Magnetrol®

Failure Modes, Effects, and Diagnostic Analysis

Orion Switches Models

ORS-300 and ORS -100

9/8/2004

Table of Contents

A. Description

This report describes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Orion Model ORS-300 Reed Switch and ORS-100 Snap Switch. The FMEDA performed on these Orion products includes all related hardware. For full certification purposes, the product along with all requirements of IEC 61508 must be considered.

Management Summary

This report summarizes the results of the Failure Modes, Effects and Diagnostic Analysis (FMEDA) of the Model ORS-300 Reed Switch and ORS-100 Snap 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 IEC 61508 of a device.

The Model ORS-300 Reed Switch and ORS-100 Snap Switch are devices classified as Type A according to IEC 61508. The FMEDA analysis assumes the diagnostic signal is being transmitted to a device capable of detecting the fault conditions.

Table 1: Failure rates of the Model ORS-300 Reed Switch & Model ORS-100 Snap Switch

	ORS 300	ORS 100
λ^{DU}	265	1351
SFF	80%	50%

The failure rates in Table 1 assume the switches are wired open to indicate an alarm condition.

These failure rates can be used in a probabilistic model of a Safety Instrument 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

SILVER (FMEDA Tool V4R0.6a), a failure rate database developed by exida.com. 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.
Fail-Safe State	The Fail–Safe state is equivalent to the condition of the output of the device if it stopped operating entirely. For switch outputs this is the normally open 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.
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.

3. Assumptions

- The failure categories listed are only safe and dangerous, both detected and undetected.
- For ORS-300, the 80% Safe Failure Fraction is because the system consists of a reed switch and wires. MLI is not included in this evaluation. The switch is assumed wired so that open indicates an alarm.
- For ORS-100, the 50% Safe Failure Fraction is due to the snap switch mechanism because it is unknown whether it fails in an alarm or non-alarm manner.
- 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.
- Failure rates are based off of actual field information and field failures. Only field failures are considered.
- 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 Benign classification of MIL-HNBK-217F.

4. Failure Rates

Table 2:

Model ORS 300 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Safe	80%	1058
Fail Dangerous Undetected	20%	265

Model ORS 100 Failure Rates

Failure Category		Failure rate (in Fits)
Fail Safe	50%	1351
Fail Dangerous Undetected	50%	1351

5. Safe Failure Fraction

Table 3: Model ORS 300 and ORS 100 Safe Failure Fraction

Model	SFF
ORS 300	80%
ORS 100	50%

For ORS 300, because the SFF is greater than 60%, and the switch is a Type A device, it is suitable for SIL 2.

For ORS 100, because the SFF is less than 60%, and the switch is a Type A device, it is suitable for SIL 1.

6. (PFD)ave

ORS 300 Reed Switch average Probability of Failure on Demand (PDF_{ave}) for a one year Proof Test is:

PFD(avg)(1yr) = $(\lambda^{DU}/2)$* 1 yr = $265*10^{-9}/2 * 8760$ hr = $1.16*10^{-3}$

PFD(avg)(1yr) = **0.0016**

This PFD_{ave} value is less than .01 and suitable for Type A SIL 2 application.

SIL range (max) 0.01

PFD(avg)(1yr) % of SIL Range 16%

ORS 100 Snap Switch average Probability of Failure on Demand (PDF_{ave}) for a one year Proof Test is:

PFD(avg)(1yr) = $(\lambda^{DU}/2)$* 1 yr = $1351*10^{-9}/2 * 8760$ hr = $5.9*10^{-3}$

PFD(avg)(1yr) = **0.0059**

This PFD_{ave} value is less than 0.1 and suitable for Type A SIL 1 application.

SIL range (max) 0.1

PFD(avg)(1yr) % of SIL Range 5.9%

7. 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.

8. Release Signatures

Paul Snider	John S. Benway
Senior Compliance Engineer	Manager, Evaluation Engineering
September 8, 2004	September 8, 2004