



Failure Modes, Effects and Diagnostic Analysis Summary

Project:

Pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x
series

Customer:

Barksdale GmbH
Reichelsheim
Germany

Contract No.: Barksdale 11/05-020

Report No.: Barksdale 11/05-020 R001

Version V2, Revision R0, July 2020

Philipp Hanzik

Management summary

This report summarizes the results of the hardware assessment carried out on the pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x series. Table 1 gives an overview of the different versions 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. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview ¹

Type	Comment
9681x, 9692x	Piston pressure switch, for hazardous areas, Ex i approval
9671x	Diaphragm seal piston sensor, for vacuum measurement, Ex i approval
B.T / B.X	Bourdon tube pressure switches with direct-acting pressure sensor and the snap-acting micro switch, Ex i approval, B.X types additional with Ex d approval
D.T / D.X	Mechanical pressure switch with metal diaphragm, Ex i approval, D.X types additional with Ex d approval
S8000/X1T	Mechanical pressure switches in diaphragm or piston design, Ex i approval
DP.T	Mechanical single/dual pressure switch, Ex i approval

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

Barksdale GmbH and *exida* together did a quantitative analysis of the pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x to calculate the failure rates using *exida*'s experienced-based data compilation for the different mechanical components.

The pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x are classified as Type A² elements according to IEC 61508, having a hardware fault tolerance of 1 and can be classified as 2_H devices when the listed failure rates are used. **When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL3 at HFT=1 for low demand mode applications.** If Route 2_H is not applicable for the entire element, the architectural constraints will need to be evaluated per Route 1_H.

¹ All versions are available in several pressure ranges and switching contact materials (gold or silver). The listed versions are representative for the type series.

² Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

All types can be used as monitoring devices which are switching at increasing pressure (max) or decreasing pressure (min).

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 1.1.1.

The failure rates according to IEC 61508:2010 2nd edition for the pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x series are listed in the following tables.

Table 2: Summary – IEC 61508:2010 failure rates³ for increasing pressure detection

Redundant (red.) design with two switches is specified in the following table separately. All types are with Ex i approval, B.X and D.X additional with explosion proof housing and Ex d approval.

Failure rates (in FIT) according to <i>exida</i> Profile 3											
Failure category	9681x, 9692x	9681x, 9692x (red.)	9671x	9671x (red.)	B.T / B.X	B.T / B.X (red.)	D.T / D.X	D.T / D.X (red.)	DP.T	DP.T (red.)	S8000 / X1T
Fail Safe Detected (λ_{SD})	0	0	0	0	0	0	0	0	0	0	0
Fail Safe Undetected (λ_{SU})	132	252	140	260	128	252	127	253	187	313	130
Fail Dangerous Detected (λ_{DD}) ⁴	0	27	0	27	0	32	0	29	0	29	0
Fail Dangerous Undetected (λ_{DU})	82	55	72	45	65	32	57	27	119	89	86

Total failure rate (safety function)	214	334	212	332	193	316	184	309	306	431	216
SIL AC ⁵	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3

³ It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

⁴ The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch is considered to be a safety measure for the primary switch providing a DC of 90% by considering a common cause factor of 10%.

⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. It is based on Route 2H.

Table 3: Summary – IEC 61508:2010 failure rates⁶ for decreasing pressure detection

Redundant (red.) design with two switches is specified in the following table separately. All types are with Ex i approval, B.X and D.X additional with explosion proof housing and Ex d approval.

Failure rates (in FIT) according to <i>exida</i> Profile 3											
Failure category	9681x, 9692x	9681x, 9692x (red.)	9671x	9671x (red.)	B.T / B.X	B.T / B.X (red.)	D.T / D.X	D.T / D.X (red.)	DP.T	DP.T (red.)	S8000 / X1T
Fail Safe Detected (λ_{SD})	0	0	0	0	0	0	0	0	0	0	0
Fail Safe Undetected (λ_{SU})	145	265	144	264	140	266	137	260	197	320	145
Fail Dangerous Detected (λ_{DD}) ⁷	0	27	0	27	0	29	0	32	0	32	0
Fail Dangerous Undetected (λ_{DU})	69	42	68	41	53	23	47	14	109	77	71
<hr/>											
Total failure rate (safety function)	214	334	212	332	193	318	184	306	306	429	216
SIL AC⁸	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3	SIL3

⁶ It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

⁷ The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch is considered to be a safety measure for the primary switch providing a DC of 90% by considering a common cause factor of 10%.

⁸ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. It is based on Route 2H.

1.1.1 Assumptions


The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the pressure switches D.T, D.X, B.T, B.X, X1T, 8000, 9671x, 9681x, 9692x series.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions and process fluids.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- The pressure switches are installed per the manufacturer's instructions.
- The pressure switches are in low demand use.
- The stress levels are average for an industrial outdoor environment and can be compared to *exida* Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings. Only the described versions and circuit functions are used for safety applications.

1.2 Release Signatures

A handwritten signature in blue ink, appearing to read "Hanzik".

B.Eng. Philipp Hanzik, Safety Engineer

A handwritten signature in black ink, appearing to read "S. Aschenbrenner".

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner, CEO