



Failure Modes, Effects, and Diagnostic Analysis

Tuffy II Level Switch High and Low Level Applications

Table of Contents

A. DESCRIPTION	3
1. Model Designations	3
2. Wiring Requirements.....	4
3. Management Summary.....	5
B. FAILURE MODES, EFFECTS, AND DIAGNOSTIC ANALYSIS	6
1. Standards	6
2. Definitions	6
3. Assumptions.....	7
4. Failure Rates.....	7
5. Safe Failure Fraction.....	8
6. $(PFD)_{AVG}$	8
C. LIFETIME OF CRITICAL COMPONENTS.....	9
D. PROOF TEST PROCEDURE.....	9
E. LIABILITY.....	9
F. RELEASE SIGNATURES.....	9

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Tuffy II 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 Tuffy II Level Switch model numbers and DPDT switch mechanisms listed below.

Models: abc-xxxx-dex

Where "abc" describes basic Model Type

"abc" = T31, T32, T33, T34, T35

"xxxx" describes process connection size and type

"dex" describes Process connection material / design code, switch type and housing

"d" describes process connection material / design code:

"d" = A, B, C, D, E, F, G, H, J, K, L, M, N, P, R, T, 1 and 2

And "e" describes Switch Type:

"e" = 1 and 3 for Non-HS DPDT Switches

And "f" = describes Housing Material and Approval

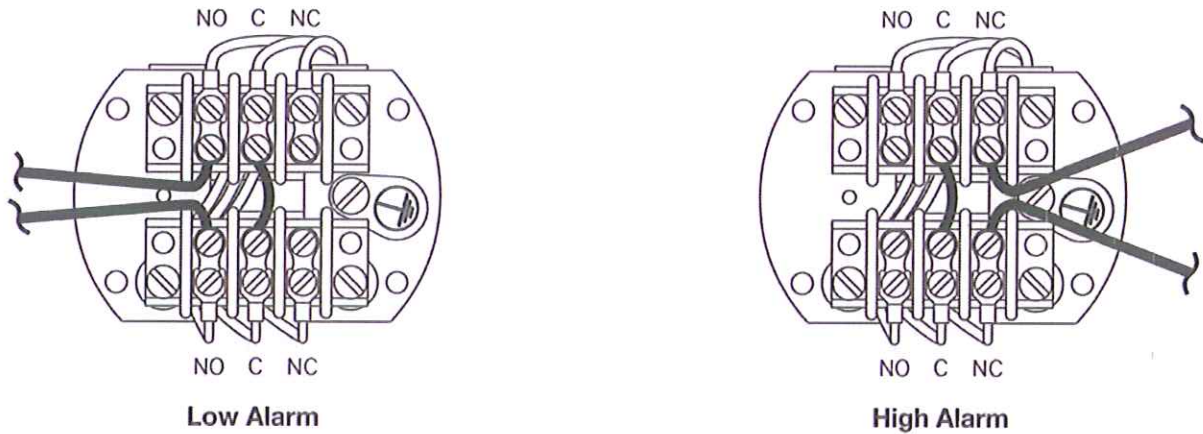
"f" = A, B, C, D, M, N, P, R, 1, 2, 3 or 4

2. Wiring Requirements

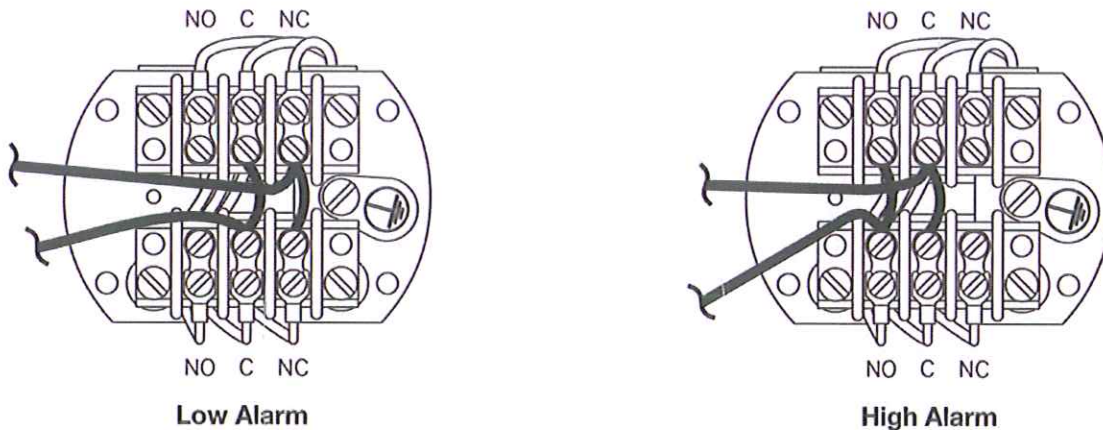
All Tuffy II Level Switches within the scope of this report must be specified with a DPDT switch mechanism. The DPDT switch mechanism must be wired in one of the following redundant methods.

Figure 1. DPDT Switches

DPDT Switches Wired in Series to Open on Alarm



DPDT Switches Wired in Parallel to Close on 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 Tuffy II 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 Tuffy II Level Switch is a device 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 Tuffy II Level Switch with a DPDT switch wired redundantly is:

$$\lambda_{DU} = 47 * 10^{-9} \text{ failures per hour} \quad \text{for Low Level application}$$

$$\lambda_{DU} = 65 * 10^{-9} \text{ failures per hour} \quad \text{for High Level application}$$

Table 1: Failure rates according to IEC 61508 for the Magnetrol Tuffy II Level Switch

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
Low Trip	0 FIT	136 FIT	0 FIT	47 FIT	74.3%
High Trip	0 FIT	118 FIT	0 FIT	65 FIT	64.4%

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 for 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

Failure rates are derived from *Exida's FMEDA Tool, V7.1.9*, failure rate database. 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. $1 \text{ FIT} = 1 \times 10^{-9}$ failures per hour.
$\text{PFD}_{\text{AVG}}(1\text{yr})$	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 unit must utilize a DPDT switch with contacts wired for redundant safety.
- The unit must be installed in a clean process condition to ensure the mechanism and float do not become fouled by the process material.
- 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.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment and can be compared to the IEC 60654-1 Class Dx (outdoor location) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- 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: Tuffy II Switch Failure Rates

Failure Category	Failure Rate (in Fits)	
	Low Level	High Level
Fail Dangerous Detected λ_{dd}	0	0
Fail Dangerous Undetected λ_{du}	47	65
Fail Safe Detected λ_{sd}	0	0
Fail Safe Undetected λ_{su}	136	118

5. Safe Failure Fraction

Table 3: Tuffy II Level Switch Safe Failure Fraction

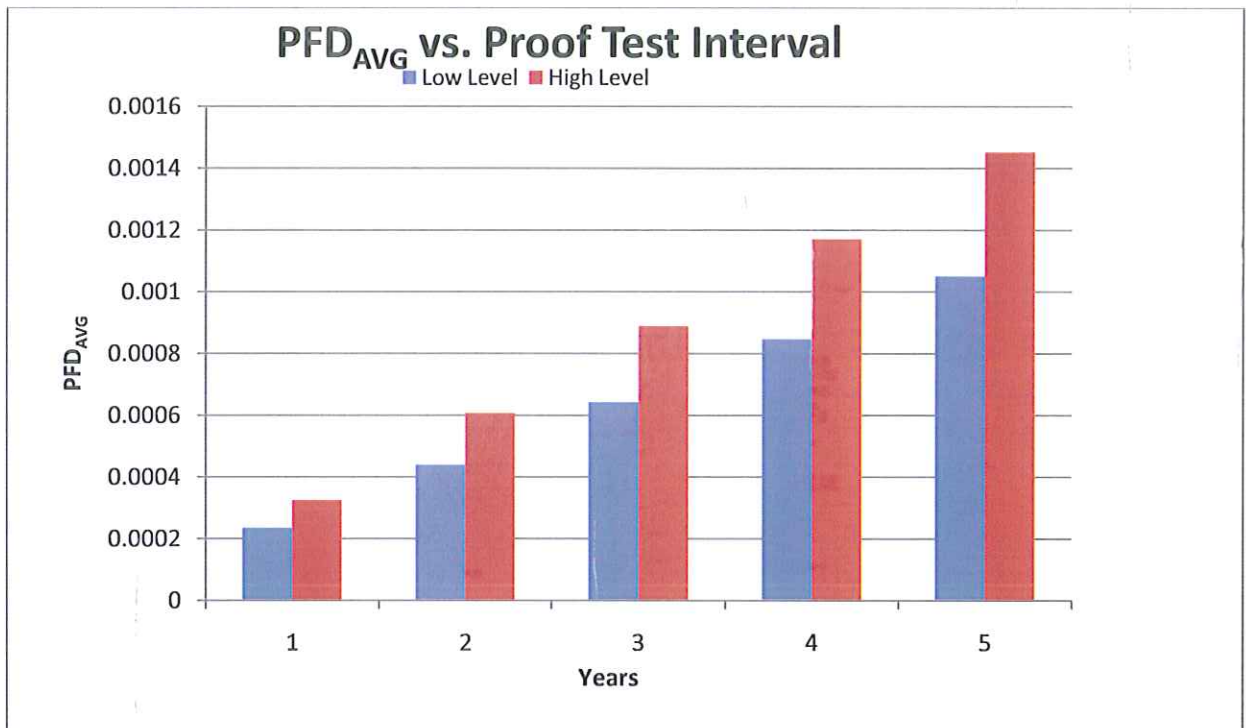
Application	SFF
Low Level	74.3 %
High Level	64.4 %

For Tuffy II Level 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}

The Tuffy II Level Switch average Probability of Failure on Demand (PFD_{AVG}) for a Proof Test Interval ranging from 1 to 5 years is given in Table 4 below. These calculations are based on a Proof Test Coverage of 99% as stated in Table 5.

Table 4: PFD_{AVG} for Proof Test Intervals of 1 to 5 years



The PFD_{AVG} for both Low Level and High Level applications with a 1 year Proof Test Interval is as follows

Low Level .000235 High Level .000325

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

SIL range max = 0.01

Low level PFD_{AVG} (1yr) % of SIL Range = 2.35%

High level PFD_{AVG} (1yr) % of SIL Range = 3.25%

C. Lifetime of Critical Components

There are no aluminum or tantalum electrolytic capacitors used: there are no electrical components that limit the useful lifetime of the system. Based on general field failure data, a useful life period of approximately 15 years is expected for the Tuffy II Level Switch.

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 Tuffy II Level Switches.


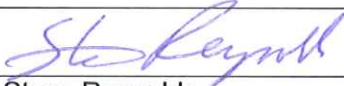
Table 5: Steps for Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Use a multi-meter to confirm the operation of the switch mechanism. Confirm switch contacts are closed or open and that wires are not shorted to adjacent contacts.
3	Inspect exterior and interior of the housing for signs of environmental integrity. Assure all mechanisms are in an operating condition. All fasteners must be tight. The hardware, brackets, springs, pivot pin, and switch mechanism must be free from signs of damage. Manually trip the switch mechanism by moving the switch magnet. Assure free movement of the assembly with no binding and that the spring return operates properly. Using the multi-meter as described in Step 2 above, ensure the switch contacts change states as the mechanism is moved manually. Return the mechanism to starting position.
4	Move the process level sufficiently to cause the switch mechanism to change states. Ensure the switch mechanism moves in response to the process movement. Ensure the contacts change states using a multi-meter as described in part 2 above.
5	Restore the installation to full operation
	Steps 1 – 3 provide 73% coverage of the D.U. FITS. Steps 1–4 provide 99% coverage of the D.U. FITS.

E. Liability

The FMEDA analysis is based on *exida's* FMEDA Tool. Magnetrol and *exida* 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

	
Paul Snider	Steve Reynolds
Senior Compliance Engineer	Manager Evaluation Engineering
January 28, 2011	January 28, 2011