FLUID COMPONENTS INTERNATIONAL LLC

# FS10A Flow Switch/Monitor FMEDA Report


## Failure Modes, Effects and Diagnostic Analysis

Project:
FS10 Flow Switch/Monitor

Company:
Fluid Components International LLC
San Marcos, California
United States

Contract Number: Q13/01-043
Report No.: FCI 13/01-043 R001
Version V1, Revision R3, April 3, 2013
Griff Francis

## 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 FS10 Flow Switch/Monitor, hardware revision as defined documents in Table 2.5.1 and software revision v4.02. 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 FS10 Flow Switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The FS10 Flow Switch is a universal flow monitor and switch specifically designed for gas and liquid process analyzer sampling systems. The FS10 Flow Switch installs into a standard tube tee fitting or a SP76 (NeSSI) modular manifold.

The FS10 Flow Switch utilizes thermal-dispersion flow measurement. The instrument's wetted parts are 316L stainless steel with Hastelloy-C sensor tips. FS10 Flow Switch electronics are packaged in a fully-sealed, aluminum housing.

The electronics can be integral mounted with the sensor element resulting in unibody, self-contained unit or the electronics can be separated from the sensor for remote. The remote configuration is used when the sensor installation area is subjected to high temperatures, or to mount the front panel and display in a more accessible location.

The instrument provides a top-mounted, flow rate monitoring LED array for visual indication of proper flow rate to the analyzer or sampling system, an alarm/trip indication, and as confirmation that the unit is powered and operating. The flow switch's setpoint is user settable via two push-buttons accessible at the top of the unit, or via its RS232 serial interface. The LEDs, push-buttons and serial interface are not part of the safety function.

A choice of electronic outputs is available. The switch output can be either an open collector (transistor) or a 1A relay. The switch settings are user programmable for trip control of hysteresis and time delay. Optionally available for trending is a 4-20mA output which is settable to represent flow rate in mass flow or standard volume units.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the FS10 Flow Switch.

**Table 1 Version Overview**

| | |
|---|---|
| Option 1 | relay output, alarm on low flow |
| Option 2 | relay output, alarm on high flow |
| Option 3 | transistor output, alarm on low flow |
| Option 4 | transistor output, alarm on high flow |
| Option 5 | current output, alarm on low flow |
| Option 6 | current output, alarm on high flow |

The FS10 Flow Switch is classified as Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows the product versions have a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents when the current output is used) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The failure rates for the FS10 Flow Switch are listed in Table 2, Table 3 and Table 4.

**Table 2 Failure rates FS10 Flow Switch- relay output, alarm on low or high flow**

| Failure Category | Failure Rate (FIT) |
|---|---|
| Fail Safe Detected | 900 |
| Fail Safe Undetected | 240 |
| Fail Dangerous Detected | 860 |
| Fail Dangerous Undetected | 232 |
| No Effect | 202 |
| External Leak | 10 |

**Table 3 Failure rates FS10 Flow Switch- transistor, alarm on low or high flow**

| Failure Category | Failure Rate (FIT) |
|---|---|
| Fail Safe Detected | 900 |
| Fail Safe Undetected | 220 |
| Fail Dangerous Detected | 860 |
| Fail Dangerous Undetected | 213 |
| No Effect | 205 |
| External Leak | 10 |

[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 4 Failure rates FS10 Flow Switch- current output, alarm on low or high flow**

| Failure Category | Failure Rate (FIT) | |
|---|---|---|
| Fail Safe Undetected | | 217 |
| Fail Dangerous Detected | | 1784 |
| Fail Detected (detected by internal diagnostics) | 1760 | |
| Fail High (detected by logic solver) | 14 | |
| Fail Low (detected by logic solver) | 10 | |
| Fail Dangerous Undetected | | 215 |
| No Effect | | 198 |
| External Leak | | 10 |

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 5 lists the failure rates for the FS10 Flow Switch according to IEC 61508, ed2, 2010.

**Table 5 Failure rates according to IEC 61508 in FIT**

| Device Configuration | $\lambda_{SD}$ | $\lambda_{SU}$[2] | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF[3] |
|---|---|---|---|---|---|
| relay output,<br>alarm on low or high flow | 900 | 240 | 860 | 232 | 90% |
| transistor output,<br>alarm on low or high flow | 900 | 220 | 860 | 213 | 90% |
| current output,<br>alarm on low or high flow | - | 217 | 1784 | 215 | 90% |

A user of the FS10 Flow Switch 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 an element level.