Failure Modes, Effects, and Diagnostic Analysis

Magnetrol Thermatel®
Enhanced Model TA2
Software v2.x
Thermal Dispersion Mass Flow Transmitter
Table of Contents

A. DESCRIPTION........................................................................................................... 3
   1. Model Designations.............................................................................................. 3
   2. Management Summary....................................................................................... 3

B. FAILURE MODES, EFFECTS, AND DIAGNOSTIC ANALYSIS.............................. 4
   1. Standards.............................................................................................................. 4
   2. Definitions............................................................................................................ 4
   3. Assumptions......................................................................................................... 5
   4. Failure Rates....................................................................................................... 6
   5. Safe Failure Fraction............................................................................................ 6
   6. PFD_{AVG}........................................................................................................... 6

C. LIFETIME OF CRITICAL COMPONENTS.............................................................. 7

D. PROOF TEST PROCEDURE................................................................................... 7

E. LIABILITY................................................................................................................. 8

F. RELEASE SIGNATURES.......................................................................................... 8
A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Thermatel® Enhanced Model TA2 Thermal Dispersion Mass Flow Transmitter, Software v2.x (hereafter called "Enhanced Model TA2"). The FMEDA performed on the Enhanced Model TA2 includes all electronics and related hardware.

Flow measurement products employing thermal dispersion technology are subject to a large variety of process conditions and installation configurations that can have a dramatic impact on the ability to measure flow reliably. Not all of these conditions can be controlled or mitigated. It is recommended that these FMEDA numbers be used as a measure of the quality of the design of the product. The installation and application requirements of the end user application for a thermal dispersion device must be thoroughly examined before any consideration is made of using thermal dispersion devices in a safety system. For full certification purposes the software along with all requirements of IEC61508 must be considered.

1. Model Designations

The FMEDA analysis in this report is only applicable for the following Enhanced Model TA2 model numbers.

Models: TA2-Axxx-yyyy, where: xxx describes the electronic options of the unit, and yyy describes the agency approvals and materials of the enclosure and transducer.

2. Management Summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Enhanced Model TA2. 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.

The Enhanced Model TA2 is a Complex Device classified as Type B according to IEC61508, having a hardware fault tolerance of 0. This AC / DC Line powered unit contains self-diagnostics programmed to output either 3.6 mA or 22 mA during a failure state. The FMEDA analysis assumes the diagnostic signal is being transmitted to a logic solver programmed to detect over-scale and under-scale currents.

Failure rates of the Enhanced Model TA2 are:

<table>
<thead>
<tr>
<th>Fail High</th>
<th>13 x 10^{-9} failures per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Low</td>
<td>419 x 10^{-9} failures per hour</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>217 x 10^{-9} failures per hour</td>
</tr>
</tbody>
</table>

Table 1: Enhanced Model TA2 IEC 61508 Format Failure Rates

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}$</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>SFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>783 FIT</td>
<td>855 FIT</td>
<td>217 FIT</td>
<td>88.3%</td>
<td></td>
</tr>
</tbody>
</table>
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.

B. Failure Modes, Effects, and Diagnostic Analysis

1. Standards

This evaluation is based on the following:


Failure rates are derived from Exida's FMEDA Tool V7.1.13, 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.

Diagnostic Coverage  Failure rate found through internal automatic diagnostic testing. The percentage of failures compared to the total failure rate in any mode. Options are set to locate failures that cause the unit to go to 3.6 mA or 22 mA for the current output. The upscale or downscale setting is user selectable.

Fail Safe  A non-process failure that forces the output to a fail-safe state. The fail-safe state for a 4-20 mA loop is typically a loop value below 3.6 mA.

Fail Dangerous  A failure that makes either the measured input value or the calculated output value change by more than 2% (of span), but the output still stays within the valid output range.

Fail Dangerous Detected  Dangerous failures that are detected by the device typically by internal diagnostics. These failures can be detected by the logic solver.
Fail Dangerous Undetected: Dangerous failures that are not detected by the device and, therefore, are not detected by the logic solver.

Fail Low: The fault indication is active (current output < 3.8 mA).

Fail High: The fault indication is active (current output > 20.5 mA).

No Effect: Faults that have no impact on the safety function of the device.

FIT: 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 to respond to a demand 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. Fail high and fail low can be classified as safe detected by a logic solver. The No Effect category represents component failure modes that have no effect on the safety function (classified as fail safe according to IEC 61508 but will not cause a false trip). These failures are used in the Safe Failure Fraction calculation.

- 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 effect on the safety function are not considered in the analysis.

- The logic solver programming is such that Fail High (>20.5 mA) and Fail Low (< 3.8 mA) failures are detected regardless of the effect (good or bad) on the safety function.

- 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-HDBK-217F.

- The failure rates of the device supplying power to Magnelrol's device are not included.
4. Failure Rates

**Table 2: Enhanced Model TA2 Failure Rates**

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>Failure rate (FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Undetected</td>
<td>2</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>855</td>
</tr>
<tr>
<td>Fail Detected (detected by internal diagnostics)</td>
<td>423</td>
</tr>
<tr>
<td>Fail High (detected by logic solver)</td>
<td>13</td>
</tr>
<tr>
<td>Fail Low (detected by logic solver)</td>
<td>419</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>217</td>
</tr>
<tr>
<td>Residual Effect</td>
<td>774</td>
</tr>
<tr>
<td>Annunciation Undetected</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 2 assumes that a detected failure will force the output to the selected upscale or downscale fail-safe state.

5. Safe Failure Fraction

**Table 3: Enhanced Model TA2 Safe Failure Fraction**

<table>
<thead>
<tr>
<th>Model</th>
<th>SFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced TA2</td>
<td>88.3%</td>
</tr>
</tbody>
</table>

Because the SFF is greater than 60%, and the Model Enhanced TA2 is a Type B device, it is suitable for SIL 1.

6. PFD_{AVG}

The Enhanced Model TA2 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 Section D.
Table 4: PFD\textsubscript{AVG} for Proof Test Intervals of 1 to 5 years

The PFD\textsubscript{AVG} for both Low Flow and High Flow applications with a 1 year Proof Test Interval is 0.00105

This PFD\textsubscript{AVG} value is less than 0.01 and suitable for a Type B SIL 2 application.

\[
PFD\textsubscript{AVG} (1\text{yr}) = 0.00105 \\
\text{SIL range max} = 0.01 \\
\text{SIL range min} = 0.001 \\
PFD\textsubscript{AVG} (1\text{yr}) \% \text{ of SIL Range} = 0.56\%
\]

C.  Lifetime of Critical Components

Liquid electrolytic capacitors are used in the Enhanced Model TA2. Based on general field failure data, a useful life period of approximately 10 years is expected for the Enhanced Model TA2.

D.  Proof Test Procedure

The suggested proof test is described below in Table 5 consists of both a full process range excursion and an analog output test. This test will detect approximately 99% of the possible DU failures in the Enhanced Model TA2 Transmitters.
Table 5: Steps for Proof Test

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bypass the 4-20mA loop safety function and take appropriate action to avoid a false trip.</td>
</tr>
<tr>
<td>2</td>
<td>Use HART communication or the local user interface to retrieve any diagnostics and take appropriate action to resolve faults or warnings.</td>
</tr>
<tr>
<td>3</td>
<td>Use HART communication or the local user interface “A01 Loop Test” utility (under “Diagnostics”) to command the transmitter to go to the high alarm current output and verify that the analog current reaches that value.</td>
</tr>
<tr>
<td>4</td>
<td>Use HART communication or the local user interface “A01 Loop Test” utility (under “Diagnostics”) to command the transmitter to go to the low alarm current output and verify that the analog current reaches that value.</td>
</tr>
<tr>
<td>5</td>
<td>By varying process flow, perform a calibration check at three points over the full operating range of process flow.</td>
</tr>
<tr>
<td>6</td>
<td>Remove the bypass and restore the unit to normal operation.</td>
</tr>
</tbody>
</table>

Step 3 tests for the unit’s maximum loop output current drive capability or for excessive wiring resistance in the loop. This also tests for other possible failures.

Step 4 tests for the unit’s minimum loop output current drive capability.

If step 5 is performed by using other than the actual process application, the proof test may not detect failures related to the operating conditions.

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Steve Reynolds</td>
<td>John Benway</td>
</tr>
<tr>
<td>Evaluation Engineering Manager</td>
<td>New Product Development Engineering Manager</td>
</tr>
<tr>
<td>July 25, 2011</td>
<td>July 25, 2011</td>
</tr>
</tbody>
</table>