



Failure Modes, Effects, and Diagnostic Analysis

Magnetrol Echotel Model 355 Non-Contact Ultrasonic 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. $(\text{PFD})_{\text{AVG}}$	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 Model 355 Non-Contact Ultrasonic Transmitter. The FMEDA performed on the Model 355 includes all electronics and related hardware.

Level products employing through air technology are subject to a large variety of process conditions and tank configurations that can have a dramatic impact on the ability to measure the level reliably from empty to full. 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 through air level device must be thoroughly examined before any consideration is made of using through air level 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 Model 355 Ultrasonic Transmitter model numbers.

Models: 355-xxxx-yyy Where: xxxx 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 Magnetrol Model 355 Non-Contact Ultrasonic Transmitter. 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 Model 355 is a **Complex Device** classified as **Type B** according to IEC61508, having a hardware fault tolerance of 0. This 24 VDC loop 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 Model 355 are:

$\lambda_H =$	$24 \cdot 10^{-9}$ failures per hour
$\lambda_L =$	$43 \cdot 10^{-9}$ failures per hour
$\lambda_{DU} =$	$59 \cdot 10^{-9}$ failures per hour

Table 1: Model 355 IEC 61508 Format Failure Rates

Failure Category	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
	0	86 FIT	367 FIT	59 FIT	88.5%

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:

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.
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.
FITs	Failures in time. 1 FIT = 1×10^{-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-HNBK-217F.
- The failure rates of the device supplying power to Magnetrol's device are not included.
- The installation, mounting configuration, and operation of the unit are per the Installation and Operating Manual 51-661. See the recommendations of Section 2.3 in regards to mounting location.
- The measurement range must be within the guidelines of Installation and Operating Manual 51-661 Section 3.2 which addresses application conditions.

- The product must be operated within the specification limits in the Installation and Operating Manual 51-661 Section 3.6.
- These calculations assume the assembly and testing of the product assure no production defects.

4. Failure Rates

Table 2: Model 355 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Safe Undetected		22
Fail Dangerous Detected		369
Fail Detected (detected by internal diagnostics)	302	
Fail High (detected by logic solver)	24	
Fail Low (detected by logic solver)	43	
Fail Dangerous Undetected		59
Residual Effect		59
Annunciation Undetected		6

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: Model 355 Safe Failure Fraction

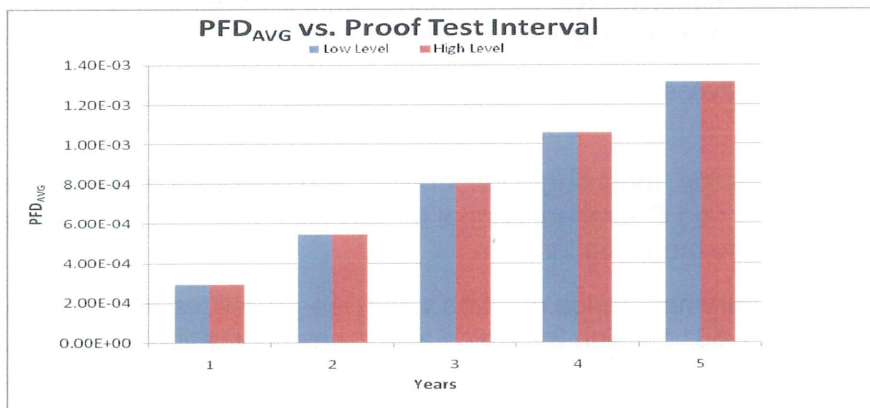
Model	SFF
355	88.5%

Because the SFF is greater than 60%, and the Model 355 is a Type B device, it is suitable for SIL 1.

6. PFD_{AVG}

The Model 355 Ultrasonic Transmitter 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 0.000290.

This PFD_{AVG} value is less than 0.1 and suitable for a Type B SIL 1 application.

SIL range max = 0.1

PFD_{AVG} (1yr) % of SIL Range 0.29%

C.

D. Lifetime of Critical Components

There are tantalum electrolytic capacitors used in the Model 355. Based on general field failure data, a useful life period of approximately 15 years is expected for the 355 Ultrasonic Transmitter.

E. 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 Model 355 Ultrasonic Transmitters.

Table 5: Steps for Proof Test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Use HART communication or the local user interface to retrieve any diagnostics and take appropriate action.
3	Use the HART communication or the local user interface "Diagnostics" -- "Test 4-20 Loop" function to command the transmitter to go to the high alarm current output and verify that the analog current reaches that value.
4	Use the HART communication or the local user interface "Diagnostics" -- "Test 4-20 Loop" function to command the transmitter to go to the low alarm current output and verify that the analog current reaches that value.
5	Perform a calibration check at three points over the full working range of the actual process fluids.
6	Remove the bypass and otherwise restore normal operation.

Step 3 tests for compliance voltage problems such as low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.


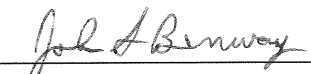
Step 4 tests for possible quiescent current related failures.

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.

F. 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.

G. Release Signatures

	
Paul Snider	John Benway
Senior Compliance Engineer	Evaluation Engineering Manager
October 12, 2010	October 12, 2010