Magnetrol®

Failure Modes, Effects, and Diagnostic Analysis

Magnetrol Model TDx
Thermal Dispersion Switch

Table of Contents

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Model TDx Series Thermal Dispersion Switch. The FMEDA performed on the Model TDx Series includes all electronics and related hardware. For full certification purposes the Model TDx software along with all requirements of IEC61508 must be considered.

B. Management Summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Model TDx Series Thermal Dispersion Switch. The FMEDA was performed to determine failure rates, and the Safe Failure Fraction (SFF), which can be used to achieve functional safety certification per IEC61508 of a device.

Version overview:

Model TD1	24 Vdc Thermal Dispersion Switch; DPDT Relay
Model TD2	24 Vdc, 120 – 240 VAC Thermal Dispersion Switch; DPDT Relay; 4-20 mA output

The Model TDx Series is a **Complex Device** classified as **Type B** according to IEC61508, having a hardware fault tolerance of 0. The Model TDx Series Thermal Dispersion Switch is a 24 Vdc or 120 Vac to 240 Vac power device that provides relay and 4-20 mA outputs. The 4-20 mA output supplies a general measure of the flow rate and is not intended to be a control output to a safety instrumented function. The current output is not modified by internal diagnostics. For this FMEDA the 4-20 mA function of the Model TDx was not considered part of the safety instrumented function.

The Model TD1and TD2 failure rates are shown in Table 1.

The Model TDx has only one output failure state. That is its Fail-Safe State. The Fail-Safe State of the Model TDx has the relay de-energized. The relay contact positions with the relay de-energized is the Fail-Safe output of the TDx.

Table 1: Model TDx IEC 61508 Format Failure Rates

Failure Category	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
TD1	0	65	252	140	69.3%
TD2	0	46	390	161	73.0 %

Both Dangerous Detected failures and process alarms cause the relay to de-energize. Therefore, they both look the same to the logic solver.

These failure rates can be used 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 more complete listing of failure rates is provided in Table 2.

C. 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 used in Silver 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.
Fail-Safe State	The Fail–Safe state is equivalent to the condition of the output of the device if it lost power. For relay outputs this is the de-energized state of the relay contacts.
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. Relay is de-energized.
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.
No Effect	Faults that have no impact on the safety function of the device.
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.
- The Fail-Safe State of the TDx is the relay contact position with the relay de-energized.
- 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.
- Components that cannot have an affect on the safety function are not considered in the analysis.
- 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 Fixed classification of MIL-HNBK-217F.
- The failure rates of the device supplying power to Magnetrol's device are not included.

4. Failure Rates

Note: For TD2 units. Fail detected (internal diagnostic) and Fail Fail-Safe (inherently) failures cause the relay to de-energize. Therefore, both these types of failures look the same to the logic solver when just monitoring the relay contacts. Fail detected (inherent diagnostic) failures can be determined by monitoring both the relay and the 4-20 mA output. A fault indication in the 4-20 mA loop circuit is >22mA or <3.6mA.

Table 2a: Model TD1 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Fail–Safe (detected by logic solver)		252
Fail Detected (internal diagnostic)	72	
Fail Fail–Safe (inherently)	180	
Fail Dangerous Undetected		140
No Effect		65

Table 2b: Model TD2 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Fail–Safe (detected by logic solver)		390
Fail Detected (internal diagnostic)	72	
Fail Fail–Safe (inherently)	318	
Fail Dangerous Undetected		161
No Effect		46

5. Safe Failure Fraction

Table 3: Model TDx Safe Failure Fraction

Model	SFF
TD1	69.3%
TD2	73.0%

Because the SFF is greater than 60%, and the TD1 and TD2 are Type B devices, they are suitable for SIL 1 with a Hardware Fault Tolerance of 0.

6. PFD_{AVG}

Model TD1

The Model TD1 is a 1oo1 (one out of one) level switch. The average Probability of Failure on Demand (PFD_{AVG}) for a one year Proof Test Interval is:

PFD_{AVG}(1yr) = $(\lambda^{DU}/2)* 1\text{ yr} = 1.40*10^{-7}/2 * 8760\text{ hr} = 6.13*10^{-4}$

This PFD_{AVG} value is less than 10^{-1} and suitable for Type B SIL 1 application.

SIL range (max) 0.1

PFD_{AVG} (1yr) % of SIL Range 0.61%

Model TD2

The Model TD2 is a 1oo1 (one out of one) level switch. The average Probability of Failure on Demand (PFD_{AVG}) for a one year Proof Test Interval is:

PFD_{AVG}(1yr) = $(\lambda^{DU}/2)* 1\text{ yr} = 1.61*10^{-7}/2 * 8760\text{ hr} = 7.05*10^{-4}$

This PFD_{AVG} value is less than 10^{-1} and suitable for Type B SIL 1 application.

SIL range (max) 0.1

PFD_{AVG}(1yr) % of SIL Range 0.71%

D. 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.

E. Life time of critical components:

All components except electrolytic capacitors are generally accepted as having a useful lifetime of up to 50 years. An electrolytic capacitor used in the TDx circuitry can be considered to have a useful lifetime based on the following:

$$L_{actual} = L_{max} * 2^{(Tmax - Tcap)/10}$$

Where:

L_{actual} = lifetime (hours) at actual operating temperature

L_{max} = lifetime (hours) at max operating temperature (10,000 hours)

T_{max} = max operating temperature (105° C)

T_{cap} = Capacitor temperature at 40° $C_{ambient}$ (66.6° C)

$$L_{actual} = 10000 * 2^{(105 - 66.6)/10}$$

$$L_{actual} = 16.3 \text{ years}$$

The useful lifetime of the product is at least 15 years.

F. Release Signatures

Name: Paul Snider	*Name* John S. Benway
Title: Sr. Compliance Engineer	*Title:* Evaluation Engineering Manager
Date: February 13, 2006	*Date:* February 13, 2006