Failure Modes, Effects and Diagnostic Analysis

Project:
Trimod Besta Level Switches

Customer:

Besta Ltd.
Uster
Switzerland

Contract No.: BESTA 12/05-006-C

Report No.: BESTA 12/05-006-C R001

Version V1, Revision R1, January 2013

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management Summary

This report summarizes the results of the mechanical assessment carried out on the Trimod Besta Level Switches in the version listed in the mechanical drawings referenced in section 2.4.1. Trimod Besta Level Switches are composed of switch-, flange and float modules. Table 1 gives an overview of the considered modules.

The mechanical assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Overview of the considered switch modules

[V1]	A, B, DA, DB, XA, XB, ZK 2A, 2B, 2DA, 2DB, X2A, X2B,U..A, U..B, XU..A, XU..B, Z2K 5A, 5B, 5DA, 5DB, X5A, X5B, 5U..A, 5U..B, X5U..A, X5U..B, Z5K Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium ¾"NPT, 54 = Stainless steel ¾" NPT 42 = Aluminium chromated ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production
[V2]	AA, BB, DAA, DBB, XAA, XBB, ZKK, 2AA, 2BB, 2DAA, 2DBB, X2AA, X2BB, XU..AA, XU..BB, Z2KK 5AA, 5BB, 5DAA, 5DBB, X5AA, X5BB, X5U..AA, X5U..BB, Z5KK Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium ¾"NPT, 54 = Stainless steel ¾" NPT 42 = Aluminium chromated ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production
[V3]	I, IN, IE9, INE9, DI, DIN, DIE9, DINE9, XI, XIN, XIE9, XINE9, 2I, 2IN, 2INE9, 2DI, 2DIN, 2DINE9, 5I, 5IN, 5INE9, 5DI, 5DIN, 5DINE9 HI, HIN, HIE9, HINE9, TDI, TDIN, TDIE9, TDINE9 Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium ¾"NPT, 54 = Stainless steel ¾" NPT 42 = Aluminium chromated ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production
[V4]	II, DII, IIE9, XII, XIIE9, 2II, 2DII, 5II, 5DII, 2IIE9, 2DIIE9, 5IIE9, 5DIIE9 HII, HIIE9, TDII, TDIIE9 Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium ¾"NPT, 54 = Stainless steel ¾" NPT 42 = Aluminium chromated ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production

[V5]	HA, HB, ZHK, TDA, TDB, ZTDK 5HA, 5HB, 5TDA, 5TDB, Z5HK, Z5TDK Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium chromated ¾"NPT, 54 = Stainless steel ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production
[V6]	HAA, HBB, ZHKK, TDAA, TDBB, ZTDKK 5HAA, 5HBB, 5TDAA, 5TDBB, Z5HKK, Z5TDKK Modules with cable glands: 10 = Marine Standard W, 30 = Marine Standard Z Modules with threads: 40 = Aluminium chromated ¾"NPT, 54 = Stainless steel ¾" NPT Available Ex-approvals: 1 = GOST-R Ex, 3 = INMETRO, 5 = IECEx, 8 = ATEX Ship registers: ABS, BV, CCS, DNV, GL, LR, RINA, RMRS Exxx/SPECxxx = customized production
[V7]	C 01C 05, DC 01C 05, C 329C 05, DC 329C 05 Exxx/SPECxxx = customized production

All the above mentioned models except [V7] can be combined with the following flange and float modules:

Trimod Besta Flange Modules

Flange modules: Standard: 01, 011, 0118
Special: 03, 04, 06, 038, 048, 068
Industry: DIN, ANSI, BS, JIS
Fix- and composite flange modules
Bracket lengths: F = 68mm, L/Z = 102mm, S/Y = 142mm
Sealing units made of: 1.4571, 8 = Hastelloy, N = Nace
Slip-on flanges made of: H II, 13 CrMo 44, A 350-LF2
Exxx/SPECxxx = customized production
Available standards: P = PED

Trimod Besta Float Modules

Float modules: 01, 02, 03, 04, 041, 07, 26, 27, 031, 032, 76
011, 012, 013, 051, 052, 053, 054, 071, 072, 073, 074, 761, 762, 763, 764
090, 091, 092, 093, 095, 140, 141, 142, 145, 146
08T1, 28T1, 081T1, 082T1, 083T1, 084T1
G1, H1, G2, H2, G3, H3, G5
Exxx/SPECxxx = customized production
Made of: 1.4571, 4xx = Hastelloy, N = Nace
Available standards: P = PED

The Trimod Besta Level Switches are Type A[1] elements with a hardware fault tolerance of 0.

exida did a quantitative analysis of the Trimod Besta Level Switches to calculate the failure rates using Profile 3 [2] data of *exida*'s component database (see [N2] and [N3]) for the different mechanical components. The results are documented in the following tables:

The failure rates are valid for the useful life of the considered Trimod Besta Level Switches (see Appendix 2) when operating as defined.

[1] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

[2] See appendix 3 for detailed definitions.

Table 2: Summary – Failure rates per IEC 61508:2010

	[V1]	[V2]	[V3]	[V4]	[V5]	[V6]	[V7]
λ_{Safe}	**81**	**157**	**20**	**35**	**81**	**157**	**76**
λ_{DD} [3]	**0**	**136**	**0**	**20**	**0**	**136**	**0**
λ_{DU}	**139**	**71**	**97**	**87**	**161**	**93**	**128**

No effect	131	142	123	133	140	151	88
No part	50	50	50	50	50	50	50
λ_{AU} [4]	0	8	0	1	0	8	0

λ_{Total}	**220**	**364**	**117**	**142**	**242**	**386**	**204**

SFF	**36%**	**80%**	**16%**	**38%**	**33%**	**75%**	**37%**

SIL AC [5]	**SIL1**	**SIL2**	**SIL1**	**SIL1**	**SIL1**	**SIL2**	**SIL1**

[3] The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch / sensor is considered to be a safety measure for the primary switch / sensor providing a DC of 90% by considering a common cause factor of 10%.

[4] The AU failures result from the fact that the redundant switch / sensor is considered to be a safety measure and therefore is contributing to the "annunciation" failure category.

[5] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the FMEDA carried out on the Trimod Besta Level Switches in the version listed in the mechanical drawings referenced in section 2.4.1. The FMEDA is part of a full functional safety assessment according to IEC 61508.

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the described Trimod Besta Level Switches, meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirement per IEC 61508.

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, 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

Besta Ltd.	Manufacturer of the Trimod Besta Level Switches.
exida	Performed the mechanical FMEDA.

Besta Ltd. contracted *exida* in August 2012 with the certification of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	EMCR Handbook, 2011 Update	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update
[N4]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by RMG

[D1]	LTKEN1111_TMB_Catalogue_EN_web.pdf	LEVEL SWITCH CATALOGUE “Trimod Besta”; LTKEN 2011.11, English
[D2]	LCXEN_FloatChamber_EN_screen.pdf	FLOAT CHAMBERS BROCHURE“Trimod Besta”; LCXE1006 (English)
[D3]	Zerifizierte Trimod Niveau Schwimmerschalter English 02.doc	Overview of Trimod Besta Level Switches
[D4]	SIL Stücklisten.xls	Comparison of individual parts lists
[D5]	SILA 01 04.pdf	Mechanical drawing „A 01 04“; SILA 01 04 of 01.10.12
[D6]	SILBB 01 04.pdf	Mechanical drawing „BB 01 04“; SILBB 01 04 of 02.10.12
[D7]	SILHA 01 04.pdf	Mechanical drawing „HA 01 04“; SILHA 01 04 of 03.10.12
[D8]	SILIE9 01 04.pdf	Mechanical drawing „IE9 01 04“; SILIE9 01 04 of 03.10.12
[D9]	SILZK8 01 04.pdf	Mechanical drawing „ZK8 01 04“; SILZK8 01 04 of 02.10.12
[D10]	SIL C 01 05.pdf	Mechanical drawing „C 01 05“; SIL C 01 05 5040 of 03.10.12

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.4.2 Documentation generated by *exida*

[R1]	FMEDA_V8_Trimod_A0104_Micro_Standard_V0R2.efm of 18.10.12
[R2]	FMEDA_V8_Trimod_AA0104_redundant_Micro_Standard_V0R3.efm of 19.10.12
[R3]	FMEDA_V8_Trimod_HIE90104_NJ2-11-SN _Standard-Amplifier_V0R4.efm of 24.10.12
[R4]	FMEDA_V8_Trimod_HIIE90104_NJ2-11-SN _redundant_Standard-Amplifier_V0R4.efm of 24.10.12
[R5]	FMEDA_V8_Trimod_HA0104_Micro_Standard_V0R2.efm of 18.10.12
[R6]	FMEDA_V8_Trimod_HAA0104_redundant_Micro_Standard_V0R2.efm of 19.10.12
[R7]	FMEDA_V8_Trimod_C01C05_Micro_Standard_V0R2.efm of 18.10.12
[R8]	Summary_V1R0.xls of 24.10.12
[R9]	Hinweis.docx of 24.10.12

3 Description of the analyzed device

The Trimod Besta Level Switches are considered to be Type A elements with a hardware fault tolerance of 0.

The considered switches are equipped with micro switches or proximity switches and are also available in explosion proof versions according to ATEX/IECEx.

The modular design (see Figure 1) allows individual combinations of float, flange and switch modules. Switch housings are standard IP65 enclosure, but depending on environmental conditions IP67 or IP68 are also available. For hazardous areas, hermetically sealed micro switches or flameproof housings can be used.

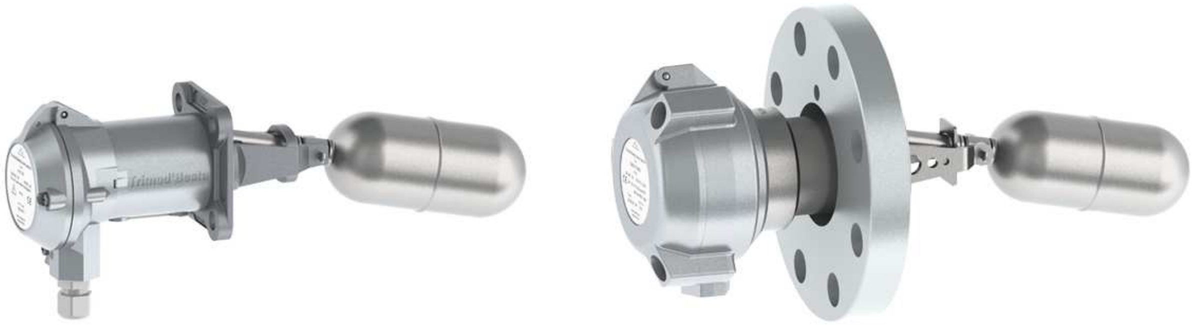

Figure 1: Modular level switch system

Figure 2 shows some possible applications. Further applications are described in detail in [D1].

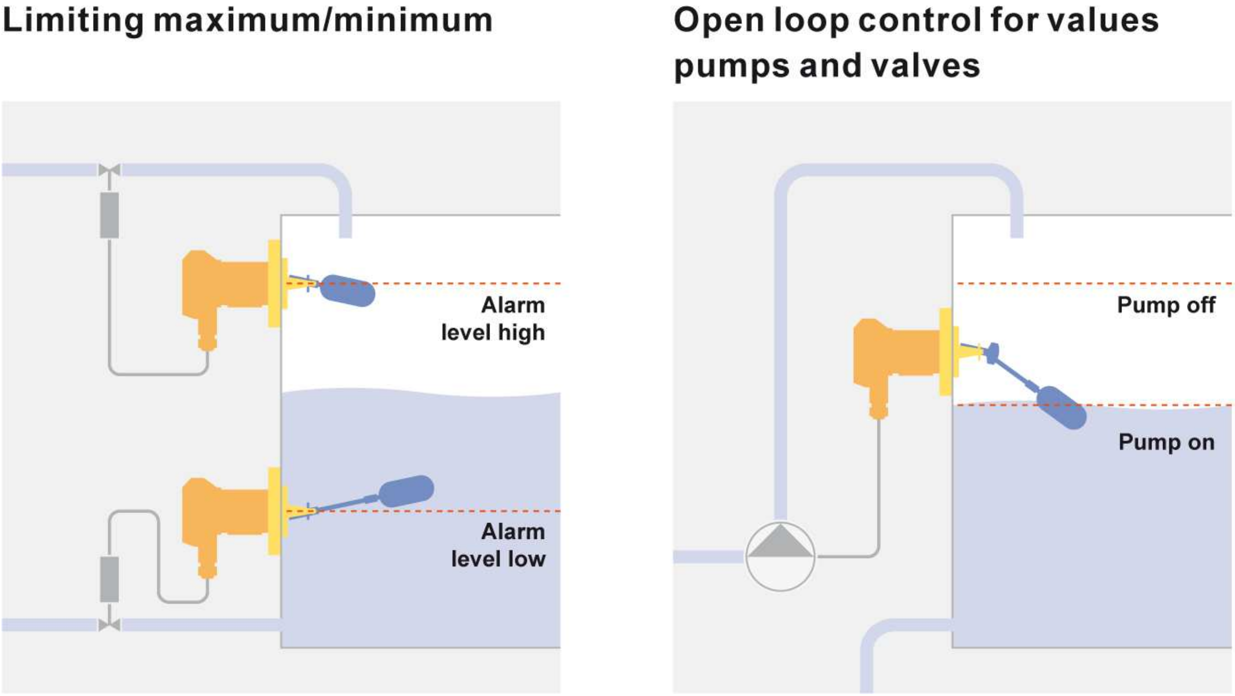

Figure 2: Application examples

4 Failure Modes, Effects, and Diagnostics Analysis

The mechanical Failure Modes, Effects, and Diagnostic Analysis was done by *exida*. The results are documented in [R1] to [R7]. The effect of the failure modes were analyzed theoretically. Due to the simplicity of the design, no practical fault insertion tests were deemed to be necessary. The analysis 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 Trimod Besta Level Switches, the following definitions for the failure of the device were considered.

Fail-Safe State
The fail-safe state is defined as the output being de-energized.

Fail Safe
A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

Fail Dangerous
A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,

b) decreases the probability that the safety function operates correctly when required.

Annunciation
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).

No effect
Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.

No part
Component that plays no part in implementing the safety function but is listed for completeness.

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 in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension 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 a proprietary mechanical component failure rate database derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. 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 *exida* Profile 3 data. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.
For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

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 such as *exida* SILStat^{TM} 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.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Trimod Besta Level Switches.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions and process fluids.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- All devices are operated in the low demand mode of operation.
- Only the described configurations are used for safety applications.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The devices are installed per the manufacturer's instructions.
- The redundant switches / inductive sensors are connected in such a way that each of them is able to bring the element into a safe state.
- The optional test actuator does not influence the safety function.
- The optional float chamber does not influence the safety function.
- The stress levels are average for an industrial outdoor environment and can be compared to *exida* Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.

4.3 Results

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

$\lambda_{\text{total}} = \lambda_{\text{safe}} + \lambda_{\text{dangerous}}$

SFF = $1 - \lambda_{\text{dangerous}} / \lambda_{\text{total}}$

4.3.1 Trimod Besta Level Switches in version [V1]

The FMEDA carried out on the Trimod Besta Level Switches in version [V1] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	***exida* Profile 3 [FIT]**
Fail Safe (λ_{Safe})	**81**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**139**

No effect	131
No part	50
Fail Annunciation Undetected (λ_{AU})	0

Total failure rate of the safety function (λ_{Total})	**220**

Safe failure fraction (SFF)	**36%**

SIL AC [6]	**SIL1**

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.2 Trimod Besta Level Switches in version [V2]

The FMEDA carried out on the Trimod Besta Level Switches in version [V2] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	*exida* Profile 3 [FIT]
Fail Safe (λ_{Safe})	**157**
Fail Dangerous Detected (λ_{DD}) [7]	**136**
Fail Dangerous Detected (λ_{dd})	68
Fail Annunciation Detected (λ_{AD})	68
Fail Dangerous Undetected (λ_{DU})	**71**

No effect	142
No part	50
Fail Annunciation Undetected (λ_{AU}) [8]	8

Total failure rate of the safety function (λ_{Total})	**364**

Safe failure fraction (SFF)	**80%**

SIL AC [9]	**SIL2**

[7] The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch / sensor is considered to be a safety measure for the primary switch / sensor providing a DC of 90% by considering a common cause factor of 10%.

[8] The AU failures result from the fact that the redundant switch / sensor is considered to be a safety measure and therefore is contributing to the "annunciation" failure category.

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.3 Trimod Besta Level Switches in version [V3]

The FMEDA carried out on the Trimod Besta Level Switches in version [V3] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	***exida* Profile 3 [FIT]**
Fail Safe (λ_{Safe})	**20**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**97**

No effect	123
No part	50
Fail Annunciation Undetected (λ_{AU})	0

Total failure rate of the safety function (λ_{Total})	**117**

Safe failure fraction (SFF)	**16%**

SIL AC [10]	**SIL1**

[10] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.4 Trimod Besta Level Switches in version [V4]

The FMEDA carried out on the Trimod Besta Level Switches in version [V4] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	*exida* Profile 3 [FIT]
Fail Safe (λ_{Safe})	**35**
Fail Dangerous Detected (λ_{DD}) [11]	**20**
Fail Dangerous Detected (λ_{dd})	10
Fail Annunciation Detected (λ_{AD})	10
Fail Dangerous Undetected (λ_{DU})	**87**

No effect	133
No part	50
Fail Annunciation Undetected (λ_{AU}) [12]	1

Total failure rate of the safety function (λ_{Total})	**142**

Safe failure fraction (SFF)	**38%**

SIL AC [13]	**SIL1**

[11] The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch / sensor is considered to be a safety measure for the primary switch / sensor providing a DC of 90% by considering a common cause factor of 10%.

[12] The AU failures result from the fact that the redundant switch / sensor is considered to be a safety measure and therefore is contributing to the "annunciation" failure category.

[13] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.5 Trimod Besta Level Switches in version [V5]

The FMEDA carried out on the Trimod Besta Level Switches in version [V5] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	*exida* Profile 3 [FIT]
Fail Safe (λ_{Safe})	**81**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**161**

No effect	140
No part	50
Fail Annunciation Undetected (λ_{AU})	0

Total failure rate of the safety function (λ_{Total})	**242**

Safe failure fraction (SFF)	**33%**

SIL AC [14]	**SIL1**

[14] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.6 Trimod Besta Level Switches in version [V6]

The FMEDA carried out on the Trimod Besta Level Switches in version [V6] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	*exida* Profile 3 [FIT]
Fail Safe (λ_{Safe})	**157**
Fail Dangerous Detected (λ_{DD}) [15]	**136**
Fail Dangerous Detected (λ_{dd})	68
Fail Annunciation Detected (λ_{AD})	68
Fail Dangerous Undetected (λ_{DU})	**93**

No effect	151
No part	50
Fail Annunciation Undetected (λ_{AU}) [16]	8

Total failure rate of the safety function (λ_{Total})	**386**

Safe failure fraction (SFF)	**75%**

SIL AC [17]	**SIL2**

[15] The device does not contain any internal diagnostics. The DD failures result from the fact that the redundant switch / sensor is considered to be a safety measure for the primary switch / sensor providing a DC of 90% by considering a common cause factor of 10%.

[16] The AU failures result from the fact that the redundant switch / sensor is considered to be a safety measure and therefore is contributing to the "annunciation" failure category.

[17] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

4.3.7 Trimod Besta Level Switches in version [V7]

The FMEDA carried out on the Trimod Besta Level Switches in version [V7] leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates:

Failure category	*exida* Profile 3 [FIT]
Fail Safe (λ_{Safe})	**76**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**128**

No effect	88
No part	50
Fail Annunciation Undetected (λ_{AU})	0

Total failure rate of the safety function (λ_{Total})	**204**

Safe failure fraction (SFF)	**37%**

SIL AC [18]	**SIL1**

[18] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

5 Using the FMEDA results

5.1 Example PFD$_{AVG}$ calculation

The following section describes how to apply the results of the FMEDA.

An average Probability of Failure on Demand (PFD$_{AVG}$) calculation is performed for a single (1oo1) Trimod Besta Level Switch with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in sections 4.3.1 to 0. A mission time of 10 years, a proof test coverage of 90% (see appendix 1.1), a Mean Time To Restoration of 24 hours and a maintenance capability of 100% have been assumed. Table 3 lists the results when the proof test interval equals 1 year.

For SIL1 applications, the PFD$_{AVG}$ value for the entire safety function needs to be < 1.00E-01.

For SIL2 applications, the PFD$_{AVG}$ value for the entire safety function needs to be < 1.00E-02.

Table 3: Sample PFD$_{AVG}$ results

Configuration	PFD$_{AVG}$	% of SIL2 range
[V1]	1.16E-03	12%
[V2]	5.98E-04	6%
[V3]	8.06E-04	8%
[V4]	7.25E-04	7%
[V5]	1.34E-03	13%
[V6]	7.81E-04	8%
[V7]	1.07E-03	11%

The resulting PFD$_{AVG}$ graph for [V5] generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 3.

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The results must be considered in combination with PFD$_{AVG}$ values of other devices of a Safety Instrumented Function in order to determine suitability for a specific Safety Integrity Level.

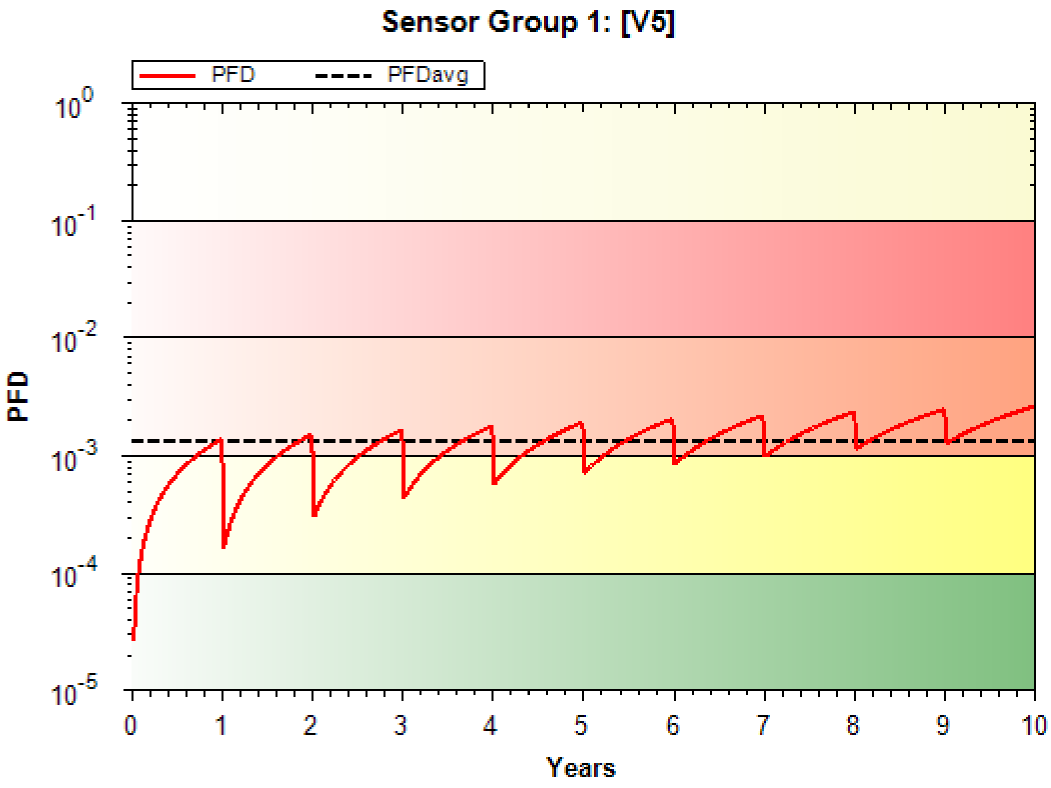

Figure 3: PFD$_{\text{AVG}}$ value for [V5] with proof test interval of 1 year

6 Terms and Definitions

FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
MTTR	Mean Time to Restoration
PFD_{AVG}	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
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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 History:	V1R1:	Missing devices IE9, XIE9, IIE9 added, January 23, 2013
	V1R0:	Review comments incorporated; November 5, 2012
	V0R1:	Initial version; October 24, 2012
Authors:	Stephan Aschenbrenner	
Review:	V0R1:	Steven F. Close (*exida*); November 6, 2012
		Vladimiro Imhof (Besta); October 30, 2012
Release status:	Released to Besta Ltd. as part of a full IEC 61508 assessment	

7.3 Release Signatures

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

Steven F Close

Steven F. Close, Senior Safety Engineer

Appendix 1: Possibilities to reveal dangerous faults during the proof test

According to section 7.4.5.2 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.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 4.

Table 4 Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Inspect the device for any visible damage, corrosion or contamination.
3	Force the device to reach a defined “MAX” threshold value and verify that the output goes into the safe state.
4	Force the device to reach a defined “MIN” threshold value and verify that the output goes into the safe state.
5	Restore the loop to full operation
6	Remove the bypass from the safety PLC or otherwise restore normal operation

It is assumed that this test achieves a proof test coverage (PTC) of at least 90%.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 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 4.2.3) this only applies provided that the useful lifetime[19] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions.

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

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

Table 5 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 5: Useful lifetime of components with reduced useful lifetime contributing to λ_{du}

Type	Useful life
Mechanical parts	Approximately 10 years

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

[19] 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 3: Description of the considered profiles

Appendix 3.1: *exida* mechanical database

Profile	Profile according to IEC60654-1	Ambient Temperature [°C]		Temperature Cycle [°C / 365 days]
		Average (external)	Mean (inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25
4	D1	25	30	35

PROFILE 1:

Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

PROFILE 2:

Mechanical field products have minimal self-heating and are subjected to daily temperature swings.

PROFILE 3:

Mechanical field products may have moderate self-heating and are subjected to daily temperature swings.

PROFILE 4:

Unprotected mechanical field products with minimal self-heating, are subject to daily temperature swings and rain or condensation.