Magnetrol®

Failure Modes, Effects, and Diagnostic Analysis

Magnetrol Model 910 AC / DC
Ultrasonic Level Switch

Rev 0

October 13 2010

Table of Contents

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Magnetrol Model 910 Ultrasonic Level Switch. The FMEDA performed on the Model 910 Ultrasonic Level Switch includes all electronics, probe and related hardware. For full certification purposes 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 910 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 910	**AC and DC Powered Ultrasonic Level Switch; DPDT Relay**

The Model 910 Ultrasonic Level Switch is a **non-Complex Device** classified as **Type A** according to IEC61508, having a hardware fault tolerance of 0. The Model 910 Ultrasonic Level Switch is a 24 V_{dc} , 120 V_{ac} or 220 V_{ac} power device that provides relay outputs. The scope of this report covers all three voltage power options.

The Model 910 failure rates are shown in Table 1

The Model 910 has only one safe output failure state. That is its Fail-Safe State. The Fail-Safe State of the Model 910 has the relay de-energized. The relay contact positions with the relay de-energized is the Fail-Safe output of the 910.

Table 1: Model 910 IEC 61508 Format Failure Rates

Failure Category	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Dry is Safe	0 FIT	194 FIT	0 FIT	65.1 FIT	74.8%
Wet is Safe	0 FIT	113 FIT	0 FIT	145 FIT	43.7%

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

Exida FMEDA Tool a failure rate database developed by *exida Consulting LLC*

The rates used 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.
Residual	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 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

- Relay contacts must be wired for redundant safety, so that failure of one set of relay contacts cannot cause a dangerous failure
- The process condition is assumed to be suitable for contact ultrasound so that the Model 910 is expected to operate normally in response to this process
- The failure categories listed are only safe and dangerous, both detected and undetected.
- The Fail-Safe State of the 910 is the relay contact position with the relay de-energized.
- Process leaks into the housing and/or housing leaks are not considered dangerous failures
- 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 of these types of failures look the same to the logic solver.

Table 2: Model 910 Failure Rates

Failure Category		Failure rate (in Fits) Dry is Safe		Failure rate (in Fits) Wet is Safe	
Fail Fail–Safe (detected by logic solver)		158		77.3	
Fail detected (internal diagnostic)		0		0	
Fail Fail–Safe (inherently)		158		77.3	
Fail Dangerous Undetected		65.1		145	
No effect		35.5		35.5	
Annunciation Undetected		0		0	

5. Safe Failure Fraction

Table 3: Model 910 Safe Failure Fraction

Failure Category	SFF
Dry is Safe	74.8%
Wet is Safe	43.8%

Because the SFF is between 60% and 90%, and the 910 is a Type A device, when wired in the Dry is Safe state, it is suitable for SIL 2 with a Hardware Fault Tolerance of 0.

Because the SFF is less than 60%, and the 910 is a Type A device, when wired in the Wet is Safe state, it is suitable for SIL 1 with a Hardware Fault Tolerance of 0.

6. PFD_{AVG}

Model 910

The Model 910 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:

PFDavg = [(Proof Test Efficiency) * (λ^{DU})*(1 yr *8760 hrs/yr) / 2] + [(1-.99) ([(λ^{DU}) (10 yrs * 8760 hrs/yr) / 2] + [(DD FITS * 24 hours)]

With a Proof Test Efficiency of 99% and Dry is Safe Application:

$PFD_{AVG}(1yr)$ = [(0.99*λ^{DU}* 8760_{hours}) / 2] + [(1-.99*λ^{DU} * 10 * 8760)/2] +[λ^{DD} * 24 hours]

= [(0.99 * 6.51e-8*8760) /2] +[(0.01*6.51e-8*10*8720)/2] +[0.0*24]

=3.11e-4

This PFD_{AVG} value is less than 10^{-2} and suitable for Type A SIL 2 application.

SIL range (max) 0.01
PFD_{AVG} (1yr) % of SIL Range 3.12%

With a Proof Test Efficiency of 99% and Wet is Safe Application:

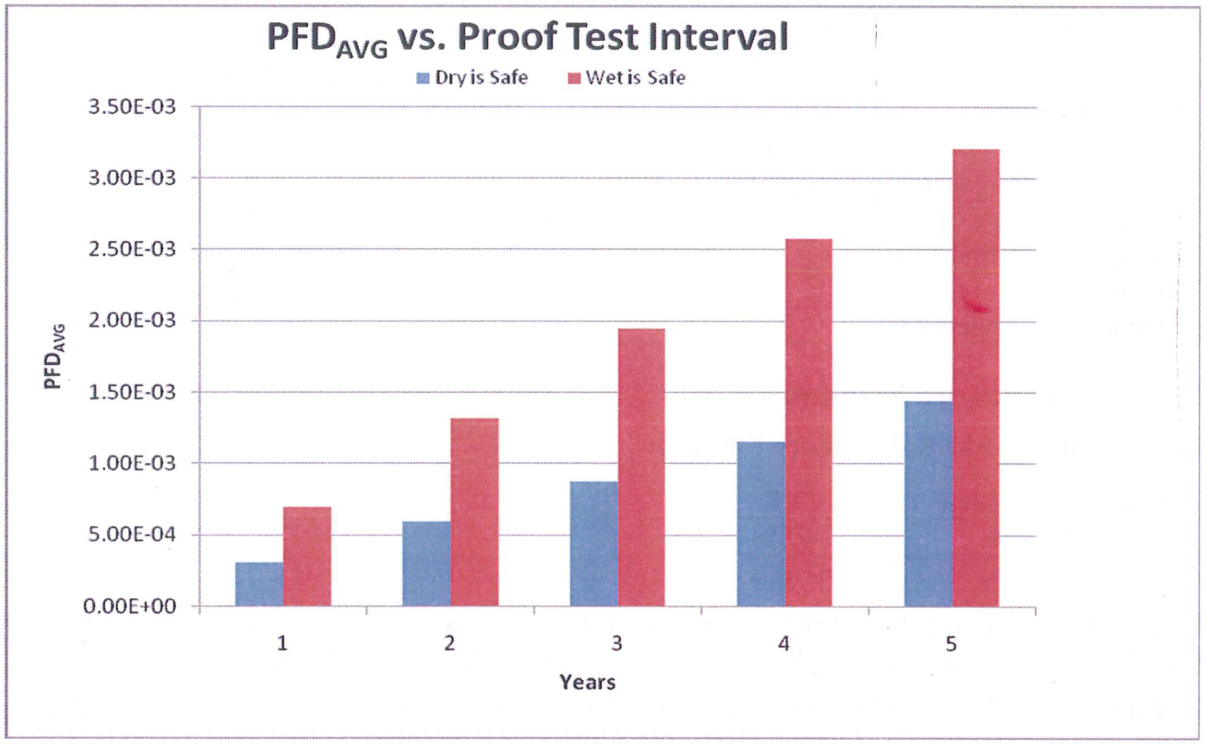
$PFD_{AVG}(1yr)$ = [(0.99*λ^{DU}* 8760_{hours}) / 2] + [(1-.99*λ^{DU} * 10 * 8760)/2] +[λ^{DD} * 24 hours]

= [(0.99 * 1.45e-7*8760) /2] +[(0.01*1.45e-7*10*8720)/2] +[0.0*24]

=6.92e-4

This PFD_{AVG} value is less than 10^{-1} and suitable for Type A SIL 1 application.

SIL range (max) 0.1
PFD_{AVG} (1yr) % of SIL Range 0.69%



D. Liability

The FMEDA analysis is based on *exida Consulting LLC's SILVER* Tool. Magnetrol and *exida Consulting LLC* 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. Proof Test Procedure

A suggested proof test is described below in Table 4. This test will detect approximately 99% of the possible DU failures in Ultrasonic Level Switches.

Table 4: Steps for Proof Test

Step	Action
1	Remove the Model 910 from control of the process
2	Inspect the physical condition of the unit
3	Force the gap to see a WET process condition. Using a Digital Multi-meter, ensure that both relay contacts change state
4	Force the gap to see a DRY process condition. Using a Digital Multi-meter, ensure that both relay contacts change state
5	Return Model 910 to process control

F. 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 910 circuitry can be considered to have a useful lifetime based on the following:

$$L_{actual} = L_{max} * 2^{(Tmax - Tcap) / 10}$$

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)

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

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

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

G. Release Signatures

Name: Paul Snider	*Name* Steve Reynolds
Title: Sr. Compliance Engineer	*Title:* Evaluation Engineering Manager
Date: October 13, 2010	*Date:* October 13, 2010