



Failure Modes, Effects, and Diagnostic Analysis

**Magnetrol Model 962 AC / DC
Ultrasonic Level Switch**

Table of Contents

A. Description	3
B. Management Summary.....	3
C. Failure Modes, Effects, and Diagnostic Analysis	4
1. Standards	4
2. Definitions	4
3. Assumptions	5
4. Failure Rates	5
5. Safe Failure Fraction	5
6. PFD_{AVG}.....	6
D. Liability	6
E. Lifetime of Critical Components.....	6
F. Release Signatures	6

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; DPDT Relay
-----------	--------------------------------------------

The Model 962 Ultrasonic Level Switch is a **Complex Device** classified as **Type B** according to IEC61508, having a hardware fault tolerance of 0. The Model 962 Ultrasonic Level Switch is an 18 - 32 Vdc or 102 – 265 Vac power device that provides relay outputs.

The Model 962 failure rates are shown in Table 1

The Model 962 has only one output failure state. That is its Fail-Safe State. The Fail-Safe State of the Model 962 has the relay de-energized. The relay contact positions with the relay de-energized is the Fail-Safe output of the 962.

Table 1: Model 962 IEC 61508 Format Failure Rates

Failure Category	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
962	0 FIT	130 FIT	427 FIT	52 FIT	91.5%

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: 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.
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 = 1×10^{-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.
- The Fail-Safe State of the 962 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 Magnetrol’s device are not included.

4. Failure Rates

Note: 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.

Table 2: Model 962 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Fail-Safe (detected by logic solver)		427
Fail Detected (internal diagnostic)	146	
Fail Fail-Safe (inherently)	281	
Fail Dangerous Undetected		52
No Effect		130
Annunciation Undetected		0

5. Safe Failure Fraction

Table 3: Model 962 Safe Failure Fraction

Model	SFF
962	91.5%

Because the SFF is greater than 90%, and the 962 is a Type B device, it is suitable for SIL 2 with a Hardware Fault Tolerance of 0.

6. PFD_{AVG}

Model 962

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

$$\begin{aligned}
 \text{PFD}_{\text{AVG}}(1\text{yr}) &= [(\lambda^{\text{DU}} / 2) * 1 \text{ yr}_{(\text{hours})}] + (\lambda^{\text{DD}} * 8 \text{ hours}) \\
 &= [52 * 10^{-9} / 2 * 8760] + (427 * 10^{-9} * 8) = 2.31 * 10^{-4}
 \end{aligned}$$

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 2.3%

D. 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.

E. Life time of critical components:

All components except electrolytic capacitors are generally accepted as having a useful lifetime of up to 50 years. An electrolytic capacitor used in the 962 circuitry can be considered to have a useful lifetime based on the following:

$$L_{\text{actual}} = L_{\text{max}} * 2^{(T_{\text{max}} - T_{\text{cap}}) / 10}$$


Where:
 L_{actual} = lifetime (hours) at actual operating temperature
 L_{max} = lifetime (hours) at max operating temperature (10,000 hours)
 T_{max} = max operating temperature (105° C)
 T_{cap} = Capacitor temperature at 40° C_{ambient} (66.6° C)

$$L_{\text{actual}} = 10000 * 2^{(105 - 66.6) / 10}$$

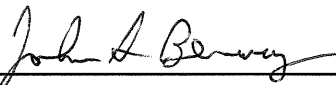
$$L_{\text{actual}} = 16.3 \text{ years}$$

The useful lifetime of the product is at least 15 years.

F. Release Signatures



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



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