ONE SERIES
ELECTRONIC SWITCH

Safety Manual

UNITED ELECTRIC CONTROLS

1XSW-SM-01

This page intentionally left blank.

ONE SERIES ELECTRONIC SWITCH
SAFETY MANUAL

TABLE OF CONTENTS

1. Introduction 4
1.1 Terms & Abbreviations 4
1.2 Acronyms 5
1.3 Device Support 5
1.4 Related Literature 6
1.5 Reference Standards 6
2. Device Description 7
3. Designing a SIF Using the Device 7
3.1 Safety Function 7
3.2 Environmental Limits 7
3.3 Application Limits 7
3.4 Design Verification 7
3.5 SIL Capability 8
3.5.1 Systematic Integrity 8
3.5.2 Random Integrity 8
3.5.3 Safety Parameters 8
3.6 Connecting the Device to the SIS Logic Solver 8
3.7 General Requirements 9
4. Installation and Commissioning 10
4.1 Installation 10
4.2 Physical Location and Placement 10
4.3 Connections 10
5. Operation and Maintenance 11
5.1 Proof Test without Automatic Testing 11
5.2 Troubleshooting, Repair and Replacement 12
5.3 Hardware and Software Configuration 12
5.4 Useful Life 12
5.5 Manufacturer Notification 12
Appendix 13
Sample Start-up Checklist 15
Device Settings Worksheet 17

1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the One Series Electronic Switch, hereby referred to as “device.” It is the end user’s responsibility to follow the necessary requirements outlined in this manual in order to meet 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	The outputs are placed in a user-defined safe state that does not result in a dangerous process condition. IAW remains open.
Fail Safe	Failure that causes the outputs to go to the user-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 user-defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and 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).

1.3 Device Support

United Electric Controls

180 Dexter Avenue

Watertown, MA 02472 USA

InsideSales@ueonline.com

Telephone: +1 617 923-6977

Fax: +1 617 926-4354

For a list of our domestic and international regional sales offices, please visit www.ueonline.com/about-ue/sales-offices/.

Product Support (Cont.)

Lost Password:

Contact InsideSales@ueonline.com, +1 617 923-6977, or go online at www.ueonline.com/uuc to obtain a unique unlock code. The Kanban number from the device nameplate is required (see Figure 1).

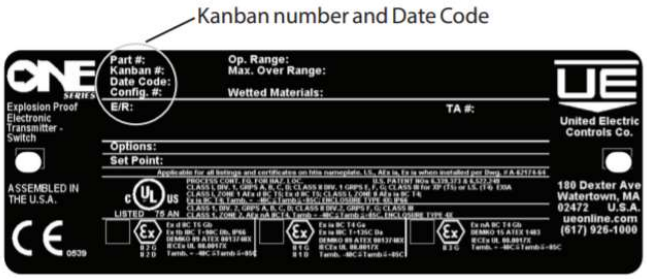

Figure 1

1.4 Related Literature

Hardware Documents:

- One Series Electronic Switch Installation and Maintenance Instructions IM_1XSW-xx
- One Series Electronic Switch FMEDA report UE 21/01-054 R001
- One Series Electronic Switch product brochure 1X-B-xx
- Guidelines/References:
  - Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, Second Edition, ISBN-13: 978-1-934977-16-3, exida
  - Control System Safety Evaluation and Reliability, Third Edition, ISBN-13: 978-1-934394-80-9, ISA
  - Safety Instrumented Systems Verification: Practical Probabilistic Calculations, ISBN-13: 978-1556179099, 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 61511-1 Mod.) Functional Safety: Safety Instrumented Systems for the Process Industry Sector

2 DEVICE DESCRIPTION

The device senses the temperature or pressure of a system and provides control outputs used to monitor or shut down that system before an unsafe condition occurs.

The switch output is a discrete output. The IAW output is a discrete output based on self-diagnostics that provides the user with an indication of device health. IAW output operates in DTT. Any diagnostic failure that causes an IAW fault will force all outputs to the fail-safe state. All outputs of the device operate in a mode selected by the user that can be configured to de-energize a process.

Detailed information on the installation, programming and operation of the device along with System Context Diagrams may be found in the installation manual IM_1XSW-xx.

3 DESIGNING A SIF USING THE DEVICE

3.1 Safety Function

IAW and Switch outputs have been assessed for safety instrumented systems usage.

The designer must verify the achieved SIL level of the designed function.

3.2 Environmental Limits

The designer of a SIF must check that the device is rated for use within the expected environmental constraints. Refer to the device brochure 1X-B-xx for environmental limits.

3.3 Application Limits

The materials of construction of the device are specified in the device brochure 1X-B-xx. It is especially important that the designer check for material compatibility considering on-site conditions. If the device is to be 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, UE 21/01-054 R001. 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 device and its failure rates.

Design Verification (Cont.)

When using the device 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 device. 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 device 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 device 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 device is a Type B Device. Therefore, based on the SFF between 90% and 99%, when the device 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 FMEDA report for the device, UE 21/01-054 R001.

3.6 Connecting the device to the SIS Logic-solver

The device is connected to the safety rated logic solver via (up to) two discrete diagnostic status outputs. The logic solver is actively performing the safety function by monitoring and interpreting the device outputs, designed to diagnose potentially dangerous process conditions and failures within the device via the I Am Working (IAW) diagnostic.

The device 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 for details on using the various logic outputs in the device installation manual IM_1XSW-xx.

3.7 General Requirements

The system's response time shall be less than the process safety time. The device Switch and IAW Outputs will move to its safe state in less than 100 milliseconds under specific delay filter settings. For available settings and a description of the delay filter operation, refer to the device installation manual IM_1XSW-xx. The diagnostic interval time is 600 seconds.

All SIS components including the device must be operational before process start-up. At power up, there may be a brief delay before the outputs are stable. The end-user must consider this in the application and not rely on the device 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.

End-user shall verify that the device is suitable for use in safety applications by confirming the device nameplate is properly marked.

Personnel performing maintenance and testing on the device shall be competent to do so.

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

The useful life of the device is discussed in the FMEDA report, UE 21/01-054 R001.

4 INSTALLATION AND COMMISSIONING

4.1 Installation

The device must be installed per standard practices outlined in the device installation manual IM_1XSW-xx.

The device must not be modified.

The environment must be checked to verify that environmental conditions do not exceed the device's published ratings outlined in device brochure 1X-B-xx.

The device must be accessible for physical inspection.

Detailed programming and operating instructions are found in the device installation manual IM_1XSW-xx. 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 end-user is responsible for securing passwords. The device settings worksheet in the Appendix provides a place to record all settings as read. While in the programming menu, IAW and switch outputs remain active.

The Plugged Port Detection is turned off from the factory. If this feature is desired, it must be enabled using the programming menu referenced in the device installation manual IM_1XSW-xx.

4.2 Physical Location and Placement

The device shall be accessible with sufficient room for connections and shall allow manual proof testing.

Piping to the device 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 device shall be mounted in a low vibration environment. If excessive vibration is 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 device are to be made per the device installation manual IM_1XSW-xx.

Recommended methods for process connections to the device can be found in the installation manual IM_1XSW-xx. The length of tubing between the device 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 device 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 the device 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 recommended proof test consists of simulating a process upset and injecting a fault of the device, and observing the reaction of the SIF to these upsets. The results of the proof test should be recorded and any failures detected that compromise functional safety should be reported to United Electric Controls.

1. Power cycle the device prior to proof testing to clear out any soft errors that may have occurred.
2. Bypass the PLC (programmable logic controller) or take other appropriate action to avoid a false trip.
3. Verify the correct output under normal conditions. The switch should be in the non-tripped state. The IAW output should be in the closed state. We recommend checking switch connections outside of the device to avoid removing the device cover.
4. Change the process variable so that the switch changes to the tripped state. Verify that the IAW output remains closed.
5. Change the process variable (extreme over range pressure of 150% of the sensor's range is suggested for pressure or 110% for temperature) so that the IAW output goes to the fault state (open). Verify that the IAW output opens when this error appears on the display.

   Alternatively, if you only want to test the final connection of the IAW wiring, you could unplug the IAW wiring from your final element to verify that the connection switches from closed to open. This would avoid the need to enact an error on the device.
6. Restore the process variable to normal and verify that outputs have returned to their non-tripped state.
7. Restore the loop to full operation.
8. Remove the bypass from the PLC or otherwise restore normal operation.

Reference section B.2 in the FMEDA report, UE 21/01-054 R001 for proof test coverage.

The person(s) performing the proof test of the device 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. Follow the device's software flow chart in the device installation manual IM_1XSW-xx to change the programming.

5.2 Troubleshooting, Repair and Replacement

Should a fault occur, a complete list of fault codes and troubleshooting steps for the device can be found in the device installation manual IM_1XSW-xx.

Repair and replacement procedures for the device are obtained by contacting United Electric Controls technical support at 617-923-6977 or InsideSales@ueonline.com.

5.3 Hardware and Software Configuration

The model number of the device is found within the PART# field on the device nameplate (see Figure 1, pg. 6). 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 device is 50 years.

It is the end user's responsibility to properly decommission the device. The device should be disposed of per local regulations.

5.5 Manufacturer Notification

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

APPENDIX

The appendix includes two documents for guiding deployment of the device into a SIS. They should be part of any Safety Management Plan.

1. Start-up Checklist to provide guidance during device deployment.
2. Device Settings Worksheet to record settings.

This page intentionally left blank.

START-UP CHECKLIST

The following checklist should be used as a guide to deploy the device 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 Rise, Open on Fall, Close on Rise, Close on Fall or Window Open, Window Close)			
	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			

START-UP CHECKLIST (Cont.)

#	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			

DEVICE SETTINGS WORKSHEET:

Record all device settings for easy reference. For a detailed explanation of device features, refer to the device installation manual IM_1XSW-xx.

Device ID: _____

Range: _____

Kanban#: _____

Password: _____

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

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

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

Display Offset: _____ (Nominally 0.0)

Span: _____ (Nominally the Upper Range Limit of the Device)

Latch Mode: ☐ Off (Default) ☐ On

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

Filter:
Pressure ☐ Off (Default) ☐ On / Setting: ☐ ¼Sec ☐ ½Sec ☐ 1Sec ☐ 2Sec
Temperature ☐ On (Default) / Setting: ☐ ½Sec (Default) ☐ 1Sec ☐ 2Sec

Trip Delay: ☐ Off (Default) ☐ On / Setting: _____ (0 to 999.9 sec.)

FOR A LIST OF OUR INTERNATIONAL AND DOMESTIC REGIONAL SALES OFFICES, PLEASE VISIT WWW.UEONLINE.COM

UNITED ELECTRIC CONTROLS
180 Dexter Avenue
Watertown, MA 02472 USA
Telephone: +1 617 926-1000
Fax: +1 617 926-2568
http://www.ueonline.com