PRECISION SENSORS
A Division of UNITED ELECTRIC CONTROLS

STASET GEN 3 SERIES

SAFETY MANUAL

REVISION HISTORY			
REV	DESCRIPTION	AUTHOR	DATE
-	INITIAL RELEASE	R. OLAH	5-18-2021
A	ADDED TABLES	R. OLAH	1-7-2022

Table of Contents

1 Introduction

This safety manual provides information necessary to design, install, verify, and maintain a Safety Instrumented Function (SIF) utilizing the Staset Gen 3 series. This manual provides necessary requirements for meeting the IEC 61508, IEC 61511, or ISO 13849 functional safety standards.

1.1 Terms and Definitions

Term	Definition
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 judgement – based on evidence – of the safety achieved by safety-related systems
Fail-Safe State	State where the output relay is de-energized
Fail Safe	Failure that causes the system to go to the defined fail-safe state without a demand from the process
Fail Detected	Failure that causes the output signal to go to the predefined alarm state
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 automatic testing
Fail Dangerous Detected	Failure that is dangerous but detected by automatic testing
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 and Abbreviations

Abbreviation	Explanation
FMEDA	Failure Modes Effects and Diagnostic Analysis

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
PFDavg	Average Probability of Failure on Demand
SFF	Safe Failure Faction. The faction 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. A 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 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 Product Support

Product support can be obtained from:

Precision Sensors Division, United Electric Controls, 340 Woodmont Road, Milford, CT 06460

www.precisionsensors.com

(1) (203) 877-2795

1.4 Related Literature

Hardware Documents

- Staset Gen 3 Series Installation and Maintenance Instructions

Guidelines / References

- Safety Integrity Level Selection – Systematic Method Including Layer of Protection Analysis, ISBN 1-55617-777-1, ISA
- Control System Safety Evaluation and Reliability, 2nd Edition, ISBN 1-55671-638-8, ISA
- Safety Instrumented Systems, Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2000 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 Staset Gen 3 series combines a switch, an analog output, and a pressure display in a 1 $^{1}/_{8}$" package. The switch output is ISO13849 PLe capable and IEC61508 SIL3 capable. The switch set points are factory set, specified by the customer. The switch state during normal operation is defined by the customer.

The analog output is available as either a voltage output or a 4-20 mA output. The voltage output comes standard as 0-10 VDC, however, other ranges between 0-11 VDC are available upon request. The voltage output can also be scaled to ranges between the available pressure ranges.

The pressure display is a 0.49" OLED which indicates the sensed pressure and the desired pressure units specified by the customer.

Other features include a switch status LED which shows red or green depending on the switch state and a switch window mode. The switch window mode allows the switch to be in one state, either open or closed, between a band and the opposite state when outside the band. The high and low set points for the band are factory set.

The pressure sensor used on the Staset Gen 3 product line features a rugged 0.002" thick, 316L stainless steel diaphragm. In addition, 316L stainless steel is used on all wetted surfaces.

While the operating temperature range is 0° C to 60° C (32° F to 140° F), the process media can be up to 80° C (158° F).

When operating within the listed specifications, an accuracy of ±0.25% is achieved.

Pressure connections are available in a variety of industry standard configurations. Electrical connections are available as standard free leads or factory installed crimp type connectors.

Detailed information for the product is contained on a product envelope drawing that defines the relevant pressures, physical and electrical interfaces, and applicable temperature and electrical ratings. Detailed installation instructions can be found in the Staset Gen 3 series installation manual.

3 Designing a SIF Using the Staset Gen 3 Series

3.1 Safety Function

Each Staset Gen 3 series is configured with two factory set switch points. The switch output opens and closes based on sensor input, at the specified switch points. Only the switch output is part of the safety function. The analog output and display are not certified to be part of the safety function.

The Staset Gen 3 series is intended to be part of a safety instrumented function and the achieved SIL level of the design function must be verified by the designer.

Table 3.1.1 Hardware Configurations

Open High Iout	Staset Gen 3, 4-20mA output, switch opens above setpoint
Open High Vout	Staset Gen 3, voltage output, switch opens above setpoint
Open Low Iout	Staset Gen 3, 4-20mA output, switch opens below setpoint
Open Low Vout	Staset Gen 3, voltage output, switch opens below setpoint
Open In Window Iout	Staset Gen 3, 4-20mA output, switch opens between low and high setpoints
Open In Window Vout	Staset Gen 3, voltage output, switch opens between low and high setpoints
Open Out of Window Iout	Staset Gen 3, 4-20mA output, switch opens below low or above high setpoint
Open Out of Window Vout	Staset Gen 3, voltage output, switch opens below low or above high setpoints

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 Staset Gen 3 series product envelope drawing for environmental limits.

3.3 Application Limits

The wetted materials for each Staset Gen 3 series are listed on the applicable product drawing. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and sensed media supply conditions. If the Staset Gen 3 series are used outside of the application limits or with incompatible materials the reliability data becomes invalid.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Precision Sensors. The 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 PFDavg 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 Staset Gen 3 series and their failure rates.

When using the Staset Gen 3 series 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 is only valid for the useful lifetime of a Staset Gen 3. The failure rate 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 may not be achieved.

3.5 SIL Capability

3.5.1 Systematic Integrity

The product has met manufacturer design process requirements of SIL 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) design with this product must not be used at a SIL higher than the statement without "prior use" justification by the end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

According to IEC 61508 the architectural constraints of an element must be determined. This can be done following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2 (see section 5.2).

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

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

The failure rate data used for this analysis meets the exida criteria for Route 2_H. Therefore, the Staset Gen 3 series meets the hardware architectural constraints for up to SIL 2 at HFT = 0, for low demand applications, when the listed failure rates are used.

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

The Staset Gen 3 is classified as a Type A element. 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.

3.5.3 Safety Parameters

For detailed failure rate information refer to the FMEDA for the Staset Gen 3 series.

3.6 Connection to the SIS Logic Solver

The Staset Gen 3 is connected to the safety rated logic solver which is actively performing the safety function as well as automatic diagnostics designed to diagnose potentially dangerous failures within the Staset Gen 3, i.e. pressure tests.

3.7 General Requirements

The system's response time shall be less than the process safety time.

All SIS components including the Staset Gen 3 series must be operational before process start-up.

The user shall verify that the Staset Gen 3 is suitable for use in safety application by confirming the Staset Gen 3 nameplates are properly marked.

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

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

The useful life of the Staset Gen 3 series is discussed in the FMEDA.

4 Installation and Commissioning

4.1 Installation

The Staset Gen 3 series must be installed per standard practices outlined in the Staset Gen 3 series installation manual.

The environment must be checked to verify that environmental conditions do not exceed the parameters listed on the Staset Gen 3 series product envelope drawing.

The Staset Gen 3 must be accessible for physical inspection.

4.2 Physical Location and Placement

The Staset Gen 3 shall be accessible with sufficient room for media and electrical connections and shall allow manual proof testing.

Media connections to the switch shall be kept as short and straight as possible to minimize restrictions and potential clogging. Obstructed or otherwise compromised connections may reduce switch reliability.

The Staset Gen 3 shall be mounted in a low vibration environment. If excessive vibration can be expected, special precautions shall be taken to ensure integrity of media and electrical connections or vibration should be reduced using appropriate damping mounts.

4.3 Process Connections

The SIF designer shall ensure that the process connections used when installing the switch are rated for the operating temperatures and pressure of the system, do not restrict sensed pressure to the Staset Gen 3 series and are compatible with the operating media.

5 Operating and Maintenance

5.1 Proof Test without Automatic Testing

The object of proof testing is to detect failures within a 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 the proof testing interval, is to be determined in reliability calculations for the safety instrumented functions for which a switch is applied. The proof tests must be performed more frequently than or as frequently as specified in the calculation in order to maintain the required safety integrity of the safety integrity 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 Precision Sensors.

Table 5.1.1: Recommended Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid false trip.
2.	Inspect the transmitter for any leaks, visible damage or contamination.
3.	Perform a two-point or three-point calibration of the transmitter over the full working range.
4.	Remove the bypass and otherwise restore normal operation.

The person(s) performing the proof test should be trained in SIS operations, including bypass procedures, system maintenance, and company Management of Change procedures.

Table 5.1.2: Proof Test Coverage

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
Open High Iout	2	97%
Open High Vout	2	97%
Open Low Iout	21	79%
Open Low Vout	21	79%
Open In Window Iout	5	94%
Open In Window Vout	5	94%
Open Out of Window Iout	5	93%
Open Out of Window Vout	5	93%

5.2 Repair and Replacement

The Staset Gen 3 series is factory set and is not repairable. If a failure has occurred the switch must be replaced. The person(s) replacing the Staset Gen 3 should be trained in SIS operations, including bypass procedures, system maintenance, and company Management of Change procedures.

5.3 Useful Life

The useful life for a Staset Gen 3 is 50 years.

5.4 Manufacturer Notification

Any failures that are detected and that compromise functional safety should be reported to Precision Sensors Division of United Electric Controls. Contact technical support at (1)(203)877-2795 via www.precisionsensors.com

6 Startup Checklist

The following checklist may be used as a guide to employ the Staset Gen 3 series in a safety critical SIF compliant to IEC 61508.

#	Activity	Result	Verified	
			By	Date
	Design			
	Target Safety Integrity Level and PFDavg determined			
	Correct switch function (OPEN or CLOSED at switch points)			
	Correct pressure range chosen			
	Correct analog output range chosen			
	Design decision documented			
	Media compatibility and suitability verified			
	SIS logic solver requirements for tests defined and documented			
	Routing of process and electrical connections determined			
	Design formally reviewed and suitability formally assessed			
	Implementation			
	Physical location and environment appropriate			
	Process connections appropriate and according to applicable codes			
	Electrical connections appropriate and according to applicable codes			
	SIS logic solver automatic tests implemented			
	Maintenance instructions for proof test released			
	Verification and test plan released			
	Implementation formally reviewed and suitability formally assessed			
	Verification and Testing			
	Process connections verified and tested			
	Electrical connections verified and tested			
	SIS logic solved 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			
	Process connection or tubing blockage / partial blockage tested			
	Safety loop function tested			