Failure Modes, Effects and Diagnostic Analysis

Project:
Pressure switches series M**, B* and PC*

Customer:
ETTORE CELLA S.P.A.
Bareggio (MI)
Italy

Contract No.: CELLA 07/07-28
Report No.: CELLA 07/07-28 R001
Version V1, Revision R0, March 2008

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the pressure switches series M**, B* and PC*. Table 1 and Table 2 give an overview of the different versions and evaluated scenarios that belong to the considered pressure switches.

The mechanical assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

M**	Modular diaphragm pressure switches MAB (explosion proof, low pressure), MA (explosion proof, medium pressure), MWB (weather proof, low pressure) and MW (weather proof, medium pressure)
B*	Bourdon tube pressure switches BA (explosion proof) and BW (weather proof)
PC*	Compact diaphragm pressure switches PCA (explosion proof) and PCS (weather proof)

For safety applications only the described versions of the pressure switches, see Table 1, have been considered. All other possible variants and configurations are not covered by this report.

The failure rates used in the analysis were derived from *exida's* experienced-based data compilation.

ETTORE CELLA S.P.A. and *exida* together did a quantitative analysis of the pressure switches series M**, B* and PC* to calculate the failure rates using *exida's* experienced-based data compilation for the different mechanical components.

The pressure switches series M**, B* and PC* are classified as Type A[1] subsystems with a hardware fault tolerance of 0.

For Type A subsystems the SFF has to be between 60% to < 90% according to table 2 of IEC 61508-2 for SIL 2 subsystems with a hardware fault tolerance of 0.

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.

[1] Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

Table 2: Considered scenarios

[SC1]	Low demand mode of operation (max 60 switching actions during life including test) Oscillating pressure amplitude: 41% of the upper range limit (URL) of the instrument (medium value 62,5% of the URL) Oscillating pressure frequency: 10.000 per year Switch electrical rating: 24V 100mA DC or 220V 15A AC
[SC2]	High demand mode of operation (max 1 switching action per day) Oscillating pressure amplitude: 41% of the upper range limit (URL) of the instrument (medium value 62,5% of the URL) Oscillating pressure frequency: 6 per hour Switch electrical rating: 24V 100mA DC
[SC3]	High demand mode of operation (max 1 switching action per day) Oscillating pressure amplitude: 41% of the upper range limit (URL) of the instrument (medium value 62,5% of the URL) Oscillating pressure frequency: 6 per hour Switch electrical rating: 220V 15A AC

The scenarios given in Table 2 are presumable working conditions that according to ETTORE CELLA S.P.A do normally not lead to systematic failures during the useful life of the instruments.

The following table shows how the above stated requirements are fulfilled. MAX stands for applications where increasing pressure is monitored (over pressure protection). MIN stands for applications where decreasing pressure is monitored (low pressure protection).

Table 3: Summary for [SC1] – failure rates per IEC 61508

	B* - MIN	**B* - MAX**	**M** - MIN**	**M** - MAX**	**PC* - MIN**	**PC* - MAX**
λ_{safe} [2]	68 FIT	81 FIT	113 FIT	103 FIT	64 FIT	65 FIT
$\lambda_{dangerous}$	19 FIT	15 FIT	25 FIT	26 FIT	41 FIT	39 FIT
SFF	78%	84%	81%	80%	61%	62%
SIL AC [3]	SIL2	SIL2	SIL2	SIL2	SIL2	SIL2

Table 4: Summary for [SC2] – failure rates per IEC 61508

	B* - MIN	**B* - MAX**	**M** - MIN**	**M** - MAX**	**PC* - MIN**	**PC* - MAX**
λ_{safe} [2]	124 FIT	137 FIT	168 FIT	158 FIT	168 FIT	160 FIT
$\lambda_{dangerous}$	74 FIT	70 FIT	85 FIT	81 FIT	48 FIT	56 FIT
SFF	62%	66%	67%	66%	77%	74%
SIL AC [3]	SIL2	SIL2	SIL2	SIL2	SIL2	SIL2

[2] Note that the “safe” category includes failures that do not cause a spurious trip

[3] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

Table 5: Summary for [SC3] – failure rates per IEC 61508

	B* - MIN	B* - MAX	M** - MIN	M** - MAX	PC* - MIN	PC* - MAX
λ_{safe} [2]	129 FIT	142 FIT	173 FIT	163 FIT	173 FIT	165 FIT
$\lambda_{dangerous}$	79 FIT	75 FIT	85 FIT	86 FIT	53 FIT	61 FIT
SFF	61%	65%	66%	65%	76%	73%
SIL AC [3]	SIL2	SIL2	SIL2	SIL2	SIL2	SIL2

A user of the considered pressure switches 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 sections 5.2 to 5.7 along with all assumptions.

It is important to realize that the “residual” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the considered pressure switches (see Appendix 2) working in the considered scenarios.