Technical Information

Functional Safety Manual exida® certification

DPharp EJX™
DPharp EJA™

TI 01C25A05-11EN

Contents

< English >

< 日本語版 >

3rd Edition July 2023 (YK)

1. Safety Instrumented Systems Installation

WARNING

The contents of this section are cited from exida.com safety manual on the transmitters specifically observed for the safety transmitter purpose. 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.
For EJX910A/EJX930A, refer to Appendix1 of IM 01C25R02-01E. For EJXC40A, refer to Appendix 1 of IM 01C25W05-01EN.

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 the clause of “Setting Parameters” for setting range in the following manual.
BRAIN communication type: IM 01C25T03-01E
HART communication type: IM 01C25T01-06EN
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
Functional test: 1. Follow all Management of Change procedures to bypass logic solvers if necessary. 2. Execute HART/BRAIN command to send value to high alarm (110%) and verify that current has reached this level. However, in case of option code C2 or C3, send value to 103.1%. 3. Execute HART/BRAIN command to send value to low alarm (-2.5%) and verify that current has reached this level. However, in case of option code C2 or C3, send value to -1.2%. 4. Restore logic solvers operation and verify.	• Handheld terminal	Proof Test Coverage =52%	The output needs to be monitored to assure that the transmitter communicates the correct signal.
Perform two point calibration along with the functional test listed above.	• Handheld terminal • Calibrated pressure source	Proof Test Coverage =99%	

The proof test procedure corresponds to the following revisions.

Hardware revision	Software revision	IM No. (HART)	IM No. (BRAIN)
1.1	3.01	IM 01C25T01-06EN Ed.6 or later	IM 01C25T03-01E Ed.6 or later
1.2	3.01	IM 01C25T01-06EN Ed.6 or later	IM 01C25T03-01E Ed.6 or later
	5.01	IM 01C25T01-06EN Ed.8 or later	IM 01C25T03-01E Ed.8 or later
	5.02	IM 01C25T01-06EN Ed.8 or later	IM 01C25T03-01E Ed.8 or later

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 2 seconds of power-on startup for software revision 5.01 or later. The previous revision is within 1 second.

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 section 2 of “Functional Safety Data Sheet” 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 (β-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.
FMEDA report No.: YEC11/10-046 R001 V3R1

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
SC	Systematic Capability
SFF	Safe Failure Fraction
PFDavg	Average Probability of dangerous Failure on Demand

2. Functional Safety Data Sheet

Table 2.1 Functional Safety data

Product Category	Differential Pressure and Pressure Transmitter
Type Designation	EJX A and J Series (Except for EJX910A/930A and EJXC40A), EJA E and J Series (Except for EJAC60E/J)
Codes and Standards	IEC 61508 :2010 Parts 1-7
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.
Electronics	4-20 mA DC with digital communication BRAIN/HART protocol
Safety-related output signal	4-20 mA DC
Safety Manual	Section 1 on this document
SC	3
SIL	2(3)
Type	B
HFT	0(1)
Mode of operation	Low demand mode
λSD	0 FIT (*1)
λSU	55 FIT (*1)
λDD	354 FIT (*1)
λDU	30 FIT (*1)
SFF	93.2%
Valid hardware version	1.1 (*2) 1.2
Valid software version	3.01 5.01 5.02

*1: This number is representative of EJX-A, EJX-J, EJA-E, EJA-J series.
This number and the number for products with Diaphragm Seal (Remote Seal) are described on FMEDA report from Yokogawa.
Report No.: YEC11/10-046 R001 V3R1

*2: This is combined with only 3.01 of software version.

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

Table 2.2 Failure categories description

Fail-Safe State	Failure that deviates the process signal or the actual output by more than 2% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (< 3.6 or > 21.6 mA).
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within active scale.
Fail Dangerous Undetected (*1)	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous butt is detected by automatic diagnostics.
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> 21.6 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 mA).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

*1: 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, PFDaverage etc., the above fault is included as λDU.

< 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章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。
EJX910A/EJX930A については IM 01C25R02-01JA 付録 1 を参照してください。EJXC40A については IM 01C25W05-01JA 付録 1 を参照してください。

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

ハンドヘルドターミナル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 通信形：各製品のハードウェアマニュアル
（例：EJX110J の場合　IM 01C26B01-01）

HART 通信形：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，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
機能試験 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（110%）の値を出力させ，電流がこの水準にあるか検証します。 ただし，付加仕様 C2 または C3 の場合，103.1% で実行してください。 3. HART/BRAIN コマンドを実行してローアラーム（-2.5%）の値を出力させ，電流がこの水準にあるか検証します。 ただし，付加仕様 C2 または C3 の場合，-1.2% で実行してください。 4. ロジックソルバーの動作を復元させ，検証を行います。	・ハンドヘルドターミナル	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。
二点校正を上記の機能試験と同時に行います。	・ハンドヘルドターミナル ・校正圧力源	プルーフテストカバー率：99%	

プルーフテストの手順は下記レビジョンに対応する。

ハードウェアレビジョン	ソフトウェアレビジョン	IM 番号 (HART)	IM 番号 (BRAIN)
1.1	3.01	IM 01C26T01-06JA Ed.4 or later	各製品のハードウェアマニュアル (例：EJX110J の場合 IM 01C26B01-01 Ed.8 or later)
1.2	3.01	IM 01C26T01-06JA Ed.4 or later	各製品のハードウェアマニュアル (例：EJX110J の場合 IM 01C26B01-01 Ed.10 or later)
	5.01	IM 01C26T01-06JA Ed.6 or later	各製品のハードウェアマニュアル (例：EJX110J の場合 IM 01C26B01-01 Ed.13 or later)
	5.02	IM 01C26T01-06JA Ed.6 or later	各製品のハードウェアマニュアル (例：EJX110J の場合 IM 01C26B01-01 Ed.13 or later)

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/EJA 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，ソフトウェアリビジョン 5.01 以降の場合，電源投入から 2 秒以内に有効な信号を生成します。ソフトウェアリビジョン 5.01 以前の場合は，1 秒以内に有効な信号を生成します。

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 2 章 機能安全データシートを参照ください。
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際には，安全計装機能の PFD 計算のための共通原因故障率（β -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。
FMEDA レポート番号 : YEC11/10-046 R001 V3R1

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
SC（Systematic Capability）決定論的対応能力
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

2. 機能安全データシート

Table 2.1 Functional Safety data

Product Category	Differential Pressure and Pressure Transmitter
Type Designation	EJX A and J Series (Except for EJX910A/930A and EJXC40A), EJA E and J Series (Except for EJAC60E/J)
Codes and Standards	IEC 61508 :2010 Parts 1-7
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.
Electronics	4-20 mA DC with digital communication BRAIN/HART protocol
Safety-related output signal	4-20 mA DC
Safety Manual	Section 1 on this document
SC	3
SIL	2(3)
Type	B
HFT	0(1)
Mode of operation	Low demand mode
λSD	0 FIT (*1)
λSU	55 FIT (*1)
λDD	354 FIT (*1)
λDU	30 FIT (*1)
SFF	93.2%
Valid hardware version	1.1 (*2) 1.2
Valid software version	3.01 5.01 5.02

*1： この数値は EJX-A, EJX-J, EJA-E, EJA-J series の代表値です。この数値，および，ダイアフラムシール (リモートシール) が付属される製品の数値は，当社が提供する FMEDA レポートに記載されています。
レポート番号 : YEC11/10-046 R001 V3R1

*2： このバージョンはソフトウェアバージョン 3.01 のみと組み合わせになります。

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

Fail-Safe State	プロセス信号または実際の出力がスパンの 2%を超えて逸脱し，ユーザーが定義した閾値（トリップ点）に向かってドリフトする故障であり，出力が通常出力の範囲内にとどまるような故障。
Fail Safe	プロセスからの要求なしにデバイスを定義済みのフェイルセーフ状態に移行させる故障。
Fail Detected	出力信号が事前に定義されたアラーム状態（3.6 mA 以下または 21.6 mA 以上）となる故障。
Fail Dangerous	プロセス信号または実際の出力がスパンの 2%を超えて逸脱し，ユーザーが定義した閾値（トリップ点）から離れていく故障であり，出力が通常出力の範囲内に収まるような故障。
Fail Dangerous Undetected (*1)	危険な故障であり，自動診断で診断されていない故障。
Fail Dangerous Detected	危険な故障であるが，自動診断で検出される故障。
Fail High	出力信号が上限範囲外またはハイアラーム出力電流（21.6 mA 以上）になる原因となる故障。
Fail Low	出力信号が下限範囲外またはローアラーム出力電流（3.6 mA 以下）になる原因となる故障。
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。
Annunciation Detected	安全性に直接影響を与えるのではなく，将来の障害（診断回路内の故障など）を検出する機能に影響を与え，それが内部診断によって検出される故障。 故障検出通知の不具合は誤った診断アラームにつながります。
Annunciation Undetected	安全性に直接影響を与えるのではなく，将来の障害（診断回路内の障害など）を検出する機能に影響を与え，内部診断では検出されない故障。

*1：　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テストで検出することが可能です。
SFF, PFDaverage 等の安全関連パラメータの算出には上記故障を λDU として含んでおります。

Revision Information

Title : Functional Safety Manual

Manual number : TI 01C25A05-11EN

May 2020/1st Edition
- New publication

September 2020/2nd Edition
- Add software revision

July 2023/3rd Edition
- Update proof testing
- Update functional safety data