



Failure Modes, Effects and Diagnostic Analysis

Project:
Beacon YL60, FL60

Company:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 12/07-123
Report No.: STAHL 12/07-123 R026
Version V1, Revision R0; November 2013
Jan Hettenbach

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Beacon YL60, FL60 in the version listed in the drawings referenced in section 2.4.1.

The hardware 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) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) 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. These failure rates are valid for the useful lifetime of the Beacon YL60, FL60, see Appendix B.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.3.

The Beacon YL60 consists of two different signal sources, a strobe and a sounder. Both are independent and redundant to each other. The strobe can be considered to be a Type A¹ element with a hardware fault tolerance of 0. The sounder can be configured to different sound signals and can be considered as a Type B² element with a hardware fault tolerance of 0. Because of the different types of sound, e.g. one sound is a warning signal and the other sound is an emergency signal, a clear safe state cannot be defined because of potential misinterpretation of the sound types. Thereby, the sounder is **not** part of this FMEDA report. The failure rates according to IEC 61508:2010 for the Beacon YL60 are listed in Table 3.

The Flash light FL60 has the same internal circuit as Beacon YL60, but no sound generation unit. The failure rates are thereby identical to YL60.

The Beacon YL60, FL60 is available in different configurations which have no influence on the FMEDA results. The covered versions are listed in Table 1 and Table 2.

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 Type B element: "Complex" element (using micro controllers or programmable logic); for details details see 7.4.4.1.3 of IEC 61508-2.

Table 1: Covered types of Beacon YL60

Sounder / Strobe	YL 60 /	a	/	b	/	c	/	d	/	e
Gas Group										
Different gas groups	B / C									
Rated operational voltage + flash energy										
24 V DC / 5 Joule	D50									
48 V DC / 5 Joule	F50									
115 V AC / 5 Joule	L50									
230 V AC / 5 Joule	N50									
Lens colour										
Different lens colours	*									
Certification										
Different Regions	*									
Additions^{*1}										
Different Additions	*									

Table 2: Covered types of Flash light FL60

Strobe	FL 60 /	a	/	b	c	/	d	/	e	/	f
Gas Group											
Different gas groups	B / C										
Rated operational voltage											
24 V DC	D										
48 V DC	F										
115 V AC	L										
230 V AC	N										
flash energy											
5 Joule	50										
10 Joule	100										
20 Joule	200										
Lens colour											
Different lens colours	*										
Certification											
Different Regions	*										
Additions^{*1}											
Different Additions	*										

Table 3: Failure rates of Beacon YL60, FL60

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	13
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Undetected (λ_{DU})	217
No effect	57
No part	0
Total failure rate (safety function)	230
Safe failure fraction (SFF)³	5%
SIL AC⁴	SIL1

³ The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴ 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table of Contents

Management Summary	2
1 Purpose and Scope.....	6
2 Project Management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards and Literature used	7
2.4 Reference documents	8
2.4.1 Documentation provided by the customer	8
2.4.2 Documentation generated by <i>exida</i>	8
2.5 <i>exida</i> tools used	8
3 Product Description.....	9
4 Failure Modes, Effects, and Diagnostic Analysis.....	10
4.1 Description of the failure categories	10
4.2 Methodology – FMEDA, Failure Rates	11
4.2.1 FMEDA	11
4.2.2 Failure Rates	11
4.2.3 Assumptions	12
4.3 Results of the assessment	13
4.3.1 Failure rates of Beacon YL60, FL60	14
5 Using the FMEDA Results	15
5.1 Example PFD _{AVG} calculation.....	15
6 Terms and Definitions	16
7 Status of the Document.....	17
7.1 Liability.....	17
7.2 Releases.....	17
7.3 Release Signatures	17
Appendix A: Possibilities to reveal dangerous undetected faults during the proof test..	18
Appendix A.1: Possible proof tests to detect dangerous undetected faults	18
Appendix B: Impact of lifetime of critical components on the failure rate.....	19
Appendix C: <i>exida</i> Environmental Profiles	20

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Beacon YL60, FL60. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The FMEDA builds the basis for an evaluation whether the final element Beacon YL60, FL60 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	d7360-4 (WD9550).pdf	Schematic diagram of 18.11.2011
[D2]	YL60_Sounder_EK00_III_en.pdf	Product description YL60
[D3]	YL60 24Vdc PCB Assembly.pdf	Bill of material of YL60

2.4.2 Documentation generated by *exida*

[R1]	PFDavg Calc YL60.xls of 07.11.2012
[R2]	YL60-beacon.efm of 07.11.2012
[R3]	YL60-sounder.efm of 06.11.2012

2.5 *exida* tools used

[T1]	SILcal V7	FMEDA Tool
------	-----------	------------

3 Product Description

The strobe part of the Beacon YL60, FL60 can be considered as a Type A⁵ element according to IEC 61508, having a hardware fault tolerance of 0.

A signal from a control logic enables the strobe and the sounder of the Beacon YL60, FL60. The sound can be configured. Two different sounds are configurable and can be activated by the control logic by changing the polarity of the control signal.

Figure 2 shows the connection diagram of the Beacon YL60, FL60. Several YL60 or FL60 can be connected in series and activated by one control line.



Figure 1: Product picture of Beacon YL60, FL60

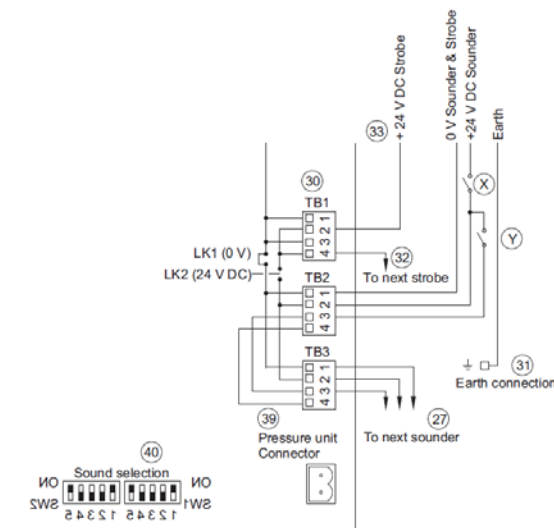


Figure 2: Connection diagram of Beacon YL60, FL60

⁵ Type A element: “Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* and supported by R. STAHL Schaltgeräte GmbH. The results are documented in [R2] and [R3].

4.1 Description of the failure categories

In order to judge the failure behavior of the Beacon YL60, FL60, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the strobe flashes without any control signal, with wrong frequency (any higher or more than half the frequency) or at least more than the half flash intensity.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: <ul style="list-style-type: none">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: <ul style="list-style-type: none">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.
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.
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). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.
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 part of the circuit diagram and 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 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 Electrical [N3] and Mechanical [N4] Component Reliability Handbook which was 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 4. 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 or physical abuse.

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™ 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 Beacon YL60, FL60.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- 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.
- All devices are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described variants are considered.
- Only the strobe part of the Beacon YL60, FL60 was considered in the FMEDA.
- The sounder can be considered as Type B⁶ element and is not part of this FMEDA report.

⁶ Type B element: "Complex" element (using micro controllers or programmable logic); for details details see 7.4.4.1.3 of IEC 61508-2.

4.3 Results of the assessment

$$DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$$

$$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

$$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{AU})) + 24\ h$$

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-3.

This assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$$SFF = (\sum \lambda_S\ avg + \sum \lambda_{DD}\ avg) / (\sum \lambda_S\ avg + \sum \lambda_{DD}\ avg + \sum \lambda_{DU}\ avg)$$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$$SFF = (\sum \lambda_S + \sum \lambda_{DD}) / (\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU})$$

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

4.3.1 Failure rates of Beacon YL60, FL60 ⁷

The FMEDA carried out on the strobe part of Beacon YL60, FL60 leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates:

Table 4: Strobe part of Beacon YL60, FL60

	<i>exida</i> Profile 1
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	13
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Undetected (λ_{DU})	217
No effect	57
No part	0
Total failure rate (safety function)	230
Safe failure fraction (SFF) ⁸	5%
SIL AC⁹	SIL1

⁷ FMEDA results are only valid for the strobe part. The sounder part of the YL60 does not fulfill SIL1 requirements.

⁸ The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

5 Using the FMEDA Results

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

5.1 Example PFD_{AVG} calculation

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 following 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).

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for Beacon YL60, FL60 considering a proof test coverage of 90% (see Appendix A.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in sections [R1]. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 5.

For SIL2 applications, the PFD_{AVG} value needs to be $< 1.00E-02$.

Table 5: PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
YL60	$PFD_{AVG} = 1.87E-03$	$PFD_{AVG} = 2.66E-03$	$PFD_{AVG} = 5.22E-03$

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval considering is approximately equal to 18.7%.

Figure 3 shows the time dependent curve of PFD_{AVG} .

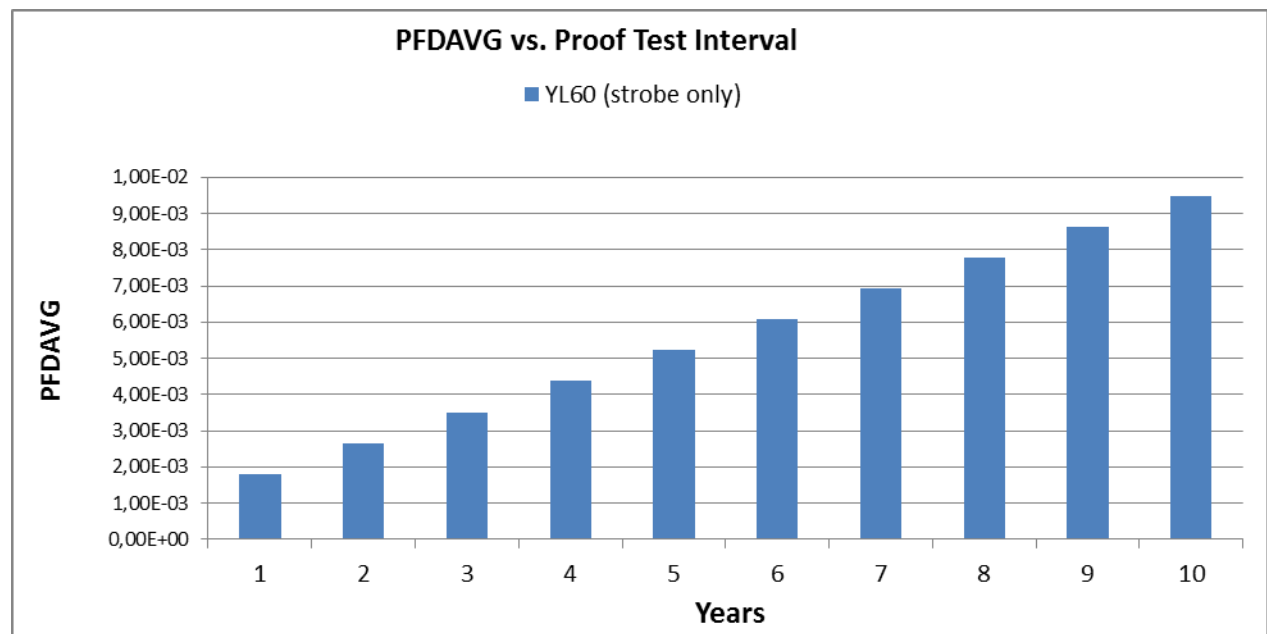


Figure 3: $PFD_{AVG}(t)$ for Beacon YL60, FL60

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.
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
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).
PLC	Programmable Logic Controller
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
Type B element	“Complex” element (all failure modes are well defined); for details see 7.4.4.1.3 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 History: V1R0: Editorial changes, FL60 added, November 26, 2013

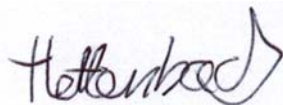
V0R1: Initial draft; August 21, 2013

Author: Jan Hettenbach

Review: V1R0: Stephan Aschenbrenner,
Andreas Bagus (R. STAHL Schaltgeräte GmbH)

Release Status: V1R0 Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures



Dipl. -Ing. (Univ.) Jan Hettenbach



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

Appendix A: Possibilities to reveal dangerous undetected 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 A shall be considered when writing the safety manual as it contains important safety related information.

Appendix A.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 6. It is assumed that this test will detect 99% of possible dangerous failures.

Table 6: Steps for proof test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Apply a control signal at the Beacon YL60, FL60.
3.	Check correct work of Beacon YL60, FL60 as flash rate and flash intensity.
4.	Remove the bypass from the safety PLC or otherwise restore normal operation.

Appendix B: 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 lifetime¹⁰ 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 – temperature in particular (for example, electrolyte capacitors can be very sensitive).

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 7 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 7: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life
Capacitor (electrolytic-liquid) - Aluminum	C2, C3, C4	90 000 hours ¹¹
Flash lamp	LP1	More than 10 years

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

¹⁰ 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.

¹¹ The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.

Appendix C: *exida* Environmental Profiles

Table 8 *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted	General Field Mounted	Subsea	Offshore	N/A
		no self-heating	self-heating			
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3	C3	N/A	C3	N/A
		also applicable for D1	also applicable for D1		also applicable for D1	
Average Ambient Temperature	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity¹²	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock¹³	10 g	15 g	15 g	15 g	15 g	N/A
Vibration¹⁴	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion¹⁵	G2	G3	G3	G3	G3	Compatible Material
Surge¹⁶						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility¹⁷						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)¹⁸	6kV	6kV	6kV	6kV	6kV	N/A

¹² Humidity rating per IEC 60068-2-3

¹³ Shock rating per IEC 60068-2-6

¹⁴ Vibration rating per IEC 60770-1

¹⁵ Chemical Corrosion rating per ISA 71.04

¹⁶ Surge rating per IEC 61000-4-5

¹⁷ EMI Susceptibility rating per IEC 6100-4-3

¹⁸ ESD (Air) rating per IEC 61000-4-2