



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

**United Electric One Series Electronic Switch**

Customer:

**United Electric**  
Watertown, MA  
USA

Contract No.: UE 05/10-35

Report No.: UE 05/10-35 R001

Version V1, Revision R4, April 20, 2007

Rudolf Chalupa

## Management summary

This report summarizes the results of the hardware assessment of the One Series Electronic Switch. The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification of a device per IEC 61508. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the One Series, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The One Series is a smart device which senses temperature or pressure and provides a discrete output. (Some versions of the One Series also provide an externally excited 4-20mA current output.). It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. The One Series can also provide an “I Am Working” output by toggling its output at a 2-20 Hz rate, essentially providing a tri-state output. Both the discrete and 4-20mA outputs have been assessed for safety instrumented systems usage. The One Series is classified as a Type B<sup>1</sup> device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the switch has a safe failure fraction between 60% and 90%<sup>2</sup> (assuming that the logic solver is appropriately programmed, see Section 4.3) and therefore may be used up to SIL 1 as a single device.

The One Series Electronic Switch is available in several models. These are listed in Table 1. Each version is available with a gauge pressure, differential pressure, or temperature sensor.

**Table 1: One Series Electronic Switch Models**

Model	Description
2W2D00	One discrete switch, 12-30VDC@40mA
2W3A00	One discrete switch, 90-130VAC/DC@100mA
2WLP41	One discrete switch, 0-140VAC/DC@600mA, powered by analog 4-20mA current loop
2WLP43	One discrete switch, 0-280VAC/DC@300mA, powered by analog 4-20mA current loop
4W3A01	One discrete switch, 24-280VAC@10A
8W2D42	Two discrete switches, #1: <a href="#">75-250VAC@1.5A</a> , #2: <a href="#">75-250VAC@1.5A</a> , analog 4-20mA current loop, powered by separate 12-30VDC
8W2D44	Two discrete switches, #1: <a href="#">75-250VAC@1.5A</a> , #2: <a href="#">0-140VAC/VDC@600mA</a> , analog 4-20mA current loop, powered by separate 12-30VDC
8W2D45	Two discrete switches, #1: <a href="#">0-140VAC/VDC@600mA</a> , #2: <a href="#">0-140VAC/VDC@600mA</a> , analog 4-20mA current loop, powered by separate 12-30VDC

<sup>1</sup> Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

<sup>2</sup> Provided that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics.

The failure rates for the One Series Electronic Switch are listed in Table 3 - Table 42. Note the following explanation of function codes:

**Table 2 One Series Electronic Switch Output Codes**

Acronym	Explanation
4-20mA	4-20mA current output – 24mA output corresponds to fault state
DTT	De-energize to trip – open output corresponds to safe state (no separate fault state)
ETT	Energize to trip – closed output corresponds to safe state (no separate fault state)
IAW	“I Am Working” – normally closed, pulse output corresponds to safe state, open output corresponds to fault state
SIL	“Safety” – normally pulsing, closed output corresponds to safe state, open output corresponds to fault state

**Table 3 Failure Rates One Series 2W2D00 DTT Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	229
Fail Safe Undetected	49
Fail Detected	149
Annunciation Detected	6
Fail Low	25
Fail Dangerous Undetected	129
Fail Undetected	84
Fail High	45
No Effect	92
Annunciation Undetected	5

**Table 4 Failure Rates One Series 2W2D00 DTT Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	253
Fail Safe Undetected	49
Fail Detected	173
Annunciation Detected	6
Fail Low	25
Fail Dangerous Undetected	125
Fail Undetected	80
Fail High	45
No Effect	92
Annunciation Undetected	5

**Table 5 Failure Rates One Series 2W2D00 IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		49	
Fail Dangerous Detected		180	
	Fail Detected	149	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		129	
	Fail Undetected	84	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 6 Failure Rates One Series 2W2D00 IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		49	
Fail Dangerous Detected		204	
	Fail Detected	173	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		125	
	Fail Undetected	80	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 7 Failure Rates One Series 2W2D00 SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		94	
	Fail Safe Undetected	49	
	Fail High	45	
Fail Dangerous Detected		176	
	Fail Detected	149	
	Annunciation Detected	6	
	Fail Low	21	
Fail Dangerous Undetected		84	
No Effect		92	
Annunciation Undetected		5	

**Table 8 Failure Rates One Series 2W2D00 SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		94	
	Fail Safe Undetected	49	
	Fail High	45	
Fail Dangerous Detected		204	
	Fail Detected	173	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		80	
No Effect		92	
Annunciation Undetected		5	

**Table 9 Failure Rates One Series 2W3A00 AC DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		266	
	Fail Safe Undetected	47	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		129	
	Fail Undetected	69	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 10 Failure Rates One Series 2W3A00 AC DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		290	
	Fail Safe Undetected	47	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		125	
	Fail Undetected	66	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 11 Failure Rates One Series 2W3A00 AC IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		219	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		129	
	Fail Undetected	69	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 12 Failure Rates One Series 2W3A00 AC IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		243	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		125	
	Fail Undetected	66	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 13 Failure Rates One Series 2W3A00 AC SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		90	
	Fail Safe Undetected	47	
	Fail High	43	
Fail Dangerous Detected		219	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		69	
No Effect		121	
Annunciation Undetected		11	

**Table 14 Failure Rates One Series 2W3A00 AC SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		90	
	Fail Safe Undetected	47	
	Fail High	43	
Fail Dangerous Detected		243	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		66	
No Effect		122	
Annunciation Undetected		11	



**Table 15 Failure Rates One Series 2W3A00 DC DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		265	
	Fail Safe Undetected	47	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		111	
	Fail Undetected	69	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 16 Failure Rates One Series 2W3A00 DC DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		289	
	Fail Safe Undetected	47	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		108	
	Fail Undetected	66	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 17 Failure Rates One Series 2W3A00 DC IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		218	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		111	
	Fail Undetected	69	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 18 Failure Rates One Series 2W3A00 DC IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Undetected		242	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		108	
	Fail Undetected	66	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 19 Failure Rates One Series 2W3A00 DC SIL Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	89
Fail Safe Undetected	47
Fail High	42
Fail Dangerous Detected	218
Fail Detected	165
Annunciation Detected	6
Fail Low	47
Fail Dangerous Undetected	69
No Effect	123
Annunciation Undetected	11

**Table 20 Failure Rates One Series 2W3A00 DC SIL Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	89
Fail Safe Undetected	47
Fail High	42
Fail Dangerous Detected	242
Fail Detected	189
Annunciation Detected	6
Fail Low	47
Fail Dangerous Undetected	66
No Effect	123
Annunciation Undetected	11

**Table 21 Failure Rates One Series 2WLP4x 4-20mA Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	47
Fail Dangerous Detected	162
Fail Dangerous Undetected	136
No Effect	60

**Table 22 Failure Rates One Series 2WLP4x 4-20mA Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	47
Fail Dangerous Detected	186
Fail Dangerous Undetected	132
No Effect	60

**Table 23 Failure Rates One Series 2WLP4x DTT Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	275
Fail Safe Undetected	47
Fail Detected	170
Fail Low	58
Fail Dangerous Undetected	211
Fail Undetected	78
Fail High	133
No Effect	91

**Table 24 Failure Rates One Series 2WLP4x DTT Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	299
Fail Safe Undetected	47
Fail Detected	194
Fail Low	58
Fail Dangerous Undetected	208
Fail Undetected	75
Fail High	133
No Effect	91

**Table 25 Failure Rates One Series 2WLP4x IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 26 Failure Rates One Series 2WLP4x IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 27 Failure Rates One Series 2WLP4x SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		75	
No Effect		91	

**Table 28 Failure Rates One Series 2WLP4x SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		72	
No Effect		91	

**Table 29 Failure Rates One Series 4W3A01 DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		302	
	Fail Safe Undetected	47	
	Fail Detected	168	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		129	
	Fail Undetected	72	
	Fail High	57	
No Effect		124	
Annunciation Undetected		11	

**Table 30 Failure Rates One Series 4W3A01 DTT Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	325
Fail Safe Undetected	47
Fail Detected	191
Annunciation Detected	6
Fail Low	81
Fail Dangerous Undetected	125
Fail Undetected	68
Fail High	57
No Effect	124
Annunciation Undetected	11

**Table 31 Failure Rates One Series 4W3A01 IAW Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	47
Fail Dangerous Detected	255
Fail Detected	168
Annunciation Detected	6
Fail Low	81
Fail Dangerous Undetected	129
Fail Undetected	72
Fail High	57
No Effect	124
Annunciation Undetected	11

**Table 32 Failure Rates One Series 4W3A01 IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		278	
	Fail Detected	191	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		125	
	Fail Undetected	68	
	Fail High	57	
No Effect		124	
Annunciation Undetected		11	

**Table 33 Failure Rates One Series 4W3A01 SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		104	
	Fail Safe Undetected	47	
	Fail High	57	
Fail Dangerous Detected		255	
	Fail Detected	168	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		72	
No Effect		124	
Annunciation Undetected		11	



**Table 34 Failure Rates One Series 4W3A01 SIL Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	104
Fail Safe Undetected	47
Fail High	57
Fail Dangerous Detected	278
Fail Detected	191
Annunciation Detected	6
Fail Low	81
Fail Dangerous Undetected	68
No Effect	124
Annunciation Undetected	11

**Table 35 Failure Rates One Series 8W2D4x 4-20mA Pressure**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	47
Fail Dangerous Detected	224
Fail Detected	196
Fail Low	28
Fail Dangerous Undetected	153
No Effect	89
Annunciation Undetected	3

**Table 36 Failure Rates One Series 8W2D4x 4-20mA Temperature**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	47
Fail Dangerous Detected	248
Fail Detected	220
Fail Low	28
Fail Dangerous Undetected	149
No Effect	89
Annunciation Undetected	3

**Table 37 Failure Rates One Series 8W2D4x DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		275	
	Fail Safe Undetected	47	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 38 Failure Rates One Series 8W2D4x DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		299	
	Fail Safe Undetected	47	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 39 Failure Rates One Series 8W2D4x IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Safe Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 40 Failure Rates One Series 8W2D4x IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		299	
Fail Safe Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 41 Failure Rates One Series 8W2D4x SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		75	
No Effect		91	

**Table 42 Failure Rates One Series 8W2D4x SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		72	
No Effect		91	

Table 43 lists the failure rates for the One Series according to IEC 61508. It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

**Table 43 Failure rates according to IEC 61508**

Device	$\lambda_{sd}$	$\lambda_{su}^3$	$\lambda_{dd}$	$\lambda_{du}$	SFF
2W2D00 DTT Pressure	0 FIT	326 FIT	0 FIT	129 FIT	71.7%
2W2D00 DTT Temperature	0 FIT	350 FIT	0 FIT	125 FIT	73.7%
2W2D00 IAW Pressure	0 FIT	146 FIT	180 FIT	129 FIT	71.7%
2W2D00 IAW Temperature	0 FIT	146 FIT	204 FIT	125 FIT	73.7%
2W2D00 SIL Pressure	0 FIT	191 FIT	176 FIT	84 FIT	81.4%
2W2D00 SIL Temperature	0 FIT	191 FIT	204 FIT	80 FIT	83.2%
2W3A00 AC DTT Pressure	0 FIT	398 FIT	0 FIT	129 FIT	75.5%
2W3A00 AC DTT Temperature	0 FIT	422 FIT	0 FIT	125 FIT	77.2%
2W3A00 AC IAW Pressure	0 FIT	179 FIT	219 FIT	129 FIT	75.5%
2W3A00 AC IAW Temperature	0 FIT	179 FIT	243 FIT	125 FIT	77.2%
2W3A00 AC SIL Pressure	0 FIT	222 FIT	219 FIT	69 FIT	86.5%
2W3A00 AC SIL Temperature	0 FIT	278 FIT	243 FIT	66 FIT	87.6%
2W3A00 DC DTT Pressure	0 FIT	399 FIT	0 FIT	111 FIT	78.2%
2W3A00 DC DTT Temperature	0 FIT	423 FIT	0 FIT	108 FIT	79.7%
2W3A00 DC IAW Pressure	0 FIT	181 FIT	218 FIT	111 FIT	78.2%
2W3A00 DC IAW Temperature	0 FIT	181 FIT	242 FIT	108 FIT	79.7%
2W3A00 DC SIL Pressure	0 FIT	223 FIT	218 FIT	69 FIT	86.5%
2W3A00 DC SIL Temperature	0 FIT	223 FIT	242 FIT	66 FIT	87.6%
2WLP4x 4-20mA Pressure	0 FIT	107 FIT	162 FIT	136 FIT	66.4%
2WLP4x 4-20mA Temperature	0 FIT	107 FIT	186 FIT	132 FIT	68.9%
2WLP4x DTT Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
2WLP4x DTT Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
2WLP4x IAW Pressure	0 FIT	138 FIT	228 FIT	211 FIT	63.4%
2WLP4x IAW Temperature	0 FIT	138 FIT	252 FIT	208 FIT	65.2%
2WLP4x SIL Pressure	0 FIT	184 FIT	228 FIT	75 FIT	83.6%
2WLP4x SIL Temperature	0 FIT	154 FIT	252 FIT	72 FIT	84.9%
4W3A01 DTT Pressure	0 FIT	437 FIT	0 FIT	129 FIT	77.2%

<sup>3</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

4W3A01 DTT Temperature	0 FIT	460 FIT	0 FIT	125 FIT	78.6%
4W3A01 IAW Pressure	0 FIT	182 FIT	255 FIT	129 FIT	77.2%
4W3A01 IAW Temperature	0 FIT	182 FIT	278 FIT	125 FIT	78.6%
4W3A01 SIL Pressure	0 FIT	239 FIT	255 FIT	72 FIT	87.5%
4W3A01 SIL Temperature	0 FIT	239 FIT	278 FIT	68 FIT	88.4%
8W2D4x 4-20mA Pressure	0 FIT	139 FIT	224 FIT	153 FIT	70.4%
8W2D4x 4-20mA Temperature	0 FIT	139 FIT	248 FIT	149 FIT	72.2%
8W2D4x DTT Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
8W2D4x DTT Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
8W2D4x IAW Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
8W2D4x IAW Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
8W2D4x SIL Pressure	0 FIT	229 FIT	228 FIT	75 FIT	83.6%
8W2D4x SIL Temperature	0 FIT	154 FIT	252 FIT	72 FIT	84.9%

These failure rates are valid for the useful lifetime of the product, see Appendix A: Lifetime of critical components.

A user of the One Series Electronic Switch can utilize these failure rates 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 full table of failure rates is presented in section 4.4 along with all assumptions.

## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	23
2 Project management.....	24
2.1 <i>exida</i> .....	24
2.2 Roles of the parties involved .....	24
2.3 Standards / Literature used .....	24
2.4 Reference documents .....	25
2.4.1 Documentation provided by United Electric .....	25
2.4.2 Documentation generated by <i>exida</i> .....	26
3 Product Description.....	30
4 Failure Modes, Effects, and Diagnostics Analysis .....	31
4.1 Description of the failure categories .....	31
4.2 Methodology – FMEDA, Failure rates.....	32
4.2.1 FMEDA.....	32
4.2.2 Failure rates.....	32
4.3 Assumptions .....	32
4.4 Results .....	34
5 Using the FMEDA results.....	53
5.1 Example PFD <sub>AVG</sub> calculation for One Series.....	53
6 Terms and Definitions .....	55
7 Status of the document .....	56
7.1 Liability .....	56
7.2 Releases .....	56
7.3 Future Enhancements .....	56
7.4 Release Signatures .....	57
Appendix A: Lifetime of critical components .....	58
Appendix B Proof test to reveal dangerous undetected faults .....	59
B.1 Suggested proof test .....	59

# 1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

## Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ( $PFD_{AVG}$ ). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

## Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

## Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

### **This assessment shall be done according to option 1.**

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the One Series Electronic Switch. From this, failure rates, Safe Failure Fraction (SFF) and example  $PFD_{AVG}$  values are calculated.

The information in this report can be used to evaluate whether a sensor subsystem, including the One Series Electronic Switch, meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508.

## 2 Project management

### 2.1 *exida*

*exida* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

United Electric              Manufacturer of the One Series

*exida*                              Performed the hardware assessment per Option 1 (see Section 1)

United Electric contracted *exida* in June 2006 for the FMEDA of the One Series.

### 2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	EMCRH, <i>exida</i> 2006	Electrical and Mechanical Component Reliability Handbook, 1 <sup>st</sup> edition
[N3]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N4]	Safety Equipment Reliability Handbook, 2003	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N5]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition



## 2.4 Reference documents

### 2.4.1 Documentation provided by United Electric

[D1]	FGS306113500	Brochure, One Series Electronic Switch
[D2]		Installation and Maintenance Instructions, One Series Electronic Pressure and Temperature Switches
[D3]	6247-658 2W2D Electronic Switch Schematic.rtf	Series 3000 Main Schematic Diagram, Revision C
[D4]	6247-663 2W3A 110V Switch Schematic.rtf	Series 3000 Toxic Schematic Diagram, Revision C
[D5]	6247-667 4W3A 24-280 VAC, 10A, Daughterboard Schematic110V Switch Schematic.rtf	Series 3000 O2 Schematic Diagram, Revision C
[D6]	6247-672 2WLP 4-20mA Loop Powered Transmitter Daughter.rtf	Series 3000 Bias Schematic Diagram, Revision C
[D7]	6247-677 8W2D 4-20mA Transmitter, Dual Switch, Electronics Module Board.rtf	6247-677 8W2D 4-20mA Transmitter, Dual Switch, Electronics Module Board
[D8]	6247-677 8W2D 4-20mA Transmitter, Dual Switch, Daughter Board.rtf	6247-677 8W2D 4-20mA Transmitter, Dual Switch, Daughter Board
[D9]	2W2D_BOM.txt	Bill of Material , 2W2D
[D10]	2W3A_BOM.txt	Bill of Material, 2W3A
[D11]	2WLP_Daughter Board_BOM.txt	Bill of Material, 2WLP_Daughter Board
[D12]	4W3A_Daughter Board_BOM.txt	Bill of Material, 4W3A_Daughter Board
[D13]	8W2D Module Board BOM.txt	Bill of Material, 8W2D Module Board
[D14]	8W2D Daughter Board BOM.txt	Bill of Material, 8W2D Daughter Board
[D15]	One Series Temperature Sensor.pdf	One Series Temperature Sensor
[D16]	One Series Gauge Pressure Sensor.pdf	One Series Gauge Pressure Sensor
[D17]	One Series Differential Pressure Sensor.pdf	One Series Differential Pressure Sensor

[D18]	CHEETAH_HW_SPEC_Rev_B.doc	Hardware Specification CHEETAH
[D19]	2-Wire 4-20mA Option Product Spec.doc	Product Specification, 2-Wire 4-20mA Option
[D20]	2-Wire_AC_Product Spec.doc	Product Specification, 2-Wire_AC
[D21]	Dual 4A Switch with 4-20mA Output.doc	Product Specification, Dual 4A Switch with 4-20mA Output
[D22]	Part Descriptions.xls	Part Descriptions
[D23]	Fault Monitoring Summary.xls	Fault Monitoring Summary

#### 2.4.2 Documentation generated by *exida*

[R1]	UE 05-10-35 R001 V1 R4 FMEDA Series One.doc, 04/20/2007	FMEDA report, One Series Electronic Switch (this report)
[R2]	2W2D00 DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, De-Energize to Trip, Pressure Transducer
[R3]	2W2D00 DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, De-Energize to Trip, Temperature Transducer
[R4]	2W2D00 IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, IAW Mode, Pressure Transducer
[R5]	2W2D00 IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, IAW Mode, Temperature Transducer
[R6]	2W2D00 SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, SIL Mode, Pressure Transducer
[R7]	2W2D00 SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W2D00, SIL Mode, Temperature Transducer
[R8]	2W3A00 AC DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, De-Energize to Trip, Pressure Transducer
[R9]	2W3A00 AC DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, De-Energize to Trip, Temperature Transducer
[R10]	2W3A00 AC IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, IAW Mode, Pressure Transducer

[R11]	2W3A00 AC IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, IAW Mode, Temperature Transducer
[R12]	2W3A00 AC SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, SIL Mode, Pressure Transducer
[R13]	2W3A00 AC SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Alternating Current Application, SIL Mode, Temperature Transducer
[R14]	2W3A00 DC DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, De-Energize to Trip, Pressure Transducer
[R15]	2W3A00 DC DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, De-Energize to Trip, Temperature Transducer
[R16]	2W3A00 DC IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, IAW Mode, Pressure Transducer
[R17]	2W3A00 DC IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, IAW Mode, Temperature Transducer
[R18]	2W3A00 DC SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, SIL Mode, Pressure Transducer
[R19]	2W3A00 DC SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 2W3A00, Direct Current Application, SIL Mode, Temperature Transducer
[R20]	2WLP4x 420 Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, 4-20 mA Output, Pressure Transducer
[R21]	2WLP4x 420 RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, 4-20 mA Output, Temperature Transducer
[R22]	2WLP4x DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, De-Energize to Trip, Pressure Transducer
[R23]	2WLP4x DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, De-Energize to Trip, Temperature Transducer
[R24]	2WLP4x IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, IAW Mode, Pressure Transducer

[R25]	2WLP4x IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, IAW Mode, Temperature Transducer
[R26]	2WLP4x SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, SIL Mode, Pressure Transducer
[R27]	2WLP4x SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, SIL Mode, Temperature Transducer
[R28]	4W3A01 AC DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, De-Energize to Trip, Pressure Transducer
[R29]	4W3A01 AC DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, De-Energize to Trip, Temperature Transducer
[R30]	4W3A01 AC IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, IAW Mode, Pressure Transducer
[R31]	4W3A01 AC IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, IAW Mode, Temperature Transducer
[R32]	4W3A01 AC SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, SIL Mode, Pressure Transducer
[R33]	4W3A01 AC SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series Model 4W3A01, Alternating Current Application, SIL Mode, Temperature Transducer
[R34]	8W2D4x 420 Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, 4-20 mA Output, Pressure Transducer
[R35]	8W2D4x 420 RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 2WLP4x Models, 4-20 mA Output, Temperature Transducer
[R36]	8W2D4x DTT Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, De-Energize to Trip, Pressure Transducer
[R37]	8W2D4x DTT RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, De-Energize to Trip, Temperature Transducer
[R38]	8W2D4x IAW Pressure.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, IAW Mode, Pressure Transducer
[R39]	8W2D4x IAW RTD.xls, 04/09/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, IAW Mode, Temperature Transducer

[R40]	8W2D4x SIL Pressure.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, SIL Mode, Pressure Transducer
[R41]	8W2D4x SIL RTD.xls, 02/07/2007	Failure Modes, Effects, and Diagnostic Analysis – One Series 8W2D4x Models, SIL Mode, Temperature Transducer

### 3 Product Description

The United Electric One Series Electronic Switch is an electronic “smart” switch that provides continuous monitoring of gauge pressure, differential pressure, or temperature.

The system contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. Faults and status conditions are indicated using specified output values, see [D2].

The One Series is classified as a Type B<sup>4</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

A unique feature of the One Series is its available “I Am Working” (IAW) mode. This mode replaces the open state of the switch output with a pulse train with a 50% duty cycle and a frequency between 2 and 20 Hz (model and option dependent). This allows for dynamic fault detection during the normal state of the output as well as three output states (closed, pulse, open) allowing for the separation of the tripped and fault indications.

In IAW mode, the closed output state is the normal state of the output, the pulsing state represents the tripped condition, and the open state represents the fault state (predefined alarm state per IEC61508).

The SIL mode is an alternate implementation of the IAW mode. In SIL mode, the pulse output state is the normal state of the output, the closed state represents the tripped condition, and the open state represents the fault state (predefined alarm state per IEC61508). This maximizes diagnostic coverage at both the product and system level.

The One Series Electronic Switch is available in several models. These are listed in Table 44. Each version is available with a gauge pressure, differential pressure, or temperature sensor.

**Table 44: One Series Electronic Switch Models**

Model	Description
2W2D00	One discrete switch, 12-30VDC@40mA
2W3A00	One discrete switch, 90-130VAC/DC@100mA
2WLP41	One discrete switch, 0-140VAC/DC@600mA, powered by analog 4-20mA current loop
2WLP43	One discrete switch, 0-280VAC/DC@300mA, powered by analog 4-20mA current loop
4W3A01	One discrete switch, 24-280VAC@10A
8W2D42	Two discrete switches, #1: 75-250VAC@1.5A, #2: 75-250VAC@1.5A, analog 4-20mA current loop, powered by separate 12-30VDC
8W2D44	Two discrete switches, #1: 75-250VAC@1.5A, #2: 0-140VAC/VDC@600mA, analog 4-20mA current loop, powered by separate 12-30VDC
8W2D45	Two discrete switches, #1: 0-140VAC/VDC@600mA, #2: 0-140VAC/VDC@600mA, analog 4-20mA current loop, powered by separate 12-30VDC

<sup>4</sup> Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by exida and is documented in [R1] through [R41]. This resulted in failures that can be classified according to the following failure categories.

### 4.1 Description of the failure categories

In order to judge the failure behavior of the One Series, the following definitions for the failure of the product were considered by *exida*.

#### Fail-Safe State

4-20mA	The fail-safe state is defined as state where the output exceeds the user defined threshold.
DTT	The fail-safe state is defined as state where the output is open.
ETT / SIL	The fail-safe state is defined as state where the output is closed.
IAW	The fail-safe state is defined as state where the output is pulsing.
Fail Safe Undetected	Failure that deviates the output toward the fail-safe state but is undetected by internal diagnostics.
Fail Dangerous	Failure that deviates the measured input state by more than 2% of span away from the fail-safe state (4-20mA) or prevents the device from going to the fail-safe state in case of a demand.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics or a connected logic solver.
Fail High	Failure that causes the output signal to go to the maximum output (closed switch or 24mA nominal)
Fail Low	Failure that causes the output signal to go to the minimum output (open switch or < 4mA)
Fail Detected	Failure that causes the output signal to go to the fault state (predefined alarm state per IEC 61508) (open switch or 24mA).
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High, a Fail Low, or Fail Detected failure can either be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified.



The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

## **4.2 Methodology – FMEDA, Failure rates**

### **4.2.1 FMEDA**

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### **4.2.2 Failure rates**

The failure rate data used by exida in this FMEDA is from the *exida* proprietary component failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

## **4.3 Assumptions**

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the One Series.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The application program in the safety logic solver is configured to detect under-range (Fail Low), over-range (Fail High) and Fail Detected failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.



- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs and the diagnostic coverage provided by the online diagnostics.
- Switch is installed per the instructions and the requirements of the application.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 60654-1, Class C with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- External power supply failure rates are not included.

## 4.4 Results

The FMEDAs described in [R2] - [R41] carried out by exida on the One Series and under the assumptions described in section 4.3 lead to the following failure rates. Table 45 -

Table 84 list the failure rates for the One Series.

**Table 45 Failure Rates One Series 2W2D00 DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		229	
	Fail Safe Undetected	49	
	Fail Detected	149	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		129	
	Fail Undetected	84	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 46 Failure Rates One Series 2W2D00 DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		253	
	Fail Safe Undetected	49	
	Fail Detected	173	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		125	
	Fail Undetected	80	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 47 Failure Rates One Series 2W2D00 IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		49	
Fail Dangerous Detected		180	
	Fail Detected	149	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		129	
	Fail Undetected	84	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 48 Failure Rates One Series 2W2D00 IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		49	
Fail Dangerous Detected		204	
	Fail Detected	173	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		125	
	Fail Undetected	80	
	Fail High	45	
No Effect		92	
Annunciation Undetected		5	

**Table 49 Failure Rates One Series 2W2D00 SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		94	
	Fail Safe Undetected	49	
	Fail High	45	
Fail Dangerous Detected		176	
	Fail Detected	149	
	Annunciation Detected	6	
	Fail Low	21	
Fail Dangerous Undetected		84	
No Effect		92	
Annunciation Undetected		5	

**Table 50 Failure Rates One Series 2W2D00 SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		94	
	Fail Safe Undetected	49	
	Fail High	45	
Fail Dangerous Detected		204	
	Fail Detected	173	
	Annunciation Detected	6	
	Fail Low	25	
Fail Dangerous Undetected		80	
No Effect		92	
Annunciation Undetected		5	

**Table 51 Failure Rates One Series 2W3A00 AC DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		266	
	Fail Safe Undetected	47	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		129	
	Fail Undetected	69	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 52 Failure Rates One Series 2W3A00 AC DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		290	
	Fail Safe Undetected	47	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		125	
	Fail Undetected	66	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 53 Failure Rates One Series 2W3A00 AC IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		219	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		129	
	Fail Undetected	69	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 54 Failure Rates One Series 2W3A00 AC IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		243	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		125	
	Fail Undetected	66	
	Fail High	43	
No Effect		121	
Annunciation Undetected		11	

**Table 55 Failure Rates One Series 2W3A00 AC SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		90	
	Fail Safe Undetected	47	
	Fail High	43	
Fail Dangerous Detected		219	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		69	
No Effect		121	
Annunciation Undetected		11	

**Table 56 Failure Rates One Series 2W3A00 AC SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		90	
	Fail Safe Undetected	47	
	Fail High	43	
Fail Dangerous Detected		243	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	48	
Fail Dangerous Undetected		66	
No Effect		122	
Annunciation Undetected		11	

**Table 57 Failure Rates One Series 2W3A00 DC DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		265	
	Fail Safe Undetected	47	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		111	
	Fail Undetected	69	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 58 Failure Rates One Series 2W3A00 DC DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		289	
	Fail Safe Undetected	47	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		108	
	Fail Undetected	66	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	



**Table 59 Failure Rates One Series 2W3A00 DC IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		218	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		111	
	Fail Undetected	69	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 60 Failure Rates One Series 2W3A00 DC IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Undetected		242	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		108	
	Fail Undetected	66	
	Fail High	42	
No Effect		123	
Annunciation Undetected		11	

**Table 61 Failure Rates One Series 2W3A00 DC SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		89	
	Fail Safe Undetected	47	
	Fail High	42	
Fail Dangerous Detected		218	
	Fail Detected	165	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		69	
No Effect		123	
Annunciation Undetected		11	

**Table 62 Failure Rates One Series 2W3A00 DC SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		89	
	Fail Safe Undetected	47	
	Fail High	42	
Fail Dangerous Detected		242	
	Fail Detected	189	
	Annunciation Detected	6	
	Fail Low	47	
Fail Dangerous Undetected		66	
No Effect		123	
Annunciation Undetected		11	

**Table 63 Failure Rates One Series 2WLP4x 4-20mA Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		162	
Fail Dangerous Undetected		136	
No Effect		60	

**Table 64 Failure Rates One Series 2WLP4x 4-20mA Temperature**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	47
Fail Dangerous Detected	186
Fail Dangerous Undetected	132
No Effect	60

**Table 65 Failure Rates One Series 2WLP4x DTT Pressure**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	275
Fail Safe Undetected	47
Fail Detected	170
Fail Low	58
Fail Dangerous Undetected	211
Fail Undetected	78
Fail High	133
No Effect	91

**Table 66 Failure Rates One Series 2WLP4x DTT Temperature**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	299
Fail Safe Undetected	47
Fail Detected	194
Fail Low	58
Fail Dangerous Undetected	208
Fail Undetected	75
Fail High	133
No Effect	91

**Table 67 Failure Rates One Series 2WLP4x IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 68 Failure Rates One Series 2WLP4x IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 69 Failure Rates One Series 2WLP4x SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		75	
No Effect		91	

**Table 70 Failure Rates One Series 2WLP4x SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		72	
No Effect		91	

**Table 71 Failure Rates One Series 4W3A01 DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		302	
	Fail Safe Undetected	47	
	Fail Detected	168	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		129	
	Fail Undetected	72	
	Fail High	57	
No Effect		124	
Annunciation Undetected		11	

**Table 72 Failure Rates One Series 4W3A01 DTT Temperature**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>	
Fail Safe Undetected	325	
Fail Safe Undetected	47	
Fail Detected	191	
Annunciation Detected	6	
Fail Low	81	
Fail Dangerous Undetected	125	
Fail Undetected	68	
Fail High	57	
No Effect	124	
Annunciation Undetected	11	

**Table 73 Failure Rates One Series 4W3A01 IAW Pressure**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>	
Fail Safe Undetected	47	
Fail Dangerous Detected	255	
Fail Detected	168	
Annunciation Detected	6	
Fail Low	81	
Fail Dangerous Undetected	129	
Fail Undetected	72	
Fail High	57	
No Effect	124	
Annunciation Undetected	11	

**Table 74 Failure Rates One Series 4W3A01 IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Dangerous Detected		278	
	Fail Detected	191	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		125	
	Fail Undetected	68	
	Fail High	57	
No Effect		124	
Annunciation Undetected		11	

**Table 75 Failure Rates One Series 4W3A01 SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		104	
	Fail Safe Undetected	47	
	Fail High	57	
Fail Dangerous Detected		255	
	Fail Detected	168	
	Annunciation Detected	6	
	Fail Low	81	
Fail Dangerous Undetected		72	
No Effect		124	
Annunciation Undetected		11	

**Table 76 Failure Rates One Series 4W3A01 SIL Temperature**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	104
Fail Safe Undetected	47
Fail High	57
Fail Dangerous Detected	278
Fail Detected	191
Annunciation Detected	6
Fail Low	81
Fail Dangerous Undetected	68
No Effect	124
Annunciation Undetected	11

**Table 77 Failure Rates One Series 8W2D4x 4-20mA Pressure**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	47
Fail Dangerous Detected	224
Fail Detected	196
Fail Low	28
Fail Dangerous Undetected	153
No Effect	89
Annunciation Undetected	3

**Table 78 Failure Rates One Series 8W2D4x 4-20mA Temperature**

<b>Failure category</b>	<b>Failure rate (in FIT)</b>
Fail Safe Undetected	47
Fail Dangerous Detected	248
Fail Detected	220
Fail Low	28
Fail Dangerous Undetected	149
No Effect	89
Annunciation Undetected	3



**Table 79 Failure Rates One Series 8W2D4x DTT Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		275	
	Fail Safe Undetected	47	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 80 Failure Rates One Series 8W2D4x DTT Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		299	
	Fail Safe Undetected	47	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 81 Failure Rates One Series 8W2D4x IAW Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		47	
Fail Safe Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		211	
	Fail Undetected	78	
	Fail High	133	
No Effect		91	

**Table 82 Failure Rates One Series 8W2D4x IAW Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		299	
Fail Safe Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		208	
	Fail Undetected	75	
	Fail High	133	
No Effect		91	

**Table 83 Failure Rates One Series 8W2D4x SIL Pressure**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		228	
	Fail Detected	170	
	Fail Low	58	
Fail Dangerous Undetected		75	
No Effect		91	

**Table 84 Failure Rates One Series 8W2D4x SIL Temperature**

Failure category		Failure rate (in FIT)	
Fail Safe Undetected		63	
	Fail Safe Undetected	47	
	Fail High	16	
Fail Dangerous Detected		252	
	Fail Detected	194	
	Fail Low	58	
Fail Dangerous Undetected		72	
No Effect		91	

The failure rates that are derived from the FMEDA for the One Series are in a format different from the IEC 61508 format. Table 85 lists the failure rates for One Series according to IEC 61508, assuming that the logic solver can detect the fault state.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the One Series should be calculated. The SFF is the fraction of the overall failure rate of a subsystem that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formula for SFF:

$$SFF = 1 - \lambda_{du} / \lambda_{total}$$

Note that according to IEC61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

**Table 85 Failure rates according to IEC 61508**

Device	$\lambda_{sd}$	$\lambda_{su}^5$	$\lambda_{dd}$	$\lambda_{du}$	SFF
2W2D00 DTT Pressure	0 FIT	326 FIT	0 FIT	129 FIT	71.7%
2W2D00 DTT Temperature	0 FIT	350 FIT	0 FIT	125 FIT	73.7%
2W2D00 IAW Pressure	0 FIT	146 FIT	180 FIT	129 FIT	71.7%
2W2D00 IAW Temperature	0 FIT	146 FIT	204 FIT	125 FIT	73.7%
2W3A00 AC IAW Pressure	0 FIT	179 FIT	219 FIT	129 FIT	75.5%
2W3A00 AC IAW Temperature	0 FIT	179 FIT	243 FIT	125 FIT	77.2%
2W2D00 SIL Pressure	0 FIT	191 FIT	176 FIT	84 FIT	81.4%
2W2D00 SIL Temperature	0 FIT	191 FIT	204 FIT	80 FIT	83.2%
2W3A00 AC DTT Pressure	0 FIT	398 FIT	0 FIT	129 FIT	75.5%
2W3A00 AC DTT Temperature	0 FIT	422 FIT	0 FIT	125 FIT	77.2%
2W3A00 AC IAW Pressure	0 FIT	179 FIT	219 FIT	129 FIT	75.5%
2W3A00 AC IAW Temperature	0 FIT	179 FIT	243 FIT	125 FIT	77.2%
2W3A00 AC SIL Pressure	0 FIT	222 FIT	219 FIT	69 FIT	86.5%
2W3A00 AC SIL Temperature	0 FIT	278 FIT	243 FIT	66 FIT	87.6%
2W3A00 DC DTT Pressure	0 FIT	399 FIT	0 FIT	111 FIT	78.2%
2W3A00 DC DTT Temperature	0 FIT	423 FIT	0 FIT	108 FIT	79.7%
2W3A00 DC IAW Pressure	0 FIT	181 FIT	218 FIT	111 FIT	78.2%
2W3A00 DC IAW Temperature	0 FIT	181 FIT	242 FIT	108 FIT	79.7%
2W3A00 DC SIL Pressure	0 FIT	223 FIT	218 FIT	69 FIT	86.5%
2W3A00 DC SIL Temperature	0 FIT	223 FIT	242 FIT	66 FIT	87.6%
2WLP4x 4-20mA Pressure	0 FIT	107 FIT	162 FIT	136 FIT	66.4%

<sup>5</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

Device	$\lambda_{sd}$	$\lambda_{su}^5$	$\lambda_{dd}$	$\lambda_{du}$	SFF
2WLP4x 4-20mA Temperature	0 FIT	107 FIT	186 FIT	132 FIT	68.9%
2WLP4x DTT Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
2WLP4x DTT Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
2WLP4x IAW Pressure	0 FIT	138 FIT	228 FIT	211 FIT	63.4%
2WLP4x IAW Temperature	0 FIT	138 FIT	252 FIT	208 FIT	65.2%
2WLP4x SIL Pressure	0 FIT	184 FIT	228 FIT	75 FIT	83.6%
2WLP4x SIL Temperature	0 FIT	154 FIT	252 FIT	72 FIT	84.9%
4W3A01 DTT Pressure	0 FIT	437 FIT	0 FIT	129 FIT	77.2%
4W3A01 DTT Temperature	0 FIT	460 FIT	0 FIT	125 FIT	78.6%
4W3A01 IAW Pressure	0 FIT	182 FIT	255 FIT	129 FIT	77.2%
4W3A01 IAW Temperature	0 FIT	182 FIT	278 FIT	125 FIT	78.6%
4W3A01 SIL Pressure	0 FIT	239 FIT	255 FIT	72 FIT	87.5%
4W3A01 SIL Temperature	0 FIT	239 FIT	278 FIT	68 FIT	88.4%
8W2D4x 4-20mA Pressure	0 FIT	139 FIT	224 FIT	153 FIT	70.4%
8W2D4x 4-20mA Temperature	0 FIT	139 FIT	248 FIT	149 FIT	72.2%
8W2D4x DTT Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
8W2D4x DTT Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
8W2D4x IAW Pressure	0 FIT	366 FIT	0 FIT	211 FIT	63.4%
8W2D4x IAW Temperature	0 FIT	390 FIT	0 FIT	208 FIT	65.2%
8W2D4x SIL Pressure	0 FIT	229 FIT	228 FIT	75 FIT	83.6%
8W2D4x SIL Temperature	0 FIT	154 FIT	252 FIT	72 FIT	84.9%

The architectural constraint type for the One Series is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

## 5 Using the FMEDA results

### 5.1 Example $PFD_{AVG}$ calculation for One Series

An example average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is performed for a single (1oo1) One Series Electronic Switch, Model 2W2D00. The failure rate data used in this calculation is displayed in section 4.4. The resulting  $PFD_{AVG}$  values for a variety of proof test intervals are displayed in Figure 1.

As shown in the figure the  $PFD_{AVG}$  value for a single One Series with a pressure sensor used in De-Energize to Trip (DTT) mode with a proof test interval of one year equals  $5.65E-04$ . The  $PFD_{AVG}$  value for a single One Series with temperature sensor used in De-Energize to Trip mode with a proof test interval of one year equals  $5.48E-04$ .

The  $PFD_{AVG}$  value for a single One Series with a pressure sensor used in SIL mode with a proof test interval of one year equals  $3.69E-04$ . The  $PFD_{AVG}$  value for a single One Series with temperature sensor used in I Am Working mode with a proof test interval of one year equals  $3.52E-04$ .

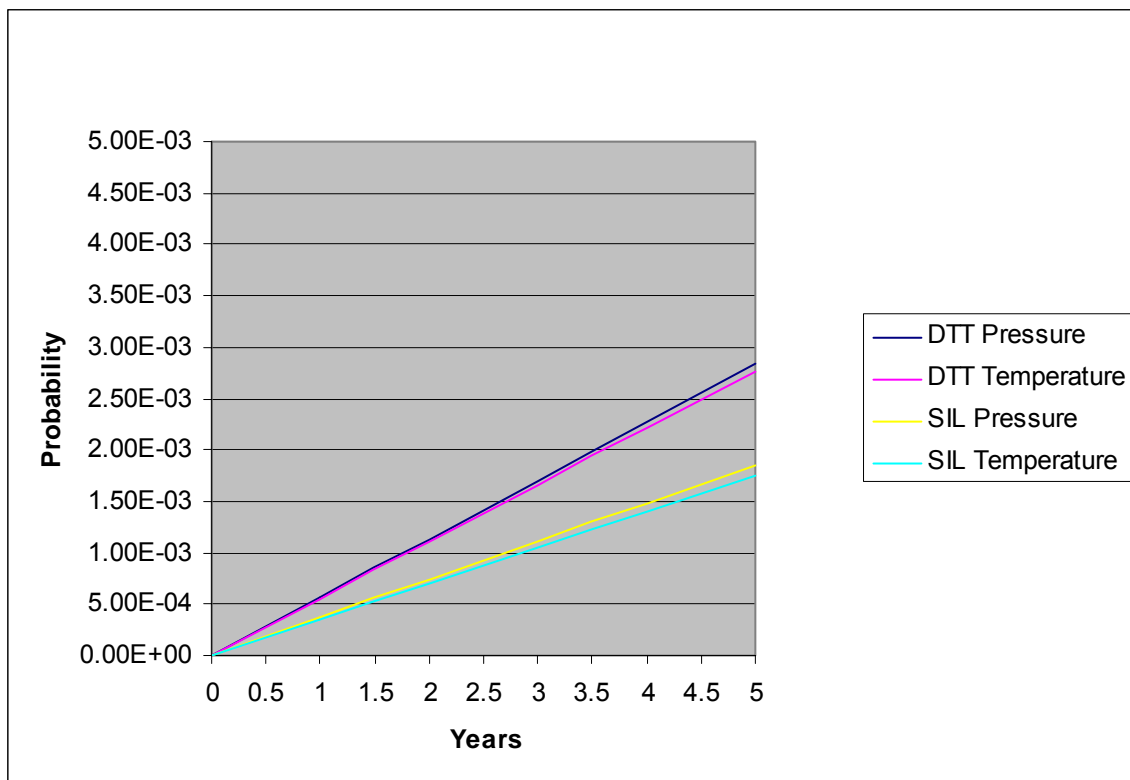


Figure 1  $PFD_{AVG}(t)$  One Series

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF), considering the appropriate parameters such as proof test interval.

For SIL 1 applications, the  $PFD_{AVG}$  value needs to be  $\geq 10^{-2}$  and  $< 10^{-1}$ . This means that for a SIL 1 application, the  $PFD_{AVG}$  value for a single One Series with a pressure sensor used in De-Energize to Trip mode with a proof test interval of one year equals 0.6% of the range. The  $PFD_{AVG}$  value for a single One Series with temperature sensor used in De-Energize to Trip mode with a proof test interval of one year equals 0.6% of the range.

The  $PFD_{AVG}$  value for a single One Series with a pressure sensor used in SIL mode with a proof test interval of one year equals 0.4% of the range. The  $PFD_{AVG}$  value for a single One Series with temperature sensor used in SIL mode with a proof test interval of one year equals 0.4% of the range.

These results must be considered in combination with  $PFD_{AVG}$  values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

## 6 Terms and Definitions

DTT	De-energize to trip
ETT	Energize-to-trip
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
High	In the context of this report, either a closed output switch or analog loop current 24mA nominal
IAW	I Am Working – this is the pulse output mode of the One Series Electronic Switch, effectively allowing tri-state operation using a PLC's discrete input.
Low	In the context of this report, either an open output switch or analog loop current $< 3.6\text{mA}$
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD <sub>AVG</sub>	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

## 7 Status of the document

### 7.1 Liability

*exida* prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

### 7.2 Releases

Version: V1

Revision: R4

Version History: V0, R1: Draft; February 9, 2007  
V0, R2 updated per internal review, February 14, 2007  
V1, R1 released to client, March 1, 2007  
V1, R2 updated per client feedback, April 3, 2007  
V1, R3 updated to distinguish IAW and SIL modes, April 9, 2007  
V1, R4: updated to eliminate typographical errors, April 20, 2007

Authors: Rudolf Chalupa

Review: V0, R1: Rachel Amkreutz (*exida*); February 13, 2007  
V0, R2 Rachel Amkreutz, February 28, 2007  
V1, R3: Rachel Amkreutz (*exida*); April 07

Release status: Draft

### 7.3 Future Enhancements

At request of client.

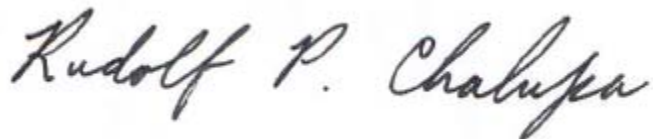


#### 7.4 Release Signatures



---

Dr. William M. Goble, Principal Partner



---

Rudolf Chalupa, Safety Engineer

## Appendix A: Lifetime of critical components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime<sup>6</sup> of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the  $PFD_{AVG}$  calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 86 shows which components are contributing to the dangerous undetected failure rate and therefore to the  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 86 Useful lifetime of electrolytic components contributing to  $\lambda_{du}$**

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours

As there are no aluminum electrolytic capacitors used, the tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The tantalum electrolytic capacitors that are used in the One Series have an estimated useful lifetime of about 50 years.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

<sup>6</sup> Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

## Appendix B Proof test to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

### B.1 Suggested proof test

A suggested proof test is described in Table 87. This test will detect approximately 99% of possible DU failures in the One Series.

**Table 87 Steps for Proof Test**

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Verify the correct output under normal conditions.
3.	Change the process variable or change the programming of the switch so that the output should go to the tripped state. Verify that the output does go to the tripped state.
4.	Change the process variable or change the programming of the switch so that the output goes to the alarm state. (Extreme Over Range or Extreme Under Range is suggested.) Verify that the output does go to the alarm state
5.	Restore the normal input values or programming. Verify that the output has returned to its non-tripped state.
6.	Restore the loop to full operation.
7.	Remove the bypass from the safety PLC or otherwise restore normal operation.