UNITED ELECTRIC CONTROLS

One Series Safety Transmitter Safety Manual

UNITED ELECTRIC CONTROLS
LEADERS IN SAFETY, ALARM & SHUTDOWN

OneST-SM-02

1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the *One Series Safety Transmitter*. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 Terms and Abbreviations

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
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems
Fail-Safe State	State where the outputs are de-energized. Defined as:
	4-20 mA Output ≤3.6mA
	Switch Status OFF
	Safety Relay Output OFF
	IAW OFF
Fail Safe	Failure that causes the outputs to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by proof testing or instrument diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by proof testing or instrument diagnostics.
Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Annunciation Detected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.

Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode	Mode where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.

1.2 Acronyms

DTT	De-Energize to Trip
DU	Dangerous Undetected
FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
IAW	I Am Working – On board diagnostics that monitor device hardware and software functions to alert the operator if a problem has occurred that could impair the safety function of the device.
MOC	Management of Change – These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFD_{avg}	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
SFF	Safe Failure Fraction – The fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety Instrumented Function - A set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level - Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
SIS	Safety Instrumented System – 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).
SRO	Safety Relay Output – A high capacity solid-state relay switch

1.3 Product Support

Product support can be obtained from:

United Electric Controls

180 Dexter Ave,

P.O. Box 9143

Watertown, MA 02471-9143

TechSupport@ueonline.com

Telephone: 617 923-6977

FAX: 617 926-2568

Lost Password: go to www.ueonline.com/uuc The Kanban number from the product nameplate is required.

1.4 Related Literature

Hardware Documents:

- *One Series Safety Transmitter* Installation and Maintenance Instructions (IM_ONE_SAFETY-01)
- SR113028.D3.6 UE 12-10-073 R001 V1 R2 One Series SAFETY TRANSMITTER FMEDA Report
- One Series ST-B-01 United Electric Controls Safety Transmitter Product Bulletin
- Guidelines/References:
  - Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, ISBN 978-1-934977-03-3, exida
  - Control System Safety Evaluation and Reliability, 3rd Edition, ISBN 978-1-934394-80-9, ISA
  - Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector

2 DEVICE DESCRIPTION

The One Series Safety Transmitter senses the temperature or pressure of a system and provides control outputs that are used to monitor or shut down that system before an unsafe condition occurs. An externally excited 4-20mA provides an analog indication of the process for use by a safety PLC. The solid state relay output provides direct control or shut down of a final element based on programmed operating modes and limits. The Switch Status output is a discrete output that mirrors the function of the solid state relay output. The IAW output is a discrete output based on self diagnostics that provides the user with an indication of device health. Any diagnostic failure that causes an IAW fault will force all outputs to the fail-safe state. All outputs of the One Series Safety Sensor operate in DTT (De-energize To Trip) mode.

Detailed information on the installation, programming and operation of the One Series Safety Transmitter along with System Context Diagrams may be found in document IM_ONE_SAFETY-01.

3 DESIGNING A SIF USING THE ONE SERIES SAFETY TRANSMITTER

3.1 Safety Function

The 4-20 mA, I Am Working, Safety Relay and Switch Status outputs have been assessed for safety instrumented systems usage.

The achieved SIL level of the designed function must be verified by the designer.

3.2 Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental constraints. Refer to the United Electric Controls *One Series ST-B-01 bulletin* for environmental limits.

3.3 Application limits

The materials of construction of the *One Series Safety Transmitter* are specified in the United Electric Controls *One Series ST-B-01* bulletin. It is especially important that the designer check for material compatibility considering on-site conditions. If the *One Series Safety Transmitter* is used outside of the application limits or with incompatible materials, the reliability data provided become invalid.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from *United Electric Controls*. This report details all failure rates and failure modes as well as the expected lifetime.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFD_{AVG} considering architecture, 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 subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the *One Series Safety Transmitter* and its failure rates.

When using the *One Series Safety Transmitter* in a redundant configuration, a common cause factor of at least 5% should be included in safety integrity calculations.

The failure rate data listed in the FMEDA report are only valid for the useful lifetime of the *One Series Safety Transmitter*. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

3.5 SIL Capability

3.5.1 Systematic Integrity

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve 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 without "prior use" justification by the end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

The *One Series Safety Transmitter* is a Type B Device. Therefore, based on the SFF between 90% and 99%, when the *One Series Safety Transmitter* is used as the only component in a sensor element subassembly, a design can meet SIL 2 @ HFT=0.

When the sensor element assembly consists of multiple components the SIL must be verified for the entire assembly using failure rates from all components. This analysis must account for any hardware fault tolerance and architecture constraints.

3.5.3 Safety Parameters

The safety accuracy of the device is 3% of the operating range.

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the *One Series Safety Transmitter*.

3.6 Connection of the *One Series Safety Transmitter* to the SIS Logic-solver

The *One Series Safety Transmitter* is connected to the safety rated logic solver via a NAMUR NE 43 4-20 mA analog and up to two discrete diagnostic status outputs. The logic solver is actively performing the safety function by monitoring and interpreting the One Series Safety Transmitter outputs, designed to diagnose potentially dangerous process conditions and failures within the *One Series Safety Transmitter* via the I Am Working (IAW) diagnostic.

The One Series Safety Transmitter may also be configured to provide the safety function directly without connections to a safety rated logic solver. Please refer to the System Context Diagrams in document IM_ONE_SAFETY-01 for details on using the various logic outputs on the One Series Safety Transmitter.

3.7 General Requirements

The system's response time shall be less than the process safety time. The *One Series Safety Transmitter,* Switch Status and Safety Relay Outputs will move to its safe state in less than 100 milliseconds under specific delay filter settings. The 4-20mA output shall stabilize to 90% of a step response within 250mSec under specific delay filter settings. For available settings and a description of the delay filter operation document refer to the product installation and maintenance manual IM_ONE_SAFETY-01.

The diagnostic interval for the One Series Safety transmitter is less than 10 seconds.

All SIS components including the *One Series Safety Transmitter* must be operational before process start-up. At power up, there may be a brief delay before the outputs are stable. The user must consider this in the application and not rely on the *One Series Safety Transmitter* for the control of the Safety Instrumented System until the outputs have stabilized. The time from power on until the outputs are stable shall be less than 10 seconds.

User shall verify that the *One Series Safety Transmitter* is suitable for use in safety applications by confirming the *One Series Safety Transmitter's* nameplate is properly marked.

Personnel performing maintenance and testing on the *One Series Safety Transmitter* shall be competent to do so.

Results from the proof tests shall be recorded and reviewed periodically.

The useful life of the *One Series Safety Transmitter* is discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the *One Series Safety Transmitter*.

4 INSTALLATION AND COMMISSIONING

4.1 Installation

The *One Series Safety Transmitter* must be installed per standard practices outlined in the Installation Manual.

The One Series Safety Transmitter must not be modified.

The environment must be checked to verify that environmental conditions do not exceed the ratings.

The *One Series Safety Transmitter* must be accessible for physical inspection.

Detailed programming and operating instructions are found in the *One Series Safety Transmitter* Installation and Maintenance Instructions manual (IM_ONE_SAFETY-01). It is the responsibility of the SIF designer to validate all device settings either through test or by re-entering the programming menu and reading back all settings. The checklist in Appendix A provides a place to record all device settings as they are read back. While in the programming menu all outputs are forced to the fail safe state:

4-20mA Output	≤3.6mA
Switch Status	Off
Safety Relay Output	Off
IAW	Off

The Plugged Port Detection and Safety Relay Fault Monitor are turned off from the factory. If these features are desired they must be enable using the programming menu. Reference One Series Safety transmitter Installation and Maintenance Instructions manual (IM_ONE_SAFETY-01) for details.

4.2 Physical Location and Placement

The *One Series Safety Transmitter* shall be accessible with sufficient room for connections and shall allow manual proof testing.

Piping to the *One Series Safety Transmitter* shall be kept as short and straight as possible to minimize restrictions and potential clogging. Long or kinked tubes may also increase the response time.

The *One Series Safety Transmitter* shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of connectors or the vibration should be reduced using appropriate damping mounts.

4.3 Connections

Connections to the *One Series Safety Transmitter* are to be made per the Installation and Maintenance Instructions (IM_ONE_SAFETY-01).

Recommended methods for process connections to the *One Series Safety Transmitter* can be found in the installation and maintenance manual IM_ONE_SAFETY-01. The length of tubing between the *One Series Safety Transmitter* and the process connection shall be kept as short as possible and free of kinks.

5 OPERATION AND MAINTENANCE

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within the *United Electric Controls One Series Safety Transmitter* that are not detected by any automatic diagnostics of the instrument. Of main concern are undetected failures that prevent the safety instrumented function from performing its intended function.

The frequency of proof testing, or proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a *United Electric Controls One Series Safety Transmitter* is applied. The proof tests must be performed at least as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to *United Electric Controls*. The suggested proof test consists of simulating a process upset and injecting a fault of the *One Series Safety Transmitter* and observing the reaction of the SIF to these upsets.

Table1: Recommended Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Verify the correct output under normal conditions. The Safety Relay Output, SRO Status and IAW Output will be in the closed state. The 4-20 mA output will provide a proportional signal to the process variable.
3.	Change the process variable or change the programming of the instrument so that the Safety Relay Output changes to the tripped state (opens). Verify that the Safety Relay Output and SRO Status opens and the IAW Output remains closed. The 4-20 mA output will provide a proportional signal to the process variable.
4.	Change the process variable so that the IAW Output goes to the fault state (opens). (Extreme Over Range of 150% of the sensor's range is suggested.) Verify that the IAW Output opens and the 4-20 mA output provides ≤3.6 mA.
5.	Restore the normal input values or programming. Verify that the outputs have returned to their non-tripped (closed) state. Verify that the 4-20 mA output is proportional to the process variable.
6.	Restore the loop to full operation.
7.	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect >99% of possible DU failures in the *One Series Safety Transmitter*.

The person(s) performing the proof test of a *One Series Safety Transmitter* should be trained in SIS operations, including bypass procedures, maintenance and company Management of Change procedures. A 2mm hex wrench is required to remove the cover. The Software Flow Chart from the One Series Safety Transmitter installation and maintenance manual IM_ONE_SAFETY-01 is required to change the programming.

5.2 Repair and replacement

Repair and replacement procedures for the *One Series Safety Transmitter* are obtained by contacting United Electric Controls technical support at 617-923-6977 or techsupport@ueonline.com.

A complete list of fault codes for the One Series Safety Transmitter may be found in the installation and maintenance manual IM_ONE_SAFETY-01.

5.3 Hardware and Software Configuration

The model number of the device is found on the PART# field on the device nameplate. Hardware and software revisions are noted on the label located on the back of the display module.

5.4 Useful Life

The useful life of the *One Series Safety Transmitter* is 50 years.

5.5 MANUFACTURER Notification

Any failures that are detected and that compromise functional safety should be reported to *United Electric Controls*. Please contact *United Electric Controls* technical support at 617-923-6977 or techsupport@ueonline.com..

Appendix A Sample Start-up Checklist

This appendix provides a Sample Start-up Checklist for a *One Series Safety Transmitter.* A Start-up Checklist will provide guidance during *One Series Safety Transmitter* deployment.

1 START-UP CHECKLIST

The following checklist may be used as a guide to employ the *One Series Safety Transmitter* in a safety critical SIF compliant to IEC61508.

#	Activity	Result	Verified	
			By	Date
	Design			
	Target Safety Integrity Level and PFD_{avg} determined			
	Correct mode chosen (Open on Rising, Open on Falling or Window mode)			
	Correct set point and deadband chosen			
	Design decision documented			
	Fluid compatibility and suitability verified			
	SIS logic solver requirements for automatic tests defined and documented			
	Routing of fluid connections determined			
	Design formally reviewed and suitability formally assessed			
	Implementation			
	Physical location appropriate			
	Fluid connections appropriate and according to applicable codes			
	SIS logic solver automatic test implemented			
	Maintenance instructions for proof test released			
	Verification and test plan released			
	Implementation formally reviewed and suitability formally assessed			

#	Activity	Result	Verified	
			By	Date
	Verification and Testing			
	Electrical connections verified and tested			
	Fluid connection verified and tested			
	SIS logic solver automatic test verified			
	Safety loop function verified			
	Safety loop timing measured			
	Bypass function tested			
	Verification and test results formally reviewed and suitability formally assessed			
	Maintenance			
	Tubing blockage / partial blockage tested			
	Safety loop function tested			

Record all device settings in the worksheet provided below:

For a detailed explanation of each feature refer to the One Series Safety Transmitter installation and maintenance manual IM_ONE_SAFETY-01

Device ID: _____
Range: _____
Kanban#: _____
Password: _____

Units of Measure: ☐ psi ☐ bar/mbar ☐ KPa/MPa ☐ Kg/cm^2 ☐ "wc (Default psi)
☐ °F ☐ °C (Default °F)

Switch Mode: ☐ Open on Rise ☐ Open on Fall
Set Point:_____
Dead Band:_____

☐ Window
Set Point (Upper):_____
Dead Band(Upper):_____
Set Point(Lower):_____
Dead Band(Lower):_____

Offset: _____ (Nominally 0.0)
Span: _____ (Nominally the Upper Range Limit of the Transmitter)

Latch Mode: ☐ On ☐ Off

Plugged Port: ☐ Off ☐ 1Min ☐ 1HR ☐ 24HR (Default Off)

SSR Fault Monitor: ☐ On ☐ Off (Default Off)

Delay: ☐ Off ☐ ¼Sec ☐ ½Sec ☐ 1Sec ☐ 2Sec (Default Off)

4mA Set: _____ (Nominally the Lower Range Limit of the device.)
20mASet: _____ (Nominally the Upper Range Limit of the device.)