Statement of Compliance

Manufacturer's Name: Dynisco Instruments

Product Name/Type: mA Pressure Sensors

Model Number(s): PT46x4, MDT4x2F

The above product complies with the following:

The above products were evaluated by exida of 64 North Main Street, Sellersville, PA 18960 and the hardware was found to comply with the requirements of IEC 61508/IEC 61511 for SIL Level 2.

Support documents Part Number(s): **975502**

The support document contains the necessary failure rate parameters used in specifying this device in a safety rated environment. If further data is required, please contact Dynisco Customer Service.

(Support documentation may or may not accompany this statement)

Revision Date: February 25, 2015
Expiration Date: None

Failure Modes, Effects and Diagnostic Analysis

Project:
Guardian Pressure Transmitter

Company:
Dynisco LLC
Franklin, MA
USA

Contract Number: Q13/06-069
Report No.: DYN 13/06-069 R001
Version V1, Revision R2, September 10, 2013
Rudolf Chalupa

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Guardian Pressure Transmitter, hardware and software revision per Section 2.5.1. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the Guardian. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Guardian Pressure Transmitter is typically used to determine melt pressure. The Guardian provides the industry standard 4-20mA signal designed to work with most logic solvers. In addition the transducer provides a de-energize to trip contact closure which opens upon detection of overpressure or an internal failure. The Guardian consists of a filled assembly and a shell assembly, the latter containing the electronics and connector. The filled assembly is mainly comprised of a process diaphragm connected to a strain gauged diaphragm via a flexible fluid filled stainless steel capillary; this isolates the strain gauge from process temperatures.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Guardian.

Table 1 Version Overview

mA	the 4-20mA output is the safety output, overscale to trip
relay	the relay output is the safety output, de-energize to trip

The Guardian is classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H. Therefore the Guardian meets the hardware architectural constraints for up to SIL 2 with a single device when the listed failure rates are used.

The failure rates for the Guardian are listed in Table 2.

Table 2 Failure rates Guardian mA

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		134
Fail Dangerous Detected		90
Fail Low (detected by logic solver)	90	
Fail Dangerous Undetected		263
No Effect		328

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table 3 Failure rates Guardian Relay

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	191
Fail Dangerous Undetected	217
No Effect	407

These failure rates are valid for the useful lifetime of the product, see Appendix A.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 4 lists the failure rates for the Guardian according to IEC 61508, ed2, 2010.

Table 4 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
Guardian mA	0	134	90	263	46.0%
Guardian relay	0	191	0	217	46.8%

A user of the Guardian can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

[2] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[3] Safe Failure Fraction, if needed, is to be calculated on an element level