Table of Contents

Table of Contents ......................................................................................................................................................................................iii
List of Tables .............................................................................................................................................................................................iii
ST80 Series Safety Instrumented System (SIS) Requirements ...............................................................................................................1
  Introduction .......................................................................................................................................................................................1
  Compliance Through FMEDA (Failure Modes, Effects And Diagnostic Analysis) ............................................................................1
  ST80 Safety Identification .................................................................................................................................................................1
  Installation in SIS Applications ..........................................................................................................................................................1
    Configuring the Instrument for SIS Application .................................................................................................................................1
  Proof Test ..........................................................................................................................................................................................2
    Recommended Proof Test ........................................................................................................................................................ 2
  Calculation of Average Probability Of Failure On Demand (PFDavg) .................................................................................................2
  Product Repair ..................................................................................................................................................................................2
  ST80 Series SIS Reference ..............................................................................................................................................................2
  Failure Rate Data ..............................................................................................................................................................................2
  Terminology ......................................................................................................................................................................................2
  Proof Test Coverage ........................................................................................................................................................................3

List of Tables

  Table 1 – Failure Rates with Good Maintenance Assumptions in FIT @ SSI=2 According to IEC 61508 ................................................2
  Table 2 – Total Coverage (Proof Test DD + Internal Diagnostics DD) ................................................................................................3
ST80 Series Safety Instrumented System (SIS) Requirements

Introduction

This document describes how to configure the ST80 Series for IEC 61508 compliance in a Safety Instrumented System (SIS) application. The safety-critical output of the ST80 Series is provided through the Channel #1 HART output or Channel #2 analog output.

Compliance Through FMEDA (Failure Modes, Effects And Diagnostic Analysis)

Safety Integrity Level, Hardware Fault Tolerance:
- SIL 1, HFT = 0
- SIL 2, HFT = 1
- SIL 3, HFT = 2

Subsystem Type:
- B

ST80 Safety Identification

Verify that the ST80 Series system firmware is v1.07L or higher. The firmware version can be identified via the HMI (models with Display) during instrument boot-up, the ST80 configuration software, or by contacting FCI directly to cross reference the unit’s serial number with its firmware version as shipped. The information in this document relates to all ST 80 Series flow meter configurations.

Installation in SIS Applications

Installations are to be performed by qualified personnel. No special installation is required in addition to the standard installation practices outlined in the ST80 Series IO&M (Document No. 06EN003490). Environmental and operational limits are listed in the manual’s Technical Specifications section.

Configuring the Instrument for SIS Application

For all safety-related applications, configure the ST80 Series flow meter in a fail-safe alarm configuration as listed below.

- Verify that materials are compatible with process conditions.
- Configure the device for fault indication per NAMUR NE43 OR the logic solver is configured to interpret 4 mA as a fault condition.
  - Low Alarm current is ≤ 3.6 mA
  - High Alarm current is ≥ 21.0 mA
  - Channel #1 4-20 mA analog output is configured for Flow
- The safety accuracy of the ST80 Series mass flow output is ±2.0% of reading and ±0.5% of full scale. Base accuracy is dependent on the process gas composition, pressure and temperature. These parameters can be found in the appropriate calibration certificate. Contact FCI if you would like to obtain a copy referenced by the unit’s serial number.
- Use the password protection feature of the ST80 firmware to prevent accidental or deliberate change of process parameters and configuration data during normal operation.
- HART protocol is only used for setup, calibration, and diagnostic purposes; not for safety critical operation.
Proof Test

Use the recommended proof test described below to identify Dangerous Undetected failures in the ST80 Series thermal mass flow meter. This test consists of cycling the power, setting the output to minimum and maximum values and a calibration check. It is recommended that the proof test be performed annually at a minimum.

Recommended Proof Test
1. Bypass the safety function and take appropriate action to avoid a false trip.
2. User digital communications (HART) to retrieve any diagnostics and take appropriate action.
3. Cycle the power to the transmitter. This executes initialization checks on RAM and ROM.
4. Use the ST80 Series configuration tool to perform a ROM CRC check.
5. Use digital communications (configuration tool) to retrieve any diagnostics and take appropriate action.
6. Perform a two-point calibration of the transmitter over the full working range. If this is performed with only electrical instrumentation, this proof test will not detect any failures of the sensor that were undetected by internal diagnostics.
7. Remove the bypass and otherwise restore normal operation.

Calculation of Average Probability Of Failure On Demand (PFDavg)

PFDavg calculation can be determined by the owner/operator of a process using the failure rate data shown in Table 1 below. Contact FCI for a copy of the FMEDA report.

Product Repair

The ST80 Series is repairable by major component replacement. All product repair and part replacement is to be performed by qualified personnel only.

ST80 Series SIS Reference

The ST80 Series must be operated in accordance to the functional and performance specifications listed in the IO&M (Document No. 06EN003490) Technical Specifications section.

Failure Rate Data

The FMEDA report includes failure rates and common cause Beta factor estimates (contact FCI for a copy of the report). Table 1 below summarizes the failure rate data.

<table>
<thead>
<tr>
<th>Device – ST80/ST80L</th>
<th>SFF</th>
<th>( \lambda_{DU} )</th>
<th>( \lambda_{DD} )</th>
<th>( \lambda_{SU} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>HART Output, AC Power Supply</td>
<td>79.8%</td>
<td>583</td>
<td>1386</td>
<td>784</td>
</tr>
<tr>
<td>HART Output, DC Power Supply</td>
<td>77.2%</td>
<td>555</td>
<td>1145</td>
<td>735</td>
</tr>
<tr>
<td>Analog Output 2, AC Power Supply</td>
<td>78.3%</td>
<td>557</td>
<td>1253</td>
<td>761</td>
</tr>
<tr>
<td>Analog Output 2, DC Power Supply</td>
<td>77.1%</td>
<td>529</td>
<td>1011</td>
<td>712</td>
</tr>
</tbody>
</table>

Terminology

SFF = Safe Failure Fraction
\( \lambda_{DU} \) = Failure rate dangerous undetected faults
\( \lambda_{DD} \) = Failure rate dangerous detected faults
\( \lambda_{SU} \) = Failure rate safe undetected faults
FIT = Failure rate in 10^{-9}/hour
Proof Test Coverage

Based on the Proof Test procedures recommended in this document, Table 2 below shows the Total Coverage of the device based on the remaining Dangerous Undetected failures not accounted for by either the Proof Test or Internal Diagnostics (Dangerous Detected).

Table 2 – Total Coverage (Proof Test DD + Internal Diagnostics DD)

<table>
<thead>
<tr>
<th>Device – ST80/ST80L</th>
<th>SFF</th>
<th>Proof Test Coverage</th>
<th>( \lambda_{DUPT} ) (FIT)</th>
<th>Total Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>HART Output, AC Power Supply</td>
<td>79.8%</td>
<td>66%</td>
<td>385</td>
<td>93.8%</td>
</tr>
<tr>
<td>HART Output, DC Power Supply</td>
<td>77.2%</td>
<td>65%</td>
<td>361</td>
<td>92.0%</td>
</tr>
<tr>
<td>Analog Output 2, AC Power Supply</td>
<td>78.3%</td>
<td>67%</td>
<td>373</td>
<td>92.8%</td>
</tr>
<tr>
<td>Analog Output 2, DC Power Supply</td>
<td>77.1%</td>
<td>65%</td>
<td>344</td>
<td>92.4%</td>
</tr>
</tbody>
</table>