Failure Modes, Effects and Diagnostic Analysis

Project:
Surge Protective Devices D9024S

Customer:
G.M. International s.r.l
Villasanta
Italy

Contract No.: GM 16/02-055
Report No.: GM 16/02-055 R006
Version V1, Revision R0; July 2016

Jürgen Hochhaus

Management summary

This report summarizes the results of the hardware assessment carried out on the D9024S with hardware version as listed in the drawings referenced in section 2.5.1. Table 1 the considered D9024S.

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.

Table 1: Description of the considered D9024S

D9024S	Two-stage surge protection for one floating Ex ia signal circuit

Only the described variants and configurations were analyzed. All other possible variants, configurations or electronics are not covered by this report.

Surge protective devices are not considered to be elements according to IEC 61508-4 section 3.4.5 as they are not performing one or more element safety functions. Therefore, there is no need to calculate a SFF (Safe Failure Fraction). Only the interference on a safety functions needs to be considered. This interference is expressed in a contribution to the overall PFD_{AVG} / PFH.

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

The following table show how the above stated requirements are fulfilled for the D9024S.

[1] See Appendix 3 for further details on the selected profile.

Table 2: Summary for D9024S – Failure rates [2]

	exida Profile 1	
	Analysis 1 [3]	**Analysis 2 [4]**
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3.6**	**3.6**
Fail Dangerous Detected (λ_{DD})	**0**	**6**
Fail Dangerous Undetected (λ_{DU})	**6.8**	**0.8**
No effect	57	57
No part	0	0
Total failure rate (interfering with safety function)	**10.4 FIT**	**10.4 FIT**
MTBF	**1684 years**	**1684 years**

The failure rates are valid for the useful life of the D9024S (see Appendix 2).

[2] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.
[3] Analysis 1 represents a worst-case analysis.
[4] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the D9024S with hardware version as listed in the drawings referenced in section 2.5.1.
The FMEDA builds the basis for an evaluation whether an element including the described D9024S meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) 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 or the correct functioning of the Surge Protective Devices.

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

G.M. International s.r.l	Supplier of the D9024S.
exida	Performed the hardware assessment.

G.M. International s.r.l contracted *exida* in February 2016 with creation of this report.

2.3 Standards / Literature used

The services delivered by *exida* 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 Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	EMCR Handbook, 2011 Update	exida LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update

2.4 *exida* tools used

[T1]	SILcal V8.0.12	FMEDA Tool
[T2]	exSILentia Ultimate V3.3.0.906	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	Schaltplan BT_TT-EX(I)-M-24DC.pdf	Circuit diagram 96 61 082 "BT.TT-M-EX(I)-24DC" Rev 01 of 17.10.07
[D2]	Kurzbeschreibung TT-XX-M-24DC.pdf	Short description of TT-*-M-24DC
[D3]	GM Int Declaration of Identity 2016_07_08.pdf	Product identity declaration from the manufacturer, 8.7.2016
[D4]	Product identity declaration D9024S signed.pdf	Product identity declaration from the supplier, 19.7.2016

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.

2.5.2 Documentation generated by the manufacturer and *exida*

[R1]	FMEDA_V8_TT-xx-M-24DC_V1R0.efm of 23.04.12
[R2]	FMEDA_V8_TT-xx-M-24DC_w_ED_V1R0.efm of 23.04.12

3 Description of the analyzed subsystems

The FMEDA of the surge protective devices D9024S has been carried out on the parts indicated in Figure 1.

The surge protective device D9024S is a modular terminal block with two-stage surge protection for one floating Ex ia signal circuit, disconnect knife on both signal paths, separate ground connection, nominal voltage: 24 VDC.

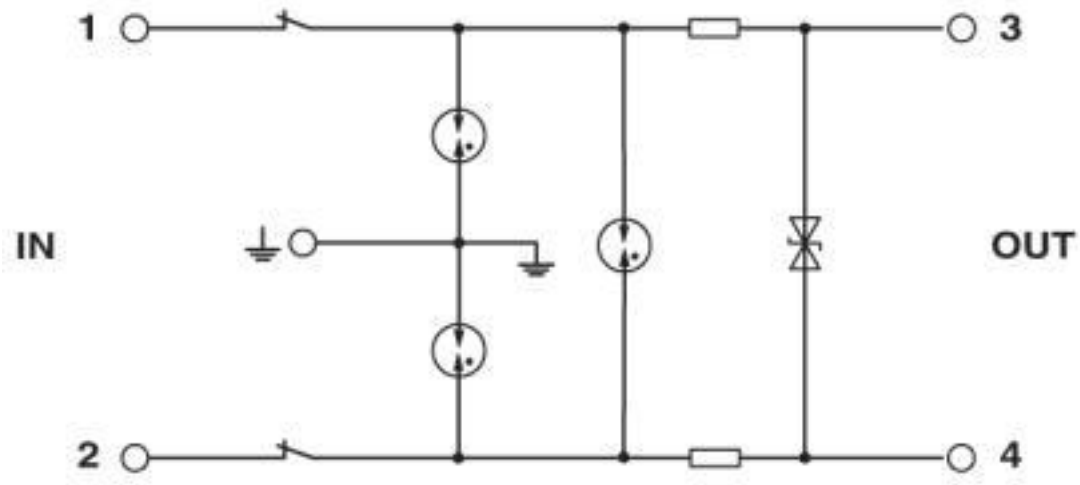


Figure 1: Block diagram of the surge protective device D9024S

The following two figures Figure 2 and Figure 3 show how the surge protective devices can be connected to other devices. All considered surge protective devices can be used with analog or binary devices.

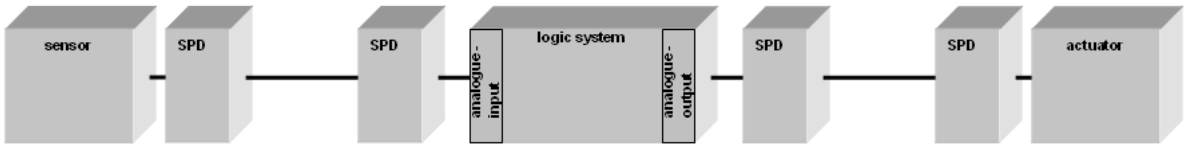


Figure 2: Connection with analog devices

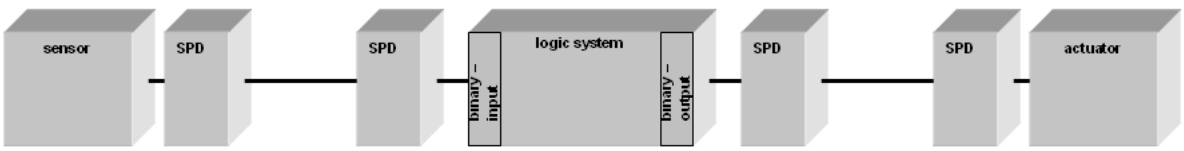


Figure 3: Connection with binary devices

Figure 4 shows how faults of the surge protective devices on the actuator side can be detected. On the sensor side faults can be detected by the safety PLC via an out of range check as the input signal will be outside the allowed range of 4-20mA or 2-10V in case of line short circuits and short circuits to GND.

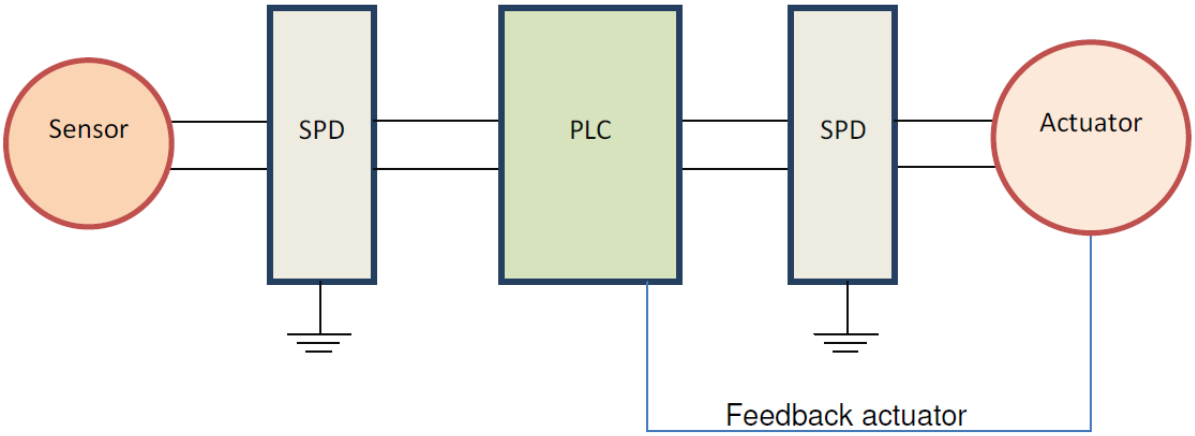


Figure 4: Connection for fault detection

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with the manufacturer of D9024S, G.M. International s.r.l, and is documented in [R1] and [R2].

4.1 Description of the failure categories

In order to judge the failure behavior of the D9024S, the following definitions for the failure of the products were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized or reaching the user defined threshold value or the predefined alarm state.
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.
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.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).
Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (DD).
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 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 the Electrical and Mechanical Component Reliability Handbook [N2] and [N3] 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 2 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the D9024S.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- The device is used within its specified limits.
- 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.
- For safety applications only the described configurations are considered.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.

4.4 Results

For the calculation the following has to be noted:

λ_{total} consists of the sum of all component failure rates. This means:

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

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

4.4.1 D9024S

The FMEDA carried out on the Surge Protection Device D9024S under the assumptions described in section 4.3 and the definitions given in section 4.1 leads to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [5]	**Analysis 2 [6]**
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3.6**	**3.6**
Fail Dangerous Detected (λ_{DD})	**0**	**6**
Fail Dangerous Undetected (λ_{DU})	**6.8**	**0.8**
No effect	57	57
No part	0	0
Total failure rate (interfering with safety function)	**10.4 FIT**	**10.4 FIT**
MTBF	**1684 years**	**1684 years**

[5] Analysis 1 represents a worst-case analysis.
[6] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

5 Using the FMEDA results

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 section describes how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

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 a single (1oo1) D9024S with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.4.1. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 3 lists the results for different proof test intervals considering a proof test coverage of 99% (see Appendix 1.1).

For SIL3 the overall PFD_{AVG} shall be better than 1.00E-03 and the PFH shall be better than 1.00-E07 1/h. As the surge protective devices (according to analysis 2) are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 5% of this range as a reasonable budget they should be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively. The calculated PFD_{AVG} / PFH values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 5% of the allowed range, i.e. to be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively.

Table 3: PFD_{AVG} / PFH values

T[Proof] = 1 year	T[Proof] = 5 years	PFH
PFD_{AVG} = 3.87E-06	PFD_{AVG} = 1.74E-05	PFH = 7.81E-10 1/h

The resulting PFD_{AVG} graphs generated from the exSILentia tool for a proof test of 1 year are displayed in Figure 5.

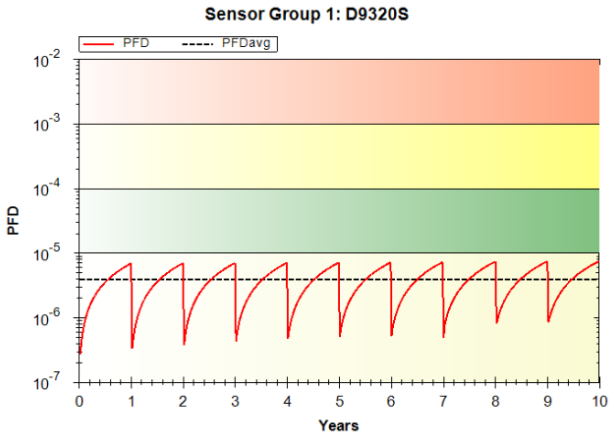


Figure 5: $PFD_{AVG}(t)$

6 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, 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 one per year and no greater than twice the proof test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTBF	Mean Time Between Failure
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
SPD	Surge Protective Device
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.

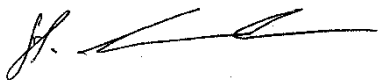
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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:	V1R0:	Released version; corrected device name; extended documents list, July 21, 2016
	V0R2:	Included review results; July 16, 2016
	V0R1:	Initial version; July 8, 2016
Author:	Jürgen Hochhaus	
Review:	V0R1:	Stephan Aschenbrenner (*exida*); July 5, 2016
Release status:	V0R2	Roberto Zilio, (G.M. International s.r.l); July 19, 2016

7.3 Release Signatures



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

Dipl.-Ing. (FH) Jürgen Hochhaus, Senior Safety engineer

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

Appendix 1.1: Proof test to detect dangerous undetected faults

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

Table 4 Steps for a possible proof Test

Step	Action
1	Bypass the connected safety device(s) or take other appropriate action to avoid a false trip
2	Force the D9024Sto reach predefined output signals over the entire range and verify that the output behaves as expected.
3	Restore the loop to full operation
4	Remove the bypass from the connected safety device(s) or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures of the D9024S.

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

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 section4.3) this only applies provided that the useful lifetime[7] 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, electrolytic 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 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.

The surge protective devices D9024S do not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation. Therefore there is no limiting factor to the useful lifetime.

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

[7] 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: *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
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
Humidity[8]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[9]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[10]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[11]	G2	G3	G3	G3	G3	Compatible Material
Surge[12]						
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 Susceptibility[13]						
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)[14]	6kV	6kV	6kV	6kV	6kV	N/A

[8] Humidity rating per IEC 60068-2-3
[9] Shock rating per IEC 60068-2-27
[10] Vibration rating per IEC 60068-2-6
[11] Chemical Corrosion rating per ISA 71.04
[12] Surge rating per IEC 61000-4-5
[13] EMI Susceptibility rating per IEC 6100-4-3
[14] ESD (Air) rating per IEC 61000-4-2