Sicherheitshandbbuch, Safety Manual
Manuel de sécurité

für Druckmessumformer und Differenzdruckmessumformer
for pressure transmitter and Differential pressure transmitter
pour Convertisseur de pression et Convertisseur de pression différentielle

Type 403022 Type 403023 Type 403026

Type 403025

Sicherheitshandbuch
Safety Manual, Manuel de sécurité

40302202T99Z000K000

V4.00/DE-EN-FR /00668077

JUMO Safety Manual
für Druckmessumformer und
Differenzdruckmessumformer

Typ 403022 Typ 403023 Typ 403026

Typ 403025

Sicherheitshandbuch

40302202T99Z000K000

V4.00/DE /00668077

Inhalt

1 Safety Manual

1.1 Allgemeines

Die Gerätefamilie JUMO dTRANS p20 besteht aus folgenden Typen:

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

1.2 Bestimmungsgemäße Verwendung

Die Druckmessumformer JUMO dTRANS p20 (Typ 403025) und JUMO dTRANS p20 Ex d (Typ: 403026) als auch die Differenzdruckmessumformer JUMO dTRANS p20 DELTA (Typ 403022) und JUMO dTRANS p20 DELTA Ex d (Typ 403023) sind Geräte zur Druck-/Differenzdruckmessung in Gasen und Flüssigkeiten ohne Feststoffanteil.
Sie werden in sicherheitstechnischen Systemen zur Minimum-, Maximum- und Bereichsüberwachung eingesetzt, die den Anforderungen der Normreihe IEC 61508-1/-2/-3:2010 genügen.
Die Typen 403025/403026 als auch die Typen 403022/403023 sind hinsichtlich Elektronik und Software identisch aufgebaut, sie unterscheiden sich lediglich im mechanischen Aufbau. Genaue Funktionalität und Ausführungsform (z.B. der Messbereiche oder der Prozessanschlüsse), werden von den jeweiligen Einsatzbedingungen bestimmt.

Die Sicherheitsfunktion der genannten JUMO dTRANS p20 Serie bezieht sich ausschließlich auf das Messen von Drücken. Der Messumformer erzeugt einen prozessbezogenen Druck-Messwert, der zum Automatisierungssystem als 4 - 20 mA Ausgangssignal übertragen wird. Der Stromausgang ist das einzige sicherheitsgerichtete Signal des Messumformers.
Das HART®-Protokoll dient lediglich der Konfiguration der Druckmessumformer.

Der Anwender ist für die richtige Wahl des für den Prozess notwendigen Materials sowie für die Einhaltung der im Typenblatt angegebenen Spezifikationen (z.B. Prozess- und Umgebungstemperatur, Überdruckbereiche, Druckstöße) verantwortlich.

Eine unsachgemäße oder nicht bestimmungsgemäße Verwendung des Gerätes kann zu applikationsbedingten Gefahren führen (z.B. Korrosion durch falsche Materialauswahl oder Produktüberlauf durch falsche Geräte-Montage bzw. Geräte-Einstellung).

Für Schäden aus unsachgemäßem oder nicht bestimmungsgemäßem Gebrauch haftet JUMO nicht.

Die Sicherheitsfunktion gilt ausschließlich für die lineare Ausgangsfunktion (klassische Druckmessung).

1.3 Gültigkeit des Safety Manual

Die in diesem Safety Manual beschriebene Bewertung hinsichtlich Funktionaler Sicherheit und die Darstellung der Zertifikate bezieht sich ausschließlich auf Geräte mit dem Grundtypergänzung „2“ mit den Softwareversionen 236.02.01 oder 236.03.01.

1.4 Mitgeltende Gerätedokumentation

Die in den mitgelieferten Betriebsanleitungen vorgegebenen Maßnahmen, Werte und Anforderungen bezüglich Montage, elektrischer Anschluss, Bedienung und Instandhaltung sind einzuhalten.

1.5 Relevante Normen

Der Ausfall der Geräte kann einen Einfluss auf die Sicherheit von Personen und/oder die Sicherheit der Umwelt haben.

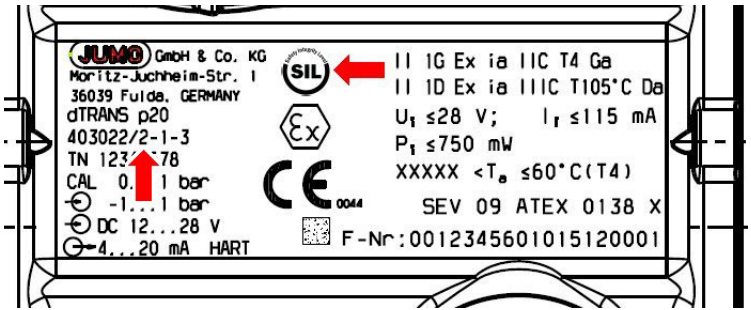
Um das Gerät hinsichtlich der funktionalen Sicherheit zu bewerten, erfolgt die Zertifizierung nach IEC 61508-1/-2/-3:2010.

Die Druckmessumformer Typ 403022, -23, -25 und -26 mit der Grundtypergänzung „2“ und den Softwareversionen 236.02.01 oder 236.03.01 erfüllen diese Anforderungen.

- Für die Sicherheitsfunktion bis SIL 2 entsprechend IEC 61508-1/-2/-3:2010:
  Funktionale Sicherheit sicherheitsbezogener elektrischer /elektronischer / programmierbarer elektronischer Systeme

1.6 Typenschild

Die SIL-Kennzeichnung und korrekte Grundtypergänzung müssen wie folgt auf dem Typenschild stehen (siehe Pfeile)!



1.7 Sicherheitsfunktion

Die Sicherheitsfunktion bezieht sich auf das Messen von Drücken. Der Druckmessumformer erzeugt einen prozessbezogenen Messwert, der zur Logikeinheit als 4...20 mA Ausgangssignal übertragen wird.

Der Stromausgang ist das einzige sicherheitsgerichtete Signal des Messumformers und liefert :

- das gültige Ausgangssignal zwischen 3,8 mA und 20,5 mA im Sinne der NAMUR-Empfehlung NE 43
- ein Ausgangssignal im Fehlerfall von ≤ 3,6 mA oder ≥ 21,0 mA im Sinne der NAMUR-Empfehlung NE 43
- eine Sicherheitsgenauigkeit von: 2% zusätzlich zu den im Datenblatt angegebenen Genauigkeitsangaben
- Sicherheitsreaktionszeit: Zum Abfangen von unkontrolliertem Software-Verhalten ist ein Watchdog-Timeout von 2.0 s einprogrammiert. Während einer dadurch ausgelösten Reset-Phase wird unabhängig vom konfigurierten Fehlerstrom immer ein minimaler Fehlerstrom ausgegeben !
- **Hinweis:** Nach 3-maligem Geräte-Reset ist von einem Fehler auszugehen.

Zu einer sicheren Fehlererkennung muss die Logikeinheit HI-Alarme (≥ 21,0 mA) und LO-Alarme (≤ 3,6 mA) erkennen und auswerten können.

Hinweis:

- Parameter P2 (Strom Messanfang) muss auf 4 mA und P3 (Strom Messende) muss auf 20 mA konfiguriert sein.
- Parameter P11 (Kennlinie "Characteristic") muss auf **LIN= linear** eingestellt sein.

Hinweis:

Der Ausgang des Druckmessumformers erfüllt während folgender Aktivitäten keine Sicherheitsfunktion:

- während Änderungen in der Konfigurationsebene
- während der Simulation („P8 Stromgeber“)
- bei Verwendung von HART®-Multidrop

- Die sicherheitsrelevanten Parameter/Einstellungen wurden vor dem sicherheitsbezogenen Betrieb über die lokale Bedienung oder über Setup-Kommunikation eingegeben.
  Kontrollieren Sie die Parameter/Einstellungen auf dem Display des Geräts
  ⇨ Betriebsanleitung im Kapitel 7 „Bedienung“ ⇨

Hinweis:
Im Gerät sind keine Maßnahmen im Sinne von "Network and system security" gemäß der Normenreihe IEC 62443 implementiert. Dies bedeutet, dass ausschließlich der Aspekt "safety" betrachtet wird.

- Die Schnittstellen (JUMO-Setup oder HART®-Protokoll) und die Bedienung vor Ort dürfen während des sicheren Betriebs nur zum Auslesen/ Überprüfen von Daten genutzt werden. Eine sichere Parametrierung ist während des Betriebs nicht möglich.
- Die Parametrierung muss nach der Inbetriebnahme verriegelt werden
  ⇨ Betriebsanleitung Kapitel 7 (Parameter P10 Key)
- Parameter P9 Err darf NICHT auf **LASt=letzter Wert** eingestellt werden, da in dieser Einstellung keine Fehlererkennung durch die nachgeschaltete Logikeinheit möglich ist. Es dürfen verwendet werden: ErLo=3,6 mA oder ErHi=21,6 mA
- Bei Inbetriebnahme muss ein kompletter Funktionstest durchgeführt werden.
  ⇨ Kapitel 1.9.2 „Sicherheitsfunktion überprüfen“

1.7.1 Geforderte Auflagen der Prüfstelle

Folgende Auflagen sind zwingend einzuhalten:

1.) Der Anlagenbetreiber muss bei einer Auslegung seiner Anlage nach IEC 61508-1/-2/-3:2010 darauf achten, dass seine gesamte Anlage die qualitativen und quantitativen Anforderungen der entsprechenden Norm erfüllt.
2.) Grundsätzlich muss bei redundantem Einsatz des Systems (HFT > 0) die nachfolgende Logik eine Auswertung der Messsignale am 4-20mA (z.B. durch Kreuzvergleich) vornehmen.
3.) Die Vorgaben in der Benutzerdokumentation sind zwingend einzuhalten.
4.) Nach dem Einbau der Druckmessumformer in der Anlage muss eine Validierung der Sicherheitsfunktion erfolgen.

1.8 Sicherheitstechnische Kenngrößen

Die folgenden Kenngrößen wurden durch eine Bauteil FMEDA unter folgenden Bedingungen errechnet:

- Fehlermodelle entsprechend den Anforderungen der IEC 61508-1/-2/-3:2010 für SIL1 bzw. SIL 2 Konformität
- Pfad 2_H und 2_S wurden für die Zertifizierung gewählt.

Annahme: Die mittlere Temperatur, die über einen langen Zeitraum betrachtet wird, beträgt 40°C.

1.8.1 Ausfallraten und SFF für Typ 403022, -23, -25 und -26

Type	Architektur	λ_{sd} [FIT]	λ_{su} [FIT]	λ_{dd} [FIT]	λ_{du} [FIT]	SFF	DC	$MTTF_d$ in Jahren	MTBF in Jahren	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 = 72h

Lifetime: 87600h (10 Jahre)

Intervall für Wiederholungsprüfung (T1):
Die Werte für PFD_{avg} in der Tabelle sind mit T1= 8760h (1Jahr) berechnet worden.

1.8.2 Berechnung von PFD_{avg}

- Bei einem SIL 2 zertifizierten System ist eine Wiederholungsprüfung notwendig.
- Der Betreiber legt das Prüfintervall fest und dieses muss bei der Ermittlung der Wahrscheinlichkeit eines gefahrbringenden Ausfalls PFD_{avg} des Sensorsystems berücksichtigt werden.
  Bei einkanaliger Systemarchitektur ergibt sich die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls PFD_{avg} des Messumformers aus dem Prüfintervall T1, der Ausfallrate der gefährlichen nicht erkennbaren Fehler λ_{du}, der **P**roof **T**est **C**overage PTC und der angenommenen Lifetime näherungsweise zu:

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

MTTR = MRT = 72h

Lifetime: maximal 87600h (10 Jahre)

Intervall für Wiederholungsprüfung T1 (kann der Betreiber selbst festlegen):
Die Werte für PFD_{avg} in der Tabelle sind mit T1= 8760h (1Jahr) berechnet worden.

1.8.3 Wiederholungsprüfung durchführen

Bei der Wiederholungsprüfung muss das Ausgangssignal des Messumformers an zwei verschiedenen Punkten (z.B. Anfangs- und Endwert des Druckmessbereiches) auf Einhaltung der Genauigkeit überprüft werden.

- Zeigt das Gerät bei der Wiederholungsprüfung Auffälligkeiten wie z.B. Genauigkeitsabweichungen oder Fehlermeldungen, dann ist das Gerät auszutauschen.
- Nach Ablauf der Lifetime von 10 Jahren genügen die Systeme nicht mehr den Anforderungen gemäß ihrer SIL-Zertifizierung und müssen ausgetauscht werden.

1.8.4 Sicherheitsrelevante Systemeigenschaften

Sicherheitseigenschaft	**Anforderung / Bemerkung**
SIL	SIL1 oder SIL2 ⇨ Kapitel 1.8.5
Betriebsart bezüglich Sicherheitsfunktion	Betriebsart mit niedriger und hoher Anforderungsrate möglich
Sicherheitsfunktion	Messung von Drücken über das Einheitssignal 4..20mA Stromschleife
Nennmessbereich	siehe Genauigkeitsangaben im Typenblatt
Sicherheitsgenauigkeit	2% zusätzlich zu den im Typenblatt angegebenen Genauigkeitsangaben
Teilsystemtyp	Typ B
Sicherheitsarchitektur	1oo1
Systematische Eignung (**S**ystematic **C**apability)	SC=2
Hardware Fehler Toleranz	HFT=0
Mittlere Ausfallwahrscheinlichkeit einer Sicherheitsfunktion bei Anforderung (Gesamtsystem)	SIL2: low-demand: $PFD_{avg}<10^{-2}$ high-demand: $PFH < 10^{-6}$
Intervall für Wiederholungsprüfung (T1)	1 Jahr (Der Betreiber kann dieses Intervall selbst festlegen.) ⇨ Kapitel 1.8.2
Lifetime	maximal 10 Jahre

Diese Eigenschaften besitzen nur Geräte mit:

- den Softwareversionen 236.02.01 oder 236.03.01
- Grundtypergänzung „2“
- Temperaturbereich -40 bis +85 °C
- Spannungsversorgungsbereich DC 12 bis 36 V (ATEX Ex ia: DC 12V bis 28V)

1.8.5 Bestimmung des SIL-Levels

Aufgrund der Architektur (1oo1) der als Typ B kategorisierten Druckmessumformer ist die Hardware-Fehlertoleranz = 0. Somit ergibt sich entsprechend dem Architekturpfad 2H der IEC 61508-2:

- dass in low-demand Anwendungen (PFD) die Druckmessumformer einkanalig (d.h. HFT = 0) bis SIL2 einsetzbar sind
- dass in high-demand Anwendungen (PFH) die Druckmessumformer einkanalig (d.h. HFT = 0) bis SIL1 und redundant (d.h. HFT≥1) bis SIL2 eingesetzt werden können.

Hinweis:

Die Geräte sind einkanalig aufgebaut (1oo1 Architektur) und besitzen einen HFT = 0.

Für einen HFT = 1 sind 2 Druckmessumformer vorzusehen, deren Ausgangssignal über eine sicherheitstechnische Logikeinheit ausgewertet wird.

1.8.6 Beispiel zur Berechnung der Gesamtgenauigkeit der Sicherheitsfunktion

Um die Gesamtgenauigkeit der Sicherheitsfunktion zu bestimmen, addieren Sie zu den Genauigkeitsangaben aus dem Typenblatt eine Sicherheitsgenauigkeit von 2 % des Nennmessbereiches.

Die Sicherheitsgenauigkeit beschreibt die maximale Auswirkung eines zufälligen Einzelfehlers auf den Messwert, welche noch als unkritisch eingestuft wird.
Die resultierende Gesamtgenauigkeit dient dazu, eine Sicherheitsreserve bei der Prozessüberwachung einzubauen.
Damit auch dann die Anlage sicher abgeschaltet wird, falls ein zufälliger Einzelfehler auftreten sollte.
Gesamtgenauigkeit der Sicherheitsfunktion = ± [Genauigkeitsangabe aus dem Typenblatt + 2 % Sicherheitsgenauigkeit].

Beispiel:
Füllstandskontrolle und Überfüll-Überwachung eines Flüssigkeitstank mit einer Füllhöhe von 5 Meter.

Genauigkeitsangabe aus dem Typenblatt, inkl. Langzeitstabilität: z.B. 0,2 %

Zusätzliche Sicherheitsgenauigkeit: 2,0 %

Gesamtgenauigkeit der Sicherheitsfunktion: 2,2 %

Eine Genauigkeit von 2,2 % bezogen auf 5 Metern Höhe ergibt 0,11 m.

Der Messumformer JUMO dTRANS p20 kontrolliert den Füllstand und gibt diesen als 4-20 mA Signal an das Prozessleitsystem weiter.

Die Überfüllsicherung in der Prozessüberwachung ist auf den Wert (5 m – 0,11 m = **4,89 m**) einzustellen.

Damit ist ein sicheres Abschalten auch bei Auftreten eines zufälligen Einzelfehlers vor Erreichen der Überfüllung sichergestellt.

1.8.7 Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung PFD_{avg}

Die folgende Tabelle zeigt die Abhängigkeit des „Safety Integrity Level“ (SIL) von der „mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems" (PFD_{avg}) nach IEC 61508-1/-2/-3:2010. Dabei wird der „low-demand mode“ betrachtet, d. h. die Anforderungsrate an das sicherheitsbezogene System ist durchschnittlich einmal im Jahr.

Tabelle low-demand PFD nach IEC 61508-1/-2/-3:2010

Sicherheits-Integritätslevel (SIL)	Betriebsart mit niedriger Anforderungsrate PFD_{avg} (low-demand mode)
4	$\geq 10^{-5}$ ... $<10^{-4}$
3	$\geq 10^{-4}$ ... $<10^{-3}$
2	$\geq 10^{-3}$ ... $<10^{-2}$
1	$\geq 10^{-2}$ ... $<10^{-1}$

Sensor, Logikeinheit und Aktor bilden zusammen ein sicherheitsbezogenes System, das eine Sicherheitsfunktion ausführt. Die „mittlere Wahrscheinlichkeit gefährlicher Ausfälle des gesamten sicherheitsbezogenen Systems“ (PFD_{avg}) teilt sich auf die Teilsysteme Sensor, Logikeinheit und Aktor üblicherweise gemäß der folgenden Abbildung auf.

Übliche Aufteilung der „mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall“ (PFD_{avg}) auf die Teilsysteme

Die Angaben bezüglich der Funktionalen Sicherheit in diesem Sicherheitshandbuch beziehen sich auf den Messumformer als Teilsystem (Sensor).

1.8.8 Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde PFH

Die folgende Tabelle zeigt die Abhängigkeit des „Safety Integrity Level“ (SIL) von der „mittleren Häufigkeit eines gefahrbringenden Ausfalls je Stunde" (PFH) nach IEC 61508-1/-2/-3:2010.

Tabelle high-demand PFH nach IEC 61508-1/-2/-3:2010

Sicherheits-Integritätslevel (SIL)	Betriebsart mit hoher Anforderungsrate 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 Sicherheitsrelevante Systemeigenschaften

Die Druckmessumformer sind als 1oo1-Architektur realisiert.

Die Gerätesoftware überwacht zahlreiche Variablen auf gültige Bereichsgrenzen.
Zusätzlich werden Registerinhalte zum Vergleich zurückgelesen und ggf. korrigiert.
Ein aktivierter Watchdog mit Timeoutzeit von 2 s schützt vor unkontrolliertem Software-Verhalten.

1.9 Geräteparametrierung

Zur sicheren Geräteparametrierung sind folgende Schritte durchzuführen:

Schritt	Tätigkeit
1	Über Parameterebene alle sicherheitsrelevanten Parameter einstellen ⇨ Betriebsanleitung Kapitel 7.3 Ebenenkonzept Die Parametrierung ist über den Bedienknopf, sowie über Setup- oder HART®-Schnittstelle möglich.
2	Sicherheitsfunktion überprüfen siehe ⇨ Kapitel 1.9.2 „Sicherheitsfunktion überprüfen“
3	Parameter verriegeln ⇨ Betriebsanleitung Kapitel 7.3.2 Parameterebene (Parameter P10 Tastatursperre)

1.9.1 Sicherheitsrelevante Parameter einstellen

Grundsätzlich sind alle Parameter nach den Anforderungen des sicherheitsbezogenen Systems zu konfigurieren. Wir empfehlen die eingestellten Parameter zu dokumentieren.

Inbetriebnahmeprotokoll JUMO dTRANS p20 SIL
Gerätebezeichnung:
Messstelle:
Seriennummer:
Firma:
Segmenttest erfolgreich? JA [ ]

Parameter	**Erklärung**	**Auswahlmöglichkeiten ***	**Wertvorgabe**	**Geprüft?**
P0 Den	Dichtekorrektur	0,01 … **1,00** … 99,99		
P1 Uni	Maßeinheit des Drucks	inH2O, inHG, ftH2O, mmH2O, mmHG PSI, bar, mbar, kg/cm^2, kPa, TORR, MPa, mH2O		
P2 mA	Strom Messanfang	**4.00 mA** (keine anderen Werte erlaubt)		
P3 mA	Strom Messende	**20.00 mA** (keine anderen Werte erlaubt)		
P4 sec	Dämpfung	**0,0** … 100.0 s		
P5 RS	Messanfang	Nennmessbereich		
P6 RE	Messende	Nennmessbereich		

Inbetriebnahmeprotokoll JUMO dTRANS p20 SIL				
P8 mA	Stromgeber	darf **nicht** aktiviert werden, wenn die Sicherheitsfunktion ausgeführt wird		
P9 Err	Strom im Fehlerfall	ErLo = 3.6 mA **ErHi = 21.6 mA** ~~LASt = letzter Wert~~		
P10 Key	Tastatursperre	**O = keine Sperre** LA = alle, Schnittstelle frei LO = alle, ohne Messanfang LS = alle, ohne Messanfang und Ende LALL = alle, inkl. Schnittstelle nach der Geräteparametrierung auf "LALL" umstellen		
P11 Chr	Kennlinie	**Lin = linear** ~~SLin = linear bis Beginn Radizierung~~ ~~SoFF = aus bis Beginn Radizierung~~		
P15 OFF	Offset des Druckwertes (Nullpunktverschiebung)	Nennmessbereich		
* **Fett gekennzeichnete Werte geben die Werkseinstellung an** * ~~durchgestrichene~~ Werte dürfen nicht eingestellt sein				
Datum:				
Uhrzeit:				
Prüfer:				
Unterschrift				

1.9.2 Sicherheitsfunktion überprüfen

Überprüfen Sie die Sicherheitsfunktion vorzugsweise im eingebauten Zustand. Wenn dies nicht möglich ist, können Sie die Sicherheitsfunktion auch im ausgebauten Zustand überprüfen. Beachten Sie dabei, dass der Druckmessumformer zur Prüfung in der gleichen Einbaulage wie in der Anlage montiert wird.

Voraussetzung: Tastatursperre/Verriegelung ist deaktiviert.

Während dieser Überprüfung arbeitet das Gerät **nicht** sicherheitsgerichtet!

Wir empfehlen folgende Schritte durchzuführen:

Schritt	Tätigkeit
1	Kontrollieren Sie den Status auf Warnungen und Fehlermeldungen
2	Kontrollieren Sie Parameter, die im Kapitel 1.9.1 „Sicherheitsrelevante Parameter einstellen“ aufgeführt sind
3	Kontrollieren Sie die Messbereichsgrenzen
4	Kontrollieren Sie den Nullpunkt z.B. im druckfreien Zustand
5	Kontrollieren Sie das obere Ende der eingestellten Messspanne (P6 RE) durch Anlegen eines definierten Drucks
6	Aktivieren Sie die Tastatursperre/Verriegelung (Parameter P10)
7	Erstellen Sie ein neues Inbetriebnahmeprotokoll

⇨ Betriebsanleitung Kapitel „7 Bedienung“

1.10 Verhalten im Betrieb und bei Störung

Das Verhalten im Betrieb und bei Störung wird in der Betriebsanleitung beschrieben.

Nach Inbetriebnahme, Reparatur im Sicherheitssystem oder Änderung von sicherheitstechnischen Kenngrößen ist die Sicherheitsfunktion erneut zu prüfen siehe Kapitel 1.9.2 „Sicherheitsfunktion überprüfen“.

Sollte während einer Funktionsprüfung ein Fehler erkannt werden, müssen Maßnahmen ergriffen werden, die die Funktionsfähigkeit des Sicherheitssystem wieder gewährleisten. Dies kann z. B. durch Austausch des Messumformers geschehen.

Es wird eine entsprechende Dokumentation der durchgeführten Prüfungen empfohlen.

2 Anhang

2.1 Begriffe und Abkürzungen gemäß IEC 61508-1/-2/-3:2010

Name	Beschreibung
Aktor	Teil eines sicherheitstechnischen Systems, das die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen.
EUC	**E**quipment **U**nder **C**ontrol (EUC) Einrichtung, Maschine, Apparat oder Anlage, verwendet zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten.
E / E / PE	Elektrisch/elektronisch/programmierbar elektronisch (E/E/EP): basierend auf elektrischer (E) und / oder elektronischer (E) und/oder programmierbar elektronischer (PE) Technologie
Ausfall / Versagen	Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion bereitzustellen oder Betrieb einer Funktionseinheit ist in irgendeiner Art anders als gefordert.
Diagnosedeckungsgrad	**D**iagnostic **C**overage (DC) Anteil der gefahrbringenden Ausfälle, die durch automatische diagnostische Online-Prüfungen erkannt werden. Der Anteil der gefahrbringenden Ausfälle wird mittels der Raten gefahrbringender Ausfälle, die zu den erkannten gefahrbringenden Ausfällen gehören, geteilt durch die Gesamtrate der gefahrbringenden Ausfälle berechnet.
Fehler	Nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen.
Funktionale Sicherheit	Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt.

Name	Beschreibung
Funktionseinheit	Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer angegebenen Aufgabe geeignet ist.
Gefahrbringender Ausfall	Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der a) verhindert, dass eine Sicherheitsfunktion bei Anforderung ausgeführt wird (Anforderungsbetriebsart) oder den Ausfall einer Sicherheitsfunktion verursacht (Betriebsart mit kontinuierlicher Anforderung), so dass die EUC in einen gefährlichen oder möglicherweise gefährlichen Zustand gebracht wird; oder b) die Wahrscheinlichkeit vermindert, die Sicherheitsfunktion bei Anforderung ordnungsgemäß auszuführen.
Ungefährlicher Ausfall	Ausfall eines Elements und/oder Teilsystems und/oder Systems, das Anteil an der Ausführung der Sicherheitsfunktion hat, der a) zur Fehlauslösung der Sicherheitsfunktion führt, die EUC (oder Teile davon) in einen sicheren Zustand zu bringen oder den sicheren Zustand aufrechtzuerhalten; oder b) die Wahrscheinlichkeit der Fehlauslösung der Sicherheitsfunktion erhöht, die EUC (oder Teile davon) in einen sicheren Zustand zu bringen oder den sicheren Zustand aufrechtzuerhalten
Gefährdung	Potentielle Schadensquelle
Sicherheit	Freiheit von unvertretbarem Risiko
Sicherheitsfunktion	Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird, und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten.
Sicherheits-Integrität	Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderte Sicherheitsfunktion unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt.

Name	Beschreibung
Sicherheits-Integritätslevel (SIL)	Eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt.
Sicherheitsbezogenes System	System, das sowohl - die erforderlichen Sicherheitsfunktionen ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch - dazu vorgesehen ist, selbst oder mit anderen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen.
Sicherheitstechnisches System (SIS)	Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en).
Lambda: λ	Ausfallrate pro Stunde
Lambda **D**angerous: λ_D	Rate gefahrbringender Ausfälle je Stunde
Lambda **D**angerous **D**etect: λ_{DD}	Rate erkannter gefahrbringender Ausfälle je Stunde
Lambda **D**angerous **U**ndetect: λ_{DU}	Rate unerkannter gefahrbringender Ausfälle je Stunde
Lambda **S**afe: λ_S	Rate sicherer Ausfälle je Stunde
Lambda **S**afe **D**etect: λ_{SD}	Rate erkannter sicherer Ausfälle je Stunde
Lambda **S**afe **U**ndetect: λ_{SU}	Rate unerkannter sicherer Ausfälle je Stunde
BPCS	Betriebs- und Überwachungseinrichtungen als ein System
DC	**D**iagnostic **C**overage (Diagnosedeckungsgrad)

Name	Beschreibung
FIT	**F**ailure **I**n **T**ime (Fehler pro Zeit ($1x10^{-9}$ pro h)
HFT	**H**ardware **F**ailure **T**olerance (Hardware-Fehlertoleranz)
PFD	**P**robability of **F**ailure **D**etected (Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung))
PFD_{avg}	**P**robability of **F**ailure **D**etected **av**erag**e** (Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung)
PFH	**P**robability of dangerous **F**ailure per **H**our (Wahrscheinlichkeit gefahrbringender Ausfälle pro Stunde)
MooN	Architektur mit M aus N-Kanälen
MTBF	**M**ean **T**ime **B**etween **F**ailure (Mittlere Zeitdauer zwischen zwei Ausfällen)
MTTR	**M**ean **T**ime **T**o **R**estoration (mittlere Dauer bis zur Wiederherstellung)
MTTF	**M**ean **T**ime **T**o **F**ailure (mittlere Dauer bis zum gefahrbringenden Ausfall)
MRT	**M**ean **R**epair **T**ime (mittlere Reparaturdauer)
SFF	**S**afe **F**ailure **F**raction (Anteil sicherer Ausfälle)
SIL	**S**afety **I**ntegrity **L**evel (Sicherheits-Integritätslevel)
SC	**S**ystematic **C**apability (systematische Eignung)
PTC	**P**roof **T**est **C**overage (Diagnosedeckungsgrad während der Wiederholungsprüfung)

The manufacturer may use the mark:

Revision 3.0 September 1, 2025
Surveillance Audit Due September 30, 2028

PRODUCT CERTIFICATION BODY #1004

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.

C. Krupke
Evaluating Assessor

Certifying Assessor

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

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)

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, V3R0

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

80 N Main St
Sellersville, PA 18960

T-111, V5R2

Zertifikate für zugelassene Geräteausführungen stehen auf der Website des Herstellers zum Download zur Verfügung.

JUMO GmbH & Co. KG

Moritz-Juchheim-Straße 1
36039 Fulda, Germany

Telefon: +49 661 6003-715
Telefax: +49 661 6003-606
E-Mail: mail@jumo.net
Internet: www.jumo.net

Lieferadresse:
Mackenrodtstraße 14
36039 Fulda, Germany

Postadresse:
36035 Fulda, Germany

Technischer Support Deutschland:

Telefon: +49 661 6003-9135
Telefax: +49 661 6003-881899
E-Mail: support@jumo.net

JUMO Safety Manual

for pressure transmitter and
Differential pressure transmitter

Type 403022 Type 403023 Type 403026

Type 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 61508-1/-2/-3:2010 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.

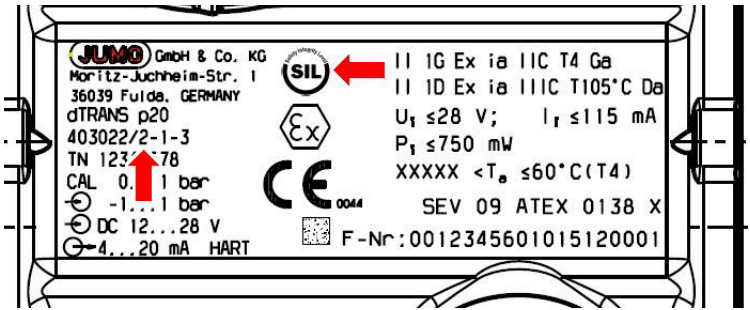
To assess the device in terms of functional safety, certification according to IEC 61508-1/-2/-3:2010 has been performed.

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 61508-1/-2/-3:2010: 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 61508-1/-2/-3:2010 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 61508-1/-2/-3:2010 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.

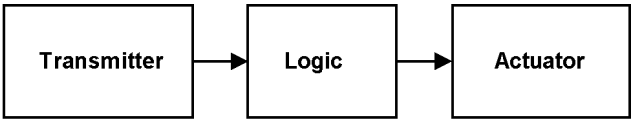
1.8.7 Average probability of dangerous failure on demand PFD_{avg}

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 61508-1/-2/-3:2010.
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 61508-1/-2/-3:2010

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 ac-

tuator 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 61508-1/-2/-3:2010.

Table high demand PFH according to IEC 61508-1/-2/-3:2010

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 61508-1/-2/-3:2010

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**erag**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 3.0 September 1, 2025
Surveillance Audit Due
September 30, 2028

PRODUCT CERTIFICATION BODY #1004

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.

C. Krupke
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, V3R0

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

80 N Main St
Sellersville, PA 18960

T-111, V5R2

Certificates for approved device versions are available for download on the manufacturer's website.

JUMO GmbH & Co. KG
Street address:
Moritz-Juchheim-Straße 1
36039 Fulda, Germany
Delivery address:
Mackenrodtstraße 14
36039 Fulda, Germany
Postal address:
36035 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
Email: mail@jumo.net
Internet: www.jumo.net

JUMO UK LTD
JUMO House
Temple Bank, Riverway
Harlow, Essex, CM20 2DY, UK
Phone: +44 1279 63 55 33
Fax: +44 1279 62 50 29
Email: sales@jumo.co.uk
Internet: www.jumo.co.uk

JUMO Process Control, Inc.
6724 Joy Road
East Syracuse, NY 13057, USA

Phone: +1 315 437 5866
Fax: +1 315 437 5860
Email: info.us@jumo.net
Internet: www.jumousa.com

JUMO Safety Manual

for Convertisseur de pression et
Convertisseur de pression différentielle

Type 403022 Type 403023 Type 403026

Type 403025

Manuel de sécurité

40302202T99Z002K000

JUMO

Sommaire

Sommaire

1 Manuel de sécurité (Safety Manual)

1.1 Généralités

La famille d'appareils JUMO dTRANS p20 se compose des types suivants

- 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 Utilisation conforme aux prescriptions

Les convertisseurs de pression JUMO dTRANS p20 (type 403025) et JUMO dTRANS p20 Ex d (type 403026) tout comme les convertisseurs de pression différentielle JUMO dTRANS p20 DELTA (type 403022) et JUMO dTRANS p20 DELTA Ex d (type 403023) sont destinés à mesurer la pression/pression différentielle dans des gaz et des liquides sans teneur en matière solide. Ils sont utilisés dans les systèmes de sécurité pour la surveillance min., max. et des plages qui répondent aux exigences de la norme CEI 61508-1/-2/-3:2010.
Les types 403025/403026 ainsi que les types 403022/403023 sont montés de la même manière en ce qui concerne l'électronique et les logiciels, ils se distinguent seulement par la structure mécanique. Les fonctionalités précises et l'exécution (par ex. les étendues de mesure ou les raccords de process) sont définies par les conditions d'utilisation respectives

La fonction de sécurité de la série JUMO dTRANS p20 est de mesurer exclusivement la pression. Le convertisseur de mesure produit une valeur mesurée de pression qui est transmise au système d'automatisation sous forme de signal de sortie 4 - 20 mA. La sortie de courant est l'unique signal de sécurité du convertisseur de mesure.
Le protocole HART® sert seulement à la configuration du convertisseur de pression.

L'utilisateur est respondsable du choix du matériel nécessaire au process ainsi qu'au respect des spécifications indiquées dans la fiche technique (par ex. température du process et température ambiante, plages de surpression, coups de bélier).

Une utilisation incorrecte ou inappropriée de l'appareil peut entraîner des dangers liés à l'application (par ex. corrosion du fait du

mauvais choix du matériau ou trop-plein du produit à cause d'un mauvais montage-appareil et/ou du réglage de l'appareil).

JUMO n'est nullement responsable des dégâts dus à une utilisation non conforme ou inappropriée.

La fonction de sécurité vaut exclusivement pour la fonction de sortie linéaire (mesure classique de la pression).

1.3 Validité du manuel de sécurité (Safety Manual)

L'évaluation décrite dans ce Safety Manual concernant la sécurité fonctionnelle et la représentation des certificats se rapporte essentiellement aux appareils avec extension au type de base „2“ avec la version software 236.02.01 ou 236.03.01.

1.4 Documentation de l’appareil

Veuillez respecter les mesures, les valeurs et les exigences indiquées dans cette notice relatives au montage, au raccordement électrique, au fonctionnement et à la mise en service.

1.5 Normes importantes

Une défaillance de ces appareils peut avoir une influence sur la sécurité des personnes et / ou la protection de l’environnement.

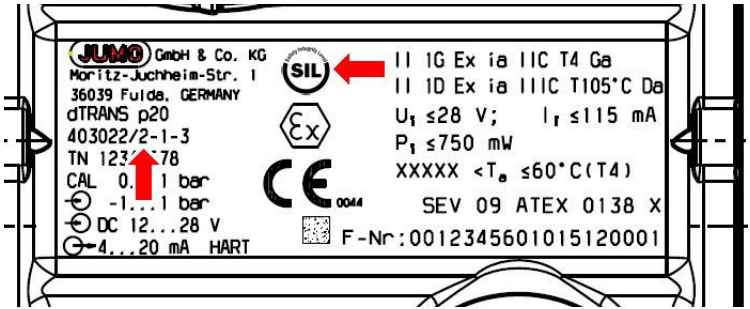
L'appareil est évalué en matière de sécurité fonctionnelle selon la certification CEI 61508-1/-2/-3:2010.

Les convertisseurs de pression, types 403022, -23, -25 et -26 avec extension au type de base „2“ et la version software 236.02.01 ou 236.03.01 répondent à ces exigences.

- Pour la fonction de sécurité jusqu'à SIL 2 suivant CEI 61508-1/-2/-3:2010 :
  Sécurité fonctionnelle des systèmes électriques /électroniques programmables relatifs à la sécurité

1.6 Plaque signalétique

Le marquage SIL et l'extension correcte du type de base doivent se trouver comme suit sur la plaque signalétique (voir flèche) !



1.7 Fonction de sécurité

La fonction de sécurité consiste à mesurer la pression. Le convertisseur de mesure produit une valeur mesurée de pression qui est transmise à l'unité logique sous forme de signal de sortie 4 - 20 mA.

La sortie de courant est l'unique signal de sécurité du convertisseur de mesure et délivre :

- le signal de sortie valable entre 3,8 mA et 20,5 mA dans le sens de la recommandation NAMUR NE 43
- d'un signal de sortie en cas d'erreur de ≤ 3,6 mA ou ≥ 21,0 mA dans le sens de la recommandation NAMUR NE 43
- d'une précision de sécurité de 2 % par rapport aux indications de précision figurant dans la fiche produit
- Temps de réaction de sécurité : un watchdog-timeout de 2.0 s est programmé pour intercepter le comportement incontrôlé du logiciel. Au cours d'une phase de réinitialisation ainsi déclenché, un courant de défaut minimum est toujours émis indépendamment du courant de défaut configuré !
- **Remarque :** après 3 réinitialisations de l'appareil. on peut présumer qu'il s'agit d'une erreur.

Pour une détection sûre d'erreur, l'unité logique doit pouvoir détecter et évaluer l'alarme-HI (≥ 21,0 mA) et l'alarme-LO (≤ 3,6 mA).

Remarque :

- Le paramètre P2 (début de mesure courant) doit être configuré sur 4 mA et P3 (fin de mesure courant) sur 20 mA.
- Le paramètre P11 ("Caractéristique") doit être réglé sur **LIN= linéaire**.

Remarque :

la sortie du convertisseur de pression ne réalise aucune fonction de sécurité pendant les activités suivantes :

- durant des modifications au niveau de configuration
- durant la simulation („générateur de courant P8“)
- lors de l'utilisation de HART®-Multidrop

- Les paramètres/réglages importants pour la sécurité ont été saisis avant le fonctionnement de sécurité via la commande locale ou via la communication Setup.
  Vérifier les paramètres/réglages sur l'écran de l'appareil.
  ⇨ Notice de mise en service dans chapitre 7 „Commande“

Remarque :

Aucune mesure dans le sens "Network and system security" suivant la norme CEI 62443 n'a été implémentée dans l'appareil. Cela signifie que seul l'aspect "safety" a été pris en compte.

- Les interfaces (JUMO-Setup ou protocole HART®) et la commande in situ ne peuvent être utilisées, pendant le fonctionnement sûr, que pour la lecture/vérification des données. Un paramétrage sûr pendant le fonctionnement est impossible.
- Le paramétrage doit être verrouillé après la mise en service
  ⇨ Notice de mise en service chapitre 7 (Paramètre P10 Key)
- Le paramètre P9 Err ne doit PAS être paramétré sur **LASt=dernière valeur**, car aucune détection d'erreur par l'unité logique connectée en aval n'est possible dans cette configuration. ErLo=3,6 mA ou ErHi=21,6 mA peuvent être utilisés
- Un test de fonctionnement complet doit être effectué lors d'une mise en service.
  ⇨ Chapitre 1.9.2 "Vérifier la fonction de sécurité"

1.7.1 Conditions requises des essais

Les conditions suivantes doivent être strictement respectées :

1.) L'exploitant doit veiller, lors de la conception de son installation selon CEI 61508-1/-2/-3:2010, que toute son installation soit conforme du point de vue qualitatif et quantitatif à la norme correspondante.
2.) Pour une utilisation redondante du système (HFT> 0), la logique suivante doit évaluer les signaux de mesure à la sortie 4-20 mA (par exemple, par recoupement).
3.) Les conditions évoquées dans la documentation doivent être strictement respectées.
4.) La fonction de sécurité doit être validée une fois le convertisseur de mesure intégré dans l'installation.

1.8 Caractéristiques de sécurité

Les grandeurs caractéristiques suivantes ont été calculées à l'aide d'un composant FMEDA dans les conditions suivantes :

- Modèles d'erreur relatifs aux exigences de CEI 61508-1/-2/-3:2010 pour conformité SIL 1 ou SIL 2
- Les routes 2_H et 2_S ont été sélectionnées pour la certification.

Supposition : la température moyenne, qui est étudiée pendant une longue période, est de 40°C.

1.8.1 Taux de défaillances et SFF pour types 403022, -23, -25 et -26

Type	Architecture	λ_{sd} [FIT]	λ_{su} [FIT]	λ_{dd} [FIT]	λ_{du} [FIT]	SFF	DC	$MTTF_d$ en années	MTBF en années	PTC	PFDavg	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 = 72h

Lifetime: 87600h (10 ans)

Intervalle pour contre-essai (T1) :
les valeurs pour PFD_{avg} du tableau ont été calculées avec T1= 8760h (1 an).

1.8.2 Calcul de PFD_{avg}

- Un contre-essai est nécessaire pour un système certifié SIL 2.
- L'utilisateur détermine un intervalle d'essai et il faudra en tenir compte lors de la définition de la probabilité d'une défaillance dangereuse PFD_{avg} du capteur.
  Pour une architecture de système à un canal, il résulte la probabilité moyenne d'une défaillance dangereuse PFD_{avg} du convertisseur de mesure de l'intervalle d'essai T1, le taux de défaillance d'erreurs dangereuses non détectées λ_{du}, le **P**roof **T**est **C**overage PTC et le cycle de vie approximatif accepté :

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

MTTR = MRT = 72h

Lifetime: 87600h max. (10 ans)

Intervalle pour contre-essai T1 (l'utilisateur peut le définir lui-même) :
les valeurs pour PFDavg du tableau ont été calculées avec T1= 8760h (1 an)

1.8.3 Effectuer contre-essai

Lors du contre-essai, le signal de sortie du convertisseur de mesure doit être contrôlé à deux points différents (par ex valeur initiale et finale de l'étendue de pression) quant au respect de l'exactitude.

- Si l'appareil montre des anomalies lors du contre-essai, comme par ex. des écarts de précision ou des messages d'erreur, l'appareil doit être remplacé
- Lorsque le cycle de vie de 10 ans est dépassé, les systèmes ne sont plus conformes aux exigences de la certification SIL et doivent être remplacés.

1.8.4 Caractéristiques du système importantes pour la sécurité

Caractéristiques de sécurité	**Condition / Remarque**
SIL	SIL 1 ou SIL 2 ⇨ Chapitre1.8.5
Mode de fonctionnement concernant la fonction de sécurité	Mode de fonctionnement avec taux de sollicitation faible ou élevé possible
Fonction de sécurité	Mesure de la pression via un signal normalisé 4 à 20mA dans la boucle de courant
Etendue de mesure nominale	voir indications de précision dans la fiche technique
Précision de sécurité	2 % par rapport aux indications de précision données dans la fiche technique
Type de sous-système	Type B
Architecture de sécurité	1oo1
Aptitude systématique (**S**ystematic **C**apability)	SC=2
Tolérance aux erreurs matérielles	HFT=0
Probabilité de défaillance moyenne sur sollicitation d'une fonction de sécurité (système global)	SIL 2: low-demand: $PFD_{avg}<10^{-2}$ high-demand: $PFH < 10^{-6}$
Intervalle pour contre-essai (T1)	1 an (l'utilisateur peut définir lui-même cet intervalle.) ⇨ Chapitre1.8.2
Cycle de vie (Lifetime)	10 ans max.

Seuls les appareils avec :

- version software 236.02.01 ou 236.03.01
- Extension du type de base „2“
- Plage de température comprise entre -40 et +85 °C
- Plage d'alimentation comprise entre DC 12 et 36 V (ATEX Ex ia : DC 12V et 28V)

1.8.5 Détermination du niveau SIL

En raison de l'architecture (1oo1) du convertisseur de pression, type B, la tolérance aux erreurs matérielles = 0.
Il en résulte ainsi selon la route d'architecture 2H de la norme CEI 61508-2:

- que dans les applications low-demand (PFD) les convertisseurs de pression à un canal (c.-à-d. HFT = 0) peuvent être utilisés jusqu'à SIL 2
- que dans les applications high-demand (PFH) les convertisseurs de pression à un canal (c.-à-d. HFT = 0) peuvent être utilisés jusqu'à SIL 1 et redondant (c.-à-d. HFT[3]1) jusqu'à SIL 2

Remarque :

Les appareils disposent d'un seul canal (architecture 1oo1) et ont une HFT = 0.

Pour un HFT = 1, 2 convertisseurs de pression sont prévus dont le signal de sortie est évalué via une unité logique de sécurité.

1.8.6 Exemple de calcul de la précision globale de la fonction de sécurité

Pour définir la précision globale de la fonction de sécurité, veuillez additionner aux indications de précision de la fiche technique une précision de sécurité de 2 % de l'étendue de mesure nominale.

La précision de sécurité décrit l'effet maximal d'un défaut isolé aléatoire sur la valeur mesurée lequel est encore classé comme non critique.
La précision globale qui en résulte sert à créer une réserve de sécurité pour la surveillance du process.
Pour que l'installation soit mise à l'arrêt en toute sécurité au cas où un défaut isolé aléatoire apparaisse.
Précision globale de la fonction de sécurité = ± [indications de précision de la fiche technique + 2 % de la précision de sécurité].

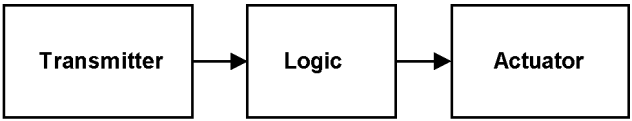
Exemple :
Contrôle du niveau et surveillance du trop-plein d'un réservoir de liquide avec un niveau de remplissage de 5 mètres.
Indications de précision dans la fiche technique, y compris la stabilité à long terme : par ex. 0,2 %
Précision de sécurité supplémentaire : 2,0 %
Précision totale de la fonction de sécurité : 2,2 %
Une précision de 2,2 % par rapport à une hauteur de 5 m donne 0,11 m.
Le convertisseur de mesure JUMO dTRANS p20 contrôle le niveau et le transmet sous forme de signal 4-20 mA au système de conduite de process.
Le détecteur de trop-plein dans la surveillance du process doit être réglé à (5 m – 0,11 m = **4,89 m**) .
Un arrêt en toute sécurité, avant d'atteindre le trop-plein, est de ce fait assuré même en cas d'un défaut isolé aléatoire.

1.8.7 Probabilité moyenne de défaillances dangereuses sur sollicitation PFD^{avg}

Le tableau suivant montre la dépendance du „Safety Integrity Level“ (SIL) de la „probabilité moyenne de défaillances dangereuses d'une fonction de sécurité de tout le système de sécurité" (PFDavg) suivant CEI 61508-1/-2/-3:2010.
„Low demand mode“ est pris en considération, c.-à-d. le taux de sollicitation du système de sécurité est d'une fois par an en moyenne.
Tableau low-demand PFD suivant CEI 61508-1/-2/-3:2010

Niveau d'intégrité de sécurité (SIL)	Mode de fonctionnement avec faible taux de sollicitation PFD_{avg} (low-demand mode)
4	$\geq 10^{-5}$ ... $<10^{-4}$
3	$\geq 10^{-4}$ ... $<10^{-3}$
2	$\geq 10^{-3}$ ... $<10^{-2}$
1	$\geq 10^{-2}$ ... $<10^{-1}$

Capteur, unité logique et acteur constituent ensemble un système relatif à la fonction de sécurité. La „probabilité moyenne de défaillances dangereuses d'une fonction de sécurité de tout le système de sécurité“ (PFD_{avg}) se répartit entre capteur, unité logique et acteur comme indiqué sur la figure ci-dessous.



Répartition habituelle de la „probabilité moyenne de défaillances dangereuses lors de l'exécution sur sollicitation de la fonction de sécurité de“ (PFDavg) sur le sous-système

Les indications concernant la sécurité fonctionnelle fournies dans ce manuel de sécurité se rapportent au convertisseur de mesure en tant que sous-système (capteur)

1.8.8 Fréquence moyenne d'une défaillance dangereuse par heure PFH

Le tableau suivant montre la dépendance de „Safety Integrity Level“ (SIL) de la „fréquence moyenne d'une défaillance dangereuse par heure" (PFH) suivant CEI 61508-1/-2/-3:2010.

Tableau high-demand PFH suivant CEI 61508-1/-2/-3:2010

Niveau d'intégrité de sécurité (SIL)	Mode de fonctionnement avec taux de sollicitation élevé 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 Caractéristiques du système importantes pour la sécurité

Les convertisseurs de pression sont réalisés avec l'architecture 1oo1.

Le logiciel de l'appareil surveille de nombreuses variables (limites valides)
De plus, les contenus des répertoire sont, à titre de comparaison, relus et corrigés le cas échéant.
Un watchdog activé avec un temps mort (timeout) de 2 s protège d'un comportement incontrôlé du logiciel.

1.9 Paramétrage de l'appareil

Pour un paramétrage sûr de l'appareil, les étapes suivantes doivent être exécutées :

Etape	Action
1	Régler tous les paramètres importants au niveau de paramétrage ⇨ Notice de mise en service, chapitre 7.3 Concept des niveaux Le paramétrage s'effectue via le bouton de commande et via l'interface HART® ou le Setup.
2	Vérifier la fonction de sécurité, voir ⇨ Chapitre 1.9.2 "Vérifier la fonction de sécurité"
3	Verrouiller le paramètre ⇨ Notice de mise en service chapitre 7.3.2 Niveau de paramétrage (Paramètre P10 Verrouillage du clavier)

1.9.1 Régler les paramètres liés à la sécurité

Tous les paramètres doivent être configurés selon les exigences relatives au système de sécurité. Nous vous recommandons de documenter les paramètres configurés.

Protocole de mise en service JUMO dTRANS p20 SIL				
Désignation de l'appareil :				
Point de mesure :				
Numéro de série :				
Société :				
Test du segment réussi ? OUI[ ]				
Paramètre	**Explication**	**Sélections ***	**Valeur prédéfinie**	**testée ?**
P0	Correction de densité	0,01 … **1,00** … 99,99		
P1 Uni	Unité de mesure de la pression	inH2O, inHG, ftH2O, mmH2O, mmHG PSI, bar, mbar, kg/cm^2, kPa, TORR, MPa, mH2O		
P2 mA	Début de mesure courant	**4.00 mA** (autres valeurs non autorisées)		
P3 mA	Fin de mesure courant	20.00 mA (autres valeurs non autorisées)		
P4 sec	Amortissement	**0,0** à 100.0 s		
P5 RS	Début de mesure	Etendue de mesure nominale		
P6 RE	Fin de mesure	Etendue de mesure nominale		

Protocole de mise en service JUMO dTRANS p20 SIL				
P8 mA	Le générateur de courant	**ne** doit **pas** être activé lorsque la fonction de sécurité est exécutée		
P9 Err	Courant en cas d'erreur	ErLo = 3.6 mA **ErHi = 21.6 mA** ~~LASt = dernière valeur~~		
P10 Key	Commuter le verrouillage du clavier	**O = pas de verrouillage** LA = tous, interface libre LO = tous, sans début de mesure LS = tous, sans début ni fin de mesure LALL = tous, y compris l'interface sur "LALL" après le paramétrage de l'appareil		
P11 Chr	Caractéristique	**Lin = linéaire** ~~SLin = linéaire jusqu'au début de l'extraction de la racine~~ ~~SoFF = off jusqu'au début de l'extraction de la racine~~		
P15 OFF	Offset de la valeur de pression (Déplacement du zéro)	Etendue de mesure nominale		
*** Les valeurs en gras donnent le réglage d'usine** ***** les valeurs ~~barrées~~ ne doivent pas être réglées				
Date :				
Heure :				
Contrôleur :				
Signature				

1.9.2 Vérifier la fonction de sécurité

Vérifiez la fonction de sécurité, de préférence une fois montée Si ce n'est pas possible, vous pouvez également vérifier la fonction de sécurité en état démontée. Veuillez faire en sorte que le convertisseur de pression à vérifier soit monté dans la même position que dans l'installation.

Condition : verrouillage du clavier/verrouillage est désactivé.

Pendant ce contrôle, l'appareil **ne** fonctionne **pas** de manière sécurisé !

Nous vous recommandons d'effectuer les étapes suivantes :

Etape	Action
1	Vérifiez l'état des avertissements et des messages d'erreur
2	Contrôlez les paramètres, énoncés dans le chapitre Chapitre 1.9.1 "Régler les paramètres liés à la sécurité"
3	Contrôlez les limites de l'étendue de mesure
4	Contrôlez le point zéro, par ex. en état sans pression
5	Vérifiez l'extrémité supérieure de l'échelle (P6 RE) en applicant une pression définie
6	Activez le verrouillage du clavier/verrouillage (Paramètre P10)
7	Créez un nouveau protocole de mise en service

⇨ Notice de mise en service chapitre 7 „Commande“

1.10 Comportement en cours de fonctionnement et en cas de panne

Le comportement en cours de fonctionnement et en cas de panne est décrit dans la notice de mise en service.

Il faut revérifier la fonction de sécurité après mise en service, réparation au niveau du dispositif de sécurité ou modification des caractéristiques de sécurité, voir Chapitre 1.9.2 "Vérifier la fonction de sécurité".

Lorsqu'une erreur est détectée au cours du test de fonctionnement, il faut prendre des mesures qui garantissent à nouveau le bon fonctionnement du dispositif de sécurité. Cela peut être le remplacement du convertisseur de mesure, par exemple.

Une documentation des essais effectuées est recommandée

2 Annexe

2.1 Termes et abréviations suivant CEI 61508-1/-2/-3:2010

Nom	Description
Acteur	Normes applicables concernant la sécurité des procédés industriels.
EUC	**E**quipment **U**nder **C**ontrol (EUC) Dispositifs, machines, appareils ou installations, utilisés pour la fabrication, la transformation des matières, le transport, les activités médicales et autres.
E / E / PE	Sécurité fonctionnelle des systèmes électriques, électroniques, électroniques programmables relatifs à la sécurité
Défaillance / Panne	La fin de la capacité d'une unité fonctionnelle, de mettre à disposition une fonction requise ou le fonctionnement d'une unité fonctionnelle est d'une certaine manière différent que ce qui était exigé.
Degré de couverture du diagnostic	**D**iagnostic **C**overage (DC) Proportion de défaillances dangereuses qui sont détectées par des tests de diagnostic automatique en ligne. La proportion de défaillances dangereuses est calculée en utilisant le taux de défaillances dangereuses appartenant aux défaillances dangereuses détectées, divisé par le taux total de défaillances dangereuses.
Erreur	Ecart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte.
Sécurité fonctionnelle	Sous-ensemble de la sécurité globale se rapportant à l'Equipement (EUC) et au système de commande de l'Equipement (EUC) qui dépend du fonctionnement correct des systèmes E/E/PE relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.

Nom	Description
Unité fonctionnelle	Unité composé du hardware ou du software ou des deux, habilitée à exécuter une tâche définie.
Défaillance dangereuse	Défaillance d'un éléments et/ou d'un sous-système et/ou d'un système qui prend part à l'exécution de la fonction de sécurité, qui a) empêche qu'une fonction de sécurité soit exécutée sur demande (mode de demande), ou empêche la défaillance d'une fonction de sécurité provoquée (mode continu à la demande), de sorte que EUC est placé dans un état dangereux ou potentiellement dangereux ; ou b) réduit la probabilité d'exécuter correctement la fonction de sécurité en cas de demande.
Risque tolérable	Défaillance d'un éléments et/ou d'un sous-système et/ou d'un système qui prend part à l'exécution de la fonction de sécurité, qui a) qui conduit au déclenchement intempestif de la fonction de sécurité, de mettre EUC (ou une partie) dans un état de sécurité ou de maintenir dans un état de sécurité ; ou b) qui augmente la probabilité du déclenchement intempestif de la fonction de sécurité, de mettre EUC (ou une partie) dans un état de sécurité ou de maintenir dans un état de sécurité
Risque	Source de dommage potentielle
Sécurité	Abscence de risque inacceptable
Fonction de sécurité	Fonction à réaliser par un système E/E/PE relatif à la sécurité, par un système relatif à la sécurité basé sur une autre technologie, ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'équipement (EUC) par rapport à un événement dangereux spécifique
Intégrité-Sécurité	Probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée.

Nom	Description
Niveau d'intégrité (SIL)	Niveau discret (parmi quatre possibles) permettant de spécifier les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité. SIL 1 étant le plus faible niveau quand SIL 4 est le plus élevé.
Système de sécurité	Système - qui, à la fois met en oeuvre les fonctions de sécurité requises pour atteindre un état de sécurité de l'équipement (EUC) ou pour maintenir un tel état et - qui est également prévu pour atteindre, par lui même ou grâce à des systèmes E/E/PE relatifs à la sécurité et autres mesures de réduction du risque, le niveau d'intégrité de sécurité nécessaire à la mise en oeuvre des fonctions de sécurité requises.
Système instrumenté de sécurité (SIS)	Système instrumenté de sécurité pour exécuter une ou plusieurs fonctions de sécurité. Un système instrumenté de sécurité (SIS) se compose de capteur(s), d'un système de traitement logique et d'actionneurs.
Lambda: λ	Taux de défaillance par heure
Lambda **D**angerous: λ_D	Taux de défaillance dangereuse par heure
Lambda Δangerous Δetect: λ_{DD}	Taux de défaillances dangereuses détectées par heure
Lambda Δangerous Υndetect:λ_{DU}	Taux de défaillances dangereuses non détectées par heure
Lambda Σafe: λ_S	Taux de défaillances sûres par heure
Lambda Σafe Δetect: λ_{SD}	Taux de défaillances détectées par heure
Lambda Σafe Υndetect: λ_{SU}	Taux de défaillances non détectées par heure
BPCS	Système de contrôle de procédé de base
DC	**D**iagnostic **C**overage (taux de couverture des tests de diagnostic)

Nom	Description
FIT	**F**ailure **I**n **T**ime (erreur par heure ($1x10^{-9}$ par h)
HFT	**H**ardware **F**ailure **T**olerance (Tolérance d'erreur du hardware)
PFD	**P**robability of **F**ailure **D**etected (probabilité de défaillances dangereuses si demande)
PFDavg	**P**robability of **F**ailure **D**etected **av**era**g**e (probabilité moyenne de défaillances dangereuses si demande)
PFH	**P**robability of dangerous **F**ailure per **H**our (probabilité de défaillances dangereuses par heure)
MooN	Architecture avec M provenant de canaux N
MTBF	**M**ean **T**ime **B**etween **F**ailure (temps moyen entre deux défaillances)
MTTR	**M**ean **T**ime **T**o **R**estoration (temps moyen avant remise en service)
MTTF	**M**ean **T**ime **T**o **F**ailure (temps moyen jusqu'à la panne)
MRT	**M**ean **R**epair **T**ime (temps moyen de réparation)
SFF	**S**afe **F**ailure **F**raction (part de défaillances sûres)
SIL	**S**afety **I**ntegrity **L**evel (niveau d'intégrité de sécurité)
SC	**S**ystematic **C**apability (aptitude systématique)
PTC	**P**roof **T**est **C**overage (degré de couverture du diagnostic pendant le contre-essai)

3 Certificat

JUMO 2203088 C001

exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 2 CAPABLE

Revision 3.0 September 1, 2025
Surveillance Audit Due
September 30, 2028

ANAB
ANSI National Accreditation Board
ACCREDITED
PRODUCT CERTIFICATION BODY
#1004

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.

exida Certification

C. Krupke
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, V3R0

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

80 N Main St
Sellersville, PA 18960

T-111, V5R2

Les certificats pour les modèles d'appareils homologués peuvent être téléchargés sur le site web du fabricant.

JUMO GmbH & Co. KG
Adresse :
Moritz-Juchheim-Straße 1
36039 Fulda, Allemagne
Adresse de livraison :
Mackenrodtstraße 14
36039 Fulda, Allemagne
Adresse postale :
36035 Fulda, Allemagne
Téléphone : +49 661 6003-0
Télécopieur : +49 661 6003-607
E-Mail: mail@jumo.net
Internet: www.jumo.net

JUMO FRANCE SAS
7 rue des Drapiers
B.P. 45200
57075 Metz Cedex 3, France
Téléphone : +33 3 87 37 53 00
E-Mail: info.fr@jumo.net
Internet: www.jumo.fr

Service de soutien à la vente :
0892 700 733 (0,80 € TTC/minute)

JUMO Automation
S.P.R.L. / P.G.M.B.H. / B.V.B.A.
Industriestraße 18
4700 Eupen, Belgique
Téléphone : +32 87 59 53 00
Télécopieur : +32 87 74 02 03
E-Mail: info.be@jumo.net
Internet: www.jumo.be

JUMO Schweiz AG
Laubisrütistrasse 70
8712 Stäfa, Suisse
Téléphone : +41 44 928 24 44
Télécopieur : +41 44 928 24 48
E-Mail: info.ch@jumo.net
Internet: www.jumo.ch

JUMO