Magnetrol®

Failure Modes, Effects, and Diagnostic Analysis

Displacer Level Switch
Single Stage Mechanical Units
High and Low Level Applications

Rev. 0 July 6, 2006

Table of Contents

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Displacer Level Switch series in both low and high level applications. The FMEDA only applies to the models and switch mechanisms listed in the Model Designation section and wired per one of the methods described in the Wiring Requirements section. The FMEDA performed on these Magnetrol products includes all related hardware. For full certification purposes, the product along with all requirements of IEC 61508 must be considered.

1. Model Designations

The FMEDA analysis in this report is only applicable for the Single Stage Displacer Level Unit model numbers and DPDT switch mechanisms listed below.

Models: abc-xxxx-dex

Where "abc" describes basic Model Type
"abc" = A10, A15
B34, B74,
C34, C74,
H13, H15, H31, H32, H51, H52
N15, N32, N52

dex describes switch type

For Non Hermetically Sealed (Non-HS) switches:

"d" describes Switch Type:
"d" = A, B, C, D E, F, M, U, V, W, X, 2 and 3

And "e" describes Switch Mechanisms:
"e" = D, N, W, B, F, X, I, S for DPDT Switches

Or d & e = LA, LD, LK, LN, LB, LE, LL, LO, SA, SD,
SK, SN, SB, SE, SL, SO

For Hermetically Sealed (HS) switches:

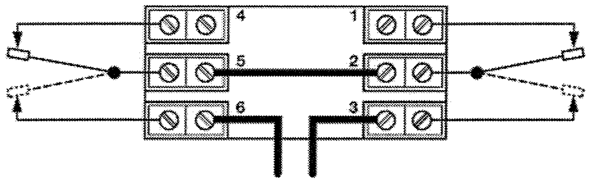
dex = HSD, HSE, HSF, HSQ, HSR, HSS, HST,
HSW, HSX, HSY, HSZ, HS5, HS6, HS7,
HS8
HME, HMF, HMR, HMS, HMT, HMX, HMY,
HMZ, HM6, HM7, HM8
HET, HEW
HWV, HWZ, HWW
HB9

2. Wiring Requirements

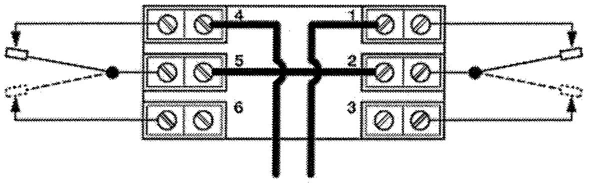
All Displacer Level Switches within the scope of this report must be specified with a DPDT switch mechanism. The DPDT switch mechanism must be wired in one of the following redundant methods

Figure 1. Non HS Switches

DPDT Switches Wired in Series to Open on Alarm

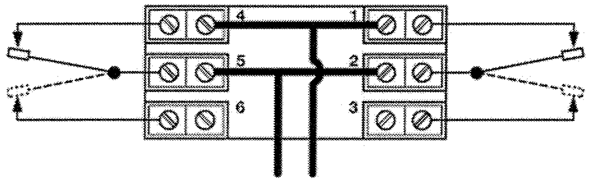


Low Alarm

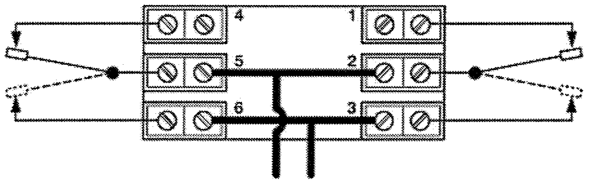


High Alarm

DPDT Switches Wired in Parallel to Close on Alarm



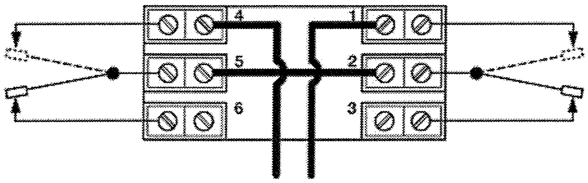
Low Alarm



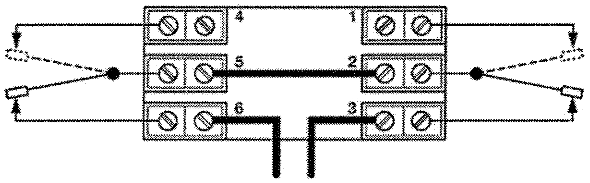
High Alarm

Figure 2. HS Switches

DPDT Switches Wired in Series to Open on Alarm

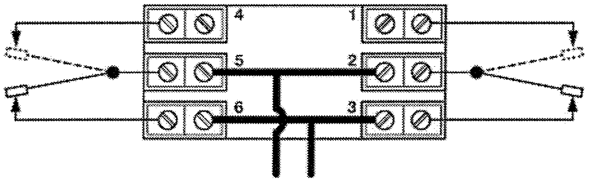


Low Alarm

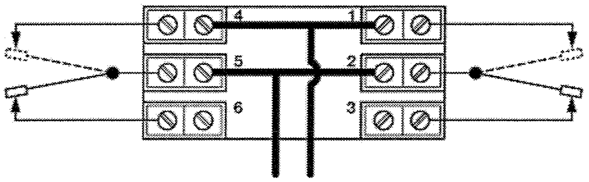


High Alarm

DPDT Switches Wired in Parallel to Close on Alarm



Low Alarm



High Alarm

An alternative method is to wire the two sets of DPDT contacts independently to the Logic Solver. The Logic Solver can then arbitrate between the information on the two sets of contacts. If both sets agree, the measurement is as indicated. If they disagree, then there is a fault in the device. The user can decide the appropriate logic required for the particular application.

3. Management Summary

This report summarizes the results of the Failure Modes, Effects and Diagnostic Analysis (FMEDA) of the Magnetrol Displacer Level Switch unit series in low and high level applications. The FMEDA was performed to determine failure rates, and the Safe Failure Fraction (SFF), which can be used to achieve functional safety certification per IEC 61508 of a device.

The Magnetrol Displacer Level Switch unit series are devices classified as Type A according to IEC 61508, having a hardware fault tolerance of 0. The FMEDA analysis assumes the device is installed as either a Low or High Level Alarm application when considering the state of the device for the various failure mechanisms. The units are available with DPDT switches only. The switches must be wired by one of the methods shown in the Wiring Requirements section. The DPDT switch is wired with both sets of contacts wired redundantly. Using these assumptions, the analysis shows that these devices have a safe failure fraction between 60 and 90% and therefore may be used up to SIL 2 as a single device.

The failure rate for the Displacer Level Switch Units with a DPDT switch wired redundantly is:

$\lambda^{DU} = 40 * 10^{-9}$ failures per hour for Low Level application
$\lambda^{DU} = 28 * 10^{-9}$ failures per hour for High Level application

Table 1: Failure rates according to IEC 61508 for the Magnetrol Displacer Level Switch Mechanical Unit series

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	**SFF**
Low Trip	0 FIT	15 FIT	71 FIT	40 FIT	68.2%
High Trip	0 FIT	0 FIT	98 FIT	28 FIT	77.7%

These failure rates can be used in a probabilistic model of a Safety Instrument Function (SIF) to determine suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL). A more complete listing of failure rates is provided in Table 2.

B. Failure Modes, Effects, and Diagnostic Analysis

1. Standards

This evaluation is based on the following:

IEC 61508:2000 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems

SILVER (FMEDA Tool V4R0.6a), a failure rate database developed by exida.com. The rates have been chosen in a way that is appropriate for safety integrity level verification calculations. Actual field failure results with average environmental stress are expected to be superior to the results predicted by these numbers. The user of this information is responsible for determining the applicability to a particular environment.

2. Definitions

FMEDA
A Failure Modes Effect and Diagnostic Analysis is a technique which combines online diagnostic techniques and the failure modes relevant to safety instrumented system design with traditional FMEA techniques which identify and evaluate the effects of isolated component failure modes.

Safe Failure
A failure that causes the device or system to go to the defined fail-safe state without a demand from the process. Safe failures are either detected or undetected.

Dangerous Failure
A failure that does not respond to a demand from the process (i.e. is unable to go to the defined fail-safe state). Dangerous Failures are either detected or undetected.

Hardware Fault Tolerance
The ability of a component / subsystem to continue to be able to undertake the required SIF in the presence of one or more dangerous faults in hardware.

FITs
Failures in time. 1 FIT = 1 x 10^{-9} failures per hour.

PFD_{AVG}(1yr)
Average Probability of Failure on Demand for a one year proof test interval. Probability the unit will fail in the period of one year between functional checks of the unit. The percentage of the range indicates how much of the total allowed PFD range for a particular SIL level for the SIF is consumed by the device.

3. Assumptions

- The failure categories listed are only safe and dangerous, both detected and undetected.
- Failure of one part will fail the entire unit.
- Failure rates are constant; normal wear and tear is not included.
- Increase in failures is not relevant.
- Failure rates are based on actual field information and field failures. Only field failures are considered.
- The average temperature over a long period of time is 40°C.
- The stress levels are typical for an industrial environment and can be compared to the Ground Benign classification of MIL-HNBK-217F.
- This report only applies to the models and switch mechanisms listed in the Model Designations section of this report.
- The unit is installed as either a Low or High Level Alarm.
- The unit must be wired according to the Wiring Requirements section of this report.
- The unit must be installed in accordance with the proper installation requirements as stated in the manufacturer's I & O manual.

4. Failure Rates

Table 2: Displacer Switch Mechanical Unit Failure Rates

Failure Category	Failure Rate (in Fits)		Failure Rate (in Fits)	
	Low Level		High Level	
Fail Dangerous Detected	71		98	
Fail High (detected by the logic solver)	0		98	
Fail Low (detected by the logic solver)	71		0	
Fail Dangerous Undetected	40		28	
No Effect	15		0	

5. Safe Failure Fraction

Table 3: Displacer Switch Mechanical Unit Safe Failure Fraction

Application	SFF
Low Level	68.2 %
High Level	77.7 %

For Displacer Switches, because the SFF is between 60 and 90%, and the switch is a Type A device, it is suitable for SIL 2 with a hardware fault tolerance of 0.

6. PFD$_{AVG}$

Displacer Switch Mechanical units average Probability of Failure on Demand (PFD$_{AVG}$) for a one year Proof Test is:

For Low Level Application:

$$\mathbf{PFD_{AVG}\ (1yr)} = [(\lambda^{DU}/2) * 1\ yr_{(hours)}] + (\lambda^{DD} * 8\ hours)$$

$$= [40*10^{-9}/2 * 8760\ hr] + (71*10^{-9} * 8)$$

$$= 1.76*10^{-4}$$

PFD$_{AVG}$ (1yr) = <u>0.000176</u>

This PFD$_{AVG}$ value is less than 0.01 and suitable for a Type A SIL 2 application.

SIL range (max) 0.01

PFD$_{AVG}$ (1yr) % of SIL Range 1.76%

For High Level Application:

$$\mathbf{PFD_{AVG}\,(1yr)} = [(\lambda^{DU}/2) * 1\ yr_{(hours)}] + (\lambda^{DD} * 8\ hours)$$

$$= [28*10^{-9}/2 * 8760\ hr] + (98*10^{-9} * 8\ hours)$$

$$= 1.23*10^{-4}$$

PFD_{AVG} (1yr) = 0.000123

This **PFD_{AVG}** value is less than 0.01 and suitable for Type A SIL 2 application.

SIL range (max) 0.01

PFD_{AVG} (1yr) % of SIL Range 1.23%

C. Lifetime of Critical Components

All components except electrolytic capacitors are generally accepted as having a useful lifetime of up to 50 years. There are no electrolytic capacitors used in displacer level switches.

Therefore, the useful lifetime of the product is at least 50 years.

D. Proof Test Procedure

A suggested proof test is described below in Table 4. This test will detect approximately 99% of the possible DU failures in Displacer Level Switches.

Table 4: Steps for Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Place a multimeter set to measure continuity across the common and either Normally Closed (NC) or Normally Open (NO) contacts
3	Change process level sufficiently to cause the switch mechanism to change state
4	Ensure via the multimeter that in-fact the switch mechanism did change state.
5	Check both normally open and normally closed contacts by repeating steps 2 through 4 for the other set of switch contacts.
6	Restore the installation to full operation.

E. Liability

The FMEDA analysis is based on *exida.com's SILVER* Tool. Magnetrol and *exida.com* accept no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

F. Release Signatures

	John J Benway
Paul Snider	John Benway
Senior Compliance Engineer	Manager Evaluation Engineering
July 6, 2006	July 6, 2006