

Safety manual for Fisher™ FIELDVUE™ 4400 Digital Position Transmitter

This supplement applies to

Instrument Level	SIS
Device Type	0x1314
Device Revision	1
Hardware Revision	1
Firmware Revision	3.1.2

1. Purpose

This safety manual provides information necessary to design, install, verify, and maintain a Safety Instrumented Function (SIF) utilizing the Fisher 4400 digital position transmitter. It describes the conditions of use for the 4400 in safety applications. This document must be thoroughly reviewed and implemented as part of the safety lifecycle. This information is necessary for meeting the IEC61508 or IEC61511 functional safety standards.

⚠ WARNING

This instruction manual supplement is not intended to be used as a stand-alone document. It must be used in conjunction with the Fisher 4400 Instruction Manual ([D104738X012](#))

Failure to use this instruction manual supplement in conjunction with the above referenced document could result in personal injury or property damage. If you have any questions regarding these instructions or need assistance in obtaining this document, contact your [Emerson sales office](#).

2. Description of the Device

The FIELDVUE 4400 transmitter senses the position of rotary or sliding-stem valves, vents, dampers, or other devices. It provides a precise 4-20 mA feedback signal to indicate equipment position with digital capability via HART® communication for process variable notifications and alerts/alarms. Position sensing uses a linkageless feedback design that eliminates direct contact with the measured device (e.g. valve, regulator, level, louver, or other devices).

4400 SIS Default Settings

Application	Position	Position
Alarm Switch	Switch One (Low) Alarm	High Alarm
	Switch Two (High) Alarm	
Safety Recovery	Auto	Manual
	Manual	
Trip Alarm Current Settings	Device Malfunction	Enable
	Reference Voltage Failed	Enable
	PV Analog Output Readback Limit Failed	Enable
	Instrument Temperature Sensor Alert	Enable
	Hall Sensor Alert	Enable
	Hall Diagnostic Alert	Enable
	Program Memory Failed	Enable
	NVM Error	Enable
	RAM Test Error Alert	Enable
	Watchdog Reset Executed	Enable
	PV HiHi Alert	Disable
	PV LoLo Alert	Disable

3. Terms, Abbreviations, and Acronyms

4400	Digital position transmitter, product model designation for Safety Instrumented System applications.
Device Response Time	Time required for the digital position transmitter to carry out its part of the safety function, includes time taken to sense a change in input (magnet array position) and transmit a corresponding output signal.
Diagnostic test interval	Time taken to detect internal faults.
Fault Reaction Time	Time taken to respond once a fault is detected.
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer, open protocol for digital communication superimposed over a direct current.
HFT	Hardware Fault Tolerance
λ	Failure rate. λ_{DD} : dangerous detected; λ_{DU} : dangerous undetected; λ_{SD} : safe detected; λ_{SU} : safe undetected.
Low Demand Mode	Mode of operation of a safety instrumented function where the demands to activate the SIF are less than once every two proof test intervals.
Magnet Assembly	Magnet connected to valve stem or similar of monitored equipment
PF_{AVG}	Average Probability of Failure on Demand
Process Safety Time	Period of time between a failure occurring in the system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed
Safety	Freedom from unacceptable risk of harm.
Safety Function	Function of a device or combination of devices intended to be used within a Safety Instrumented System to reduce the probability of a specific hazardous event to an acceptable level.
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
Type B Element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

4. Related Literature

- FIELDVUE 4400 Digital Position Transmitter Instruction Manual, [D104738X012](#)
- Bulletin 62.3:4400 - FIELDVUE 4400 Digital Position Transmitter, [D104739X012](#)
- exida FMEDA Report for FIELDVUE 4400 Position Transmitters
Report No.: EPM 21/11-233 R001

5. Safety Requirements

Average Probability of Failure on Demand (PFD_{AVG})

Table 1 shows the achievable Safety Integrity Level (SIL) in Low Demand Mode of operation, depending on the average probability of failure.

Table 1. Achievable Safety Integrity Level (SIL) in Low Demand Mode

Safety Integrity Level (SIL)	PFD_{AVG} with Low Demand Mode
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Safety Integrity of the hardware

Table 2 shows the achievable Safety Integrity Level (SIL) depending on the Safe Failure Fraction (SFF) and the Hardware Fault Tolerance (HFT) for safety related Type-B subsystems.

Table 2. Achievable Safety Integrity Level depending on the Safe Failure Fraction and Hardware Fault Tolerance

Safe Failure Fraction	Hardware Fault Tolerance (HFT)		
	A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function		
	0	1	2
< 60%	Not Permitted	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

6. Safety Characteristics

The specified characteristics are applicable under the following assumptions that have been made during the FMEDA.

- The mean time to restoration after a device has failed is approximately 24 hours.
- The architectural constraint type for the 4400 position transmitter is Low Demand mode.
- The hardware fault tolerance of the device is 0 (HFT = 0).
- To avoid unwanted or unauthorized modification, the set parameters must be protected.
- Proof test interval: ≤ 1 year.
- Safety accuracy: 2% of full span.
- Only a single component failure will fail the entire 4400 position transmitter.
- Failure rates are constant, wear out mechanism is not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.

- Stress levels are average for an industrial environment and can be compared to the exida profile 2 with temperature limits within manufacturer’s rating (see table 3 and 4 below). Other environmental characteristics are assumed to be within manufacturer’s rating.
- A practical fault injection test can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The HART® protocol is only used for setup, calibration and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed, calibrated, and maintained per manufacturer's instructions.
- External power supply failure rates are not included.
- 4400 MTBF = 116 years
- Diagnostic Test Interval: Range from 500 milliseconds to 15 minutes

Table 3. exida Profiles, Electronic

exida Electronic Database				
Profile	According to IEC60654-1	Ambient Temperature (°C)		Temperature Cycle (°C/365 days)
		Average (External)	Mean (Inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25
Profile 1:	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.			
Profile 2:	Low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings.			
Profile 3:	General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings.			

Table 4. exida Profiles, Mechanical

exida Mechanical Database				
Profile	According to IEC60654-1	Ambient Temperature (°C)		Temperature Cycle (°C/365 days)
		Average (External)	Mean (Inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25
4	D1	25	30	35
Profile 1:	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.			
Profile 2:	Mechanical field products have minimal self heating and are subjected to daily temperature swings.			
Profile 3:	Mechanical field products may have moderate self heating and are subjected to daily temperature swings.			
Profile 4:	Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.			

7. Safety Instrumented System Design

Safety Instrumented System (SIS) is an implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

When using the 4400 in a safety instrumented system, the following items must be reviewed and considered.

- SIL Capability
- Safety Function
- Failure Rates
- Application Limits
- Environment Limits

SIL Capability

- Systematic Integrity

SIL 2 Capable – The 4400 position transmitter has met manufacturer design process requirements of IEC61508 Safety Integrity Level 2.

- Random Integrity

The 4400 position transmitter is classified as a Type B device according to IEC61508. The complete element subsystem will need to be evaluated to determine the SFF. If the SFF of the subsystem is > 90% and the $PFD_{avg} < 10^{-2}$, the design can meet SIL2 @ HFT = 0. If the SFF of the subsystem is between 60% and 90%, and the $PFD_{avg} < 10^{-1}$, the design can meet SIL1 @ HFT = 0.

Safety Function

The safety function of the 4400 transmitter is to measure position of rotary or sliding-stem valves, vents, dampers, or other devices and transmit a 4-20mA analog signal within a measurement safety accuracy of $\pm 2\%$ of full span. It includes the whole hardware and software measurement chain.

The safety function of the 4400 limit switch output is to transmit a discrete signal that represents a user configurable threshold of position. The safe state of limit switch is open.

Note

The two safety functions implemented by a single 4400 digital position transmitter cannot be used together to reduce the risk for the same hazard scenario.

Table 5. Normal and Alarm States for FIELDVUE 4400 Position Transmitter

Output Function	Normal State	Safety Accuracy	Alarm State ⁽¹⁾
4-20 mA position transmitter	Actual position	$\pm 2\%$	>21.0 mA or <3.6 mA
1. Configurable high or low. Values are per NAMUR NE43.			

Failure Rates

The failure rate data listed in table 6 is valid for the 15-year useful lifetime of the 4400 position transmitter. Its useful lifetime is highly dependent on the subsystem itself and its operating conditions. The failure rate will increase after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the useful lifetime may yield results that are too optimistic.

Table 6. Failure Rates for FIELDVUE 4400 Position Transmitter

Failure Category	Failure Rate (FIT)	
	Analog Signal	Limit Switch , DTT
Fail Safe Detected, λ_{SD}	0	374
Fail Safe Undetected, λ_{SU}	0	153
Fail Dangerous Detected, λ_{DD}	960	427
Fail Detected (detected by internal diagnostics)	444	-
Fail High (detected by logic solver)	65	-
Fail Low (detected by logic solver)	451	-
Fail Dangerous Undetected, λ_{DU}	16	36
No Effect	133	228
Annunciation Detected	61	80
Annunciation Undetected	28	47
SFF	98.3%	96.3%

Application Limits

- Safety Instrumented Function design verification must be done for the entire collection of equipment used in the Safety Instrumented Function including the 4400 digital position transmitter. The SIS must fulfill the requirements according to the Safety Integrity Level, especially the limitation of average Probability of Failure on Demand (PFDavg).
- The 4400 position transmitter can only be used for final element position applications.
- The system response time is dependent on the entire final element subsystem. The user must verify the system response time is less than the process safety time for each final element. The 4400 position transmitter safety function has a fault reaction time upon fault detection of < 1 second plus the mean time to repair.
- Measurement signal used by logic solver must be the analog 4-20 mA signal.
- The logic solver must recognize both high/low alarms. If the logic solver loop uses IS barriers, caution must be taken to ensure the loop continues to operate properly under the low alarm condition.
- Safe failure in which 4-20 mA current is driven out of range (<3.6 mA or > 21 mA).
- Device Response Time: less than 1 second
- When using the 4400 position transmitter in redundant applications, the owner-operator of the facility should institute common causes training and more detailed maintenance procedures specifically oriented toward common cause defense.
- The Limit Switch must be configured to Normally Closed when used in a SIL application.

Environmental Limits

- Operating ambient temperature: -40°C to 80°C (-40°F to 176°F)
- Humidity: tested per IEC61298-3 Section 6
- Electromagnetic Compatibility: tested per IEC61326-3-2
- Vibration: tested per ISA 75.13 and FTEP 3B1

8. Installation and Commissioning Guidelines

1. Verify that the 4400 is suitable for use in Safety Instrumented Function.
2. Verify nameplate markings are suitable for the hazardous location (if required).
3. Verify appropriate connections to the logic solver are made by referring to the instruction and safety manual of the logic solver.
4. For maximum availability and benefit of digital position transmitter features, the unit must be properly configured and calibrated, the Instrument Mode set to In Service, and the protection enabled. With protection set, calibration and other protected parameters cannot be changed, including Instrument Mode.
5. The sensor safety function of the 4400 along with the SIS safety function must be tested after installation to ensure that it meets safety demand and applicable process safety time requirements.

9. General Requirements

Refer to 4400 instruction manual for mounting, starting up, and configuring and calibrating the 4400 position transmitter.

4400 position transmitter shall be mounted so that they are easily accessible for service, configuration, and monitoring. Exposure to corrosive atmosphere, excessive vibration, shock, or physical damage shall be prevented.


10. Operation, Periodic Inspection, Test, and Repair

Periodic testing, consisting of proof test, is an effective way to reduce the PFDavg of the 4400 position and the final element it is attached to. The SIL for the 4400 position transmitter is based on the assumption that the end user will carry out these tests and inspection at least once per year. The system check must be carried out to prove that the safety functions meet the IEC specification and result in the desired response of the safety system as a whole. Results of periodic inspections and tests should be recorded and reviewed periodically.

Maintenance

- The effective time to repair the 4400 position transmitter is approximately 2 hours. This comprises of removal, replacement, and recalibration. This value can be used to determine the total mean time to restore (MTTR).
- 4400 position transmitter preventative maintenance consists of visual inspection of the transmitter and feedback assembly and regular proof testing. Except for the feedback array/magnet assembly there are no repairable or replaceable parts on the 4400 position transmitter. If the instrument is exposed to the upper or lower extremes of the environmental limits, the interval for inspection and proof testing of the position transmitter may need to be reduced.

Protection

When protection is enabled, setup and calibration of the 4400 position transmitter are not permitted by local user interface or by remote HART communication. Only reading data is allowed. The switch setting under the terminal cover will show a lock icon () to indicate that the 4400 is currently protected.

Decommissioning Guidelines

When decommissioning a 4400 position transmitter, proper procedures must be followed. Decommissioning includes the following steps:

1. Avoid personal injury or property damage from sudden release of mechanical energy, process pressure, or bursting of parts. Before proceeding with any decommissioning procedures:
 - Always wear protective clothing, gloves, and eyewear to prevent personal injury or property damage.
2. Bypass the transmitter subsystem or take appropriate action to avoid a false trip.
3. Bypass the safety function or take appropriate action to avoid a false trip.
4. Disconnect the electrical wiring to and from the 4400 instrument.
5. Remove the 4400 instrument, mounting parts from the final element assembly.

Application

The 4400 digital position transmitter can be applied to most final element assemblies. The 4400 position transmitter can be used for final control elements to meet the safety system requirements of IEC61508.

Benefits

The 4400 position transmitter provides the following benefits to operation:

- Suitable for use in environments up to SIL 2 (Safe Failure Fraction = 98.36%) as independently assessed (full assessment) by exida.com as per IEC61508/61511-1.
- Continuous self-test with > 21 mA or < 3.6 mA fault indication fully compliant with NAMUR NE-43.
- Intrinsic Safe, Explosion-proof approvals.
- Two-wire, loop-powered transmitter for position feedback.

Proof testing

According to section 7.4.5.2f of IEC61508-2, proof tests must be undertaken regularly to reveal dangerous faults which are undetected by diagnostic tests. Proof test coverage is a measure of how many undetected dangerous failures are detected by the proof test. It is a testing of safety system components to detect any failures not detected by automatic online diagnostics followed by repair of those failures to an equivalent as-new state. A proof test is a test that is manually initiated. It is an effective way to reduce the PFDavg of the 4400 position transmitter. As part of the test, the capability of the SIF to achieve the defined safe state must be verified. The Safety Function must be verified. The proof test interval must be established for the SIF based on the failure rates of all the elements within the function and the risk reduction requirements. This determination is a critical part of the design of the SIS. A proof test will detect 95% of possible dangerous failures undetected in the 4400 position transmitter. Proof testing is a vital part of the safety lifecycle and is critical to ensuring that a system achieves its required safety integrity level throughout the safety lifecycle.

Note

Any time the SIF needs to be disabled, such as to perform a proof test or to take corrective action, appropriate measures must be taken to ensure the safety of the process.

Note

To ensure corrective action, continuous improvement, and accurate reliability prediction, the user must also work with their local Emerson service representative to see that all failures are reported.

Test steps for the Fisher 4400

Following are the steps to detect Dangerous Undetected (DU) failure. The procedure will detect approximately 95% of possible DU failures in the 4400 position transmitter.

Proof Test Procedure:

Analog Signal

1. Bypass the safety function and take appropriate action to avoid a false trip and any safe actions against dangerous atmospheres.
2. Inspect the instrument for loose, degraded or dirty components, proper wiring and electrical connections, correct mounting and any physical damage.
3. Observe the tightening torques for the mounting hardware.
4. Use HART communications to retrieve Alarm High / Low setting, any diagnostics alerts and take appropriate action. Alarm High / Low setting should be checked against the plant safety requirement for that particular application. If setting is High, go to step 5. If setting is Low, go to step 6.
5. Retrieve PV HiHi alert setting. Send a HART command (Enable Trip Alarm Current and set PV HiHi alert threshold to activate the PV HiHi alert) to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. This will test for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. Continue to step 7.
6. Retrieve PV LoLo alert setting. Send a HART command (Enable Trip Alarm Current and set PV LoLo alert threshold to activate the PV LoLo alert) to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This will test for possible quiescent current related failures.
7. Perform a five-point calibration check. If the calibration check is correct, the proof test is complete. Proceed to step 9. If not correct, proceed to step 8.
8. If the calibration check is off by more than 2%, contact the factory for assistance. If the calibration check is correct, the proof test is complete.
9. Reinstall the digital position transmitter if the assembly was removed previously. Ensure the Alarm setting is correct and reinstate the PV HiHi/LoLo Alert settings.
10. Lock the settings by write protection.
11. Record proof test results and any failures in your company's SIF inspection database.
12. Remove the bypass and otherwise restore normal operation.

Limit Switch

1. Bypass the safety function and take appropriate action to avoid a false trip and any safe actions against dangerous atmospheres.
2. Inspect the instrument for loose loose, degraded or dirty components, proper wiring and electrical connections, correct mounting and any physical damage.
3. Observe the tightening torques for the mounting hardware.
4. Use HART communications to retrieve Limit Switches setting, any diagnostics alerts and take appropriate action. Limit Switches setting should be checked against the plant safety requirement for that particular application. Note that the Limit Switches must be configured to Normally Closed when used in a SIL application.
5. Ensure that the 4400 is in a position such that the limit switches are at the Normal (Closed) position.
6. Retrieve PV HiHi alert setting. Send HART commands (Enable Trip and set PV HiHi alert threshold to activate the PV HiHi alert) to the 4400 to cause the limit switches to go to safe state (open state) and verify that the limit switches reach that value. This will test for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
7. Retrieve PV LoLo alert setting. Send a HART command (Enable Trip and set PV LoLo alert threshold to activate the PV LoLo alert) to the 4400 to cause the limit switches to go to safe state (open state) and verify that the limit switches reach that value. This will test for possible quiescent current related failures.
8. Perform a five-point calibration check. If the calibration check is correct, the proof test is complete. Proceed to step 10. If not correct, proceed to step 9.
9. If the calibration check is off by more than 2%, contact the factory for assistance. If the calibration check is correct, the proof test is complete.
10. Reinstall the digital position transmitter if the assembly was removed previously. Ensure the Alarm setting is correct and reinstate the PV HiHi/LoLo Alert settings.
11. Lock the settings by write protection.
12. Record proof test results and any failures in your company's SIF inspection database.
13. Remove the bypass and otherwise restore normal operation.

Neither Emerson, nor any of its affiliated entities, assume responsibility for the selection, use, or maintenance of any product. Responsibility for proper selection, use, and maintenance of any product remains solely with the purchaser and end user.

Fisher is a mark owned by one of the companies in the Emerson business unit of Emerson Electric Co. Emerson and the Emerson logo are trademarks and service marks of Emerson Electric Co. HART is a registered trademark of FieldComm Group. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available upon request. We reserve the right to modify or improve the designs or specifications of such products at any time without notice.

Emersons

Marshalltown, Iowa 50158 USA

Sorocaba, 18087 Brazil

Cernay, 68700 France

Dubai, United Arab Emirates

Singapore 128461 Singapore

www.Fisher.com

