Magnetrol®

Failure Modes, Effects, and Diagnostic Analysis

Magnetrol Model 962 Loop Powered Ultrasonic Level Switch

Rev 1.1 *March 27, 2006*

Table of Contents

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Model 962 Ultrasonic Level Switch. The FMEDA performed on the Model 962 Ultrasonic Level Switch includes all electronics and related hardware. For full certification purposes the Model 962 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 962 Ultrasonic Level 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 962	24 Vdc Ultrasonic Level Switch

The Model 962 Ultrasonic Level Switch 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. Additionally, any output that exceeds the nominal values of 8mA and 16 mA by a tolerance of + / - 1.6 mA must be detected as a fault by the logic solver. 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 962 failure rates are shown in Table 1.

Table 1: Model 962 IEC 61508 Format Failure Rates

Failure Category	$\lambda^{(SD)}$	$\lambda^{(SU)}$	$\lambda^{(DD)}$	$\lambda^{(DU)}$	**SFF**
Model 962	0 FIT	110 FIT	362 FIT	42 FIT	91.8%

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.

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 mA or greater than 22 mA. Additionally, values greater than +/- 1.6 mA from the nominal 8 mA and 16 mA values are considered in the fail safe state. 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 10% (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.

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. Fail high and fail low can be classified as dangerous 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.

4. Failure Rates

Table 2: Model 962 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Dangerous Detected		362
Fail Detected (detected by internal diagnostics)	138	
Fail High (detected by the logic solver)	35	
Fail Low (detected by the logic solver)	189	
Fail Dangerous Undetected		42
No Effect		110
Annunciation Undetected		0

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

5. Safe Failure Fraction

Table 3: Model 962 Safe Failure Fraction

Model	SFF
962	91.8%

Because the SFF is greater than 90%, and the Model 962 is a Type B device, it is suitable for SIL 2.

6. PFD$_{AVG}$

The Model 962 is a 1oo1 (one out of one) level transmitter. The average Probability of Failure on Demand (PFD$_{AVG}$) for a one year Proof Test Interval is:

$$\textbf{PFD}_{\textbf{AVG}}\textbf{(1yr)} = [(\lambda^{DU}/2) * 1\ \text{yr}_{(\text{hours})}] + (\lambda^{DD} * 8\ \text{hours})$$
$$= [42*10^{-9}/2 * 8760] + (362*10^{-9} * 8) = 1.87*10^{-4}$$

This PFD$_{AVG}$ value is less than 10^{-2} and suitable for Type B SIL 2 application.

SIL range (max) 0.01

PFD$_{AVG}$(1yr) % of SIL Range 1.87%

D. Lifetime of Critical Components

All components except electrolytic capacitors are generally accepted as having a useful lifetime of up to 50 years. There are no electrolytic capacitors used on the Model 962

Therefore, the useful lifetime of the product is at least 50 years.

E. 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.

F. Release Signatures

Name: Paul Snider
Title: Sr. Compliance Engineer
Date: March 27, 2006

John S Benway

Name: John S. Benway
Title: Evaluation Engineering Manager
Date: March 27, 2006