FLUID COMPONENTS INTERNATIONAL LLC

ST100 Series Thermal Mass Flow Meter
FMEDA Report

Failure Modes, Effects and Diagnostic Analysis

Project:
ST100 Thermal Mass Flow Meter

Company:
Fluid Components International
San Marcos, California
USA

Contract Number: Q11/11-073
Report No.: FCI 11/11-073 R001
Version V1, Revision R1, April 24, 2012
Rudolf P. 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 ST100 Thermal Mass Flow Meter, hardware revision as described in Section 2.5.1 and core board software revision v2.92. 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 and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the ST100. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The ST100 Series is a thermal dispersion, industrial process grade air/gas flow meter. It is suitable for all air and gas flow measurement applications in line sizes from 1" to 100" [25 to 2500 mm] and larger. The instrument provides direct mass flow measuring and measures flow rate, totalized flow and temperature; the STP versions add pressure measurement. The measurements are made available to the user by way of 4-20mA analog output channels with HART or pre-selected digital bus protocols. The optional graphics display provides real-time process variable values along with flow range and process description information.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the ST100.

Table 1 Version Overview

Single Probe AC Supply	Thermal flowmeter with single probe, output 4-20mA with HART, 85 to 265 Vrms AC supply; ST100, ST110, STP100, STP110
Single Probe DC Supply	Thermal flowmeter with single probe, output 4-20mA with HART, 24VDC supply: ST100, ST110, STP100, STP110
Dual Probe AC Supply	Thermal flowmeter with two probes, configured to provide average reading if both probes functional and reading from remaining probe if one probe becomes non-functional, output 4-20mA with HART, 85 to 265 Vrms AC supply: ST102, ST112, STP102, STP,112
Dual Probe DC Supply	Thermal flowmeter with two probes, configured to provide average reading if both probes functional and reading from remaining probe if one probe becomes non-functional, output 4-20mA with HART, 24VDC supply: T102, ST112, STP102, STP,112

The ST100 is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device has a Safe Failure Fraction between 60% and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 1 as a single device. The complete subsystem, of which the ST100 is the sensor element, will need to be evaluated to determine the Safe Failure Fraction.

The failure rates for the ST100 are listed in Table 2 - Table 5.

---

[1] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

Table 2 Failure rates ST100, Single Probe AC Supply

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		314
Fail Dangerous Detected		1697
Fail Detected (detected by internal diagnostics)	867	
Fail High (detected by logic solver)	36	
Fail Low (detected by logic solver)	794	
Fail Dangerous Undetected		567
No Effect		1946
Annunciation Detected		230

Table 3 Failure rates ST100, Single Probe DC Supply

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		317
Fail Dangerous Detected		1716
Fail Detected (detected by internal diagnostics)	867	
Fail High (detected by logic solver)	36	
Fail Low (detected by logic solver)	813	
Fail Dangerous Undetected		570
No Effect		1959
Annunciation Detected		230

Table 4 Failure rates ST100, Dual Probe AC Supply

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		404
Fail Dangerous Detected		2458
Fail Detected (detected by internal diagnostics)	1584	
Fail High (detected by logic solver)	36	
Fail Low (detected by logic solver)	838	
Fail Dangerous Undetected		415
No Effect		2442
Annunciation Detected		460

Table 5 Failure rates ST100, Dual Probe DC Supply

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		407
Fail Dangerous Detected		2477
Fail Detected (detected by internal diagnostics)	1584	
Fail High (detected by logic solver)	36	
Fail Low (detected by logic solver)	857	
Fail Dangerous Undetected		418
No Effect		2455
Annunciation Detected		460

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 6 lists the failure rates for the ST100 according to IEC 61508, ed2, 2010.

Table 6 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
Single Probe AC Supply	0	314	1927	567	79.8%
Single Probe DC Supply	0	317	1946	570	79.9%
Dual Probe AC Supply	0	404	2918	415	88.9%
Dual Probe DC Supply	0	407	2937	418	88.9%

A user of the ST100 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 needs to be calculated on (sub)system level