energies

MDPI

Article

A Functional Safety Assessment Methodology for Explosion Protection with Application to a Variable Frequency Drive System

Shiguang Li [1,2,*] and Xiaojie Wu [1]

[1] School of Electrical and Power Engineering, China University of Mining and Technology, 1 Daxue Road, Xuzhou 221116, China; xjwu@cumt.edu.cn
[2] China National Quality Supervision and Testing Center of Explosion-Proof Equipment (Guangdong), Guangzhou Academy of Special Equipment Inspection and Testing, 3598 Huangpu East Road, Huangpu District, Guangzhou 510760, China
* Correspondence: exdshiguangli@gmail.com; Tel.: +86-1382-2251-874

Abstract: Modern explosion protection equipment, protected by traditional explosion protection technology (as defined by the international electrotechnical commission (IEC) publication IEC60079-ff series standards) and electrical/electronic/programmable electronic (E/E/PE) safety-related systems, is becoming ever more complex in coal mine development and petrochemical industry; thus, the possibility of failures in their operation is also growing. It is well-known that E/E/PE safety-related systems can be used to actively control dangerous sources, with real and expected levels of reliability, if they have been qualified according to the IEC61508-ff series standards. To uniformly evaluate the safety integrity level (SIL) of the explosion protection function of traditional explosion protection technology and E/E/PE safety-related system technology, this study analyzed the ability of these types of protection to remove the ignition risk residual, evaluating the failure rates of safety devices. The key objective of this paper is the presentation of a new equipment protection level (EPL) assessment method for explosion protection equipment based on a functional safety assessment. The method is applied to a variable frequency drive (VFD) system, and the results show that the EPL of the explosion protection equipment evaluated by this method is consistent with the EPL corresponding to the traditional explosion protection type of the IEC60079-ff series standard. Meanwhile, the flexible configuration of explosion protection safety devices and E/E/PE safety-related systems enables explosion protection equipment of different EPL levels to be designed.

Keywords: functional safety; explosion protection; failure rate; safety integrity level; explosive atmosphere; variable frequency drive

check for updates

Citation: Li, S.; Wu, X. A Functional Safety Assessment Methodology for Explosion Protection with Application to a Variable Frequency Drive System. *Energies* **2021**, *14*, 7872. https://doi.org/10.3390/en14237872

Academic Editor: Herodotos Phylaktou

Received: 22 August 2021
Accepted: 8 November 2021
Published: 24 November 2021

1. Introduction

Since the introduction of the functional safety international accepted series standard IEC61508-ff, functional safety has gradually formed a complete safety assessment system. IEC61508-0 introduces the concept of the safety lifecycle, explains the applicability and relevance of electrical/electronic/programmable electronic safety-related systems, clearly puts forward the functional safety of safety-related systems, and details the general procedures and methods for realizing functional safety. On this basis, functional safety standards for specific industrial applications have also been published, such as the IEC61511 standard for the process industry, the IEC61513 standard for the nuclear industry, the IEC62061 standard for the mechanical industry, and the international organization for standardization (ISO) publication ISO26262 standard for automotive electronics [1].

At present, the application of functional safety in explosive environments is mainly aimed at the safety management of petrochemical process instrumentation. For explosion protection equipment, the European Commission project SAFEC (Contract No CT98-2255 Determination of safety categories of electrical devices used in potentially explosive atmospheres) advances the SIL level functional safety assessment method of E/E/PE safety-related systems in explosion protection equipment, and formulates the EN50495: 2010 standard in the form of results [2]. The article [3] presents a methodology based on the principles of functional safety for quantitative risk assessment, which was mainly directed towards the assessment of explosion risks at workplaces. Faranda analyzes the risk of lithium batteries and evaluates the functional safety integrity level (SIL) of the safety control system of a lithium battery power supply device [4]. Fumagalli, meanwhile, studies the possibility of the safe use of an enhanced light-emitting diode light source in hazardous area Zone 1 (as defined by IEC60079-10-1) based on the functional safety assessment method [5].

This paper is organized as follows: In the next section, a summary of the definition of functional safety and the concept of explosion protection function. Then, based on the Failure Mode and Effect Analysis (FMEA) method, the functional safety assessment of the explosion protection function defined in this article is carried out. This is followed by a section describing the application of the method proposed in this article to carry out the functional safety assessment of an explosion-proof function of an example, and compares and analyzes the estimation results of different safety device combinations.

2. Functional Safety and Explosion Protection Function

According to the definition in the IEC62061 standard and IEC61508-ff standards, safety-related systems meet the following two conditions: one is that the required safety function must be realized to achieve or maintain the safety status of the equipment under control; the other one is achieving the safety integrity required by the safety function with other E/E/PE safety-related systems, other technical safety-related systems, or external risk-reduction facilities [6].

The E/E/PE safety-related system mentioned in IEC62061: 2005 standard and the safety device defined in the EN50495: 2010 standard are limited to the safety technologies for electronic or electrical implementation. For more general applicability, similar to ISO 13849, IEC62061: 2021 is extended to non-electrical technology, such as hydraulic, pneumatic, and mechanical technologies. It is clear that the concept of functional safety is not limited to safety technologies for electronic or electrical implementations but is also applicable to safety technologies for non-electrical implementations.

To prevent an explosion, appropriate electromechanical measures are adopted to prevent the simultaneous occurrence of the three elements of an explosion (flammable substances, combustion-supporting substances, and ignition sources). Then, these electromechanical measures can be considered as a kind of safety-related system or safety device. There are two main types of these measures: one prevents igniting the surrounding explosive environment, which is known as the explosion protection type as defined in the IEC60079-ff series standard. The other comprises E/E/PE safety-related systems consisting of sensors, logic controllers, and actuators. Therefore, the function of preventing an explosion caused by potential ignition sources is defined as the explosion protection function, and the reliability of a single electromechanical measure that realizes the explosion protection function is defined as the explosion protection performance in this paper.

This paper proposes a method based on functional safety assessment to comprehensively evaluate the explosion protection function of traditional electromechanical explosion protection measures and/or E/E/PE safety-related systems as safety devices, so as to give the safety integrity level SIL of the explosion protection function and determine the equipment protection level by the SIL level. Part of the aim of this study was to develop a method enabling the flexible configurations of electromechanical explosion protection measures and E/E/PE safety-related systems, to design different EPL levels of explosion protection equipment. We also aimed to provide a new evaluation method for the realization of the special protection type defined in the IEC60079-33 standard.

The difference between traditional explosion protection equipment, according to IEC60079-ff series standard, and explosion protection equipment based on the functional safety assessment method, is shown in Figure 1.

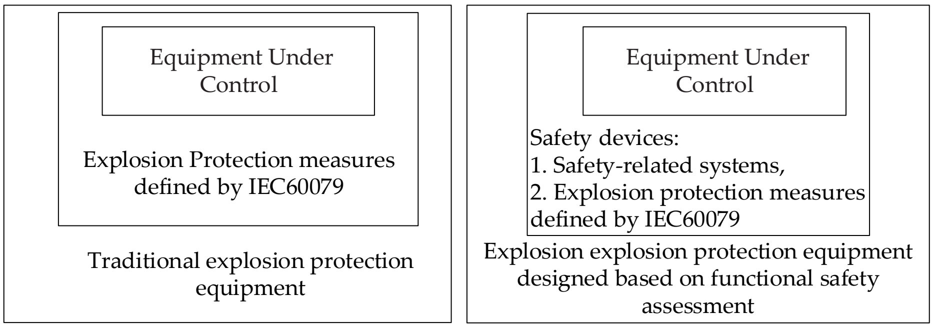
Equipment Under Control
Explosion Protection measures defined by IEC60079
Traditional explosion protection equipment
Equipment Under Control
Safety devices:
1. Safety-related systems,
2. Explosion protection measures defined by IEC60079
Explosion explosion protection equipment designed based on functional safety assessment

Figure 1. Outline of explosion protection equipment based on functional safety assessment.

3. Proposed Methodology for Evaluation of the Explosion Protection Equipment's Protection Levels (EPLs) Based on an Assessment of Functional Safety

Referring to IEC61508-1: 2010 and EN50495: 2010, the SIL evaluation process of the explosion protection function is shown in Figure 2 [7]. Many parameter variables are given in the standard, but the traditional explosion protection technologies and E/E/PE safety-related system protection measures are quite different, and the measures are more independent. Therefore, the common cause of failure of the system can be ignored, meaning $\beta = 0$. The diagnostic coverage (*DC*) is only for the E/E/PE safety-related system with an automatic diagnostic function that did not exist in electromechanical measures of traditional explosion protection equipment, and the diagnosis is determined by manual inspection.

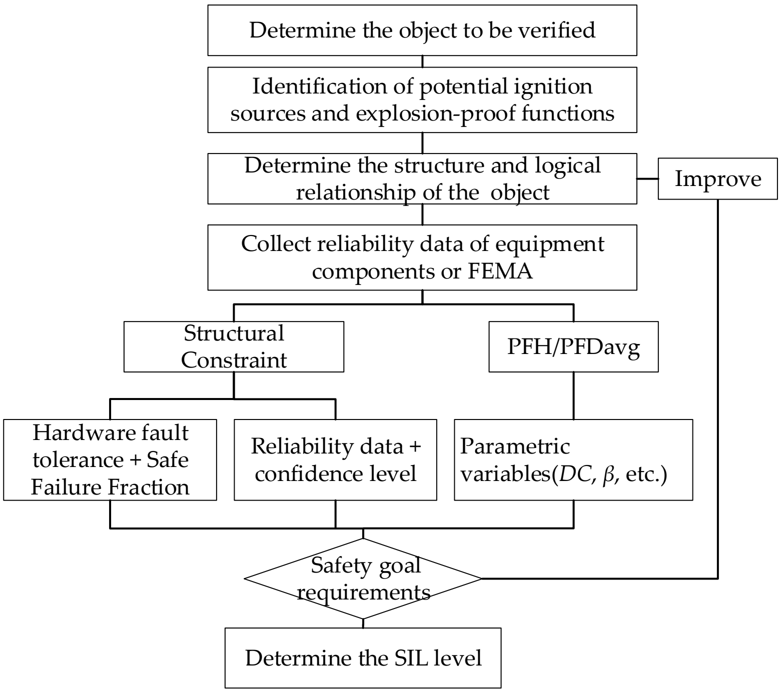
Determine the object to be verified
Identification of potential ignition sources and explosion-proof functions
Determine the structure and logical relationship of the object
Improve
Collect reliability data of equipment components or FEMA
Structural Constraint
PFH/PFDavg
Hardware fault tolerance + Safe Failure Fraction
Reliability data + confidence level
Parametric variables(DC, β, etc.)
Safety goal requirements
Determine the SIL level

Figure 2. Flow chart of safety integrity level (SIL) verification for explosion protection functions. PFD, probability of a failure on demand; PFH, probability of a dangerous failure per hour; avg, average; FMEA, failure mode and effect analysis; *DC*, diagnostic coverage; β, beta.

3.1. Potential Ignition Source Analysis and Explosion Protection Function Identification

The EN1127-1 standard proposed 13 types of potential ignition sources. The ignition sources of electrical equipment are mainly thermal surfaces and electrical sparks [8,9]. The static electricity of non-metallic materials in the equipment is limited by selecting materials with a surface resistance of no more than $10^9\ \Omega$.

According to the definition of explosion protection function, it is necessary to analyze the ignition source of the controlled equipment, and analyze the safety devices used by the different ignition sources of the equipment. The fault tree analysis method for identifying the explosion protection function of electromechanical equipment is given, as shown in Figure 3.

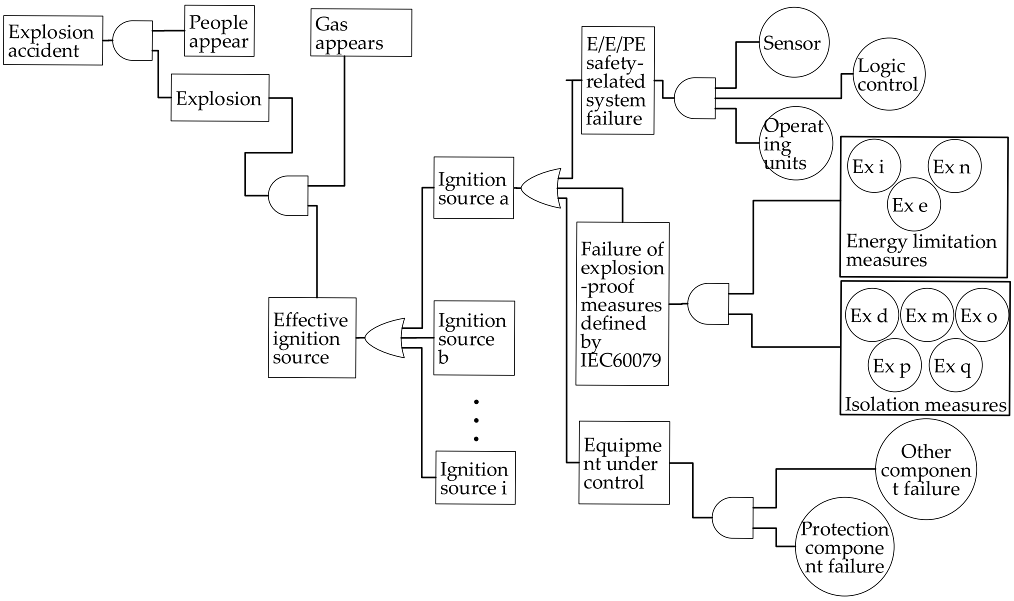

Figure 3. Explosion protection function identification based on fault tree analysis method.

To evaluate the effectiveness of safety devices that realize an explosion protection function, the reliability data of safety devices must be obtained. In this paper, the FMEA method recommended by IEC61508-ff is used for analysis, and the required data are obtained by combining this with the reliability database of industrial products.

3.2. Failure Mode and Effect Analysis (FMEA)

The failure modes of each component are analyzed according to the characteristics of the component. Each failure mode can be divided into four categories according to its impact on the safety device, as shown in Table 1 [10]. Compared with the FMEA analysis of ordinary products, safe faults mean that an effective ignition source cannot be formed when the fault occurs.

Table 1. Failure rates for different failure modes.

Failure Modes	Detected Faults	Undetected Faults
Safe faults	$\lambda_{\text{sd}} = \sum_{i=1}^{n} \lambda_{\text{sd}}(i)$	$\lambda_{\text{su}} = \sum_{i=1}^{n} \lambda_{\text{su}}(i)$
Dangerous faults	$\lambda_{\text{dd}} = \sum_{i=1}^{n} \lambda_{\text{dd}}(i)$	$\lambda_{\text{du}} = \sum_{i=1}^{n} \lambda_{\text{du}}(i)$

Key: sd = safe detected; dd = dangerous detected; su = safe undetected; du = dangerous undetected; *n* = number of components.

The total failure rate of components is the sum of the failure rates of each failure mode:

$$\lambda_{\text{tot}} = \lambda_{\text{su}} + \lambda_{\text{sd}} + \lambda_{\text{du}} + \lambda_{\text{dd}} = \frac{1}{MTBF} \tag{1}$$

where λ_{tot} is the total failure rate, indicating the number of failures per unit time, and *MTBF* is the mean time between failures.

The failure rate of failure modes cannot be directly obtained; first, we need to obtain the proportion of failure rates of different failure modes by FMEA analysis. The total failure rates of usual electronic components and mechanical components can be obtained from the general industrial database, manufacturers, government statistics, and reliability tests. For some unusual components, they can be obtained by expert evaluation methods. Component faults are divided into multiple failure types according to the causes. If only the total failure rate is known, the failure rate of each type is estimated by formula (2).

$$\lambda_{\text{failure type}} = \frac{\lambda_{\text{tot}}}{\text{number of failure types}} \tag{2}$$

3.3. Failure Analysis and Failure Rate Calculation of Safety Devices

There are many technical requirements for explosion protection equipment defined in IEC60079-ff series standards. To evaluate the failure rate of the explosion protection function, the key measures to achieve the explosion protection function are mainly considered.

3.3.1. Failure Analysis of Flameproof (Ex d) Type

The realization of an explosion protection function of the flameproof type mainly depends on the mechanical construction of a flameproof enclosure: strength of enclosure material, width of joints, gaps (depends on the fastener's flameproof surface flatness), and sealing of cable glands [11].

According to formula (1), the *MTBF* can be used to calculate the total failure rate, λ_{tot}, and then calculate the failure rate of various failure modes. Because the flameproof enclosure is not a standard part, there is no available mature database to obtain the *MTBF*. Therefore, this paper estimates the failure rates of various failure types of protection flameproof "affecting the explosion protection function, and calculates the total failure rate.

1. Failure Analysis for Strength of Enclosure

The strength of the enclosure material decreases due to various reasons such as wear thinning, which means the strength is unable to meet the original strength requirements. The thickness is used to evaluate the possible wear of the enclosure. In flameproof equipment, the minimum thickness of the enclosure can be calculated by a formula according to the material properties, shape of enclosure, stress, and other parameters of the enclosure. The calculation method is not detailed here; however, more details are found in [12].

It is assumed that the minimum required thickness of the enclosure is denoted as a, and the actual thickness of the enclosure is denoted as b, $b \geq a$. If $b < a$ due to wear, it is considered that the flameproof enclosure has lost its safety function. Assuming that the wear found by inspection a year later (8760 h) is recorded as c, the failure rate of the enclosure is:

$$\lambda_{\text{enclosure}} = \frac{1}{\frac{b-a}{c} \times 8760}\ \frac{1}{\text{h}} \tag{3}$$

2. Failure Analysis for Width of Joints

The dangerous failure of joints occurs as a result of decreased width due to wear, and the calculation method is the same as (3). It is assumed that the required width of joints is denoted as a, and the actual width of joints is denoted as b. When $b > a$, the failure rate of the width of joints is:

$$\lambda_{\text{width}} = \frac{1}{\frac{b-a}{c} \times 8760}\ \frac{1}{\text{h}} \tag{4}$$

3. Failure Analysis Sealing Performance for Cable Glands

The failure of sealing parts such as cable glands will affect the flameproof safety. According to the "Handbook of Reliability Prediction Procedures for Mechanical Equipment" [12], the failure rate of the sealing parts can be calculated by the following formula:

$$\lambda_{SE}= \lambda_{SE,B} \times C_P \times C_Q \times C_{DL} \times C_H \times C_F \times C_V \times C_T \times C_N \quad (5)$$

where $\lambda_{SE,B}$ is the base failure rate, 2.4×10^{-6} h^{-1}; C_P is the fluid pressure factor; C_Q is the allowable leakage factor; C_{DL} is the seal size factor; C_H is the contact stress and seal hardness factor; C_F is the seat smoothness factor; C_V is the fluid viscosity factor; C_T is the temperature factor; C_N is the contaminants factor. The values of these factors can be determined according to different sealing conditions. Any type of failure of the sealing parts will affect the flameproof safety, which should be considered as a dangerous failure.

4. Failure Analysis of Flameproof Gap

The influencing factors of the flameproof gap are mainly the flatness of the joint surface and the reliability of the fasteners. The flatness of the joint surface of the flameproof equipment after processing is stable, so the main determinant factor is the fastener. The reliability of fasteners can be calculated by the following formula [12]:

$$\lambda_F= \lambda_{F,B} \times C_{SZ} \times C_L \times C_T \times C_I \times C_{SC} \times C_K \quad (6)$$

where $\lambda_{F,B}$ is the base failure rate; C_{sz} is the size deviation factor; C_L is the loading factor; C_T is the temperature factor; C_I is the severity of the in-service cyclic shock factor; C_{SC} is the surface coating factor; C_K is the stress concentration factor. The values of these factors can be determined according to different conditions.

In summary, for flameproof equipment, it is assumed that the failures can be found and corrected in time through inspection and measurement every year. Considering the uncertainty of personnel inspections, 90% of failures are expected to be detectable and 10% of failures undetectable. Since each part provides only flameproof protection, the hardware fault tolerance is 0. The failure mode of the explosion protection function is shown in Table 2.

Table 2. Failure mode of flame-proof enclosure.

Fail Parts	Failure Modes	Safe/Dangerous	Detected/Undetected
Enclosure	Wear thinning	Dangerous	90% detected, 10% undetected
Joints	Narrower due to wearing	Dangerous	90% detected, 10% undetected
Sealing parts	Fail	Dangerous	90% detected, 10% undetected
Fastener	Fail	Dangerous	90% detected, 10% undetected

3.3.2. Failure Analysis of Increased Safety Explosion Protection Function

According to the definition of IEC60079-7:2015, the explosion protection function of increased safety construction is mainly realized by strengthening protective measures: the enclosure protection degree, mechanical strength of the connector, electrical strength of the insulation material, and electrical protection components [13]. Similar to the safety device for the flameproof type, the failure rate of each failure type is analyzed by FMEA to obtain λ_{tot}, as shown in Table 3.

Table 3. Failure mode of flameproof enclosure.

Failed Parts	Failure Modes	Safe/Dangerous	Detected/Undetected
Sealing parts	Fail	Dangerous	90% detected, 10% undetected
Connectors	Fail	Dangerous	90% detected, 10% undetected
Insulating materials	Breakdown	Dangerous	90% detected, 10% undetected
Electrical protection device	Fail	Dangerous	90% detected, 10% undetected

3.3.3. Failure Analysis of Intrinsically Safe Circuit Explosion Protection Function

The intrinsically safe circuit is mainly composed of fuses, a voltage limiting diode, and a current limiting resistor, as shown in Figure 4. Its energy limitation is realized by voltage-limiting and current-limiting measures. The faults allowed for voltage-limiting and current-limiting measures according to different levels: ia, ib, and ic are 2, 1, and 0, respectively.

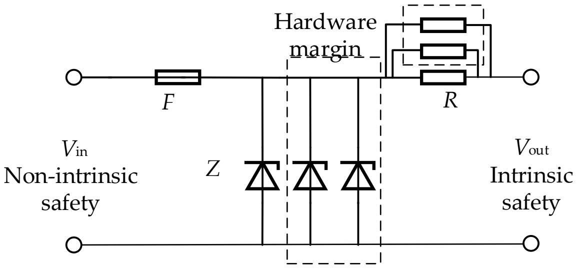

Figure 4. Intrinsically safe protection circuit.

According to the MIL-HDBK-217 "Reliability prediction handbook for electronic equipment", the total failure rates of each component are obtained and the failure modes of the safety barrier are listed in Table 4.

Table 4. Failure mode of intrinsic safety circuit.

Failed Parts	Failure Modes	Safe/Dangerous	Detected/Undetected	Percentage of Failure Type
Fuse	Cannot open	Dangerous	50% detected, 50% undetected	49%
	Opens slowly	Dangerous	50% detected, 50% undetected	43%
	Opens unexpectedly	Safe	50% detected, 50% undetected	8%
Zener diode	Open circuit	Dangerous	50% detected, 50% undetected	18%
	Short circuit	Safe	50% detected, 50% undetected	13%
	Drift	Dangerous	50% detected, 50% undetected	69%
Resistor R	Open circuit	Safe	50% detected, 50% undetected	91.9%
	Drift	Dangerous	50% detected, 50% undetected	8.1%

3.3.4. Failure Analysis of Equipment under Control

It can be seen from the fault tree analysis that the failure of the controlled equipment is caused by the simultaneous failure of functional components and protection components, and forms an effective ignition source.

1. Failure Analysis of Functional Components

Functional components are electronic equipment designed by electronic components. Therefore, for the FMEA analysis of electronic equipment, the failure rate is obtained from the general industrial reliability database. For example, the main components of a VFD system in an explosive environment are the inverter and motor. According to MIL-HDBK-217 [14], the failure rate of the motor can be calculated by the following formula:

$$\lambda_{\text{motor}} = \lambda_b \times \pi_E \times \pi_Q \tag{7}$$

where λ_b is the basic failure rate, related to the rotational speed; π_E is the environment factor; π_Q is the quality factor. The failure rate of a motor is listed in Table 5.

Table 5. Failure mode of motor.

Failure Modes	Safe/Dangerous	Detected/Undetected	Percentage of Failure Type
Winding fault	Dangerous	Detected	60%
Bearing fault	Dangerous	Detected	22%
Operating fault	Dangerous	50% detected, 50% undetected	9%
Start failure	Safe	Detected	9%

The failure analysis of the frequency converter is shown in Table 6. According to the data of a manufacturer, the failure rate of the inverter is generally 7 × 10^{-6} h^{-1}.

Table 6. Failure mode of frequency converter.

Failed Parts	Failure Mode	Safe/Dangerous	Detected/Undetected	Percentage of Failure Type
Converter	Diode failure	Dangerous	50% detected, 50% undetected	16%
DC link	Capacitor wear	Dangerous	50% detected, 50% undetected	17%
Inverter	Output failure	Dangerous	50% detected, 50% undetected	50%
Controller	Failure to control	Dangerous	50% detected, 50% undetected	17%

2. Failure of Electrical Protection Components

Electrical protection components are mainly realized by circuit breakers, fuses, and other switching components. The failure mode is shown in Table 7.

Table 7. Failure mode of electrical protection component.

Failed Parts	Failure Mode	Safe/Dangerous	Detected/Undetected	Percentage of Failure Type
Electrical protection component	Cannot open	Dangerous	90% detected, 10% undetected	45%
	Short circuit	Dangerous	90% detected, 10% undetected	40%
	Open circuit	Safe	90% detected, 10% undetected	10%
	Close failure	Safe	90% detected, 10% undetected	5%

3.3.5. Failure Analysis of E/E/PE Safety-Related System

The E/E/PE safety-related system for explosion protection equipment, or the E/E/PE safety-related system that forms part of the explosion protection equipment, can be evaluated according to the EN50495: 2010 standard in the same way as for general safety products, such as the pressure control system of a pressurized motor [15,16].

The E/E/PE safety-related system for explosion protection equipment is that the components must be protected by explosion protected measures, the response time must be greater than the formation time of the effective ignition source, and the function must be verified by experiments.

3.4. Determination of SIL

After FMEA analysis, the failure rate of the system is obtained, and the probability of a failure on demand (*PFD*)/probability of a dangerous failure per hour (*PFH*), along with the safety failure fraction (*SFF*), can be calculated. Then, the SIL level of the safety device is determined according to these two parameters.

For explosion protective equipment, it is necessary to continuously provide safety functions, so the *PFH* parameter is selected for SIL level determination. The PFHs of different system structures have different calculation formulas. For simple systems, the calculation formula of the *PFH* is shown in Equation (8).

$$PFH = \lambda_{\text{du}} \tag{8}$$

where *SFF* is the safe failure fraction, it can be calculated by the summarized failure rates of the different failure modes using the following formula:

$$SFF = \frac{\lambda_{\text{sd}}+\lambda_{\text{su}}+\lambda_{\text{dd}}}{\lambda_{\text{tot}}} \tag{9}$$

After the *PFH* and *SFF* are obtained, the SIL is determined according to Tables 8 and 9 [17]. In IEC61508-1:2010, clause 7.6.2.9 states the average frequency of a dangerous failure of the safety function [h^{-1}] for a high demand mode of operation.

Table 8. Safety integrity levels: Target failure measures for safety function [17].

Safety Integrity Level	Low-Demand Mode of Operation PFD	High-Demand or Continuous Mode of Operation PFH
SIL 4	$10^{-5} \ll \text{PFD} < 10^{-4}$	$10^{-9} \ll PFH < 10^{-8}$
SIL 3	$10^{-4} \ll \text{PFD} < 10^{-3}$	$10^{-8} \ll PFH < 10^{-7}$
SIL 2	$10^{-3} \ll \text{PFD} < 10^{-2}$	$10^{-7} \ll PFH < 10^{-6}$
SIL 1	$10^{-2} \ll \text{PFD} < 10^{-1}$	$10^{-6} \ll PFH < 10^{-5}$

Table 9. Hardware safety integrity: Architectural constrains on Type A safety-related subsystems [17].

Safe Failure Fraction *(SFF)*	**Subsystem**		
	Hardware Fault Tolerance (HFT)		
	0	**1**	**2**
<60%	SIL 1	SIL 2	SIL 3
60%~<90%	SIL 2	SIL 3	SIL 4
90%~<99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

Hardware Fault Tolerance is defined by the number of independent faults, which may occur in the safety device, without losing the safety function. HFT = 1 means the safety function can maintain the safety function with 1 fault.

According to the definition of IEC61508-0: 2010, the explosion protection construction discussed in this paper belongs to a type A subsystem.

3.5. EPLs Evaluation Based on SIL

According to the definition of EPL in the IEC60079-0 and IEC60079-26 standards, explosion protection equipment can be divided into different EPLs according to the possibility of explosion protection equipment becoming an ignition source and the different characteristics of an explosive gas environment, explosive dust environment, and coal mine methane environment. Based on the standard definition and reference [17], the corresponding relationship between the EPL, the possibility of annual casualties, and the target safety integrity level is given in Table 10. The table reformed from the table a4 of SAFEC makes the link between requirements for the Ex area of applicative operation and functional safety. The use of this table is based on ignition risk analysis. Ignition risk analysis of electrical apparatus starts with the evaluation of potential ignition sources even under the presumption of faults related to the equipment. The SIL refers to the explosion-protected function of a potential ignition source, and the EPLs refer to the level of the equipment itself, when the SIL of all the explosion-protected functions corresponding to all potential ignition sources meets the risk level required to be reduced to the minimum requirement hazardous area Zone X. At this time, the SIL level is equivalent to the corresponding EPL.

Table 10. Relationship among EPL, fatalities per year and SIL [17].

Zone	**Definition**	**Possibility of Casualties per Year 10^{-6} [h^{-1}]**	**Conditions for Forming Ignition Source**	**Applicable EPLs**	**Protection Level**	**SIL**
0	Areas with continuous explosion environment ≥1000 h/y	0.0057	Normal operation, rare faults, expected faults	Ga, Ma, Da	Very high	SIL3
1	Areas with occasional explosive environment 10 ≥ Zone < 1000 h/y	0.57~0.057	Normal operation, expected faults	Gb, Mb, Db	High	SIL2
2	Impossible to occur or occasionally occurs under fault condition ≥10 h/y	5.7	Normal operation	Gc, Dc	General	SIL1

Where 'M' means the equipment for mine, 'G' represents the equipment for explosive gas environment, and 'D' represents the equipment for explosive dust environment.

According to the corresponding relationship of Table 10, to achieve different EPLs, the SIL level of the explosion protection equipment can be given by the method described in this paper. Ga corresponds to SIL3, which can be designed by a single explosion protection safety device, such as Ex ia or Ex ma, or by using two independent safety devices, such as Ex d and Ex mb, or using a safety-related system composed of separate explosion protection safety devices, an E/E/PE system such as Ex d, and temperature control systems. As shown in the fault tree analysis in Figure 3, the failure rate is obtained by using the method of independent parallel implementation of the explosion protection function of safety devices, and the PFD/PFH and SFF are calculated to determine the SIL level and the EPL level of safety devices. This method is more applicable than the traditional explosion protection measures in IEC60079-ff, especially when the explosion protection type in IEC60079-ff cannot achieve a higher EPL level, such as the special type for Zone 0.

4. Application on VFD System

The VFD system has been widely used in coal mines, petrochemicals, and other dangerous places for energy savings. Therefore, this paper selects the VFD system as an example to apply the explosion protection function evaluation method to determine the SIL level and EPL level of the explosion protection function.

4.1. Composition of VFD System and Safety Device in Explosive Environment

The VFD system in an explosive environment is mainly composed of a converter, explosion protection motor, and explosion protection construction, as shown in Figure 5. There are two main kinds of potential ignition sources in a VFD system: hot surfaces and electric sparks.

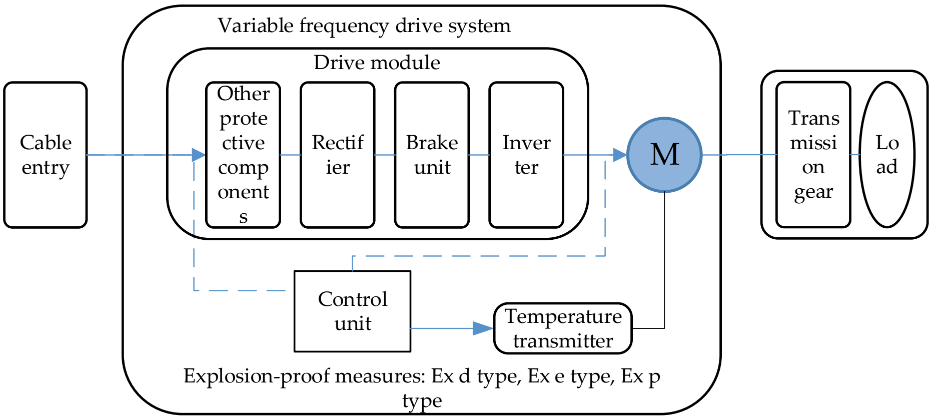
Variable frequency drive system
Drive module
Cable entry
Other prote ctive comp onent s
Rectif ier
Brake unit
Inver ter
M
Trans missi on gear
Lo ad
Control unit
Temperature transmitter
Explosion-proof measures: Ex d type, Ex e type, Ex p type

Figure 5. Block diagram of VFD system for explosive environment.

Therefore, the explosion protection function 1 of the explosive-proof VFD system is to prevent spark ignition, and the explosion protection function 2 is to prevent hot surfaces.

In this paper, the mining VFD system for a belt conveyor is taken as an example for evaluation, and its configuration is shown in Table 11. Then, the fault tree analysis in Figure 3 is refined into Figure 6.

Table 11. Hardware configuration of a mining VFD system for a belt conveyor.

Parts	Electrical Parameter	Safety Device	
		Type of Explosion Protection	Safety Parameters
Convertor	BPJ-132/660K, VAC660V, 132 kW, 140 A, Volt = 0~660 V, f = 0~50 Hz, 1164 × 910 × 915 mm (W × D × H)	Ex d [ib]	thickness of cast steel enclosure 8 mm, width of joints 27 mm, gap 0.4 mm.
Motor	YB3-280S-4, VAC660V, f = 50 Hz, 75 kW, 80.4 A, 1480 r/min, 550 × 1110 mm (∅ × L)	Ex e	thickness of cast steel enclosure 6 mm, width of joints 25 mm, gap 0.5 mm.
Safety temperature control system	-	Ex ib	thermal couple, logic controller, contactor, 1001 structure.

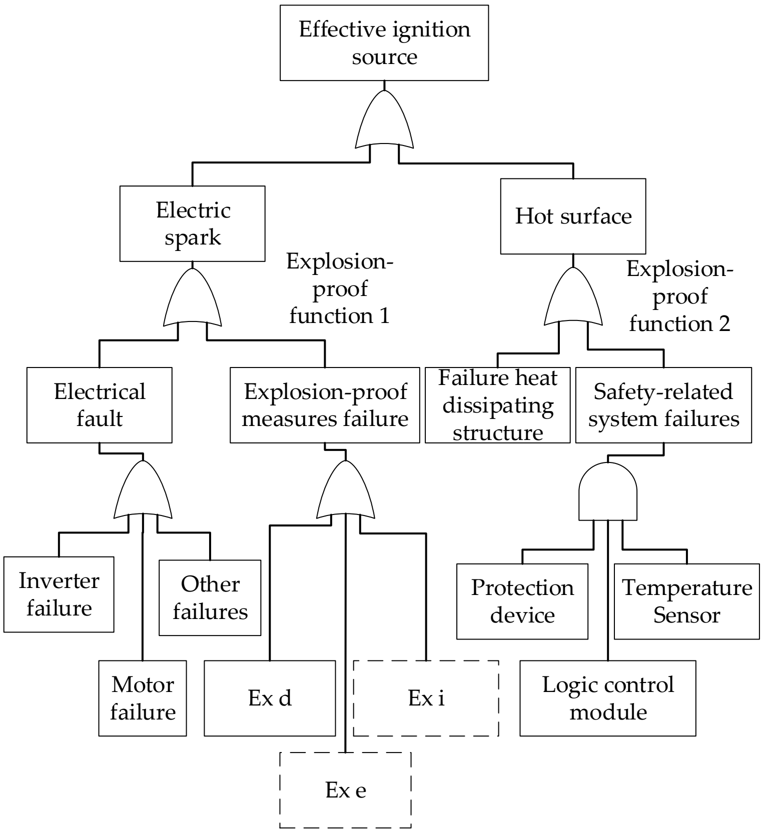
Effective ignition source
Electric spark
Hot surface
Explosion-proof function 1
Explosion-proof function 2
Electrical fault
Explosion-proof measures failure
Failure heat dissipating structure
Safety-related system failures
Inverter failure
Other failures
Motor failure
Protection device
Temperature Sensor
Ex d
Ex i
Ex e
Logic control module

Figure 6. Fault tree analysis of Explosion protection VFD system.

4.2. SIL Level Verification of Explosion Protection VFD System

For the entire VFD system, there may be three safety function modules: flameproof-type safety device, increased safety-type safety device, and safety temperature control module. The motor and converter are protected by a flameproof enclosure or increased safety construction, and the temperature control module can be added to give additional temperature protection. Therefore, electric sparks have been protected by traditional explosion-protected measures. The following is mainly aimed at the explosion protection function of potential hot surface ignition sources. The failure rate results of different explosion-proof VFD systems are shown in Table 12.

Table 12. Failure rates of different explosion-proof VFD systems.

Explosion Protection Configurations of Equipment	**Total Failure Rate λ_{tot}/h^{-1}**	**Partitioning of the Component Failure Rate/h^{-1}**			
		λ_S	λ_D	λ_{du}	λ_{dd}
Safety temperature control system	1.2×10^{-6}	0.21×10^{-6}	0.97×10^{-6}	0.04×10^{-6}	0.93×10^{-6}
Type Ex d enclosure	4.52×10^{-6}	0	4.52×10^{-6}	4.52×10^{-7}	4.07×10^{-6}
Type Ex e motor	9.87×10^{-6}	0.62×10^{-6}	8.07×10^{-6}	0.52×10^{-6}	7.55×10^{-6}
Type Ex d frequency converter + type Ex d motor	9.04×10^{-6}	0	9.04×10^{-6}	9.04×10^{-7}	8.14×10^{-6}
Type Ex d frequency converter + type Ex e motor	13.21×10^{-6}	0.62×10^{-6}	12.59×10^{-6}	0.97×10^{-6}	11.62×10^{-6}
Type Ex d frequency converter + type Ex e motor + safety temperature control system	8.86×10^{-6}	0.31×10^{-6}	8.55×10^{-6}	7.12×10^{-7}	7.84×10^{-6}

This paper verifies three different safety device configurations, as follows:

1. The system consists of a flameproof-type frequency converter and flameproof-type motor. The failure rate of the system should be the sum of two parts:

$$\lambda_{\text{tot}} = \lambda_{\text{D}} + \lambda_{\text{S}} = 9.04 \times 10^{-6}\ \text{h}^{-1}$$

$$PFH = \lambda_{\text{DU}} = 9.04 \times 10^{-7}\ \text{h}^{-1}$$

$$SFF = \frac{\lambda_{\text{sd}} + \lambda_{\text{su}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{\lambda_{\text{s}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{0 + 8.14 \times 10^{-6}}{9.04 \times 10^{-6}} = 90\%$$

The results show that the whole system is SIL level 2, according to the EPL Gb of equipment in Table 10, and is applicable to Zone 1.

2. The system consists of a flameproof-type frequency converter and increased safety-type motor. The failure rate of the system should be the sum of two parts:

$$\lambda_{\text{tot}} = \lambda_{\text{D}} + \lambda_{\text{S}} = 13.21 \times 10^{-6}\ \text{h}^{-1}$$

$$PFH = \lambda_{\text{DU}} = 9.7 \times 10^{-5}\ \text{h}^{-1}$$

$$SFF = \frac{\lambda_{\text{sd}} + \lambda_{\text{su}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{\lambda_{\text{s}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{0.62 \times 10^{-6} + 11.62 \times 10^{-6}}{13.21 \times 10^{-6}} = 93\%$$

The results show that the whole system is SIL level 1, according to the EPL Gc of equipment in Table 10, and is applicable to Zone 2.

3. The system is composed of a flameproof frequency converter and increased safety motor. The motor adds a temperature control module for additional temperature protection on the basis of increased safety protection. The temperature control of the whole motor will fail only if the temperature control function of the increased safety construction and the temperature control module fail at the same time. We assume the failure rate of the increased safety construction to be as follows: a 50% spark ignition failure rate and a 50% temperature control failure rate:

$$\lambda_{\text{DU}} = 4.52 \times 10^{-7} + 0.26 \times 10^{-6} + 0.26 \times 10^{-6} \times 0.04 \times 10^{-6} \approx 7.12 \times 10^{-7}$$

$$\lambda_{\text{tot}} = \lambda_{\text{D}} + \lambda_{\text{S}} = 8.86 \times 10^{-6}\ \text{h}^{-1}$$

$$PFH = \lambda_{\text{DU}} = 7.12 \times 10^{-7}\ \text{h}^{-1}$$

$$SFF = \frac{\lambda_{\text{sd}} + \lambda_{\text{su}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{\lambda_{\text{s}} + \lambda_{\text{dd}}}{\lambda_{\text{tot}}} = \frac{0.31 \times 10^{-6} + 7.84 \times 10^{-6}}{8.86 \times 10^{-6}} = 92\%$$

The results show that after adding the safety temperature control system, the SIL level of the system increases from SIL 1 to SIL 2, and the EPL level increases to EPL Gb, which is suitable for Zone 1.

5. Conclusions

According to the definition, the SIL of the explosion protection safety function is for a certain potential ignition source. The VFD system components have multiple ignition sources. When combined, the newly emerging hot surface ignition source does not meet the requirements of the corresponding explosion protection function SIL. It is not allowed to be used in the corresponding hazardous area. According to the provisions of the IEC60079-ff series standards, a VFD system composed of certified EPL Gb components can be used in Zone 1. At this time, the actual application is dangerous. Therefore, VFD systems composed of increased-safety motors cannot be used in hazardous areas Zone 1 in China. The example given in Section 4 is that a VFD system composed of increased-safety motors has passed the SIL assessment, and its safety level can be comparable to the EPL level. Equivalent, the premise of equivalence is that the explosion-protected function SIL corresponding to all potential ignition sources meets the requirements of Table 10. The IEC60079-0:2007 Annex

E prompts this safety issue, but does not give a specific method. This article attempts to solve similar problems by means of functional safety assessment. From the perspective of safety risks, the method proposed in this article is feasible.

1. The traditional explosion protection equipment defined in IEC60079-ff can be considered as safety devices and used for functional safety assessments.
2. The failure mode and effect of the explosion protection type as a safety device were analyzed, and the method for calculating the failure rate of an explosion protection type was given.
3. An increased safety VFD system with a safety temperature control device can improve the EPL level for Zone 1.
4. An improved explosion protection function safety assessment method was proposed to achieve an EPL safety level that cannot be achieved by the traditional IEC60079-ff explosion protection equipment, via a flexible configuration of the explosion protection and E/E/PE safety devices.

Author Contributions: Conceptualization, S.L. and X.W.; methodology, S.L.; writing—review and editing, S.L.; supervision, X.W.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Langeron, Y.; Barros, A.; Grall, A.; Bérenguer, C. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. *J. Loss Prevent. Proc.* **2008**, *21*, 437–449. [CrossRef]
2. Kosmowski, K.T. Functional safety concept for hazardous systems and new challenges. *J. Loss Prevent. Proc.* **2006**, *19*, 298–305. [CrossRef]
3. Lebecki, K. Functional Safety in Industrial Explosion Protection. *Trans. VŠB Tech. Univ. Ostrav. Saf. Eng. Ser.* **2012**, *VII*, 44–48. [CrossRef]
4. Faranda, R.S.; Fumagalli, K.; Bielli, M. Lithium-ion batteries for explosive atmosphere. In Proceedings of the 2019 Petroleum and Chemical Industry Conference Europe (PCIC Europe), Paris, France, 7–9 May 2019.
5. Fumagalli, K.; Martina, M.; Corbo, P. Light emitting diodes (LED) for installation in zone 1: A feasible procedure to determine the equivalent protection level. In Proceedings of the 2015 Petroleum and Chemical Industry Conference Europe (PCIC Europe), Berlin, Germany, 14–16 June 2016.
6. Smith, D.J.; Simpson, K.G. *Safety Critical Systems Handbook: A Straight Forward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849*; Elsevier: Amsterdam, The Netherlands, 2010; ISBN 0080967825.
7. Jespen, T. ATEX—Ignition sources. In *ATEX—Explosive Atmospheres*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 163–169.
8. *Explosion Prevention and Protection. Basic Concepts and Methodology*; EN 1127-1 (2001); European Committee for Standardisation: Brussels, Belgium, 1997.
9. Catelani, M.; Ciani, L.; Luongo, V. The FMEDA approach to improve the safety assessment according to the IEC61508. *Microelectron. Reliab.* **2010**, *50*, 1230–1235. [CrossRef]
10. Magyari, M.; Burian, S.; Friedmann, M.; Moldovan, L. Factors affecting the flameproof motor enclosures design for exploitation in explosive gas mixtures. *Environ. Eng. Manag. J.* **2012**, *11*, 1311–1316. [CrossRef]
11. Logistics Technology Support Group of Carderock Division Naval Surface Warfare Center. *Handbook of Reliability Prediction Procedures for Mechanical Equipment*; Carderock Division, Naval Surface Warfare Center: West Bethesda, ML, USA, 1992.
12. IEC. *IEC 60079-7(2015)—Electrical Apparatus For Explosive Gas Atmospheres—Part 7: Increased Safety 'e'*; IEC: Geneva, Switzerland, 2015.
13. Morris, S.F. Use and application of MIL-HDBK-217. *Solid State Technol.* **1990**, *33*, 65–70. [CrossRef]
14. Gavranic, I.; Ban, D.; Zarko, D. Explosion protected electrical drives—Risk assessment and technical diagnostics. In Proceedings of the Power Electronics and Motion Control Conference(EPE-PEMC 2008), Poznan, Poland, 1–3 September 2008.
15. Fae, E.; Patra, M.; Spohr, S.; Almin, J. Safety devices in Ex applications. Are you complying with Ex regulations? In Proceedings of the PCIC Europe Annual Electrical and Automation Knowledge Sharing Event, Antwerp, Belgium, 5–7 June 2018.

16. International Electro Technical Commission (Ed.) *IEC 2010.61508-1:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 1: General Requirements*; IEC: Geneva, Switzerland, 2010.
17. Brown, J.W.H.A. *The SAFEC Project*; The European Commission: Brussels, Belgium, 2019.