

## Contents

<b>Certificate</b> .....	<b>1</b>
<b>&lt; English &gt;</b>	
<b>1. Safety Instrumented Systems Installation</b> .....	<b>4</b>
1.1 Scope and Purpose .....	4
1.2 Using the transmitter for an SIS Application.....	4
1.2.1 Safety Accuracy .....	4
1.2.2 Diagnostic Response Time.....	4
1.2.3 Setup.....	4
1.2.4 Required Parameter Settings.....	5
1.2.5 Proof Testing.....	5
1.2.6 Repair and Replacement.....	6
1.2.7 Startup Time.....	6
1.2.8 Firmware Update.....	6
1.2.9 Reliability Data .....	6
1.2.10 Lifetime Limits.....	6
1.2.11 Environmental Limits.....	6
1.2.12 Application Limits.....	6
1.3 Definitions and abbreviations .....	7
1.3.1 Definitions.....	7
1.3.2 Abbreviations.....	7
<b>2. Functional Safety Data Sheet</b> .....	<b>8</b>
<b>&lt; 日本語版 &gt;</b> .....	
<b>1. 安全計装システムの設置にあたって</b> .....	<b>10</b>
1.1 適用範囲と目的.....	10
1.2 安全計装システム用途における EJX/EJA のご使用.....	10
1.2.1 安全確度 .....	10
1.2.2 診断応答時間.....	10
1.2.3 設定.....	10
1.2.4 必要なパラメータの設定 .....	11
1.2.5 ブルーフテスト .....	11
1.2.6 修理・交換.....	12
1.2.7 起動時間.....	12
1.2.8 ファームウェアの更新.....	12
1.2.9 安全性データ.....	12
1.2.10 耐用年数の制限 .....	12
1.2.11 環境の制限.....	12
1.2.12 用途の制限.....	12
1.3 用語と略語.....	13
1.3.1 用語.....	13
1.3.2 略語.....	13
<b>2. 機能安全データシート</b> .....	<b>14</b>

This document is the Functional Safety Manual of EJX \*\*\* A / J, EJA \*\*\* E / J.

## Certificate



Product Service

# CERTIFICATE

No. Z10 105352 0001 Rev. 00

**Holder of Certificate:** Yokogawa Electric Corporation  
2-9-32, Nakacho  
Musashino-shi, Tokyo  
180-8750 JAPAN

**Certification Mark:**



**Product:** Pressure Meters

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

**Test report no.:** YM94108T

**Valid until:** 2024-08-01

**Date,** 2019-08-02

( Matthias Ramold )

Page 1 of 3  
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®



Product Service

# CERTIFICATE

No. Z10 105352 0001 Rev. 00

## Parameters:

Rated input	10.5 to 42.0Vdc
Rated output	4 to 20mA
Operating temperature	-55°C to +85°C
Humidity	0 ~ 100 % RH
Safety function	Safety analog output of 4 to 20 mA DC signal corresponding to the measured differential and static pressure. (HFT=0) SIL2 (HFT=1) SIL3

## Tested according to:

IEC 61508-1:2010  
IEC 61508-2:2010  
IEC 61508-3:2010  
IEC 61511-1:2016  
IEC 61511-1:2016/AMD1:2017  
IEC 61326-3-2:2017  
IEC 61010-1:2010  
IEC 61010-1:2010/AMD1:2016  
EN 61010-1:2010/A1:2019

## Factory(ies):

103932

## Model(s):

Pressure Transmitter EJX and EJA Series

EJX aaaa-bcdef-ghijk-lmnopqrs-tuvw/xx

EJX aaaa-bcdef-ghijk-lmno-pqrs/xx for only EJX117J

EJX aaaa-bcdef-ghijk-lmno-p/xx for only EJX213J

with:

aaaa	Transmitter
	110A,110J Differential pressure transmitter
	115A,115J Differential pressure transmitter
	117J Sanitary Type Differential Pressure Transmitter
	118A,118J Diaphragm sealed differential pressure transmitter
	120A,120J Differential pressure transmitter
	130A,130J Differential pressure transmitter
	210A,210J Flange mounted differential pressure transmitter
	213J Sanitary Type Liquid Level Transmitter
	310A,310J Absolute pressure transmitter
	430A,430J Gauge pressure transmitter
	438A,438J Diaphragm sealed gauge pressure transmitter
	440A,440J Gauge pressure transmitter
	510A,510J Absolute pressure transmitter
	530A,530J Gauge pressure transmitter
	533J Sanitary Type Gauge Pressure Transmitter
	610A Absolute pressure transmitter
	630A Gauge pressure transmitter

Page 2 of 3

TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®



Product Service

# CERTIFICATE

No. Z10 105352 0001 Rev. 00

b	Output signal	
D	4 to 20 mA DC with digital communication (BRAIN protocol)	
E	4 to 20 mA DC with digital communication (HART 5 protocol)	
J	4 to 20 mA DC with digital communication (HART 5/HART 7 protocol)	
c to xx	Non-safety related codes (any code)	

I (=L) to w are not applicable depending on the model.

EJA aaaa-bcdef-ghijk-lmnopqrs-tuvw/xx

EJA aaaa-bcdef-ghijk-lmno-pqrs/xx for only EJA117J

EJA aaaa-bcdef-ghijk-lmno-p/xx for only EJA213J

with:

aaaa	Transmitter	
110E,110J	Differential pressure transmitter	
115E,115J	Differential pressure transmitter	
117J	Sanitary Type Differential Pressure Transmitter	
118E,118J	Diaphragm sealed differential pressure transmitter	
120E,120J	Differential pressure transmitter	
130E,130J	Differential pressure transmitter	
210E,210J	Flange mounted differential pressure transmitter	
213J	Sanitary Type Liquid Level Transmitter	
310E,310J	Absolute pressure transmitter	
430E,430J	Gauge pressure transmitter	
438E,438J	Diaphragm sealed gauge pressure transmitter	
440E,440J	Gauge pressure transmitter	
510E,510J	Absolute pressure transmitter	
530E,530J	Gauge pressure transmitter	
533J	Sanitary Type Gauge Pressure Transmitter	
610E	Absolute pressure transmitter	
630E	Gauge pressure transmitter	
b	Output signal	
D	4 to 20 mA DC with digital communication (BRAIN protocol)	
E	4 to 20 mA DC with digital communication (HART 5 protocol)	
J	4 to 20 mA DC with digital communication (HART 5/HART 7 protocol)	
c to xx	Non-safety related codes (any code)	

I (=L) to w are not applicable depending on the model.

---

## 1. Safety Instrumented Systems Installation



### **WARNING**

---

When using the transmitter for Safety Instrumented Systems (SIS) application, the instructions and procedures in this section must be strictly followed in order to preserve the transmitter for that safety level.

---

### 1.1 Scope and Purpose

This section provides an overview of the user responsibilities for installation and operation of the transmitter in order to maintain the designed safety level for Safety Instrumented Systems (SIS) applications. Items that will be addressed are proof testing, repair and replacement of the transmitter, reliability data, lifetime, environmental and application limits, and parameter settings.

### 1.2 Using the transmitter for an SIS Application

#### 1.2.1 Safety Accuracy

The transmitter has a specified safety accuracy of 2%. This means that the internal component failures are listed in the device failure rate if they will cause an error of 2% or greater.

#### 1.2.2 Diagnostic Response Time

The transmitter will report an internal failure within 5 seconds of the fault occurrence.

#### 1.2.3 Setup

During installation the transmitter must be setup with engineering units parameters. This is typically done with a handheld terminal. These parameters must be verified during the installation to insure that the correct parameters are in the transmitter. Engineering range parameters can be verified by reading these parameters from the optional local display or by checking actual calibration of the transmitter.

For details, refer to Clause Setting Parameters for setting range.

BRAIN: IM 01C25T03-01E

HART: IM 01C25T01-06EN Appendix 3

The calibration of the transmitter must be performed after parameters are set.

### 1.2.4 Required Parameter Settings

The following parameters need to be set in order to maintain the designed safety integrity.

**Table 1.1 Required Parameter Settings**

Item	Description
Burnout direction switch	To specify if the output should go 21.6 mA or higher or 3.6 mA or lower upon detection of an internal failure.
Write protection switch	The write function should be disabled.

### 1.2.5 Proof Testing

The objective of proof testing is to detect failures within the transmitter that are not detected by the diagnostics of the transmitter. Of main concern are undetected failures that prevent the safety instrumented function from performing its intended function. See table 1.2 for proof testing method.

The frequency of the proof tests (or the proof test interval) is to be determined in the reliability calculations for the safety instrumented functions for which the transmitter is applied. The actual proof tests must be performed more frequently or as frequently as specified in the calculation in order to maintain required safety integrity of the safety instrumented function.

The following tests need to be specifically executed when a proof test is performed. The results of the proof test need to be documented and this documentation should be part of a plant safety management system. Failures that are detected should be reported to Yokogawa.

The personnel performing the proof test of the transmitter should be trained in SIS operations including bypass procedures, transmitter maintenance, and company management of change procedures.

**Table 1.2 Proof Testing**

Testing method	Tools required	Expected outcome	Remarks
<b>Functional test:</b> 1. Follow all Management of Change procedures to bypass logic solvers if necessary. 2. Execute HART/BRAIN command to send value to high alarm (21.6 mA) and verify that current has reached this level. 3. Execute HART/BRAIN command to send value to low alarm (3.6 mA) and verify that current has reached this level. 4. Restore logic solvers operation and verify.	<ul style="list-style-type: none"> <li>Handheld terminal</li> </ul>	Proof Test Coverage =52%	The output needs to be monitored to assure that the transmitter communicates the correct signal.
Perform three point calibration along with the functional test listed above.	<ul style="list-style-type: none"> <li>Handheld terminal</li> <li>Calibrated pressure source</li> </ul>	Proof Test Coverage =99%	

---

### 1.2.6 Repair and Replacement

If repair is to be performed with the process online the transmitter will need to be bypassed during the repair. The user should setup appropriate bypass procedures.

In the unlikely event that the transmitter has a failure, the failures that are detected should be reported to Yokogawa.

When replacing the transmitter, the procedure in the installation manual should be followed.

The personnel performing the repair or replacement of the transmitter should have a sufficient skill level.

### 1.2.7 Startup Time

The transmitter generates a valid signal within 1 seconds of power-on startup.

### 1.2.8 Firmware Update

In case firmware updates are required, they will be performed at factory. The replacement responsibilities are then in place. The user will not be required to perform any firmware updates.

### 1.2.9 Reliability Data

Refer to Table 2.1 Functional Safety data in this document for failure rates and failure modes.

The transmitter is certified up to SIL2 for use in a simplex (1oo1) configuration, depending on the PFDavg calculation of the entire Safety Instrumented Function.

The development process of the transmitter is certified up to SIL3, allowing redundant use of the transmitter up to this Safety Integrity Level, depending the PFDavg calculation of the entire Safety Instrumented Function.

When using the transmitter in a redundant configuration, the use of a common cause factor ( $\beta$ -factor) of 2% is suggested. (However, if the redundant transmitters share an impulse line or if clogging of the separate impulse lines is likely, a common cause factor of 10% is suggested.)

Note that the failure rates of the impulse lines need to be accounted for in the PFDavg calculation.

### 1.2.10 Lifetime Limits

The expected lifetime of the transmitter is 50 years. The reliability data listed the FMEDA report is only valid for this period. The failure rates of the transmitter may increase sometime after this period. Reliability calculations based on the data listed in the FMEDA report for transmitter lifetimes beyond 50 years may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

### 1.2.11 Environmental Limits

The environmental limits of the transmitter are specified in the user's manual IM 01C25.

### 1.2.12 Application Limits

The application limits of the transmitter are specified in the user's manual IM 01C25. If the transmitter is used outside of the application limits, the reliability data listed in 1.2.9 becomes invalid.

---

## 1.3 Definitions and abbreviations

### 1.3.1 Definitions

#### Safety

Freedom from unacceptable risk of harm

#### Functional Safety

The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment/machinery/plant/apparatus under control of the system

#### Basic Safety

The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition

#### Verification

The demonstration for each phase of the life-cycle that the (output) deliverables of the phase meet the objectives and requirements specified by the inputs to the phase. The verification is usually executed by analysis and/or testing

#### Validation

The demonstration that the safety-related system(s) or the combination of safety-related system(s) and external risk reduction facilities meet, in all respects, the Safety Requirements Specification. The validation is usually executed by testing

#### Safety Assessment

The investigation to arrive at a judgment -based on evidence- of the safety achieved by safety-related systems

Further definitions of terms used for safety techniques and measures and the description of safety related systems are given in IEC 61508-4.

### 1.3.2 Abbreviations

FMEDA	Failure Mode, Effects and Diagnostic Analysis
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLC	Safety Lifecycle
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFDavg	Average Probability of dangerous Failure on Demand
MTBF	Mean Time Between Failures

## 2. Functional Safety Data Sheet

**Table 2.1 Functional Safety data**

Certificate/Reg.-No.	Z10 105352 0001 Rev.00
Product Category	Pressure Transmitter
Type Designation	EJX A Series, EJX J Series, EJA E Series, EJA J Series
Codes and Standards	IEC 61508:2010
Valid Until	2024-08-01
Scope and Result	Sensors for pressure measurement of liquids and gases. The sensors of the EJX and EJA Series comply with the requirements of the stated standards and can be used in a safety-related system with a hardware fault tolerance HFT=0 up to SIL 2 and under consideration of the minimum required hardware fault tolerance HFT=1 in a redundant structure up to SIL 3. Output currents 21.6 mA have to be considered by the downstream safety device as failure condition.
Safety-related output signal	4-20 mA
SIL	2(3)
Type	B
HFT	0(1)
Mode of operation	Low demand mode
$\lambda$ SD	103 FIT
$\lambda$ SU	123 FIT
$\lambda$ DD	171 FIT
$\lambda$ DU	31 FIT
SFF	92.7%
PFDavg (*1)	$1.37 \times 10^{-4}$
MTBF	267 years
Recommended proof test interval	1 year

\*1: PFDavg is calculated by  $T = 8760$  (H) = 1 year, Single channel architecture (HFT = 0).

In order to judge the failure behavior of the EJX/EJA transmitter, define the failure of the device.

**Table 2.2 Failure categories description**

Safe state	Safe state is indicated by outside of normal output range for output signal. Normal output range is defined as 3.6 – 21.6 mA(Safety accuracy 2%).
Dangerous state	Dangerous state is the output signal shows a measurement error exceeding 2%.
$\lambda$ SD	Failure rate for safe detected failures (*1)
$\lambda$ SU	Failure rate for safe undetected failures (*2)
$\lambda$ DD	Failure rate for dangerous detected failures (*3)
$\lambda$ DU	Failure rate for dangerous undetected failures (*4)
No effect	Failure of a component that is part of the safety function but that has no effect on the safety function. (*5)

\*1: There is a malfunction that transitions the output signal to Safe state due to a failure of the diagnostic circuit.

\*2: There is a breakdown in which the transmitter does not start up.

Failure diagnosis is impossible with the transmitter itself, but it can be diagnosed as a Safe state with a logic solver.

\*3: It is a failure of the sensor circuit and the AMP circuit.

It is a dangerous fault but a fault detected by automatic diagnosis.

The output signal becomes Safe State with diagnostic function.

\*4: There are faults that are not diagnosed by automatic diagnosis due to dangerous faults.

- Failure that takes 5 sec or more to transit to safe state in case of failure

- Failure within normal output range at failure

- Failure to output in the direction different from the direction set in the burnout direction at the time of failure

However, the above fault can be detected by proof test.

For the calculation of safety related parameters such as SFF, PFDavg etc., the above fault is included as  $\lambda$ DU.

\*5: It is indicator malfunction or failure of the protection circuit. It is not included in the failure rate calculation due to a failure that does not affect the output signal.

**Table 2.3 Safety Related Parameter (Ambient temperature 40°C)**

Device: EJX/EJA series

Signal Output	HW Rev.	SW Rev.	$\lambda$ SD (FIT)	$\lambda$ SU (FIT)	$\lambda$ DD (FIT)	$\lambda$ DU (FIT)	SFF (%)	PFDavg	MTBF
4-20 mA output	1.2	3.01	103	123	171	31	92.7	1.37×10 <sup>-4</sup>	267

PFDavg is calculated by T = 8760 (H) = 1 year, Single channel architecture (HFT = 0).

## < 日本語版 >

### 1. 安全計装システムの設置にあたって



#### 警告

EJX/EJA を安全計装システム（Safety Instrumented Systems: SIS）用途として用いる際には、EJX/EJA の安全度を保つために本付録で述べる指示と手順を遵守してください。

#### 1.1 適用範囲と目的

本項では、安全計装システム用途として設計された安全度を保つ上で求められる、EJX/EJA の設置と操作の際に必要な使用上の注意点と行うべき作業の概要について述べます。ここで取り上げる項目は、伝送器のプルーフテストと修理・交換、安全性データ、耐用年数、環境および用途に関する制限、パラメータの設定です。

#### 1.2 安全計装システム用途における EJX/EJA のご使用

##### 1.2.1 安全確度

EJX/EJA の規定安全確度は 2 % です。これは内部部品の故障により生じる誤差が 2 % 以上の場合に、機器の故障として扱われるということです。

##### 1.2.2 診断応答時間

EJX/EJA は内部故障の発生を 5 秒以内に通知できます。

##### 1.2.3 設定

ハンドヘルド端末等の設定ツールを用いて、レンジと単位を設定してください。伝送器の設置後、レンジと単位が正しく設定されていることをご確認ください。

詳細は下記マニュアルの「パラメータの設定」の測定レンジの設定の項を参照ください。

BRAIN：各製品のハードウェアマニュアル

（例：EJX110J の場合 IM 01C26B01-01JA）

HART：IM 01C26T01-06JA

伝送器の校正は、パラメータの設定後に行ってください。

## 1.2.4 必要なパラメータの設定

安全度を保つために、以下のパラメータ設定が必要です。

表 1.1 設定パラメータ

項目	説明
バーンアウト方向スイッチ	内部故障検出時の出力の値を 21.6 mA 以上あるいは 3.6 mA 以下に指定します。
ライトプロテクトスイッチ	書き込み機能を無効にします。

## 1.2.5 プルーフテスト

伝送器の意図した通りの安全機能の実行を阻害するような、自己診断で検知されない故障を検出するためにプルーフテストの実施が必要です。

プルーフテストの間隔は、EJX/EJA を含む安全計装機能ごとに行われる安全度計算により決定します。安全計装機能の安全度を維持するには、安全度計算で指定した頻度またはそれ以上でプルーフテストを行う必要があります。

プルーフテストでは、以下の試験を実施する必要があります。プルーフテストの結果は文書化される必要があります、その文書はプラントの安全管理の一部とすべきです。故障が検出された場合は当社までご連絡ください。

伝送器のプルーフテストを行う作業者は、バイパス手順、EJX/EJA のメンテナンス、変更管理の手順など、安全計装システムの運用について熟知している必要があります。

表 1.2 プルーフテスト

試験方法	必要なツール	予想される結果	備考
<b>機能試験</b> 1. 必要に応じ、ロジックソルバーをバイパスするための変更管理手順にすべて従います。 2. HART/BRAIN コマンドを実行してハイアラーム (21.6 mA) の値を出力させ、電流がこの水準にあるか検証します。 3. HART/BRAIN コマンドを実行してローアラーム (3.6 mA) の値を出力させ、電流がこの水準にあるか検証します。 4. ロジックソルバーの動作を復元させ、検証を行います。	・ハンドヘルド端末	プルーフテスト カバー率：52%	伝送器が正確な信号を出しているか確認するために出力を監視する必要があります。
三点校正を上記の機能試験と同時に行います。	・ハンドヘルド端末 ・校正圧力源	プルーフテスト カバー率：99%	

### 1.2.6 修理・交換

プロセスがオンライン中に EJX/EJA の修理を行う場合は、EJX/EJA をバイパスしてください。ユーザーはバイパス手順を正しく設定する必要があります。検出された故障については当社までご連絡ください。EJX/EJA の交換に際しては、本取扱説明書の手順に従ってください。EJX の修理あるいは交換の際は、訓練を受けたエンジニアが行ってください。

### 1.2.7 起動時間

EJX/EJA は、電源投入後 1 秒以内に有効な信号を出力します。

### 1.2.8 ファームウェアの更新

ユーザーはファームウェアの更新を行うことはありません。ファームウェアの更新が必要と判断された場合、更新は引取りによって行います。

### 1.2.9 安全性データ

故障率と故障モードは本マニュアルの Table 2.1 Functional Safety data を参照ください。

EJX/EJA は単独使用において、安全計装機能全体の PFDavg 計算による安全度水準 (Safety Integrity Level:SIL) 2 までに適用できるという認証を受けています。また冗長構成では最大 SIL3 までの適用が可能として認定されています。

冗長構成で使用するには、安全計装機能の PFD 計算のための共通原因故障率 ( $\beta$ -factor) を 2% にすることを推奨します。(冗長構成の伝送器同士で導圧管を共有する場合、または導圧管が詰まる可能性がある場合には、10% にするようお勧めします)。導圧管の故障率を PFDavg の計算に算入する必要があります。

### 1.2.10 耐用年数の制限

EJX/EJA の予測耐用年数は 50 年です。FMEDA レポートの信頼性データは 50 年を有効とします。50 年を超えて使用されると EJX/EJA の故障率は上昇すると考えられるので、FMEDA レポートに記載された安全性データに基いた安全度水準は達成できない可能性があります。

### 1.2.11 環境の制限

EJX/EJA の環境に関する制限は、機器本体の取扱説明書で規定しています。

### 1.2.12 用途の制限

本取扱説明書で規定した EJX/EJA の用途に関する制限を外れて使用する場合、1.2.9 に記載された安全性データは無効です。

## 1.3 用語と略語

### 1.3.1 用語

#### 安全

受容できないリスクから免れている状態  
(JIS C 0508 の表現です。)

#### 機能安全

機器・機械・プラント・装置に対して安全と定義された状態を達成または維持するために必要な動作を実行するシステムの能力を指します。

#### 基本的安全

感電、火災、爆発などの危険から人間を保護するように機器は設計および製造されなければなりません。こうした保護は、通常使用時および 1 故障時でも常に有効でなければなりません。

#### 検証

##### 適合確認

ライフサイクルの各段階で、各段階の最初に意図した目的と要求事項に見合うものが最終的に得られたことを実証します。検証は、分析あるいは試験、またはその両方により行われるのが普通です。

##### 妥当性確認

安全関連システムあるいはその組み合わせと、外的リスク軽減施設が、あらゆる点において安全要求仕様を満たしていることを実証します。妥当性検査は、試験により行われるのが普通です。

##### 安全アセスメント

安全関連システムによって安全性が実現されたことを、証拠に基づいて判断するための調査を指します。

その他の安全手法および対策で用いられる用語の定義および安全関連システムの説明については、JIS C 0508-4 (IEC 61508-4) をご参照ください。

### 1.3.2 略語

FMEDA	(Failure Mode, Effects and Diagnostic Analysis) 故障モード, 影響および診断分析
SIF	(Safety Instrumented Function) 安全計装機能
SIL	(Safety Integrity Level) 安全度水準
SIS	(Safety Instrumented Systems) 安全計装システム
SLC	(Safety Lifecycle) 安全ライフサイクル
HFT	(Hardware Fault Tolerance) ハードウェアフォールトトレランス
SFF	(Safe Failure Fraction) 安全側故障割合
PFDAvg	(Average Probability of dangerous Failure on Demand) 作動要求時の危険側機能失敗平均確率
MTBF	(Mean Time Between Failures) 平均故障時間

## 2. 機能安全データシート

**Table 2.1 Functional Safety data**

Certificate/Reg.-No.	Z10 105352 0001 Rev.00
Product Category	Pressure Transmitter
Type Designation	EJX A Series, EJX J Series, EJA E Series, EJA J Series
Codes and Standards	IEC 61508:2010
Valid Until	2024-08-01
Scope and Result	Sensors for pressure measurement of liquids and gases. The sensors of the EJX and EJA Series comply with the requirements of the stated standards and can be used in a safety-related system with a hardware fault tolerance HFT=0 up to SIL 2 and under consideration of the minimum required hardware fault tolerance HFT=1 in a redundant structure up to SIL 3. Output currents 21.6 mA have to be considered by the downstream safety device as failure condition.
Safety-related output signal	4-20 mA
SIL	2(3)
Type	B
HFT	0(1)
Mode of operation	Low demand mode
$\lambda$ SD	103 FIT
$\lambda$ SU	123 FIT
$\lambda$ DD	171 FIT
$\lambda$ DU	31 FIT
SFF	92.7%
PFDavg (*1)	$1.37 \times 10^{-4}$
MTBF	267 years
Recommended proof test interval	1 year

\*1 : PFDavg は  $T=8760(H)=1\text{year}$ , Single channel architecture(HFT=0) で算出している。

EJX/EJA 伝送器の故障動作を判断するために、デバイスの故障に関する定義をしています。

**Table 2.2 Failure categories description**

Safe state	安全状態は、出力信号が通常出力範囲外で示されます。 通常出力範囲は 3.6 ~ 21.6 mA(安全確度 2%)と定義しています。
Dangerous state	危険な状態は、出力信号が 2%を超える測定誤差を示す状態です。
$\lambda$ SD	検出された安全な故障の故障率(*1)
$\lambda$ SU	検出されなかった安全な故障に対する故障率(*2)
$\lambda$ DD	検出された危険な故障の故障率(*3)
$\lambda$ DU	検出されなかった危険な故障に対する故障率(*4)
No effect	安全機能の一部であるが安全機能に影響を及ぼさないコンポーネントの故障(*5)

\*1： 診断回路の故障で出力信号を Safe state へ状態遷移する故障があります。

\*2： 伝送器が起動しない故障があります。

伝送器自身で故障診断不可ですが、ロジックソルバーで Safe state であると診断可能です。

\*3： センサー回路や AMP 回路の故障です。危険な故障ですが自動診断によって検出される故障です。  
診断機能で出力信号が Safe State になります。

\*4： 危険な故障で自動診断により診断されていない故障があります。

・故障時、安全状態に遷移するまで 5sec 以上かかる故障

・故障時、正常出力範囲内となる故障

・故障時、バーンアウト方向で設定した方向と異なる方向へ出力する故障

ただし、上記故障はプルーフトストで検出することが可能です。

SFF, PFDavg 等の安全関連パラメータの算出には上記故障を  $\lambda$ DU として含んでおります。

\*5： 表示器の故障や保護回路の故障です。出力信号へ影響しない故障のため、故障率計算に含んでおりません。

**Table 2.3 Safety Related Parameter (周囲温度 40°C)**

Device: EJX/EJA series

Signal Output	HW Rev.	SW Rev.	$\lambda$ SD (FIT)	$\lambda$ SU (FIT)	$\lambda$ DD (FIT)	$\lambda$ DU (FIT)	SFF (%)	PFDavg	MTBF
4-20 mA output	1.2	3.01	103	123	171	31	92.7	$1.37 \times 10^{-4}$	267

PFDavg は T=8760(H)=1year, Single channel architecture(HFT=0) で算出している。

## Revision Information

Title : Functional Safety Manual for /SLT

Manual number : TI 01C25A05-21EN

### November 2019/1st Edition

- New publication