



Failure Modes, Effects and Diagnostic Analysis

Magnetrol Model ESII Modulelevel
Electronic Level Transmitter

Table of Contents

Description	3
Management Summary	3
Failure Modes, Effects, and Diagnostic Analysis	4
Standards	4
Definitions	4
Assumptions	5
Failure Rates	5
Safe Failure Fraction	5
PFDave	6
Liability	6
Release Signatures	6

Description

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

Management Summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Model ESII Modulelevel Electronic 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 ESII Modulelevel is a smart 4-20 mA 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.

The Model ESII failure rates are:

$\lambda^H =$	23*10 ⁻⁹ failures per hour
$\lambda^L =$	234*10 ⁻⁹ failures per hour
$\lambda^{DU} =$	204*10 ⁻⁹ failures per hour

Table 1: Model ESII IEC 61508 Format Failure Rates

Failure Category	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Low Trip	234 FIT	148 FIT	23 FIT	204 FIT	66.5%
High Trip	23 FIT	148 FIT	234 FIT	204 FIT	66.5%

The failure rates in Table 1 are valid for the useful lifetime of the product, which is at least 50 years.

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.

Failure Modes, Effects, and Diagnostic Analysis

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.

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 a current less than 4 mA for the current output.
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. These failures are categorized as safe detected or safe undetected failures.
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 < 4 mA).
Fail High	The fault indication is active (current output > 20 mA).
No Effect	Faults that have no impact on the safety function of the device.

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 affect on the safety function are not considered in the analysis.
- The logic solver programming is such that Fail High (>20 mA) and Fail Low (< 4 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.

Failure Rates

Table 2: Model ESII Failure Rates

Failure Category			Failure rate (in Fits)
Fail High (detected by logic solver)			23
Fail Low (detected by logic solver)			234
	Fail detected (int. diag.)	124	
	Fail low (inherently)	110	
Fail Dangerous Undetected			204
No effect			148

Table 2 assumes that a detected failure will force the output downscale (less than or equal to 3.6 mA) and that downscale is the fail-safe condition.

Safe Failure Fraction

Table 3: Model ESII Safe Failure Fraction

Model	SFF
ESII	66.5%

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

(PFD)_{ave}

The Model ESII is a 1oo1 (one out of one) level transmitter. The average Probability of Failure on Demand (PDF_{ave}) for a one year Proof Test Interval is:

$$\text{PFD(avg)(1yr)} = (\lambda^{\text{DU}} / 2) * 1 \text{ yr} = 2.04 * 10^{-7} / 2 * 8760 \text{ hr} = 8.94 * 10^{-4}$$

This PDF_{ave} value is less than 10⁻¹ and suitable for Type B SIL 1 application.

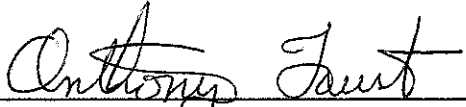
SIL range (max) 0.1

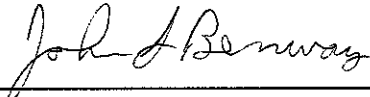
PFD(avg)(1yr) % of SIL Range 0.894%

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.

Release Signatures


Name: Anthony M. Faust
Title: Sr. Project Engineer
Date: August 25, 2004


Name: John S. Benway
Title: Evaluation Engineering Manager
Date: 25 August 2004