# SIGMAHLR

SAND PROBE RELAY

**MODEL# 7550A**

# 1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Sand Probe Relay with model numbers 7550A. This manual provides necessary user information and requirements for meeting the IEC 61508 and/or IEC 61511 functional safety standards.

## 1.1 Terms and Abbreviations

| | |
|---|---|
| Safety Freedom | Freedom from unacceptable risk of harm |
| 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 |
| 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 |
| Safety Assessment | The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems |
| Element | part of a subsystem comprising a single component or any group of components that performs one or more element safety functions |
| Fail-Safe State | state of the process when safety is achieved; A loss or significant decrease of inlet supply pressure establish high volume reverse flow exhaust. |
| Fail Safe | Failure that causes the sand probe relay to go to the defined fail-safe state without a demand from the process. |

| | |
|---|---|
| Fail Dangerous | Failure that does not permit the SIF to 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 is 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 safety function is only performed on demand, to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year and no greater than twice the proof test frequency. |
| High demand mode | Mode where the safety function is only performed on demand, to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year or greater than twice the proof test frequency. |

| | |
|---|---|
| Continuous Mode | Mode where the safety function maintains the EUC in a safe state as part of normal operation. |

## 1.2 Acronyms

| | |
|---|---|
| EUC | Equipment Under Control |
| FMEDA | Failure Modes, Effects and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| MOC | Management of Change. These are specific procedures to follow for any work activities in compliance with government regulatory authorities or requirements of a standard. |
| PFDavg | Average Probability of Failure on Demand |
| PFH | Probability of Failure per Hour |
| SFF | Safe Failure Fraction, the fraction of the overall failure rate of an element that results in either a safe fault or a diagnosed dangerous 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 is the highest level and Safety Integrity Level 1 is 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:
SigmaHLR
sales@sigmahlr.com
www.sigmahlr.com
Phone: (+1) 972-355-3453

## 1.4 Related Literature

Hardware Documents:
Installation, Operation & Maintenance Instructions. This information can be obtained on www.sigmahlr.com or contact sales@sigmahlr.com

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
- • IEC 61511:2003 Functional Safety – Safety Instrumented Systems for the Process Industry Sector (or ISA 84.00.01 if it is more appropriate)

# 2 PRODUCT DESCRIPTION

The model 7550A is a two position, three way, Normally Open flow control valve assembly that is manually reset. It is designed for use with the HLR 7620 Adaptor and the HLR 7620 Series Sand Probe Elements. A normally open flow path exists between the Inlet (I) and Outlet (O) ports. Application of media pressure at the 1/2" - 14 NPT process connection shifts the Stem to block the Inlet (I). The Outlet (O) port then becomes aligned with exhaust holes. Instrument pressure previously accumulated downstream of the Outlet port now becomes completely exhausted.

## 2.1 Hardware and Software Versions

Not applicable.

# 3 DESIGNING A SIF USING A MANUFACTURER PRODUCT

## 3.1 Safety Function

The safety function of 7550A sand probe relay is to detect critical metal loss due effects soil erosion in a pipeline. The sand will erode the sacrificial tube which will expose the probe to the pressure of flow stream which then will trigger the relay.

The listed 7550A sand probe relay model is intended to be part of a SIF 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 the listed model 7550A catalog.

### 3.3 Application limits & restrictions

Refer 7550A model catalog for any application limits & restrictions.

The materials of construction of listed sand probe relay model are specified in the individual model product spec sheets. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the listed sand probe relay model is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid. Decommissioning and disposal considerations for the product due to materials of construction are listed in installation manual.

### 3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from **SigmaHLR**. This report details all failure rates and failure modes as well as the expected lifetime. Assumptions made during the FMEDA are listed in the FMEDA report.

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 or PFH, considering safety architecture, proof test interval, proof test effectiveness, any automatic diagnostics and worst-case fault detection interval, 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 listed sand probe relay model and its failure rates. The failure rate data listed the FMEDA report are only valid for the useful life time of listed sand probe relay model. 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 required Safety Integrity Level will not be achieved.

An appropriate MTTR shall be selected based on SigmaHLR and/or plant operation and maintenance procedures.

## 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 the end user or diverse technology redundancy in the design.

### 3.5.2 Random Integrity

The Sand probe relay model in this document are Type A Element. Therefore, the sand probe relay model can be classified as a 2H device when the listed failure rates are used. When 2H data is used for all the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2H. If Route 2H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1H.

### 3.5.3 Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the listed 7550A model.

## 4 OPERATION AND MAINTENANCE

For a routine maintenance for any safety recommendations use the listed 7550A catalog for pressures & at specified operating temperatures only. Refer the spec. sheets for all necessary technical information & product limitations.

## 4.1 Proof test without automatic testing

The objective of proof testing is to detect failures within listed sand probe relay model 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 listed sand probe relay valve
models *are* applied. The proof tests must be performed at least as frequently as specified in the calculation 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 SigmaHLR.

Table1: Recommended proof Test

| Step | Action |
|---|---|
| 1 | Remove the instrument signal, & then remove the sand probe relay from service. |
| 2 | Perform a bench test to confirm the sand probe relay performs the specified safety function. |
| 3 | Inspect relay for any leaks, visible damage, or contamination. |
| 4 | Place the sand probe back in service & restore the instrument signal |

The tests to be effective the movement of the valve must be confirmed. To confirm the effectiveness of the test both travel of the valve & slew rate must be monitored & compared to expected results to validate the testing.

## 4.2 Repair and replacement

Repair procedures as recommended in the listed sand probe relay valve model spec. sheets should be followed. Contact SigmaHLR (sales@sigmahlr.com) for any further assistance.

## 4.3 MANUFACTURER Notification

Any failures that are detected and that compromise functional safety should be reported to SigmaHLR. Please contact sales@sigmahlr.com or call us at +972-355-3453 for any notifications related sand probe relay model listed in this document.