



Safety Manual

Project:

SIL Intellipoint

Customer:

AMETEK Drexelbrook

205 Keith Valley Road

Horsham, PA 19044

Project Reference:

Report No.:

Version V0, Revision R1, December 15, 2017

AMETEK

SXRXX-SM
Issue 1

Table of Contents

1	Introduction.....	3
1.1	Terms.....	3
1.2	Abbreviations	4
1.3	Product Support.....	4
1.4	Related Literature	4
1.5	Reference Standards.....	5
2	Device Description.....	5
3	Designing a SIF Using a SIL Intellipoint.....	6
3.1	Safety Function	6
3.2	Environmental limits.....	6
3.3	Application limits	6
3.4	Design Verification	6
3.5	SIL Capability.....	7
3.5.1	Systematic Integrity.....	7
3.5.2	Random Integrity.....	7
3.5.3	Safety Parameters	7
3.6	Connection of the SIL Intellipoint to the SIS Logic-solver.....	7
3.7	General Requirements.....	7
4	Installation and Commissioning	8
4.1	Installation.....	8
4.2	Physical Location and Placement.....	8
4.3	Electrical Connections	8
4.4	Commissioning	8
4.4.1	Initial Powerup Device Commissioning.....	8
4.4.2	Previously Powered Device Commissioning.....	9
5	Operations and Maintenance.....	10
5.1	Proof Testing.....	10
5.2	Proof Testing Using Process Material.....	11
5.3	Proof Testing Without Using Process Material	12
5.4	Repair and replacement.....	12
5.5	Useful Life	12
5.6	Manufacture Notification	12
6	Status of the Document	13
6.1	Releases.....	13
6.2	Future Enhancements.....	13
6.3	Release Signatures.....	13

1 Introduction

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

1.1 Terms

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 SIL Intellipoint has reported a fault by either setting the 4-20ma output to a 'fault current' or de-energizing the output relay depending on the model.
Fail Safe	Failure that causes the SIL Intellipoint 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 logic solver.
Fail Dangerous Detected	Failure that is dangerous but is detected by logic solver
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 Abbreviations

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 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 Product Support

Product support can be obtained from:

AMETEK Drexelbrook
205 Keith Valley Road
Horsham, PA 19044
Customer Service: 215-596-4250

1.4 Related Literature

Hardware Documents:

- SIL Intellipoint Installation, Operation and Maintenance Instructions

Guidelines/References:

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

1.5 Reference Standards

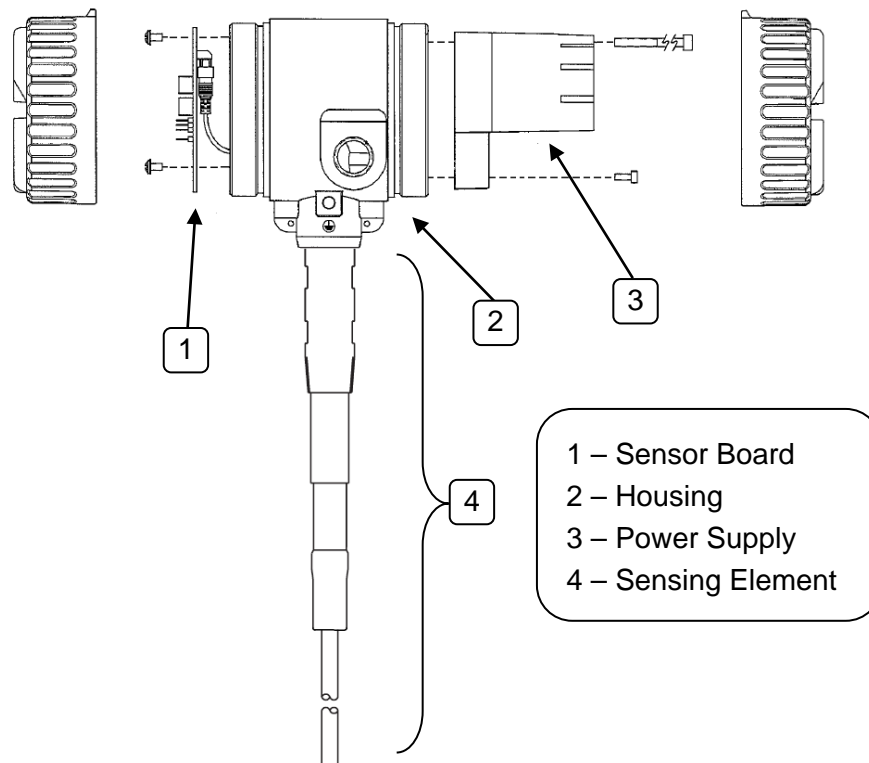
Functional Safety

- 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 components of the Safety Instrumented Function are described in this section.

The SIL Intellipoint point level switch is designed to detect the presence or absence of material in contact with the sensing element and report the detection of material. Material detection is reported via a 4-20ma analog output or via a relay contact output determined by the model SIL Intellipoint selected.



SIL Intellipoint systems are available equipped with several different sensing element designs that are approved for installation in many different process applications including standard, high temperature and floating roof applications.

3 Designing a SIF Using a SIL Intellipoint

3.1 Safety Function

The SIL Intellipoint provides fail-safe reporting via a 4-20ma output value below 6ma or above 17ma when the system detects a fault conditions. If equipped, the output relay will change state to indicate a fault or if power to the device is removed.

The AutoVerify™ self-testing function continuously monitors the entire system to ensure proper operation. Manual Certify™ changes the outputs in order to test the device output and ensure proper operation of the control systems.

The SIL Intellipoint is intended to be part of final element subsystem as defined per IEC 61508 and 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 AMETEK Drexelbrook SIL Intellipoint Brochure for environmental limits.

3.3 Application limits

The materials of construction of a SIL Intellipoint are specified in the AMETEK Drexelbrook brochure. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the SIL Intellipoint is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from AMETEK Drexelbrook. 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.

Note: The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the components and their failure rates.

When using SIL Intellipoint in a redundant configuration, a common cause factor of at least 5% should be included in safety integrity calculations.

The failure rate data listed the FMEDA report is only valid for the useful life time (10 Yrs) of a SIL Intellipoint. 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 the statement without “prior use” justification by end user or diverse technology redundancy in the design.

3.5.2 Random Integrity

The SIL Intellipoint is a Type B Device. Therefore, based on the SFF between 90% and 99%, when it is used as the only component in a final element subassembly, a design can meet SIL 2 @ HFT=0.

When the final element assembly consists of many components (this device, PLC, other process control hardware etc.) 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 Report for the SIL Intellipoint.

3.6 Connection of the SIL Intellipoint to the SIS Logic-solver

The SIL Intellipoint 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 SIF, (monitoring the device outputs for Fail-Safe State).

3.7 General Requirements

The system's response time shall be less than process safety time. The device will move to its safe state in less than 60 seconds under specified conditions.

All SIS components including the SIL Intellipoint must be operational before process start-up.

User shall verify that the SIL Intellipoint is suitable for use in safety applications by confirming the SIL Intellipoint nameplates are properly marked.

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

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

The useful life of the SIL Intellipoint is discussed in the Failure Modes, Effects and Diagnostic Analysis Report.

4 Installation and Commissioning

4.1 Installation

The SIL Intellipoint must be installed per standard practices outlined in the Installation and Operating Instructions Manual.

The environment must be checked to verify that environmental conditions do not exceed the ratings as indicated in the Installation and Operating Instructions Manual.

When installing in explosion hazardous areas [rated “potentially hazardous” (EU) or “hazardous classified” (USA)] observe all national and local regulations as well as specifications in the certificate.

The SIL Intellipoint must be powered AFTER it is installed in the application and with material BELOW (not contacting) the sensing element.

4.2 Physical Location and Placement

The SIL Intellipoint shall be accessible with sufficient room for electric connections and shall allow manual proof testing.

If the SIL Intellipoint is a flush-mount version, the placement of the device must be installed per the installation guidelines outlined in the Installation and Operating Instructions Manual.

4.3 Electrical Connections

If SIL Intellipoint is located in a hazardous environment, do not open the enclosure cover or make/break any electrical connections without first disconnecting electrical power at the source.

Electrical connections to the SIL Intellipoint must be made as outlined in the Installation and Operating Instructions Manual.

4.4 Commissioning

4.4.1 Initial Powerup Device Commissioning

The SIL Intellipoint performs automatic calibration during the first powerup sequence after shipment from the factory. This functionality requires that the SIL Intellipoint have the following preconditions meet prior to initial device powerup.

- The SIL Intellipoint must be installed per standard practices outlined in the Installation and Operating Instructions Manual.
- All required device jumper settings and functional configuration is complete and the housing covers are properly installed.
- Process material must NOT be in contact with the sensing element.

Once these preconditions are satisfied, the SIL Intellipoint can now be powered up for the first time. This will cause the SIL Intellipoint to perform its initial calibration.

It is recommended that before commissioning is complete, the SIL Intellipoint functionality be validated to meet the process needs by performing a proof test.

4.4.2 Previously Powered Device Commissioning

If SIL Intellipoint has been previously powered up, the following commissioning steps must be performed. This commissioning method requires that the SIL Intellipoint have the following preconditions meet prior to initial device powerup.

- The SIL Intellipoint must be installed per standard practices outlined in the Installation and Operating Instructions Manual.
- All required device jumper settings and functional configuration is complete.
- Process material must NOT be in contact with the sensing element.

Once these preconditions are satisfied, the SIL Intellipoint can now be powered up. The SIL Intellipoint is now ready for calibration. Conduct the calibration procedure as outlined in the Installation and Operating Instructions Manual.

Once calibrated, install all housing covers.

It is recommended that before commissioning is complete, the SIL Intellipoint functionality be validated to meet the process needs by performing a proof test.

5 Operations and Maintenance

5.1 Proof Testing

The objective of proof testing is to detect failures within SIL Intellipoint that are not detected by any automatic diagnostics of the system. The primary concern is undetected failures that prevent the safety instrumented function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a SIL Intellipoint 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 instrumented function.

One of the following proof tests are recommended to be performed based on the suitability of the test for the process application. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to AMETEK Drexelbrook.

The person(s) performing the proof test of a SIL Intellipoint should be trained in SIS operations, including bypass procedures, SIL Intellipoint maintenance and company Management of Change procedures. No special tools are required.

NOTE: The system behavior will depend on the user configured setting. This includes forward or reverse acting time delay, fault current settings and other device settings. Please refer to the Installation and Operating Instructions Manual for further information.

5.2 Proof Testing Using Process Material

Step	Action
1	Bypass the safety function by placing the logic solver in 'test mode' to avoid undesirable system behavior
2	Continuously monitor the level within the process to ensure the process will not overfill or overflow
3	Raise the process level until the material comes in contact with the sensing element and the SIL Intellipoint indicates the material has been detected. (Alarm LED turns ON for HLFS or Alarm LED OFF for LLFS) within the configured time delay window
4	Verify that the process level is within the required range for detection
5	Lower the process level until the material is no longer in contact with the sensing element and the SIL Intellipoint indicates the no material is detected (Alarm LED turns OFF for HLFS or Alarm LED ON for LLFS) within the configured time delay window.
6	If all expected behavior was observed, the proof test PASSES
7	Remove the bypass and otherwise restore normal operation.

Table1: Recommended Proof Test Using Process Material

This test will detect >90% of possible UD failures in the SIL Intellipoint safety function. This is the recommended proof test that should be performed if the application process allows for the manual control of the process material.

5.3 Proof Testing Without Using Process Material

Step	Action
1	Bypass the safety function by placing the logic solver in 'test mode' to avoid undesirable system behavior
2	Verify that the environment is safe to gain access to the sensing element.
3	Short circuit the sensing element to the housing ground.
4	Verify the SIL Intellipoint indicates the material has been detected (Alarm LED ON for HLFS or Alarm LED OFF for LLFS) within the configured time delay window.
5	Remove the short circuit from the sensing element and verify the SIL Intellipoint indicates the no material is detected (Alarm LED turns OFF for HLFS or Alarm LED ON for LLFS) within the configured time delay window.
6	If all expected behavior was observed, the proof test PASSES
7	Remove the bypass and otherwise restore normal operation.

Table2: Recommended Proof Test Without Using Process Material

This test will detect >70% of possible UD failures in the SIL Intellipoint safety function. This is the recommended proof test that should be performed if the application process does not allow for the manual control of the process material or the application process is such that the manual control of the process material is unreasonable or undesirable.

5.4 Repair and replacement

Repair procedures in the SIL Intellipoint Installation, Operation and Maintenance manual must be followed.

5.5 Useful Life

The useful life of the SIL Intellipoint is 10 years.

5.6 Manufacture Notification

Any failures that are detected and that compromise functional safety should be reported to AMETEK Drexelbrook. Please contact AMETEK Drexelbrook customer service.

6 Status of the Document

6.1 Releases

Version: V1
Revision: R1

Version History: V0, R1: *Draft; August 10, 2017*
V1, R1 *Initial Release; December 15, 2017*

Authors: AMETEK

Review: V0, R1: *Draft; August 10, 2017*

Release status: Released

6.2 Future Enhancements

At request of project.

6.3 Release Signatures

Name, Title

Name, Title

Name, Title