

## 100, 120, & 12 Series Safety Manual



**100 Series**



**120 Series**



**12 Series**

## 1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the *100, 120, & 12 Series*. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

### 1.1 Skill Level Requirement

System design, installation and commissioning, and repair and maintenance shall be carried out by suitably qualified personnel.

### 1.2 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.                                                                                                                                                                                                                                                                |
| Fail Safe                    | Failure that causes the valve 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 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.                   |

### 1.3 Acronyms

|                    |                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DTT                | De-Energize to Trip                                                                                                                                                                                                                                                                                                     |
| DU                 | Dangerous Undetected                                                                                                                                                                                                                                                                                                    |
| FMEDA              | Failure Modes, Effects and Diagnostic Analysis                                                                                                                                                                                                                                                                          |
| FIT                | Failure In Time (One FIT is $1 \times 10^{-9}$ failure per hour)                                                                                                                                                                                                                                                        |
| HFT                | Hardware Fault Tolerance                                                                                                                                                                                                                                                                                                |
| MOC                | Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.                                                                                                                                                                |
| PFD <sub>avg</sub> | 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).                                                                                                                                     |

### 1.4 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: 617-926-1000  
Fax: 617-926-2568

## 1.5 Related Literature

### Hardware Documents:

- *100 Series* Installation, Operation and Maintenance Instructions (IMP100 or IMT100)
- *100 Series* Product Bulletin (100-B)
- *120 Series* Installation, Operation and Maintenance Instructions (IMP120 or IMT120)
- *120 Series* Product Bulletin (120-B)
- *12 Series* Installation, Operation and Maintenance Instructions (IMP12 or IMT12)
- *12 Series* Product Bulletin (12-B)
- FMEDA Report (100 & 120 Series): UEC 16/02-130 R001
- FMEDA Report (12 Series): UEC 20/06-041 R001

### 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

## 1.6 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 PRODUCT DESCRIPTIONS

### 100 Series

The *100 Series* is a cost-effective pressure, vacuum, differential pressure, and temperature switch for process plants and OEM equipment. The rugged, one-piece enclosure features a slanted cover for wiring accessibility. A wide variety of microswitch and process-connection options make this versatile series ideal for applications requiring a rugged weather-proof mechanical switch. Typical applications that utilize the *100 Series* are heat tracing, freeze protection, processing equipment (pumps, compressors), inputs for annunciator panels, and fire suppression systems.

### 120 Series

Meeting hazardous location requirements through worldwide approvals and certifications, UE's *120 Series* is the choice where potentially explosive or highly corrosive atmospheres exist. The *120 Series* offers a variety of pressure, vacuum, differential pressure and temperature ranges, as well as process connections, wetted materials and sensor types. With a common flexible platform, models can quickly be adapted at the factory for special requirements, such as ranges, process connections and electrical ratings. Typical industries using *120 Series* switches include chemical, petrochemical, refinery, and oil & gas production and transmission.

### 12 Series

*12 Series* hazardous location, pressure, vacuum, differential pressure, and temperature switches are ideal for operation in tough applications where space is at a premium. A snap-action Belleville spring assembly is used in most models to provide vibration resistance and prolonged switch life. The 316 stainless steel enclosure and hermetically sealed switch provide rugged protection from the environment. Approved for use in hazardous locations worldwide, the 12 Series is installed within applications ranging from offshore oil rigs to rotating equipment, and more.

### 3 DESIGNING A SIF USING UNITED ELECTRIC CONTROLS SWITCHES

#### 3.1 Safety Function

The safety function of the switches is the micro switch changing its state when the input pressure or temperature rises above (increasing to trip), or falls below (decreasing to trip), the set point within the stated safety accuracy. The safe state is defined by the user and application.

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 limits. Refer to the specific series switch Bulletin for the switches environmental limits.

#### 3.3 Application limits

The materials of construction of each series are specified in their respective Bulletins available through United Electric Controls. It is especially important that the designer check for material compatibility considering on-site conditions. If any of United Electric Controls products are used outside of their application limits or with incompatible materials, the reliability data provided becomes invalid. The electrical ratings and pressure/temperature range information for each series offered by United Electric Controls can be found in their respective Bulletins.

#### 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 100, 120, & 12 Series and their failure rates.

When using any *United Electric Controls Switch* 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 reports are only valid for the useful life time of their mentioned series. 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 *products* have 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 these products 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 *100, 120, and 12 Series* are classified as Type A devices according to Table 2 of the IEC 61508-2 standard. According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1H approach according to 7.4.4.2 of IEC 61508 or the 2H approach according to 7.4.4.3 of IEC 61508, or the approach according to IEC 61511:2016 which is based on 2H.

The 1H approach involves calculating the Safe Failure Fraction for the entire element.

The 2H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the exida criteria for Route 2H which is more stringent than IEC 61508. Therefore, the *100/120 /12 Series* Switch meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

If Route 2H is not applicable for all devices that constitute the entire element, the architectural constraints will need to be evaluated per Route 1H.

The architectural constraint type for the *100/120/12 Series* Switch is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

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

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Reports for the series in question.

## 3.6 Connection of UE Mechanical Switches to the SIS Logic-solver

*United Electric Control Switches* can be connected to a safety rated logic solver which is actively performing the safety function. A low current switch option is recommended for use with a logic solver. *United Electric Control Switches* can also be connected directly to the final element in which the microswitch is performing the safety function.



### 3.7 General Requirements

- The system's response time shall be less than the process safety time. *United Electric Control Switches* will change state in less than 1s under specified conditions.
- All SIS components, including *United Electric Control Switches*, must be operational before process start-up.
- The user shall verify that *United Electric Control Switches* are suitable for use in safety applications by confirming the nameplate is properly marked. Product model number, range, electrical ratings and configuration ID are found on the product nameplate.
- If *United Electric Control Switches* are connected directly to the final element, it is recommended the microswitch be de-rated to 60% and if it is being used with a non-resistive load, it is also recommended the user add external transient protection.
- Personnel performing maintenance and testing on *United Electric Control Switches* shall first be assessed as being competent to do so.
- Results from the proof tests shall be recorded and reviewed periodically.
- The useful life of *United Electric Control Switches* are discussed in their respective Failure Modes, Effects and Diagnostic Analysis Reports.



## 4 INSTALLATION AND COMMISSIONING

### 4.1 Installation

- The *United Electric Control Switch* must be installed per standard practices outlined in the Installation Manuals.
- The *United Electric Control Switch* must not be modified.
- The environment must be checked to verify that environmental conditions do not exceed the ratings.
- The *United Electric Control Switch* must be accessible for physical inspection.

### 4.2 Physical Location and Placement

The *United Electric Control Switch* shall be accessible with sufficient room for connections and shall allow manual proof testing to take place.

The *United Electric Control Switch* shall be mounted in an environment experiencing vibrations within the allowable range listed in its respective bulletin. 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. The shock and vibration specifications can be found in the switches respective bulletin.

### 4.3 Connections

Connections to *United Electric Control Switches* are to be made per the Installation, Operation and Maintenance Instructions (Reference *Hardware Documents* in Section 1.5).

Recommended methods for process connections to *United Electric Control Switches* can be found in the installation and maintenance instructions. The length of tubing/piping between the *UEC Switch* and the process connection shall be kept as short as possible and free of kinks to minimize restrictions and potential clogging. Long or kinked tubes/pipes may also increase response time.

## 5 OPERATION AND MAINTENANCE

### 5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within a *United Electric Controls Switch* that are not detected by any automatic diagnostics of the system. 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 Switch* 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*.

**Table 1: Recommended Proof Test<sup>1</sup>**

| Step | Action                                                                                                                                      |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Take appropriate action to avoid a false trip.                                                                                              |
| 2.   | Inspect the device for any visible damage, corrosion or contamination.                                                                      |
| 3.   | Increase the pressure/temperature to reach the increasing set point value and verify that the electric signal proceeds into the safe state. |
| 4.   | Lower the pressure/temperature to reach the decreasing set point value and verify that the electric signal returns to the normal state.     |
| 5.   | Repeat steps 3 and 4 twice or more to evaluate the average set point value and repeatability.                                               |
| 6.   | Restore the connection to full operation.                                                                                                   |
| 7.   | Restore normal operation.                                                                                                                   |

The Proof Test Coverage for the tests listed in Table 1 will detect >85% of possible DU failures in *United Electric Controls Switches*.

The person(s) performing the proof test of a *United Electric Controls Switch* shall be trained in SIS operations, including bypass procedures, maintenance and company Management of Change procedures. No special tools are required.

### 5.2 Repair and Replacement

Repair procedures in the *United Electric Controls Switches* Installation, Operation and Maintenance manuals must be followed.

<sup>1</sup> This Proof Test represents an Increase to Trip application. For a Decrease to Trip application, steps 3 & 4 are reversed.

### 5.3 Manufacturer Notification

In case of malfunction of the system or SIF, the *United Electric Controls Switch* shall be put out of operation and the process shall be kept in a safe state by other measures.

*United Electric Controls* must be informed when the *United Electric Controls Switch* is required to be replaced due to failure. The failure shall be documented and reported to *United Electric Controls* using the contact details in Section 1.4 of this safety manual.

### 5.4 Useful Life

The useful life of *United Electric Controls Switches* are 10 years or 100,000 cycles.

## Appendix A Sample Start-up Checklist

This appendix provides a Sample Start-up Checklist for a *United Electric Controls Switch*. A Start-up Checklist will provide guidance during the *Switches* deployment.

## 1 START-UP CHECKLIST

The following checklist may be used as a guide to employ *United Electric Controls Switches* in safety critical SIF compliant to IEC61508.

| # | Activity                                                                 | Result | Verified |      |
|---|--------------------------------------------------------------------------|--------|----------|------|
|   |                                                                          |        | By       | Date |
|   | Design                                                                   |        |          |      |
|   | Target Safety Integrity Level and PFDavg determined                      |        |          |      |
|   | Correct mode chosen (Increase to trip, Decrease to Trip)                 |        |          |      |
|   | Switch mode chosen (Normally Open, Normally Closed)                      |        |          |      |
|   | Design decision documented                                               |        |          |      |
|   | Media 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                                            |        |          |      |
|   | Media 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                                        |        |          |      |
|   | Media 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                                                       |        |          |      |