MAGNETROL®

AMETEK®
SENSORS, TEST & CALIBRATION

Failure Modes, Effects, and Diagnostic Analysis

AMETEK Magnetrol Model TDx
Thermal Dispersion Switch

Revision History

Rev	Date	Author	Changes Made
1.3	2006-02-13	Paul Snider	Initial Release
2.0	2022-02-18	Kevin Haynes	Revised to 2010 version of IEC 61508 standard and using exida's current FMEDA tool (FMEDAx version 2.1.9.40711)

Table of Contents

Revision History

Rev	Date	Author	Changes Made
1.3	2006-02-13	Paul Snider	Initial Release
2.0	2022-02-18	Kevin Haynes	Revised to 2010 version of IEC 61508 standard and using exida's current FMEDA tool (FMEDAx version 2.1.9.40711)

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the AMETEK Magnetrol Model TDx Series Thermal Dispersion Switch. The FMEDA performed on the Model TDx Series includes all electronics and related hardware. From this, failure rates and example PFD_{avg} values may be calculated.

B. Management Summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the AMETEK 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 SAFE 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	157	358	161	171	79.8%
TD2	116	286	138	221	71.0 %

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 ed 2: 2010	Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems

FMEDAx (Version: 2.1.0.40711 Copyright © 2017-2020, *exida*), a failure rate database developed by *exida* LLC

The rates used in FMEDAx 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}	Average Probability of Failure on Demand

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 AMETEK Magnetrol's device are not included.
- The device is installed per the manufacturer's instructions.

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)		676
Fail Detected (internal diagnostic)	318	
Fail Fail–Safe (inherently)	358	
Fail Dangerous Undetected		171
No Effect		278

Table 2b: Model TD2 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Fail–Safe (detected by logic solver)		540
Fail Detected (internal diagnostic)	254	
Fail Fail–Safe (inherently)	286	
Fail Dangerous Undetected		221
No Effect		325

5. Safe Failure Fraction

Table 3: Model TDx Safe Failure Fraction

Model	SFF
TD1	79.8%
TD2	71.0%

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}

Using the failure rates in section 4, and the failure rate data for associated system devices, the PFD_{avg} (Probability of Failure on Demand) can be calculated for the system. The Probability of Failure on Demand calculation includes many parameters that are determined by the particular application and site. Thus, these calculations are the responsibility of the owner/operator of the process.

D. Liability

The FMEDA analysis is based on the FMEDAx Tool from *exida*. AMETEK 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.

E. Lifetime of critical components:

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the exida FMEDA prediction method, this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem and its operating conditions.

Table 4 shows the estimated useful lifetime of components contributing to the dangerous undetected failure rate.

Table 4: Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) – aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the TD1/TD2 per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

The limiting factor with regard to the useful lifetime of the system is the aluminum electrolytic capacitors. Therefore, the useful lifetime is predicted to be 10 years.

For high demand mode applications, the useful lifetime of the relays is limited by the number of cycles. The useful lifetime of the relays is > 100,000 full scale cycles or 8 to 10 years, whichever results in the shortest lifetime.

When plant/site experience indicates a shorter useful lifetime than indicated here, the number based on plant/site experience should be used.

F. Release Signatures

Name: Kevin Haynes
Title: Sr. Electrical Project Engineer
Date: February 18, 2022
2022/02/18

Name Karolina Grib
Title: New Product Development Mgr.
Date: February 18, 2022