





Italia

Add value.

Inspire trust.

OFFICIAL REPORT	R TUV IT 22 SIL 0084 REV.1
ANTIWEAR (SUZHOU) INDUSTRIAL INTELLIGENT TECHNOLOGY CO., LTD.	
TECHNICAL REPORT FOR SIL CLASSIFICATION ACCORDING TO STANDARD IEC 61508:2010 FOR IDD SERIES LIMIT SWITCHES	
Location Sesto San Giovanni	TÜV ITALIA Srl 
Date July, 11 th 2022	
Prepared by Industrie Service Division Engineer 	
Francesco Zadra	

TÜV ITALIA S.R.L.
TÜV SÜD Group

Telefono: +39 02 24130.1
Telefax: +39 02 24130.399

Direzione e Sede Amministrativa:
Via Giosuè Carducci, 125 edificio 23
20099 Sesto San Giovanni (MI)
Sede legale: Via Mauro Macchi, 27 20124 Milano
Società Unipersonale,
soggetta al controllo e al coordinamento di
TÜV SÜD AG

www.tuv.it

Registro delle imprese di Milano
n. iscrizione e Cod. Fisc. 08922920155
R.E.A.: 1255140 - P. IVA 02055510966
Cod. Identificazione CEE IT 02055510966
Capitale sociale : Euro 500.000 int. Vers.

TÜV®

SUMMARY

The aim of the study described in the present document consists in the analysis of the reliability and architectural/functional characteristics of IDD Series Limit Switches produced by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. The results are summarized in the following table:

Table 1 – SIL classification according to Standard IEC EN 61508 for IDD Series Limit Switches produced by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd.

<i>E/EE/EP safety-related system (final element)</i>	IDD Series Limit Switches produced by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd.
System type	Type A
Systematic Capability	SC3
Safety Function Definition	“Correct switching on demand (open to closed / closed to open), in low demand mode of operation”
Max SIL⁽¹⁾	SIL3
λ_{TOT}	7,699E-09
λ_{NE}	0,000E+00
λ_s	0,000E+00
$\lambda_{DD,PST}^{(2)}$	0,000E+00
$\lambda_{DU,FPT}$	7,699E-09
β and β_D factor	10%
MRT	8 h
Hardware Safety Integrity	Route 2 _H
Systematic Safety Integrity	Route 2 _s
Remarks (1) The Safety Integrity Level (SIL) of the entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} and/or PFH_d considering the redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with the minimum hardware fault tolerance (HFT) requirements. (2) Considering an automatic Partial Stroke Test.	

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

REVISIONS

Revision	Date	Description
0	08/07/2022	Draft
1	11/07/2022	Official

ABBREVIATIONS AND SYMBOLS

CCF	Common Cause Failure
DC	Diagnostic Coverage
DD	Dangerous Detectable
DU	Dangerous Undetectable
DD,PST	Dangerous Detectable by means of Partial Stroke Test
DU,FPT	Dangerous Undetectable, detectable by means of Full Proof Test
NE	No Effect
E/E/EP	Electrical, Electronic, Programmable Electronic
FMEDA	Failure Modes Effects and Diagnostic Analysis
FPT	Full Proof Test
PFD	Probability of Failure per Demand
PST	Partial Stroke Test
HFT	Hardware Fault Tolerance
SD	Safe Detectable
SIF	Safety Instrumented Function
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SU	Safe Undetectable

REFERENCES

- [1] International Standard IEC EN 61508:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1, 2, 3, 4, 5, 6, 7

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

INDEX

1	INTRODUCTION AND AIM OF THE STUDY	6
2	IEC 61508 PROBABILISTIC AND ARCHITECTURAL REQUIREMENTS	8
2.1	Hardware safety integrity requirements	8
2.1.1	Architectural constraints	8
2.1.2	Random hardware failure requirements	8
2.2	Systematic safety integrity requirements	9
2.3	Probabilistic requirements	9
2.4	Architectural/functional requirements	10
2.5	Additional discussion about the concept of “detection” and related issues	10
3	SYSTEM DESCRIPTION	11
3.1	IDD Series Limit Switches	11
3.2	Specific safety function subjected to SIL classification	12
4	ANALYSIS OF THE SYSTEM ACCORDING TO THE STANDARD IEC EN 61508	13
4.1	Estimation of reliability data	13
4.1.1	Failure rate and PFD estimation by means of functional/fatigue tests	14
4.1.2	Failure rate and PFD estimation by means of data from the field	15
4.2	Architectural/functional analysis	17
4.2.1	FMEDA Analysis	17
4.2.2	Mean Repair Time	18
4.2.3	Common Cause Failure	19
4.2.4	Hardware Fault Tolerance	19
4.3	Systematic safety integrity requirements	20
4.4	SIL classification of the system	21
5	CONCLUSIONS	22
6	DISCLAIMER	22

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official



Italia

Page 5 of 22

ANNEX 1 – Safety Manual

ANNEX 2 – Safety Requirements Specification

ANNEX 3 – Field Data

ANNEX 4 – FMEDA

ANNEX 5 – Proven in Use Assessment

ANNEX 6 – Systematic Failures Analysis

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

1 INTRODUCTION AND AIM OF THE STUDY

The aim of the study described in the present document consists of the analysis of the reliability and architectural/functional characteristics of IDD Series Limit Switches produced by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. in order to:

- perform an accurate assessment of the maximum applicable SIL, according to Standard IEC 61508:2010 [1],
- support the related *Compliance Report to IEC EN 61508* (named TUV IT 22 SIL 0090) issued by TÜV Italia.

It is worth noticing that the Standards IEC EN 61508 foresees a methodological approach at level of complete Safety Life Cycle for the design, development, commissioning, operation & maintenance, and decommissioning of complete Safety Instrumented Systems (SISs) of E/E/EP type. In this perspective, it is important to remark that the present study:

- is restricted, in terms of battery limits, to a single and elementary component (a pump), anyway suitable for use as a Final Element in a Safety Instrumented System of E/E/EP type;
- is limited, in terms of phase of assessment, to the phase of validation of the maximum level of claimable SIL downstream the completion of the related design step (included as part of Phase 10 of IEC EN 61508).

In the following Table 2, the main data about the company Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. are showed:

Company	Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd.
Site	No. 988, Yuexiu Road, Fenhu Economic Development Zone, PC: 215200, Suzhou City, Jiangsu Province, P.R. China
Web Site	www.antiwearvalve.com
Certifications	ISO 9001:2015 cert with certificate no. 10455412 issued by LRQA with valid date 2024-12-03
Reliability field data collection	According to ISO9001

Table 2 - Main information about Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official



Italia

The document is structured according to the following sections:

- Chapter 2* Review of the requirements concerning the probabilistic and architectural/functional aspects reported in the Standard IEC EN 61508:2010.
- Chapter 3* Description of the systems object of the analysis and of the safety function which is evaluated for SIL.
- Chapter 4* Description of all steps of the analysis necessary for the evaluation of the reliability and architectural/functional parameters to classify the SIL.
- Chapter 5* Summary of the results with compliance declaration.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

2 IEC 61508 PROBABILISTIC AND ARCHITECTURAL REQUIREMENTS

The Standard IEC EN 61508 [1] reports a standard procedure of assessment and analysis aimed to verify and classify the safety features of E/E/EP systems (Electrical, Electronic and Programmable Electronic), introducing the SIL concept (Safety Integrity Level).

It is essential to underline that the SIL concept, according to Standard IEC EN 61508:2010, is not strictly and solely related to the system/sub-system/component, but to a specific Safety Instrumented Function (SIF) that the system/sub-system/component carries out.

The evaluation of the highest SIL that can be assigned to a system/sub-system/component, takes place throughout an accurate examination of the complete and correct compliance with both hardware safety integrity requirements and systematic safety integrity requirements.

2.1 Hardware safety integrity requirements

The Standard IEC 61508:2010 establishes for safety systems the hardware safety integrity requirements comprising the following:

- architectural constraints on hardware safety integrity,
- requirements for quantifying the effect of random failures.

2.1.1 Architectural constraints

The highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes:

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts;
- **Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.**

2.1.2 Random hardware failure requirements

For each safety function, a reliability prediction has to be performed using the appropriate techniques. The results shall be compared to the target failure measure.

The following aspects have to be considered in the analysis:

- The architecture
- The failure rates
- The common cause failures
- The diagnostic coverage of the diagnostic test,
- The proof tests interval and coverage,
- The repair time for detected failures,
- The effect of random human error,
- The modelling methods used.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

2.2 Systematic safety integrity requirements

The Standard IEC 61508:2010 establishes for safety systems the systematic safety integrity or systematic capability requirements which determines the potential for systematic faults of that element to lead to a failure of the safety function.

The requirements for systematic safety integrity can be met by achieving one of the following compliance routes:

Route 1_s: compliance with the requirements for the avoidance of systematic faults and the requirements for the control of systematic faults, or

Route 2_s: compliance with the requirements for evidence that the equipment is proven in use, or

Route 3_s (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12.

Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. provided the analysis of systematic failures for IDD Series Limit Switches according to the tables A15-A17 and B1-B5 of the Standard IEC 61508-2, attesting a Systematic Capability SC3.

2.3 Probabilistic requirements

The Standard IEC EN 61508:2010 establishes for safety systems the probabilistic requirements reported in the following table in order to classify the highest applicable SIL levels.

Table 3 – Safety Integrity Level: categories of probabilistic targets for E/E/PE safety systems operating either in “low demand mode” or “high demand or continuous mode”

SAFETY INTEGRITY LEVEL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

A safety system (or sub-system or component) is classified by the Standard IEC 61508 as:

- “*low demand mode*” type, when the expected intervention frequency is not higher than one operation per year, or anyway, not higher than the frequency of the inspection/proof tests foreseen for the system.
- “*high demand or continuous mode of operation*” type, when the operation mode is either continuous or discontinuous with expected frequencies higher than those characterising the prior category.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

2.4 Architectural/functional requirements

In order to support an effective design process of a safety system, the Standard IEC EN 61508 merges the above mentioned probabilistic requirements with the architectural/functional constraints, in order to consistently take into account the complexity level of the system too.

According to this approach (route 2H), a correct hardware safety integrity can be achieved as a function the "Hardware Fault Tolerance".

A system characterised by a Hardware Fault Tolerance equal to N means that N+1 contemporary failures must occur to trigger the loss of the safety function: therefore it is a parameter able to take into account the redundancy levels characterising the system under examination. By determining such parameter, any other measures that could prevent or mitigate the failure effect/effects must not be considered (i.e. diagnostics).

The Standard IEC EN 61508 moreover considers two system/sub-system categories: type A and type B.

A system/sub-system can be regarded as type A, whether the following requirements are fulfilled:

- all failure modes of all equipping components are well known;
- the behaviour of the system under faulty condition can be fully and comprehensively determined;
- there is a sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failure are met.

The subsystem is regarded as type B if not all of the criteria listed above are met. Typical examples of type A devices are switch, solenoids, and relays. Type B devices are microprocessor based or devices with complex custom logic.

2.5 Additional discussion about the concept of "detection" and related issues

Concerning the concept of "detection" and related issues, the following discussion can be made on the basis of the several, distributed and often not completely aligned definitions along the standard of reference:

- the Standard IEC EN 61508-4 (section 3.8.8) defines as "*detected*" any failure that can be revealed "*by diagnostic tests, but also proof tests, operator intervention (for example physical inspection and manual tests) or through normal operation*";
- no specific definition of "*diagnostic test*" is clearly reported in the standards, but it can be derived by definitions of "*diagnostic coverage*" (IEC 61508-4, section 3.8.6) and "*diagnostic test interval*" (IEC 61508-4, section 3.8.7): these definitions seem to lead to the definition of "*diagnostic test*" as an automated and online test, performed within time intervals at least a magnitude less than the expected demand rate of the SIF of interest;
- the definition of "*proof test*" can be retrieved in IEC EN 61508-4 (section 3.8.5), where it can be read that it is "*a periodic test performed to detect failures in a safety-related systems so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition*". In the same definition it is also underlined that "*for the full proof test to be effective, it will be necessary to detect 100% of all dangerous failures*".

On the basis of the previous statements and definitions taken from the reference Standard, the following methodological approach can be defined concerning the consideration of "detection" capability and related parameters:

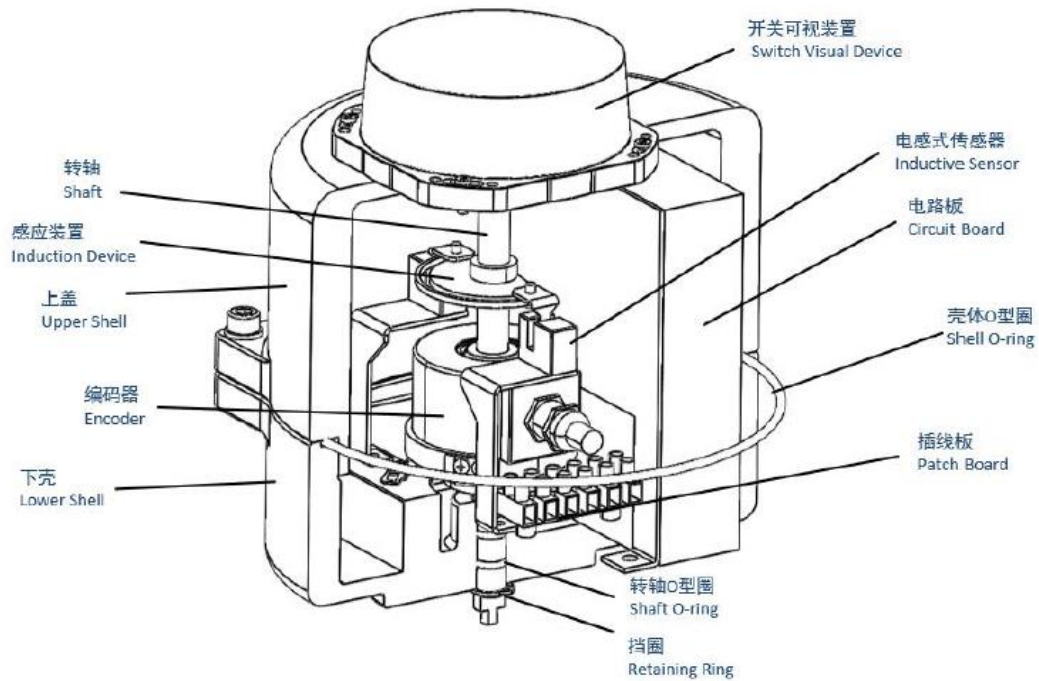
- Diagnostic tests and all types of periodical proof test, able to relieve dangerous undetected failures, must be taken into account (together with related time intervals) in the determination of the PFD for the SIF under examination (see next sections for analytical details).

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

3 SYSTEM DESCRIPTION

3.1 IDD Series Limit Switches

The drawing of a IDD Series Limit Switch is reported here below.



For more details please refer to the technical datasheet and the Safety Manual enclosed in the Annex 1 and in the Annex 2 respectively.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official



Italia

3.2 Specific safety function subjected to SIL classification

The safety function for the IDD Series Limit Switches described in the previous paragraphs, for which the SIL classification according to Standard IEC EN 61508:2010 has been carried out in the present study, is defined as follows:

“Liquid pump, the frequency converter reduces or increases the frequency to adjust the motor speed so that the outlet pipeline pressure is within the range of 0.2 ~ 1.4 MPa (the maximum pressure of the pump outlet pipeline is determined according to the set pressure of the filling system pipeline) during continuous operation of the pump”

In order to correctly comprehend such safety function, some considerations must be pointed out:

- the battery limits considered in the analysis are the ones determined by components of typologies pumps considered in the analysis, as reported in the attached technical documentation and mentioned in the previous paragraphs;
- the defined safety function complies with the battery limits defined in the previous point, regardless of the higher level effects that the safety function can involve in the complex system enclosing the pump itself, whose design characteristics are outside the scope of the present study;
- since installation and use modes of IDD Series Limit Switches in the complex systems cannot be known in advance, but considering the above mentioned function as strictly associated to emergency/safety interventions inside the overall plant with very low expected frequencies, the analysis has referred to a “low demand mode” of operation;
- the analysis has considered the pneumatic and/or mechanical failure modes able to prevent the correct and complete functioning of the pump: therefore any failure cause lying outside the battery limits of the pump has not been considered (for example, air supply to pressurise/release the pistons has been considered as always correctly available).

Boundary limits of a system for SIL classification scope represent the interface between the item to be considered and its surroundings. Safety Functions shall be defined within these boundary selections. See following figure to identify the boundary limits considered for the scope. IDD Series Limit Switches have been considered as single devices (1oo1).

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4 ANALYSIS OF THE SYSTEM ACCORDING TO THE STANDARD IEC EN 61508

4.1 Estimation of reliability data

IEC EN 61508-2 indicates that input reliability data can be estimated either using component failure data from a recognised industry source or (preferable) from experience of the previous use of the subsystem in a similar environment. In particular, reliability data have to be characterised by a single-sided lower confidence limit of at least 90% (see IEC EN 61508-2, sections 7.4.7.4÷9).

In order to evaluate the basic reliability parameters, a statistical analysis approach based on the χ^2 distribution, also mentioned and suggested by EN 61511-2 (section 11.9.2, last paragraph), has been performed.

It is important to remark that this methodology is based upon the assumption that the examined components lie in the useful period of their life cycle and, therefore, their relevant failure rates can be considered as not-time depending and failures characterised by an exponential distribution.

According to TÜV procedure, as reported in the following §§ 4.1.1 and 4.1.2, with the aim to evaluate the reliability data of the IDD Series Limit Switches, data obtained by the field experience concerning the population of IDD Series Limit Switches produced and traded by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. in the period from 2018 to 2021 have been employed.

Concerning the probabilistic analysis section, the exigency by TÜV of treating both data from the field and functional/fatigue tests is motivated by the following two considerations:

- data from the field are considered the primary source of data, as they can supply a very high statistical sample in terms of systems and related operational application and, above all, they are representative of components used in real environmental and operational conditions: due to the considerable economic value of the CZV Series Ball Valves with HPY Series Pneumatic Actuators object of the analysis and thanks to the warranty and quality policy adopted by Zhejiang Chaozhong Valves Made Co., Ltd., it can be stated with good confidence that, in general, any failure affecting the valve and actuator functionality is claimed by the final Clients.
- the functional/fatigue tests are considered as a fundamental and complementary set of statistical data, as they can supply a very high statistical sample in terms of cycles of application of the Safety Function even if, being performed within a controlled and protected environment, they could not be completely representative of the environmental conditions in which the CZV Series Ball Valves with HPY Series Pneumatic Actuators object of the analysis will actually work (i.e. external pipeline, extreme environmental conditions, etc.). In addition, it can be stated that a valve with its actuator in its actual low demand safety application will definitely perform a number of operations during its lifecycle that is widely lower in comparison with the amount of cycles that are performed during a Functional Fatigue test.

Following the previous considerations, the statistical treatment of both sources of data is essential and mandatory, being anyway the first source of data the reference for the estimation of Failure Rates and PFDs at the basis of max claimable SIL classification. The second source of data is used only to confirm (if possible) the highest level of SIL reached by means of the field data: in fact, although functional/fatigue tests can provide a large statistical basis in terms of number of cycles, usually they are performed on a very small number of components, that cannot be considered completely representative of the whole population under analysis and cannot represent an adequate statistical sample.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.1.1 Failure rate and PFD estimation by means of functional/fatigue tests

The complete functional/fatigue test report, that also include data about tests, are reported in Annex 2. Although the functional/fatigue tests do not cover the whole range of different sizes and versions of IDD Series Limit Switches object of the analysis, the variety of typologies and especially the high number of cycles can be assumed as an adequate sample in order to statistically represent the relevant size classes that have been identified for the IDD Series Limit Switches.

The test consists of a wide amount of opening and closing cycles, with the control of the structural, mechanical integrity and tight of the limit switch under examination.

Such test, consisting of switching on demand, have represented the basis for the estimation of a representative value of PFD concerning the defined classes, to be compared with the values reported in above tables, referring to the “low demand mode of operation”.

As indicated in the functional/fatigue tests report in Annex 2, tests did not show any functional anomaly. The statistical method has been therefore applied for cases without failures occurrence exposed in previous paragraphs, in order to estimate the representative values of PFD.

In the following table, on the basis of the functional/fatigue tests performed for the above mentioned IDD Series Limit Switches, the number of samples and the amount of cycles, PFD values provided by the methodological approach have been reported.

Table 4 – PFD for IDD Series Limit Switches resulting from functional/fatigue tests

System type	n. cycles	n. faults	Confidence %	PFD _{low}	PFD _{mean}	PFD _{up}	Max SIL
IDD Series Limit Switches	200.000	0	90	6,554E-09	1,667E-06	6,402E-06	SIL4

As it can be seen in the table above reported, the representative values of PFD for the IDD Series Limit Switches have been characterised by the following conservative hypotheses:

- the uncertainty range of the failure rate representative for each size class has been evaluated with reference to a confidence level conservatively equal to 90%;
- within the uncertainty range for each selected type of valve and actuator, the PFD value corresponding to the 95-th percentile (PFD_{UP}), that is to say the worst one in probabilistic terms, has been considered.

The estimated PFD for the IDD Series Limit Switches, with reference to the “low demand mode of operation” from a strictly probabilistic point of view, could be adequate to support a classification for the safety functions up to SIL4.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.1.2 Failure rate and PFD estimation by means of data from the field

By means of the information about the quantities of IDD Series Limit Switches produced and traded by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. in the period from 2018 to 2021 and the field return data due to failures, an estimation of the failure rate can be made.

With regard to the tables reported in Annex 3 and declared by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd., a total reference time of more than 166.000.000 hours (calendar time) can be considered, during which none of the components have been returned in fault conditions (failure able to prevent the carrying out of the safety function, not due to external causes, like human error).

By means of the statistical approaches for cases without failures reported in the previous paragraphs, an estimation of the failure rates relevant to the IDD Series Limit Switches has been carried out.

Table 5 – Failure rate for IDD Series Limit Switches by means of data from field

Item	q*h	n. of faults	Confidence %	$\lambda_{low} [h^{-1}]$	$\lambda_{mean} [h^{-1}]$	$\lambda_{up} [h^{-1}]$
IDD Series Limit Switches	166.317.360	11	90	7,881E-12	2,004E-09	7,699E-09

As it can be seen in Table 5, the calculation has been characterised by the following conservative hypothesis:

- the uncertainty range of the failure rate representative for each class has been evaluated with reference to a confidence level conservatively equal to 90%;
- within the uncertainty range for each class, the failure rate corresponding to the 95-th percentile (λ_{UP}), that is to say the worst one in probabilistic terms, has been considered.

Since the operating mode of the IDD Series Limit Switches according to the Standard IEC 61508 is “low demand mode operation”, the reference statistical parameter is the PFD, provided by the following formula (adapted from IEC EN 61508):

$$PFD = \lambda_{DD,PST} \cdot MTTR + \lambda_{DU,FPT} \left(\frac{1}{2} \theta_{FPT} + MRT \right)$$

which has validity for the hypothesis (generally widely accomplished) of $\lambda t < 0,1$ and $\theta \gg MRT$, and in which:

λ_{DD} = cumulative failure rate related to dangerous failure modes;

λ_{DU} = cumulative failure rate related to dangerous failure modes detectable only by means of Full Functional Proof Tests;

$\lambda_{DD,PST}$ = cumulative failure rate related to dangerous failure modes that can be detected by means of Partial Stroke Test, with characteristics of diagnostics according to the interpretation of IEC EN 61508;

$\lambda_{DU,FPT}$ = cumulative failure rate related to dangerous failure modes that can be detected by means of Full Proof Test, with characteristics of diagnostics according to the interpretation of IEC EN 61508;

λ_{NE} = cumulative failure rate related to failure modes that have no effect on the safety function;

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

θ_{PST} = time interval between two consecutive Partial Stroke Tests (expressed in hours);

θ_{FPT} = time interval between two consecutive Full Proof Tests (expressed in hours);

MRT = Mean Repair Time (expressed in hours);

$MTTR$ = Mean Time To Restoration (expressed in hours) = $\theta_{PST} + MRT$.

Assuming the following alternatives:

- time intervals for the execution of Full Functional Proof Tests in a range from 1 month (730 hours) up to three years (26.280 hours), considered by TÜV as the maximum acceptable time interval for Full Functional Proof Test for devices implementing safety related functions,
- Partial Stroke Test for IDD Series Limit Switches is not foreseen,

the resulting values of PFD, with reference to the “low demand mode of operation” for the IDD Series Limit Switches are distributed as in the following tables.

Table 6 – PFD values for different inspection/proof test intervals

IDD Series Limit Switches	
Full Proof Test Interval [months]	36
	1,012E-04
	33
	9,280E-05
	30
	8,437E-05
	27
	7,594E-05
	24
	6,751E-05
	21
	5,907E-05
	18
	5,064E-05
	15
	4,221E-05
	12
	3,378E-05
	9
	2,535E-05
	6
	1,692E-05
	3
	8,492E-06

Legend			
SIL 4	SIL 3	SIL 2	SIL 1

The following information can be extracted with regard to the considered Safety Functions from a probabilistic point of view:

- a SIL3 classification can be achieved for a wide range of Full Proof Test intervals;

Then, with reference to the overall table of PFD results, requirement can be defined for the execution of a program of Full Functional Proof Test with time interval not higher than 36 months.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.2 Architectural/functional analysis

4.2.1 FMEDA Analysis

The FMEDA analysis has been carried out in order to identify any possible weak point of the systems object of the study. Such objective has been reached by carrying out a systematic and documented examination of all possible failure modes and identifying their local and system effects and the possible preventive and compensating measures in order to mitigate them. The detail of information at single failure mode level is moreover of fundamental importance in order to support the considerations relevant to the architectural/functional aspects mentioned in the previous § 2.4.

The main general assumption for the performing of the FMEDA analysis are the following:

- the considered failure effects refers to the worst case scenario;
- the analysis is performed under the general hypothesis of single failure: the effects related to a generic failure mode must be assessed with regard to the case in which no other failure takes place with reference both to the same component and to the overall system. This assumption has a fundamental importance in order to highlight any criticality of the system in its design configuration.

In this specific case, it is important to remark that it is not possible to know the functionality and the architecture of the overall complex system in which the considered item will be installed and working. By this reason, the qualitative criticality assessment is limited to the possible worst effects at single pump level, without any considerations at system level (out of scope for the present analysis).

The meaning of each field of the FMEDA table is defined as follows:

<i>Item</i>	Definition of the considered component
<i>Failure Mode</i>	The mode or form in which the examined failure appears according to the analysis provided by the manufacturer
<i>Total Failure Rate</i>	Overall failure rate for the component (safe + dangerous) [h ⁻¹]
<i>Failure Distribution (%)</i>	Percentage factor of splitting for the failure rate over the different foreseen failure modes
<i>Failure Rate</i>	Failure rate related to a specific failure mode [h ⁻¹]
<i>Failure Classification</i>	Classification of the failure mode regarding the considered safety function
<i>Lambda</i> (SD/SU/DD,PST/DU,FPT/NE)	Classification of the failure mode in terms of impact on the identified SIF and in terms of detection: NE: no effect; DU: dangerous undetected; SU: safe undetected; DD,PST: dangerous detected with Partial Stroke Test; DU,FPT: dangerous undetected, detectable with periodical Full Proof Test.

The percentage allocation has been carried out based on the percentage weights deduced for the reference failure modes of the product from the analysis provided by the manufacturer. The complete FMEDA analysis for the IDD Series Limit Switches has been reported in Annex 4.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.2.2 Mean Repair Time

FMEDA analysis allows to systematically assign values of Mean Repair Time with regard to all possible reference failure modes of the IDD Series Limit Switches.

Regarding MRT, following considerations must be pointed out:

- MRT has been assumed as the time necessary to replace the failed item with a spare, in order to correctly evaluate the availability of the pump in the overall system, for all failure modes requiring an “*off-line*” repair;
- MRT has been assumed equal to the actual time necessary to repair on line the failed item, without removing it from the process line, for all failure modes requiring an “*on line*” repair.

According to the above mentioned assumptions and to partial MRT values depicted in FMEDA, MRT for the IDD Series Limit Switches results to be:

$$MRT = \frac{\sum_i MRT_i * \lambda_i}{\sum_i \lambda_i}$$

Where:

MRT_i = MRT related to the i-th failure mode;

λ_i = failure rate related to the i-th failure mode;

Table 7 – MRT values for IDD Series Limit Switches

Item	MRT [h]
IDD Series Limit Switches	8

A MRT value of 8 hours has been considered.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.2.3 Common Cause Failure

The Standard IEC EN 61508-6 Annex D indicates the approach of the β -factor model in order to assess the Common Cause Failure:

$$\lambda_{CCF} = \lambda_{DU} \cdot \beta + \lambda_{DD} \cdot \beta_D$$

Where:

λ_{CCF} = overall failure rate due to dangerous Common Cause Failures;

λ_{DU} = probability of dangerous undetected failure of a single channel;

β = common cause failure factor for undetectable dangerous fault, which is equal to the overall β -factor that would be applicable in the absence of diagnostic testing;

λ_{DD} = probability of dangerous detected failure of a single channel;

β_D = common cause failure factor for detectable dangerous fault.

To estimate β and β_D , tables and checklists reported in the Standard IEC EN 61508-6 Annex D have to be applied. Several issues reported in these tables refer to aspects related to the overall Safety Loop System enclosing the Pump object of the present study. These aspects concern operational/maintenance issues, architecture/redundancies/diversifications within the overall Safety Loop System, testing and commissioning aspects, experience and training of operators, environmental parameters, etc. As the most part of these issues are not under control of TÜV Italia, the β -factors have to be assumed equal to the worst values for sensors/final elements.

According to the Standard IEC EN 61508-6 Annex D, the maximum value that can be assessed for β or β_D for sensors/final elements is then equal to 10%.

4.2.4 Hardware Fault Tolerance

From the point of view of the Hardware Fault Tolerance parameter, according to technical indications provided by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd., the system under analysis consists of several components in Series and no redundancies are foreseen.

As already discussed in the previous chapters, several failure modes of the IDD Series Limit Switches are critical from the point of view of the identified Safety Function.

By this reason, regarding the considered Safety Function, the IDD Series Limit Switches are certainly characterised by the minimum level of Hardware Fault Tolerance, equal to 0.

Being the IDD Series Limit Switches Type A systems, according to IEC EN 61508-2 7.4.4.3.1, the maximum SIL that can be allocated is SIL2 for HFT = 0 and SIL3 for HFT = 1, regardless of any other probabilistic or architectural/functional consideration.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official



Italia

4.3 Systematic safety integrity requirements

As mentioned in § 2, the SIL classification for a specific safety function must take into account systematic safety integrity constraints according to IEC EN 61508-2 7.4.2.

The systematic safety integrity evaluation has been performed according to the route 2s as foreseen by the standard IEC EN 61508-2 7.4.10, in order to identify the highest safety integrity level that can be claimed for identified safety function. In particular, the following aspects have been considered:

- A specified functionality with an adequate documentary evidence of the failure collected in a database;
- Evidence that the dangerous failure rate has not been exceeded in previous use;
- Effectiveness of the system for reporting failure through statistical evidence;
- Low complexity of the element;
- The design is well established for many years;
- There are no elements that can affect the safety integrity of the element function and that are not covered by proven in use.

Furthermore the following requirements have to be considered for future applications:

- Any difference between the previous conditions of use and those that have been experienced will require an impact analysis on the differences in order to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity level(s) of the safety function(s) that use the element is not affected.
- Any future modification of a proven in use element shall be evaluated according to IEC EN 61508-2 7.8.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

4.4 SIL classification of the system

As mentioned in § 2, the SIL classification for a specific safety function must take into account both probabilistic aspects and functional/architectural issues.

Concerning the architectural/functional aspects (based on considerations relevant to Hardware Fault Tolerance), the following outcome has been obtained:

- With regard to the Safety Function expressed in section 3.2, the IDD Series Limit Switches object of the analysis are compliant for a classification up to SIL2, stated that a correct and adequate program of Full Proof Test is foreseen.

With reference to probabilistic issues, the following results have been obtained:

- for IDD Series Limit Switches, a SIL2 classification can be achieved for a wide range of Full Proof Test intervals.

With reference to systematic safety integrity,

- for IDD Series Limit Switches, a SIL3 classification can be achieved.

On the basis of all previous considerations, concerning both functional/architectural aspects and probabilistic evaluations, the IDD Series Limit Switches result to be compliant to Standard IEC EN 61508:2010:

- up to SIL2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to the considered Safety Function.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official

5 CONCLUSIONS

The methodological approaches of analysis specified by IEC EN 61508:2010 have been fully implemented, carrying out an accurate assessment of correct and complete compliance with both reliability and architectural/functional requirements indicated by the Standards.

The Safety Function for which the SIL classification according to Standard IEC EN 61508 has been carried out, is the following:

“Correct switching on demand (open to closed / closed to open), in low demand mode of operation”

For the estimation of the reliability data, both data resulting from the functional/fatigue tests performed by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. and field data related to the complete population of IDD Series Limit Switches produced and traded by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. in the period from 2018 to 2021 have been considered.

On the basis of both functional/architectural aspects and probabilistic evaluations, the IDD Series Limit Switches object of the analysis result to be compliant to Standard IEC EN 61508:2010

- *up to SIL2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to the above Safety Function.*

6 DISCLAIMER

The present technical report is exclusively based on the documentation and information provided by Antiwear (Suzhou) Industrial Intelligent Technology Co., Ltd. during the meetings or by mean of email communications.

The origin of this documentation, as well as the use of this report, is not under TÜV liability.

Document	R TUV IT 22 SIL 0084	Date	July, 11 th 2022
Revision:	1	Document Status	Official