

Report Nr. 07207334856

Applicant: Fluid Components Ltd.
1755 La Costa Meadows Drive
San Marcos, CA 92069 USA

Device under test: FLT 93 – Sensor System

Testing body: TÜV NORD CERT GmbH
Safety Related Services - SRS
Langemarckstr. 20, D-45141 Essen

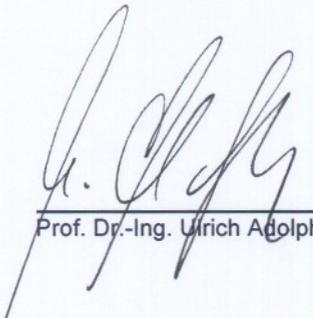
Test engineer: Mr. Dipl.-Ing. Roger Feist

Review: Mr. Dr.-Ing. Ulrich Adolph

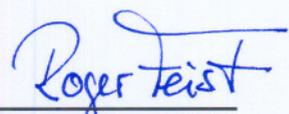
Test principles: Quantitative failure analysis with FMEDA-techniques

Date: 24.10.2007

Order-no.: 8000334856



Prof. Dr.-Ing. Ulrich Adolph



Dipl.-Ing. Roger Feist

The report consists of 8 pages

Partial duplication of this Technical Report and its use for advertising purposes is allowed with permission of the testing laboratory only. This Technical Report contains the result of the examination of the product sample submitted by the manufacturer. A general statement concerning the quality of the products from the series manufacture cannot be derived therefrom.

1 Contents

1	Contents	2
2	Management Summary	2
3	Documents	4
4	Conducted tests - FMEDA calculation	5
4.1	General	5
4.2	Procedure	5
4.3	Failure rates of the components	7
4.4	FMEDA results and estimation of PFD	8

2 Management Summary

This report describes the results of the Failure Modes, Effects and Diagnostic Analysis (FMEDA) on the FLT93 sensor system. A FMEDA is one of the steps taken to achieve functional safety certification per IEC 61508 of a device. From the resulting failure rates the Safe Failure Fraction (SFF) and example PFD-values are calculated. The FMEDA that is described in this report is regarding only random failure probabilities of the FLT93-hardware. For a full functional safety certification all requirements of the IEC 61508 must be considered.

The FLT93 Series models are multipurpose measurement instruments. Each model is a single instrument that is capable of detecting air flow, fluid flow and temperature. It is also able to detect liquid level or fluid media interfaces. The instrument has two field adjustable alarm set points, two buffered voltage outputs, as well as a built-in calibration

Because of the usage of commonly used electronic components with well known failure-behaviour and sufficient field experiences the FLT 93 Sensor system electronic is classified as a Type A subsystem according to IEC 61508-1 chapter 7.4.3.1.2. It has a hardware failure tolerance (HFT) of 0.

The analysis shows, that different internal configurations of the FLT 93 lead to different results. Therefore focus was set to the "fail-safe configuration" is regarded to be relevant. The most relevant safety-configuration of the FLT 93 is (according to the manufacturer) is:

- “fail-safe”
- “flow switch”
- “SPS connected to outputs”

For the sensor head failure rates statistical proof data provided by the manufacturer have been used. These data have not been verified by the testing body. Certain component failures increase configured switch-points or the measured value. They have different effects whether the FLT is configured to de-energise its output above a “high” sensor outputs (low flow detection) or to de-energise below a “low” sensor output, mentioned as “High Switch” or “Low Switch” in the text below. This leads to slightly different results for “low flow detection” and “high flow detection”.

The estimated failure rates under these conditions and for this mode of operation are listed in table 1.

Table 1: Failure rates for flow-switch configuration

	$\lambda_{SD} [10^{-9}/h]$	$\lambda_{SU} [10^{-9}/h]$	$\lambda_{DD} [10^{-9}/h]$	$\lambda_{DU} [10^{-9}/h]$	SFF [%]
High Switch	383	1102	82	374	82
Low Switch	320	1147	144	302	84

To cover a maximum number of different FLT configurations and usage modes several different calculations were carried out for both, high switch and low switch:

- FLT93 only regarding the electronic devices – without the sensor head.
- FLT93 with sensor-head – Failure rate from proof-data.
- FLT93 with sensor-head - Generic data
- FLT93 with maximum output load – relay not de-rated.

Details regarding the calculation and results for other configurations can be taken from chapter 4.2 – FMEDA calculation. Using the FMEDA results a sample PFD using a proof-check-interval of 1 year was calculated. For the configuration above the PFD equals:

$$\text{PFD} = 1.52 * 10^{-3} \text{ (high switch) and}$$

$$\text{PFD} = 1.32 * 10^{-3} \text{ (low switch)}$$

For SIL2-capable sensor-devices it is usually required, that the PFD-values are smaller than $3.5 * 10^{-3}$.

3 Documents

Relevant standards:

/S1/	IEC 61508-1:1998 + corrigendum 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements;
/S2/	IEC 61508-2:2000	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems;
/S3/	IEC 61508-6:2000	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of IEC 61508-2 an IEC 61508-3
/S4/	SN 29500	Failure rates of components

Submitted Files:

/C1/	Schematic diagram, 5 pages	DWG No. 015811	16 June 94
/C2/	Parts list „5294 basic“ , p.2 – p. 4/4	PL 015814-01	20 June 94
/C3/	Parts list “Input power normal line” p.2/2	PL 015905-01	20 June 94
/C4/	Parts list “relay contact rating”	PL 015334-01	27 Oct 93
/C5/	Parts list “heater wattage control, variable, –S sensing element”	PL 015920-01	15 June 94
/C6/	Installation, operation and maintenance manual FLT Series FlexSwitch	06EN003246 Rev. B	29 Sept 94

Appendices:

/A1/	FMEDA for FLT93 – High Switch	3 pages	24 Oct 2007
/A2/	FMEDA for FLT93 – Low Switch	3 pages	24 Oct 2007
/A3/	Determination of failure rates according to SN 29500	2 pages	24 Oct 2007

4 Conducted tests - FMEDA calculation

4.1 General

The FLT93 Series models are multipurpose measurement instruments. Each model is a single instrument that is capable of detecting air flow, fluid flow and temperature. It is also able to detect liquid level or fluid media interfaces. The instrument has two field adjustable alarm set points, two buffered voltage outputs, as well as a built-in calibration circuit. The alarm-outputs of the sensor are realized with 6 amp relay contacts that can be used to control customer process applications. For all safety-related applications the FLT93 must be configured in "failsafe alarm setting" as described in the installation manual chapter 3-20ff.

The operation of the sensing element is based upon the thermal dispersion principle: A low-powered heater is used to produce a temperature differential between two "Resistance Temperature Detectors" (RTD). The RTD temperature differential varies as a function of forced convection for flow measurement and as a function of fluid thermal conductivity for level and interface measurement. The measurement of the fluid's temperature is obtained from the non-heated RTD. The control circuit converts the sensing element's RTD temperature differential into an analog DC voltage signal. Dual comparators monitor the sensing element signal and activate the relay alarm circuits if the signal exceeds an adjustable set point. The control circuit contains certain removable jumpers that configure the instrument to perform in different modes.

The FMEDA is a systematic way to recognise and quantify the effects of different component-failures on the complete system. If possible, the assumptions made should be verified on the real system.

4.2 Procedure

The circuit-diagram of the FLT93 was divided in subsystems, each having a determined function in the sensing function. For each component in the subsystem the possible failure modes were analysed and divided in one of the following failure-categories:

- λ_{SD} : Failure, which is not influencing the safety-function but causes the module to go to safe state (e.g. by de-energising one of the relay) by means of an diagnostic circuit.
- λ_{SU} : Failure, which is influencing the safety function in a safe way, but remains undetected.
- λ_{DD} : Failure, which is causing a dangerous malfunction of the subsystem/ module, but is detected by internal diagnostics.
- λ_{DU} : Failure that is dangerous and is not being detected by internal diagnosis.
- λ_{NE} : Failure rate of a component which is not related to the safety function or the diagnostics. Usually it has other purposes in the circuit, e.g. EMC. It is not regarded as part of the safety function and its failure rate has not necessarily to be quantified.

Using the sum of these failure rates the overall-SFF (safe failure fraction) for the FLT93 was determined. If for a certain component/ subsystem the division in further subsystems or failure mode was not necessary, possible or sensible, 50% of the total failure rate for the subsystem have been classified to be dangerous. If components are used in a double-channel configuration (e.g. two relay in line – both must fail to be dangerous), the calculation uses a single-channel equivalent considering the Common-Cause-Failure.

For all analysis steps the failsafe configuration was assumed, thus both output relay must be energised in OK-condition. If one of the two output relay is de-energised, there is a process failure or an internal component failure in the FLT93. For the switch-point settings in the alarm circuit it was assumed, that output voltages of the front end conditioners output above 7 V and below 0.5 V lead to alarm condition. All failures not causing a drift of the measured value higher than 1% of its nominal are counted with 50% dangerous (value can drift in both directions – safe and dangerous). Failures causing an output above 7 V or below 0.5 V have been counted with 50% safe and 50% dangerous detected failures.

Furthermore it was assumed, that

- At a single point of time only one component fails.
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The stress levels are average for an industrial environment.
- External power supply failures can be excluded.
- Systematic failures like wrong connected terminals are excluded.

- The potentiometer settings are done according to the manufacturer's specification. The operating point of the internal signal "ΔV SIG1" is between 0.5V and 7.0V
- Because of the mechanical properties of the housing the influence of dirt on the circuit-board can be excluded.
- After use of the calibration potentiometer it is turned to one of its maximum values to guarantee, that random switching of the "cal switch" leads to safe state. This instruction is currently not in the user manual!
- J22 is open, J16 is closed.

4.3 Failure rates of the components

The failure rates of critical components have been extracted from /S4/, failure modes, where applicable from DIN EN 62061. The data were chosen under consideration of worst case scenarios inside the span of the assumed environments. It is expected that the failure rate recognizable in average field applications will be less than the predicted numbers.

If no failure-data for a component was found in /S4/ other sources have been taken into account. This applies especially to the use of RTD-sensors in industrial environment. In similar applications RTD-sensors have been used with an expected failure rate of 8000 FIT. The manufacturer of the FLT93 system has claimed to provide a high protection level against vibration, which is the major failure-source for RTD. To respect this fact, a second calculation was prepared with the failure rate from the manufacturers "proven in use" data. The underlying statistics have not been verified by the testing body. To determine a failure rate from the available proof-data an average number of 54 damaged sensor-heads (for any reason) has been extracted. On a basis of approximately 3000 sold devices per year and a 3 years warranty period the failure rate was determined with 70% confidence interval and distributed equally on both RTD. According to this each RTD should be better than 375 FIT.

A similar situation applies to the relay in the sensor output circuit. While specified for 6 Amp loads, they are normally used in conjunction with high-impedance PLC-inputs, thus will be used highly underrated in 99% of current applications. Again, to respect this common application a separate calculation was carried out.

4.4 FMEDA results and estimation of PFD

The analysis results for the sensor-electronic without head but with a PLC system as interfacing device are:

	$\lambda_{SD} [10^{-9}/h]$	$\lambda_{SU} [10^{-9}/h]$	$\lambda_{DD} [10^{-9}/h]$	$\lambda_{DU} [10^{-9}/h]$	SFF [%]	PFD ¹
High Switch	83	802	7	272	77	$1,19 \cdot 10^{-3}$
Low Switch	20	847	70	227	80	$0,99 \cdot 10^{-3}$

Together with a sensor head with failure rate according to the manufacturer's statistic and with a PLC system as interfacing device it yields:

	$\lambda_{SD} [10^{-9}/h]$	$\lambda_{SU} [10^{-9}/h]$	$\lambda_{DD} [10^{-9}/h]$	$\lambda_{DU} [10^{-9}/h]$	SFF [%]	PFD ¹
High Switch	383	1102	82	374	82	$1,52 \cdot 10^{-3}$
Low Switch	320	1147	144	302	84	$1,32 \cdot 10^{-3}$

If the latter calculation is done with generic data for the RTD-sensor components (not regarding the mechanical properties of the FLT-construction) the result is:

	$\lambda_{SD} [10^{-9}/h]$	$\lambda_{SU} [10^{-9}/h]$	$\lambda_{DD} [10^{-9}/h]$	$\lambda_{DU} [10^{-9}/h]$	SFF [%]	PFD ¹
High Switch	6483	7202	1607	1872	89	$8,2 \cdot 10^{-3}$
Low Switch	6420	7247	1669	1827	89	$8,0 \cdot 10^{-3}$

In cases, where the FLT is used to switch a higher load (e. g. a valve) directly, the following values, considering maximum load on the output should be used:

	$\lambda_{SD} [10^{-9}/h]$	$\lambda_{SU} [10^{-9}/h]$	$\lambda_{DD} [10^{-9}/h]$	$\lambda_{DU} [10^{-9}/h]$	SFF [%]	PFD ¹
High Switch	83	1133	7	603	67	$2,64 \cdot 10^{-3}$
Low Switch	20	1178	70	558	69	$2,44 \cdot 10^{-3}$

¹ The PFD (probability of failure on demand) values are samples calculated for a subsystem with supposed 1oo1d-architecture and a 1 year proof check interval. The required value for SIL verification according to IEC 61508 is the PFD of the complete safety-function