuracy specification from the data sheet + 2% safety accuracy].

Example:
Fill level check and overfill monitoring of a liquid tank with a filling height of 5 meters.

Accuracy specification from the data sheet, incl. long-term stability: e.g. 0.2%

Additional safety accuracy: 2.0%

Overall accuracy of the safety function: 2.2%

An accuracy of 2.2% relative to 5 meters in height results in 0.11 m.

The JUMO dTRANS p20 transmitter checks the level and outputs this to the process control system as a 4-20 mA signal.

The overfill safeguard in process monitoring must be set to a value of (5 m – 0.11 m = **4.89 m**).

This ensures safe switch-off before overfilling even if a random, one-off error occurs.

1.8.7 Average probability of dangerous failure on demand PFD_{avg}

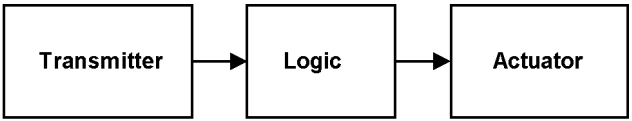
The following table shows how the "Safety Integrity Level" (SIL) depends on the "average probability of dangerous failures of a safety function of the entire safety-related system" (PFD_{avg}) according to IEC 61508.
The "low demand mode" is considered, i. e. the demand rate for the safety-related system is once a year on average.

Table low demand PFD according to IEC 61508

Safety Integrity Level (SIL)	Operating mode with low demand rate PFD_{avg} (low demand mode)
4	$\geq 10^{-5}$ ... $<10^{-4}$
3	$\geq 10^{-4}$ ... $<10^{-3}$
2	$\geq 10^{-3}$ ... $<10^{-2}$
1	$\geq 10^{-2}$ ... $<10^{-1}$

The sensor, logic unit, and actuator together form a safety-related system that performs a safety function. The "average probability of dangerous failures of the entire safety-related system" (PFD_{avg}) is usually divided up into the sensor, logic unit, and

actuator subsystems according to the following diagram.



Typical distribution of the "average probability of dangerous failures of a safety function on demand" (PFDavg) across the subsystems

The specifications relating to functional safety relate to the transmitter as a subsystem (sensor).

1.8.8 Average frequency of dangerous failure per hour PFH

The following table shows how the Safety Integrity Level (SIL) depends on the "average frequency of a dangerous failure per hour" (PFH) according to IEC 61508.

Table high demand PFH according to IEC 61508

Safety Integrity Level (SIL)	Operating mode with high demand rate PFH (high-demand mode)
4	$\geq 10^{-9}$ ... $<10^{-8}$
3	$\geq 10^{-8}$ ... $<10^{-7}$
2	$\geq 10^{-7}$ ... $<10^{-6}$
1	$\geq 10^{-6}$ ... $<10^{-5}$

1.8.9 Safety-relevant system properties

The pressure transmitters are implemented as a 1oo1 architecture.

The device software monitors numerous variables for valid range limits.
Additionally, the register content is read back and possibly corrected for comparison.
An activated watchdog with a timeout time of 2 s provides protection against uncontrolled software behavior.

1.9 Device parameterization

The following steps must be performed for safe device parameterization:

Step	Action
1	Adjust all safety relevant parameters via the Parameter level ⇨ Operating manual chapter 7.3 Level concept Parameterization is possible via the control knob, and via setup or the HART® interface.
2	Check the safety function; see ⇨ Chapter 1.9.2 "Testing the safety function"
3	Lock the parameters ⇨ Operating manual, chapter 7.3.2 (Parameter P10 Key lock)

1.9.1 Setting safety-relevant parameters

Fundamentally, all parameters must be configured to reflect the requirements of the safety-related system. We recommend documenting the parameters you set.

JUMO dTRANS p20 SIL start-up protocol
Device designation:
Measuring point:
Serial number:
Company:
Segment test successful? YES [ ]

Parameter	Explanation	Selection options *	Default value	Approved?
P0 Den	Density correction	0.01 … **1.00** … 99.99		
P1 Uni	Pressure measuring unit	inH2O, inHG, ftH2O, mmH2O, mmHG PSI, bar, mbar, kg/cm^2, kPa, TORR, MPa, mH2O		
P2 mA	Current measurement start	**4.00 mA** (no other values allowed)		
P3 mA	Current measurement end	**20.00 mA** (no other values allowed)		
P4 sec	Attenuation	**0.0** … 100.0 s		
P5 RS	Measurement start	Nominal measuring range		
P6 RE	Measurement end	Nominal measuring range		

JUMO dTRANS p20 SIL start-up protocol				
P8 mA	Current generator	must **not** be activated if the safety function is executed		
P9 Err	Current in case of malfunction	ErLo = 3.6 mA **ErHi = 21.6 mA** ~~LASt = last value~~		
P10 Key	Key lock	**O = no lock** LA = all, interface released LO = all, without measurement start LS = all, without measurement start and end LALL = all, incl. interface Switch to "LALL" after device parameterization		
P11 Chr	Characteristic line	**Lin = linear** ~~SLin = linear to start of square root extraction~~ ~~SoFF = off until start of square root extraction~~		
P15 OFF	Pressure value offset (zero offset)	Nominal measuring range		
*** Values in bold indicate the defaults** * ~~Crossed out~~ values must not be set				
Date:				
Time:				
Tested by:				
Signature				

1.9.2 Testing the safety function

Preferably test the safety function in installed state. If this is not possible, you can also test the safety function in removed state. Make sure that the pressure transmitter is installed in the same installation position as in the plant for testing.

Precondition: Key lock/Locking is deactivated.

The device is **not** safety compliant during this test!

We recommend performing the following steps:

Step	Action
1	Check the status for warnings and error messages
2	Check the parameters listed in Chapter 1.9.1 "Setting safety-relevant parameters"
3	Check the measuring range limits
4	Check the zero point, e.g. in depressurized status
5	Check the upper end of the set measuring span (P6 RE) by applying a defined pressure
6	Activate the key lock/locking (parameter P10)
7	Create a new start-up protocol

⇨ Operating manual, chapter 7 "Operation"

1.10 Behavior during operation and in case of malfunction

Behavior during operation and in case of a malfunction is described in the Operating Manual.

The safety function must be re-tested after startup, repair in the safety system, or a change to safety-related parameters; see Chapter 1.9.2 "Testing the safety function".

If an error is detected during a functional test, measures must be taken to once again ensure the functional capability of the safety system. This can be done, for example, by replacing the transmitter.

Appropriate documentation of tests that are performed is recommended.

2 Annex

2.1 Terms and abbreviations according to IEC 61508

Name	Description
Actuator	Part of a safety-related system that intervenes in the process to achieve a safe state.
EUC	Equipment under control (EUC) Equipment, machine, apparatus, or system used for manufacturing, shaping materials, for transport, medical purposes, or other activities.
E / E / PE	Electrical/electronic/programmable electronic (E/E/EP): based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology
Failure	End of the ability of a functional unit to perform a required function or operation of a functional unit differs in some way from the requirement.
Diagnostic coverage	Diagnostic coverage (DC) Number of dangerous failures detected by automatic diagnostic online tests. The number of dangerous failures is calculated as the rate of detected dangerous failures divided by the total rate of dangerous failures.
Error	An abnormal condition that can cause a reduction or the loss of the ability of a functional unit to perform a required function.
Functional safety	A part of overall safety related to the EUC and EUC control system that depends on the correct function of the safety-related E/E/EP system and other risk-mitigating actions.
Functional unit	Unit consisting of hardware or software or both that is suitable for performing a stated task.

Name	Description
Dangerous failure	Failure of an element and/or subsystem, and/or system involved in implementing the safety function, which a) prevents the safety function being executed on demand (on-demand operation type), or causes the failure of a safety function (operation with continuous demand), so that the EUC transitions to a dangerous or potentially dangerous state; or b) reduces the probability of executing the safety function correctly on demand.
Safe failure	Failure of an element and/or subsystem, and/or system involved in implementing the safety function, which a) causes false triggering of the safety function, switching the EUC (or parts of it) to a safe state, or maintaining a safe state; or a) increases the probability of false triggering of the safety function, switching the EUC (or parts of it) to a safe state, or maintaining a safe state
Hazard	Potential source of damage
Safety	Freedom from unreasonable risk
Safety function	Function performed by a safety-related E/E/PE system or other risk-mitigating actions that is intended to achieve or maintain a safe state for the plant taking a specified dangerous incident into consideration.
Safety integrity	The probability of a safety-related system performing the required safety function under all specified conditions within a specified period of time according to requirements.
Safety Integrity Level (SIL)	One of four discrete levels, equivalent to a safety integrity value range, where Safety Integrity Level 4 represents the highest level of safety integrity and Safety Integrity Level 1 the lowest.

Name	Description
Safety-related system	A system which both - performs necessary safety functions that are required to reach or maintain a safe state for the EUC and - which is designed to achieve the necessary safety integrity for the required safety functions, either autonomously, or in combination other safety-related E/E/PE systems and other risk-mitigating actions.
Safety Instrument System (SIS)	Safety instrumented system to perform one or more safety-related functions. A SIS consists of sensor(s), logic system, and actuator(s).
Lambda: λ	Failure rate per hour
Lambda **D**angerous: λ_D	Rate of dangerous failures per hour
Lambda Dangerous Detect: λ_{DD}	Rate of detected dangerous failures per hour
Lambda Dangerous Undetect: λ_{DU}	Rate of undetected dangerous failures per hour
Lambda Safe: λ_S	Rate of safe failures per hour
Lambda Safe Detect: λ_{SD}	Rate of detected safe failures per hour
Lambda Safe Undetect: λ_{SU}	Rate of undetected safe failures per hour
BPCS	Basic Process Control System
DC	**D**iagnostic **C**overage
FIT	**F**ailures **I**n **T**ime (1×10^{-9} per h)
HFT	**H**ardware **F**ailure **T**olerance

Name	Description
PFD	**P**robability of **F**ailure **D**etected (probability of a dangerous failure on demand)
PFD_{avg}	**P**robability of **F**ailure **D**etected **av**era**g**e (average probability of a dangerous failure on demand)
PFH	**P**robability of dangerous **F**ailure per **H**our
MooN	Architecture with M from N channels
MTBF	**M**ean **T**ime **B**etween **F**ailure (mean time between two failures).
MTTR	**M**ean **T**ime **T**o **R**estoration
MTTF	**M**ean **T**ime **T**o **F**ailure
MRT	**M**ean **R**epair **T**ime
SFF	**S**afe **F**ailure **F**raction
SIL	**S**afety **I**ntegrity **L**evel
SC	**S**ystematic **C**apability
PTC	**P**roof **T**est **C**overage (test coverage during regular inspection)

The manufacturer may use the mark:

Revision 2.0 September 2, 2022
Surveillance Audit Due September 30, 2025

Certificate / Certificat
Zertifikat / 合格証

JUMO 2203088 C001

exida hereby confirms that the:

Pressure transmitters JUMO dTRANS p20 DELTA (Type 403022), JUMO dTRANS p20 DELTA Ex d (Type 403023), JUMO dTRANS p20 (Type 403025) and JUMO dTRANS p20 Ex d (Type 403026)

SW Versions 236.02.01 and 236.03.01

JUMO GmbH & Co. KG
Fulda, Germany

Have been assessed per the relevant requirements of:

IEC 61508: 2010 Parts 1-3

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

Low demand: SIL 2 @ HFT = 0; Route 2_H

High demand: SIL 2 @ HFT = 1; Route 2_H

PFD_{avg}, PFH and Architecture Constraints must be verified for each application

Safety Function:
The pressure transmitters will transmit the measured pressure value within safety accuracy of +/-2% via a 4-20mA output current.
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Pressure transmitters JUMO dTRANS p20 DELTA (Type 403022), JUMO dTRANS p20 DELTA Ex d (Type 403023), JUMO dTRANS p20 (Type 403025) and JUMO dTRANS p20 Ex d (Type 403026)

Certificate / Certificat / Zertifikat / 合格証

JUMO 2203088 C001

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

Low demand: SIL 2 @ HFT=0; Route 2_H

High demand: SIL 2 @ HFT=1; Route 2_H

PFD_{avg}, PFH and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met the systematic capability through a detailed proof of proven-in-use data provided by JUMO GmbH & Co. KG. and the creation of a detailed safety case against the requirements of IEC 61508. These are intended to prove sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This element meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT

Variant	λ_S	λ_{DD}	λ_{DU}
JUMO dTRANS p20 DELTA (Type 403022), JUMO dTRANS p20 DELTA Ex d (Type 403023)	319	265	124
JUMO dTRANS p20 (Type 403025), JUMO dTRANS p20 Ex d (Type 403026)	346	311	193

- FIT = 1 failure / 10^9 hours
- λ_S corresponds to fail low/high and encloses internal failures which are not detected by the transmitter itself.

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: JUMO 22-03-088 R005, V2R0

Safety Manual: Safety Manual of JUMO dTRANS p20 (DELTA), Doc..No. 00668077 Rev.3.00

80 N Main St
Sellersville, PA 18960

T-111, V5R2

JUMO