Broad Lane, Sheffield S3 7HQ
Telephone: 0114 289 2000
Facsimile: 0114 289 2500

HEALTH & SAFETY LABORATORY

Determination of Safety Categories of Electrical Devices used in Potentially Explosive Atmospheres (SAFEC) Contract SMT4-CT98-2255 Final Report

HSL/2000/01

Co-ordinator: A J Wilday (HSL)

Authors:
A J Wilday, A M Wray (HSL)
F Eickhoff, M Unruh (DMT)
E Fae, S Halama (INERIS)
E Conde Lazaro, P Reina Perbal (LOM)

Fire and Explosion Group

SUMMARY

Contract No CT98-2255 Determination of safety categories of electrical devices used in potentially explosive atmospheres (SAFEC)

Background

Existing CENELEC standards cover different types of electrical apparatus for use in potentially explosive atmospheres. The EU ATEX 100A Directive 94/9/EC has introduced Essential Safety Requirements and a categorisation system. EN 954, under the Machinery Directive, has a different categorisation system for safety-related devices. A categorisation system needs to be developed which is compatible with these and with standards for safety-critical control systems, such as IEC 61508.

Objectives

(1) To draft a description of appropriate subdivisions of safety devices. (2) To define all safety devices which are used in the context of electrical equipment for use in potentially explosive atmospheres and study their characteristics and performance in terms of the defined subdivisions. (3) To draft a method for identifying when a particular subdivision should be used, taking into account the application and working environment of the equipment. (4) To determine the correspondence between the proposed subdivisions and the relevant essential safety requirements.

Work programme

Task 1 was to derive target failure measures in the context of the ATEX requirements. Task 2 was to assess standards such as EN 954 and IEC 61508 for suitability in specifying and certifying that the required target failure measures have been achieved. Task 3 was to identify the types of safety devices which are currently in use. Task 4 was to study these safety devices to determine their characteristics and performance in relation to the target failure measures. Task 5 was to determine a methodology for testing, validation and certification. Task 6 was to prepare the current report and proposals for standardisation.

Results and Achievements

Three types of safety device have been identified: (1) those which are fully specified by the relevant CENELEC standards; (2) simple devices which can be specified according to EN 954; and (3) complex/ programmable devices which should be specified according to IEC 61508. For simple devices, the EN 954 categories which correspond to the fault tolerance requirements of the ATEX Directive have been defined. For complex/ programmable devices, safety integrity level (SIL) as defined by IEC 61508 is a suitable target failure measure. However, it will also be necessary to define additional fault tolerance requirements to conform with the ATEX Directive. Risk reduction targets for safety functions have been calibrated by considering individual risk criteria, accident statistics and the performance of existing safety devices. Good agreement was achieved between these different calibration methods. Risk reduction requirements have been defined for the safety function of explosion prevention for each hazardous zone in terms of safety integrity level (SIL), i.e. SIL3 in zone 0; SIL2 in zone 1 and SIL1 in zone 2. The SIL target for a particular safety device may be less than this as the requirement can be allocated between the safety device and the rest of the equipment. A certification scheme has been proposed.

CONTENTS

1. INTRODUCTION

1.1 Background

Electrical apparatus, which is intended for use in potentially explosive atmospheres, sometimes relies on the correct operation of control or protective devices in order to maintain certain characteristics of the apparatus within acceptable limits. Examples of such devices are motor protection circuits (to limit temperature rise during stall conditions) and overpressurisation protection.

The approval and certification of electrical apparatus for potentially explosive atmospheres, therefore, requires that, where such control and protection devices are used, an assessment be made of their suitability for the intended purpose. This will need to be expressed in terms of some measure of confidence that the devices will be able to maintain a required level of safety at all times. This measure of confidence needs to be compatible with the EC ATEX Directive (1), CENELEC standards e.g. (2-15) for electrical apparatus for use in potentially explosive atmospheres and relevant control system standards, e.g. (16,17).

CENELEC identified the need for research to determine whether existing and proposed standards in the field of safety-related control systems are suitable for this purpose, and to develop a methodology which will provide the required support for the approval and certification process. Research proposals on this topic were invited under the Standardisation, Measurement and Testing (SMT) Programme and the SAFEC project was selected for funding. The project began in January 1999 and the end date, after agreed extension, is May 2000.

1.2 The SAFEC project

The SAFEC project (contract SMT4-CT98-2255) had the overall objective to produce a harmonised system for subdivision of safety devices which are used in potentially explosive atmospheres, together with a methodology for selecting the appropriate subdivision of safety device for any particular application.

The SAFEC partners were the Health and Safety Laboratory of the Health and Safety Executive (HSL) in the UK (the project coordinator), the Deutsche Montan Technologie (DMT) in Germany, the National Institute for Industrial Environment and Risks (INERIS) in France and the Laboratorio Oficial J.M. Madariaga (LOM) in Spain.

The SAFEC project comprised six tasks:

1. Derivation of target failure measures (all/HSL).

2. Assessment of current control system standards with reference to the target failure measures from Task 1 (HSL).

3. Identification of safety devices currently used with reference to CENELEC standards (LOM).

4. Study "used safety devices" identified in Task 3 (INERIS).

5. Determination of a methodology for testing, validation and certification (DMT).

6. Production of a final report including a proposal for incorporation in European standards (all/HSL).

The reports on these project tasks form Annexes A-E, respectively, to this final report on the project.

1.3 Scope

The scope of the SAFEC project was limited to:

a) Electrical apparatus which comes under the requirements of the ATEX Directive (1), i.e. the focus was on what can be done by the manufacturer of equipment which is for sale (rather than on what should be done by the user of equipment and covered under the 118A Directive (18)).

b) Electrical apparatus for use in explosive atmospheres for which safety devices are relevant. This includes Type “e" (increased safety) (7) and Type "p" (pressurisation) (4).

c) All types of safety devices. This includes those which are electrical, electronic or programmable electronic in nature. Some such devices may be relatively complex so that the type and consequence of failure may be indeterminate, e.g. because failures may result from latent systematic faults. Less complex safety devices are also included such as, for example, a switch which cuts off the power to flameproof equipment if it is opened; or thermal fuses (if provided by the manufacturer rather than by the user).

The SAFEC project was concerned with specifying the reliability/ fault tolerance/ integrity requirements of safety devices. Such safety devices could be located either within the hazardous area or outside it. If it were located within the hazardous area then the safety device itself would need to be designed so as not to cause an ignition. The design of safety devices so as not to itself cause ignition was not considered by the project.

Although the SAFEC project was concerned with safety devices for electrical equipment, the results may also be applicable to non-electrical equipment.

1.4 Liaison with CENELEC and CEN

The partners of the SAFEC project worked co-operatively with the members of CENELEC Technical Committee 31, Working Group 09 (WG09), which is drafting a standard on "Reliability of safety-related devices". It is intended that the SAFEC results will be utilised by WG09 in this standard. A number of joint meetings were held. Dr Eickhoff of DMT, who was one of the partners of the SAFEC project with responsibility for the delivery of Task 5, was also a member of WG09. He took over the role of convenor of WG09 in February 2000. During the course of the SAFEC project, liaison was also maintained with CEN Technical Committee 305, Working Group 2 (WG02), who are concerned with non-electrical sources of ignition. A representative of WG02 attended the joint meetings of SAFEC and WG09.

2. IDENTIFICATION OF SAFETY DEVICES

The SAFEC project is focused on safety, controlling and regulating devices. These are parts of equipment or protective systems, and have an autonomous safety function. Task 3 of the project (see Annex C), performed by LOM, was concerned with the identification of safety devices which are used within electrical apparatus for use within potentially flammable atmospheres and which therefore came within the scope of the SAFEC project. LOM reviewed relevant CENELEC standards (2-9), together with their database and manufacturers' equipment catalogues. Information relating to safety devices was extracted.

A summary of the identified safety devices is given in Table 1. Each item includes an indication whether the safety devices are already specified in existing CENELEC standards or whether the safety device would need to be handled by the standard that is being developed by WG09. It should be noted that the list is neither definitive nor exhaustive. However, it does establish a guide list of the of sorts of safety devices that needed to be studied or considered within the SAFEC project.

Table 1 Examples of identified safety devices

Description of safety device	**Specified by existing standard(s)?**
Motor protection; especially for type 'e': thermal and current relays, PT100, switches	Yes. CENELEC
Overload monitoring devices for 'e' motors, which models the temperature-time characteristic	Yes. CENELEC
Thermal protection devices and non-electronic control units for heating systems	Yes. CENELEC
Overvoltage protection	Yes. CENELEC
Monitoring units for concentration of flammable gases, oxygen or inert gas levels, e.g. gas detectors, limit detectors for end of line	Yes. CENELEC

Description of safety device	Specified by existing standard(s)?
Systems for transmission and data acquisition (SCADA) for safety purposes, e.g. mining power shut-off in Group 1	Yes. existing national standards and code of practice
PLC (programmable logic control) units, including the application software, for safety purposes	No. To be covered by WG09
Level indicators and switches for liquids used to provide safety for submersible equipment	No. To be covered by WG09
Adjustable protection elements of AC converters for 'p', 'e', 'd'. 'n' type motors (current limitation, overload protection, thermal limitation, etc...).	No. To be covered by WG09
Electronic devices controlling flow, temperature and/or level of cooling (liquid or gas) for 'd', 'p' and 'e' motors	No. To be covered by WG09
Control devices for bearings in big rotating machines. Lubrication and temperature control devices	No. To be covered by WG09
Pressure monitoring systems for 'p' type.	No. To be covered by WG09
In belt transportation systems, devices for controlling the alignment and slip of the belt.	No. To be covered by WG09
For bucket elevators anti-runback devices and belt speed meters to detect belt slip. Also control of bearings. Detectors of feed rate to avoid overloads	No. To be covered by WG09

Some issues that came out of the identification exercise were:

- In some cases it can be difficult to differentiate components and safety devices. This has to be carefully considered, because otherwise a large number of components could be considered as safety devices (for example safety barriers separating intrinsically-safe from non-intrinsically-safe circuits).

- The same device can have different safety or protecting levels depending on the particular situation in which it is applied (for example, a thermocouple, the signal of which can be used just for monitoring temperature or to activate a disconnecting switch).

A table of safety devices, based on Table 1 and Annex C was further developed in conjunction with WG09. This table is given as Table A1 in Appendix 1.

3. REVIEW OF CONTROL SYSTEM STANDARDS

Task 2 of the SAFEC project, carried out by HSL, included a review of existing control system standards. Since safety devices are defined as having an autonomous safety function (or controlling function), it was expected that control system standards might

be useful in defining the requirements for safety devices. The report on Task 2 of the project is Annex B of this report.

There are two standards which provide guidance on the design of control systems for use in safety-related applications:

- EN 954-1 (16), and
- IEC 61508 (17).

3.1 EN 954-1 requirements

EN 954-1 (16) allows control systems to be categorised as B, 1, 2, 3 or 4. The principles of EN 954-1 are based on fault tolerance. This is adequate for simple systems where there is a good understanding of the failure modes. However, it is less appropriate for more complex systems, including programmable systems, in which there is not a good understanding of fault behaviour.

EN 954-1 gives no means of assessing or ensuring the integrity of software.

EN 954-1 mentions maintenance, but gives little guidance. In any safety-related protection system (which may be called to operate only infrequently), regular manual proof testing (in the absence of automatic diagnostics) is an important factor in maintaining the integrity, which will vary approximately linearly with the frequency of the manual proof checks.

EN 954-1 is a concept standard, so does not give advice on the manufacture of the system being designed. A well-designed system that is not well manufactured or maintained could have a reduced integrity.

By assuming that subsystems are single components and applying the fault exclusion principle, it is possible to determine a Category without the need for complex calculation. However, the failure rate of a complex subsystem may be considerably higher than that of a single component. Therefore, the Category of a dual-channel subsystem cannot be considered equivalent to a dual-channel system at the component level, e.g. an interlock based on 2 relays cannot be compared with one based on two complex PLCs, even if both interlocks achieve Category 3. Hence, two systems, each having the same Category, may not necessarily have the same level of safety integrity (see 3.2 below for definition).

The Categories in EN 954-1 are not hierarchical.

3.2 IEC 61508 requirements

IEC 61508 (17) is a much later standard than EN 954-1, having been only recently published. IEC 61508 defines safety integrity levels (SIL) for safety-related control functions by taking into account:

- quantified reliability of the safety function (see Table 2). The failure-to-danger rate of the functions carried out by a safety-related system must be less than that which would lead to an unacceptable hazard rate. The quantified analysis of a system deals with the random hardware failure rate;

- qualitative reliability. The techniques used to design, maintain, etc. the system throughout its lifecycle must be sufficient to ensure that the rate of systematic failures is less than the random hardware failure rate; and

- architectural constraints, based on fault tolerance and fail-to-safety characteristics. These put a ceiling on the safety integrity level (SIL) that can be claimed for any particular system in order to ensure that uncertain reliability calculations, e.g., where reliability data are sparse, do not lead to an inflated SIL (see Table 3).

Table 2 Quantitative reliability requirements of IEC 61508

SIL	Probability of failure on demand (for low demand rate operation)	Frequency of failure (per hour) for continuous operation
4	10^{-5} - 10^{-4}	10^{-9} -10^{-8}
3	10^{-4} - 10^{-3}	10^{-8} - 10^{-7}
2	10^{-3} - 10^{-2}	10^{-7} - 10^{-6}
1	10^{-2} - 10^{-1}	10^{-6} - 10^{-5}

Table 3 Architectural constraints of IEC 61508

For type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	**1**	**2**
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

For type B safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	**1**	**2**
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99%	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

3.4 Summary of the standards with respect to the ATEX Directive

The ATEX Directive (1) (see Annex B) requires that:
The time to detect a fault of a safety device shall be small in order give a high probability of ensuring that equipment will be put into a safe state before a dangerous situation can occur.
The design should take the mode of failure of components into account and ensure that the most probable failure modes of the components lead to a safe state.
In general, safety-related systems should be mechanical, pneumatic, hydraulic, electromechanical, electrical or electronic but not programmable.
Software should be designed to minimize the probability of systematic faults.
For Category 1 equipment, if a single protection system is used, this should have a fault tolerance of two. If multiple protection systems are arranged in a redundancy configuration, the design should tolerate the failure of a single channel. Therefore, the component fault tolerance must be two (single-channel protection) and the channel failure tolerance should be at least one (multiple-channel protection).
Category 2 equipment should tolerate "normally taken into account" single faults - faults considered to be credible by the designer and/or specified in relevant CENELEC standards.
There is no fault-tolerance requirement for Category 3 equipment.
There are no requirements for fail-safe fraction, diagnostics, diagnostic coverage or component/equipment failure rates. In this respect, the ATEX Directive appears to

assume that the failure rate of a fault tolerant system is likely to be low over the lifetime of the equipment. This may be difficult to justify without further qualification.

However, these ATEX Directive requirements lead to concerns that:

- Although all the parameters required in a quantified risk assessment seem to have been covered, these parameters have been considered individually as if they are independent. Unfortunately, they are not;
- In trying to measure integrity in terms of fault tolerance, the Directive does not take into account reliability.

These concerns may not be a problem when safety devices are fully specified by existing CENELEC standards. However, the SAFEC project is concerned with specifying the requirements for safety devices which are not already fully specified and may perhaps be implemented using novel technology (PLC etc.).

A summary of how the two control system standards, EN 954 (16) and IEC 61508 (17) are useful in defining the requirements of safety devices under the ATEX Directive (1) is as follows:

1. IEC 61508 takes an overall approach to safety integrity and covers all types of electronic safety-related systems, whereas EN 954-1 is not suited for application to programmable systems.

2. IEC 61508 gives a determination of integrity but EN 954-1 is based on fault tolerance.

3. IEC 61508 uses fault tolerance only to determine a ceiling for the SIL that can be claimed for a system and even then uses this only in conjunction with diagnostic coverage (or fail-safe fraction).

4. EN 954 is based on fault tolerance; however, it does not have a category corresponding directly to a fault tolerance of 2 as required by the ATEX Directive for Category 1 of equipment-group II. EN 954 has 5 categories for describing control systems:
    - Category B has a fault tolerance of 0;
    - Category 1 has a fault tolerance of 0;
    - Category 2 has a fault tolerance of 0 but has automatic monitoring;
    - Category 3 has a fault tolerance of 1, and
    - Category 4 has:
        - a fault tolerance of 1 with automatic monitoring, **or**
        - a fault tolerance of 2 or more.

5. IEC 61508 (or industry-specific standards that will be based on it) is likely to be the dominant standard for all future safety-related systems using complex and programmable components.

6. IEC 61508 allows the integrity of systems containing programmable electronics to be determined and, as a result, will allow the integrity of these systems to be

determined in the future when they eventually become widespread in this type of application.

7. It will be realised that either standard could be used to determine the integrity of equipment intended for a hazardous atmosphere; but:
    - IEC 61508 would provide a better indication of system integrity; however,
    - neither standard would fully provide the ATEX requirements of fault tolerance which are required by legislation to be followed by any standard appropriate to equipment for use in hazardous zones.

EN 954 can be used for simple safety devices, e.g. mechanical interlocks, especially where the appropriate CENELEC standard refers to EN 954. However, it is recognised that some existing CENELEC standards make reference to EN 954 in cases where nowadays it would be more appropriate to refer to IEC 61508, particularly for complex or programmable safety devices.

Therefore, it is proposed that any industry-specific standard for complex and programmable safety devices should be based on IEC 61508 but have an additional requirement, based on fault tolerance, which will ensure that the fault tolerance requirements of the ATEX Directive are met:

- a fault tolerance of 2 is required by the ATEX Directive for the protection system of Category 1 equipment when the protection system is the sole means of protection against explosion;

- a fault tolerance of 1 is required by the ATEX Directive for the protection system of Category 2 equipment when the protection system is the sole means of protection against explosion;

- a fault tolerance of 0 is required by the ATEX Directive for the protection system of Category 3 equipment.

4. CHOICE OF TARGET FAILURE MEASURES

4.1 Types of target failure measure

The choice of target failure measure is discussed fully in Annex A. The following types of target failure measure are possible, as highlighted by the discussion of control system standards in section 3 above:

- fault tolerance - the number of faults which must be tolerated by the system before the loss of safety function;

- reliability, e.g. the maximum frequency of occurrence of faults or the maximum probability of failure on demand;

- functional safety management – to reduce the likelihood of systematic faults in hardware and software during all stages in the lifecycle.

For the purposes of this report, which is concerned only with failures to danger, and, in the absence of any alternative concise and convenient term, the term “reliability” is used to refer only to those failures which result in the system in which they occur moving to a less-safe state.

4.2 Discussion

The ATEX Directive (1) sets requirements in terms of fault tolerance. This can be summarised as follows:

- For Category 1 equipment, if a single means of protection is used, this should have a fault tolerance of two. If multiple protection systems are arranged in a redundancy configuration, the design should tolerate the failure of a single channel.

- Category 2 equipment should tolerate "normally taken into account" single faults. Such credible faults would sometimes be defined by the relevant CENELEC standards.

- There is no fault-tolerance requirement for Category 3 equipment, i.e. it shall be safe in normal operation.

However, the integrity of any system with a fault tolerance greater than 0 will be dependent on the automatic diagnostic and manual proof tests (including the intervals between them) carried out on the system. Therefore, a requirement for a particular level of fault tolerance is an incomplete requirement for defining system integrity for complex and/or programmable systems.

For example, consider a system designed to have a fault tolerance of 1. If that system is never tested, eventually a fault **will** occur. The system now has a fault tolerance of 0 and this situation will remain until a test, that will identify the fault, is carried out and the system is repaired. All that can be stated regarding a system with a fault tolerance of 1 is that its integrity is likely to be higher than that of a system with a fault tolerance of 0 and likely to be lower than that with a fault tolerance of 2. However, even this limited statement assumes that the proof-test interval and the failure rate of the components/channels are approximately the same in all cases.

Possible target failure measures, which are defined within existing standards, are:
- safety integrity level (SIL), as defined in IEC 61508 (17); and
- categories, as defined by EN 954 (16).

These were discussed in section 3 above. It is noted that CENELEC TC31 Working Group 9 (WG09) had independently reached the conclusion that IEC 61508 SIL was an appropriate target failure measure for safety devices. The draft standard which they were developing (19) was attempting to define the required SIL for safety devices on each of the different ATEX categories of electrical apparatus. However, some existing CENELEC standards make reference to EN 954.

It was decided that the target failure measures for safety devices should be as follows:

1. The fault tolerance requirement of the ATEX Directive shall be met.

2. In addition,
   - complex/programmable systems should achieve the relevant safety integrity level (SIL);
   - simple systems should meet the EN 954 category which achieves the relevant ATEX fault tolerance requirement.

However, it was also recognised that some safety devices may already be fully specified within relevant CENELEC standards, e.g. references (2-15). In these cases, it may not be necessary to further specify the safety device in terms of IEC 61508 or EN 954. Table 1 has identified some example safety devices for which this is the case.

5. CALIBRATION OF SIL REQUIREMENTS FOR COMPLEX AND/OR PROGRAMMABLE SAFETY DEVICES

5.1 Introduction

Since SIL is to be used as target failure measure for complex/programmable safety devices, it is necessary to define or calibrate the SIL required for each ATEX equipment category. The ATEX Directive (1) defines two Groups of application of electrical equipment, each of which has Categories of electrical equipment according to the level of protection required:

Group I comprises mining applications where the flammable material is methane (firedamp) or flammable dust:

- Category M1 means that the equipment is required to remain functional in an explosive atmosphere.

- Category M2 equipment is intended to be de-energised in the event of an explosive atmosphere.

Group II comprises other applications where equipment is to be used in a potentially explosive atmosphere:

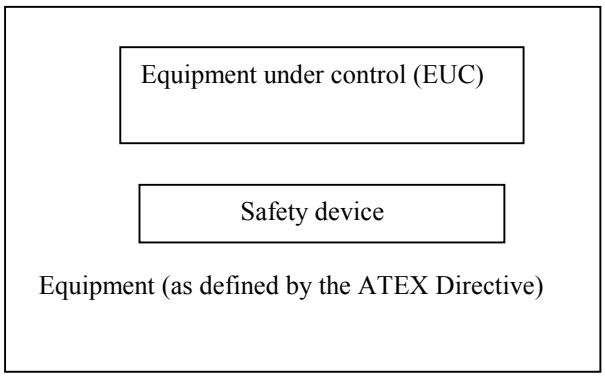
- Category 1 equipment is intended for use in Zone 0 and/or 20, where explosive atmospheres are present continuously, for long periods of time or frequently.

- Category 2 equipment is intended for use in Zone 1 and/or 21, where explosive atmospheres are likely to occur.

- Category 3 equipment is intended for use in Zone 2 and/or 22, where explosive atmospheres are less likely to occur, and if they do occur, do so infrequently and for only a short period of time.

The SIL required to be calibrated by the SAFEC project is that for a safety device which forms part of the electrical equipment. The remainder of the equipment is the "equipment under control" (EUC) as defined in IEC 61508 (17). This is illustrated in Figure 1.

Figure 1 Definition of terms



The requirement is to calibrate the SIL needed for each ATEX equipment category and hence for each hazardous zone. However, it needs to be remembered that a target SIL requirement applies to a particular safety function, not to a safety device. According to IEC 61508 (17), the safety function may be implemented by a range of technologies and each may achieve a part of the required risk reduction. This is illustrated in Figures A.1 and A.2 of Part 3, Annex A of IEC 61508, on which Figure 2 is based.

External risk reduction facilities and "other technology" safety systems may include factors such as an operating procedure for pressurised equipment which prohibits the opening of the pressurised cabinet if an external flammable atmosphere is detected (see 5.4.1, function 2). The E/E/PE safety-related systems may include both the safety device and the power supply for the apparatus being protected (see 5.4.1, function 1).

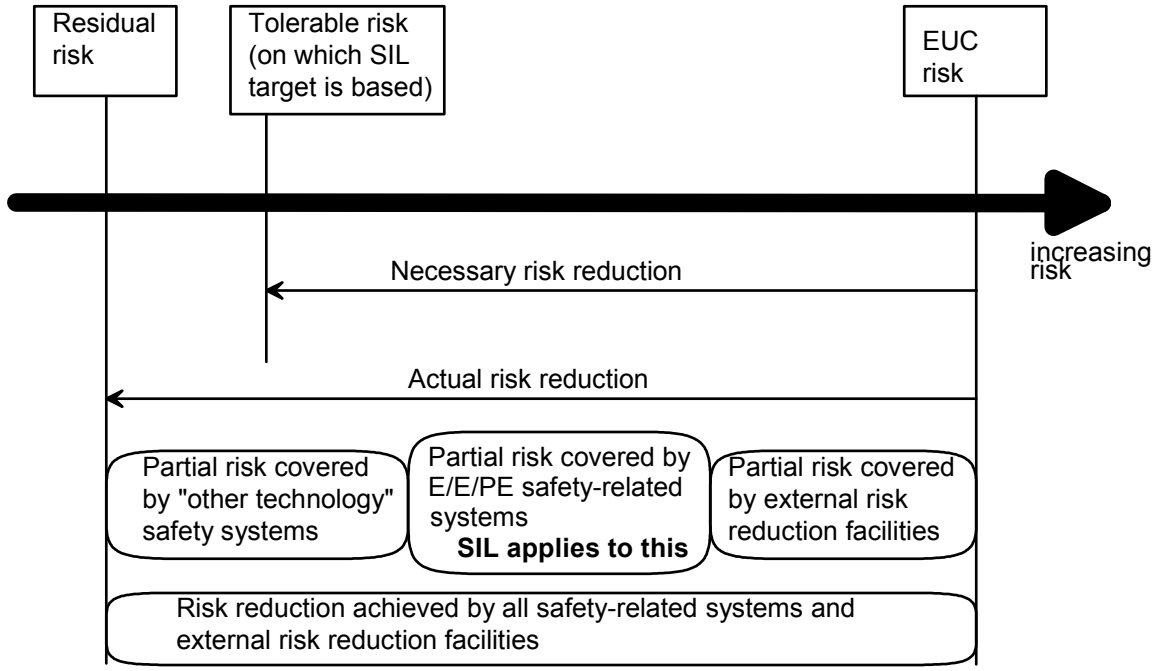


Figure 2 Risk concepts from IEC 61508

The objective here is to calibrate the required risk reduction and hence the SIL required for the safety function of preventing ignition of a potentially explosive atmosphere. Three approaches were used to calibrate the SILs required:

- Use of individual risk criteria to determine the necessary risk reduction;
- Use of accident statistics to attempt to determine the SIL for existing equipment;
- Estimation of SILs of safety devices within existing equipment.

These are discussed in more detail in the following sections.

5.2 Use of individual risk criteria.

A review of possible risk criteria was undertaken during Task 1 of the project and is included in Annex A. The use of such criteria to calibrate SILs was undertaken during Task 2 and is reported in detail in Annex B.

The probability of a flammable gas being present in a particular zone is normally defined in a qualitative way, e.g., continuous, frequent or less frequent. Reference (20) provides a convenient quantitative definition of the zones in terms of the time that flammable gas would be expected to be present. This is:

Zone 0: >1000 hours per year;
Zone 1: <=1000 but >10 hours per year, and
Zone 2: <=10 hours per year.

It should be noted that these values have not been well accepted in all industrial sectors so, although they have been considered by CENELEC working groups, they have not been incorporated in standards. For the purpose of calculations here, Zone 1 was divided into two equal zones each covering a factor of 10 leading to the values shown in Table 4. In all cases, the probability of occurrence corresponds to the worst-case probability for the particular zone.

Table 4 Probability of an explosive atmosphere being present

Zone	Quantitative assumption (hrs/yr)	Probability of occurrence (%)
0	>1000	100
1H	<1000 and >100	10
1L	<100 and >10	1
2	<10	0.1

The HSE document *Tolerability of risk from nuclear power stations* (21*)* indicates that a probability of death of 10^{-3} per year is intolerable for a worker and 10^{-4} per year is intolerable for a member of the public. In the other direction, a probability of death of 10^{-6} would be considered to be acceptable. Based on these overriding criteria, we can determine a coarse estimate of the system integrity, as shown in Table 5. The shaded column corresponds to a tolerable risk criterion of 10^{-5} per year of death. This is the criterion used in reference (22).

Table 5 Coarse estimate of integrity requirement based on risk tolerability criteria

					Unit
Probability of death to be achieved	1,000	100	10	1	per 10^6 yrs
Number of workers/members of the public present[1]	0.2	0.2	0.2	0.2	
Required risk reduction:					
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 0	0.57	0.057	0.006	0.0006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 1H	5.7	0.57	0.06	0.006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 1L	57	5.7	0.57	0.06	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 2	570	57	5.7	0.57	per 10^6 hrs
Equivalent safety integrity requirement:					
SIL required to achieve target[2], Zone 0	SIL2	SIL3	SIL4	SIL5[3]	
SIL required to achieve target, Zone 1H	SIL1	SIL2	SIL3	SIL4	
SIL required to achieve target, Zone 1L	SIL1[4]	SIL1	SIL2	SIL3	
SIL required to achieve target, Zone 2	SIL1[5]	SIL1[6]	SIL1	SIL2	

Notes to Table 5:

[1] This assumes 20 deaths per 100 explosions involving pressurization systems.

[2] This is the SIL of the overall safety function and includes all protection measures/devices. It is based directly on the maximum allowable failure frequency of the safety function, from the rows above, and assumes continuous operation of the safety function with the SIL taken from Table 2.

[3] SIL5 is outside the range of achievable SILs considered by IEC 61508; however, SIL 5 has been used here in order to make the table more meaningful.

[4, 5 and 6] SIL1 represents the minimum integrity requirement of IEC 61508 for a system defined as being safety-related; therefore, SIL1 must apply to these positions.

5.3 Use of accident statistics

It can be assumed that existing certified electrical equipment is of adequate integrity, given that there is no history of explosions which have been ignited by certified electrical equipment. Discussion with a UK manufacturer of pressurization systems has

indicated that about 18,000[1] such systems have been put into service in the UK over the past 20 years. Assuming a life expectancy in the region of 8 years, this suggests an average of about 6,000 systems have been in use over this time.

The partners were not aware of any explosions resulting from the failure of a pressurization system. Therefore, this sets a lower limit on the integrity of pressurization systems over the past 20 years, as shown in Table 6, below. The values in Table 6 were calculated on the assumption that, if no explosions occur over N operating hours, the probability of an explosion occurring in the next N operating hours is 0.5 (see also Annex B).

Table 6 suggests that the integrity of existing pressurization systems is:

SIL1, if they have been mainly used in Zone 2;
SIL2, if they have been mainly used at the lower end of Zone 1, or
SIL3, if they have been mainly used at the upper end of Zone 1.

However, as the probability of gas in the majority of Zone 1 environments will probably lie near the lower end of the zone (i.e., Zone 1L as shown in Table 6) with few at the upper end (shown as Zone 1H), Table 6 should not be considered to indicate that existing pressurization systems are able to achieve SIL3.

It is understood that pressurization systems are used:

- in Zone 1 with incendive equipment. In this case, the equipment is tripped if pressurization were to fail and an alarm is given.
- to protect Zone 2-type equipment in Zone 1. In this case, if pressurization were to fail an alarm is given.
- to protect incendive equipment in Zone 2. In this case, if pressurization were to fail an alarm is given.

[1]Determined from the number of systems supplied by the manufacturer and its share of the UK market.

Table 6 SIL indications from accident records

	Assumed zone of operation[1]			Units
	Zone 1H	Zone 1L	Zone 2	
Period of study	20	20	20	years
Number of systems in use in the UK over this period	6,000	6,000	6,000	
Total operating period	1,051,920,000	1,051,920,000	1,051,920,000	system-hours
Probability of gas presence[2]	0.032	0.0032	0.00032	
Operating period with gas present	33,661,440	3,366,144	336,614	"gas" hours
Number of known explosions	0	0	0	
Indicated dangerous failure rate for each system	0.015	0.15	1.5	per 10^6 hrs
Indicated SIL for the overall safety system[3]	SIL3	SIL2	SIL1	

Notes to Table 6:

[1] The data in each of the columns have been calculated on the basis that all systems were used in the single specified zone.

[2] It would be inappropriate to use the worst-case probabilities for the presence of flammable gas in the calculations in this particular table, as we must use an estimate of the actual probability. Without any prior knowledge of the distribution of this probability, the logarithmic mean of the range of probabilities covered by each (sub) zone has been used. This is: Zone 1H - 3.2%; Zone 1L - 0.32% and Zone 2 - 0.032%.

[3] This is the average SIL of the total configuration of safety-related systems. The pressurization control system (e.g., purge and shutdown systems) will contribute to this SIL together with other systems, e.g., the air supply.

The equipment may be used in either Zone 1 or Zone 2, but for Zone 2 the pressurisation system would be less sophisticated and without automatic purging. Table 6 strongly suggests that the overall integrity of existing pressurization systems is at least SIL1. The available data is insufficient to prove that the SIL is higher than this. The SIL estimation is based on the best information available but a number of assumptions have been made.

5.4 Estimation of SILs for existing safety devices

Again, it can be assumed that existing certified electrical equipment is of adequate integrity, given that there is no history of explosions which have been ignited by certified electrical equipment. Therefore the SILs of existing safety devices can be

assumed adequate. SILs for the following safety devices have been estimated during the SAFEC project:

- Two safety functions within a pressurisation system. This was done during Task 2 and further details are given in Annex B.

- Diode safety barrier. This was done during Task 4 and further details are given in Annex D.

- Level detection safety device. This was done during Task 4 and further details are given in Annex D.

- Pressure and temperature safety devices. This was done during Task 4 and further details are given in Annex D.

These are discussed further below.

5.4.1 Pressurisation system

A generic design of pressurisation equipment was provided by a manufacturer. This was assessed in order to estimate the SIL by component failure analysis for the two safety functions:

- Function 1: to turn off the equipment within the pressurized enclosure if the pressurization fails. The author understands that this function may not be used, depending on the application; however, for the purpose of this assessment, it will be assumed that this function is utilized. This will be referred to as Function 1.
- Function 2: to purge the enclosure prior to power being allowed to the equipment within it. This will be referred to as Function 2.

The pressurisation system design and failure rate calculations are detailed in Annex B. Component failure rates were taken from the literature and are also detailed in Annex B.

For function 1, the probability of failure on demand was estimated as 9.2×10^{-4}. However, loss of Function 1 will not lead to a failure of the pressurized enclosure unless it is associated with a simultaneous failure of the air supply. The failure rate of the air supply was estimated as 201 per 10^6 hours. This leads to an overall failure rate of the pressurized enclosure (i.e., loss of pressurization with equipment in the enclosure powered) of 0.18 per 10^6 hours, as shown in Column 2 of Table 7. This is equivalent to SIL 2. However, the overall probability of a pressurization failure with the power applied is proportional to the failure rate of the air supply, so an increase in the availability of compressed air will lead to a corresponding increase in the integrity of the safety function. For example, in practice, the air supply may:

- be a redundancy system in order to achieve a high availability for use by other systems in the plant associated with production, or

- lead to a shutdown of the plant if the air supply fails. Therefore, minimizing the probability of subsequent leakage of flammable substances.

The effect of improving the reliability of the air supply by a factor of 10 to 20 per 10^6 hours, as shown in the shaded column of Table 7. This would be equivalent to SIL 3 for the safety function.

Table 7 Determination of the hazard rate associated with Function 1

Component	Item	Item	Unit
Probability of failure on demand: Function 1 ($P=\lambda_1 T/2$)	9.2	9.2	$*10^{-4}$
Failure rate of air supply (λ_2)	201	20	per 10^6 hrs
Failure rate of pressurization with power applied ($P*\lambda_2$)	0.18	0.02	per 10^6 hrs
Safety integrity level of overall protection function (this has only been determined quantitatively and does not consider the qualitative requirements of IEC 61508)	SIL2	SIL3	

For function 2, the estimated probability of failure on demand was calculated as 1.99 x 10^{-3}, equivalent to SIL2 (based solely on the quantitative analysis and not considering any of the qualitative requirements of IEC 61508). However, the reliability of achieving the safety function could be higher than this because the human nose can detect most gases at levels well below their lower explosive limit and it is considered unlikely that a pressurized enclosure would be opened if gas were smelled. The reliability of the operator would therefore contribute to achieving the safety function.

5.4.2 Diode safety barrier

Diode safety barriers are assemblies incorporating shunt diodes or diode chains (including zener diodes) protected by fuses or resistors or a combination of these. The diodes limit the voltage applied to an intrinsically safe circuit and a following infallible current limiting resistor limits the current which can flow into the circuit. These assemblies are intended for use as interfaces between intrinsically safe circuits and non-intrinsically safe circuits.

The diode safety barrier shall comply with requirements of EN 50020 [8] which specifies in particular for safety devices that the assembly must contain :

- three diodes or three diode chains for category « ia » (safe with two faults and suitable for use in Zone 0),
- two diodes or two diode chains for category « ib » (safe with one fault and suitable for use in Zone 1).

The analysis of a category « ia » Zener diode safety barrier (see Annex D) indicates that it meets the SIL 4 level qualitative and quantitative requirements.

5.4.3 Level detection safety device

A safety low level detection system installed in a tank containing liquid or liquefied hydrocarbons was considered. The system is constituted of one detector connected to a processing unit to detect a low level in order to shut off the electric power. Such safety devices are required to prevent ignition by submersible equipment (see Table 1).

The assessment of the SIL for such a safety device is detailed in Annex D. If a processing unit design in simple chain tolerance to " 0 " failures is selected and if the following values are selected for the overall safety level detection system : a failsafe fraction (FSF) inferior to 60% and a probability of failure on demand (PFD) of $1.7*10^{-2}$, the safety level detection system can be graded as safety related control system, and is compliant with the SIL 1 level qualitative and quantitative requirements for a one year term and for operation on demand.

5.4.4 Pressure and temperature safety devices

This could include the pressure trip within a pressurisation system (i.e. the same as function 1 in 5.4.1 above) and the temperature trip used to protect a motor from overheating.

Full details of the assessment are given in Annex D. If the power supply shut off device is designed in simple chain tolerance to " 0 " failure, a failsafe fraction of 85% and a PFD of $1.35*10^{-3}$ is selected, the device meets the SIL 2 level qualitative and quantitative requirements for operation on demand for a year and for a safety related protection system.

5.5 Discussion and calibration of risk reduction targets

A summary of the results of the above calculations for the purpose of calibrating the target risk reduction (SIL) requirement are given in Table 8.

It can be seen from Table 8 that there is a good degree of convergence between the different methods of calibrating the target risk reduction requirements for the different hazardous zones. The approach of the SAFEC project has been to find targets which are in line with published risk tolerability criteria and are also achievable by existing safety devices. The lack of any history of explosions ignited by certified electrical equipment strongly suggests that current designs of safety devices are adequate.

It is proposed that the target risk reduction requirements, for the safety function of protecting against a hypothetical case in which there is a source of ignition in normal operation, be defined according to Table 9. This hypothetical case was found to be a useful concept for the purposes of SIL calibration. However, it should not be taken to

imply that the authors believe that apparatus with ignition sources during normal operation and protected only by a safety device would be a suitable design for use in a potentially explosive atmosphere. Indeed, the authors expect the results derived here to be used to fully specify safety devices within apparatus which is otherwise specified by CENELEC standards, such as references (2-15).

Table 8 Summary of calculations for calibrating target risk reduction requirement

Section of report	Description of method	Target risk reduction requirement		
		Zone 0	**Zone 1**	**Zone 2**
5.2	Use of individual risk criteria	SIL 3	SIL 2 (Note a)	SIL 1
5.3	Use of accident statistics applied to pressurised systems		SIL 2 or SIL 3	SIL 1
5.4.1	Estimated SIL for pressurisation system. Turn off equipment if pressurisation fails.		SIL 2 or SIL 3 (Note b)	
5.4.1	Estimated SIL for pressurisation system. Purge before allowing power onto equipment		SIL 2 (Note c)	
5.4.2	Estimated SIL for diode safety barrier	SIL 4		
5.4.3	Estimated SIL for low level detection system			SIL 1 (Note d)
5.4.4	Estimated SIL for pressure safety device		SIL 2 (note e)	
5.4.4	Estimated SIL for temperature safety device		SIL 2 (note f)	SIL 2 (Note f)

Notes for Table 8

(a) This is the worst case, corresponding to the higher band of assumed probability that a flammable atmosphere would be present.

(b) SIL 3 is possible given a suitably reliable air supply.

(c) The overall integrity could be increased by suitable operating procedures, such that SIL 3 may also be possible.

(d) The assumed application was within an LPG tank. This will usually be non-flammable (above UFL) and will therefore correspond to Zone 2.

(e) This could be increased given a suitably reliable air supply (see 5.4.1)

(f) The temperature safety device is assumed to be on a motor intended for use in either Zone 1 or Zone 2.

Table 9 Proposed target risk reduction requirements for the hypothetical case of protecting against an ignition source during normal operation

Hazardous Zone	ATEX equipment categories	Target SIL requirement
0 or 20	1	SIL 3
1 or 21	2	SIL 2
2 or 22	3	SIL 1

It is very important to note that these target risk reduction requirements refer to the safety function and not to the safety device. The safety function may be partly achieved by design features of the certified electrical equipment other than the safety device. Indeed, for certified electrical equipment, such design features will usually be present to prevent there being a source of ignition during normal operation.

The proposals given in Table 9 can be used to revise a Table which was developed by WG09 (19). The result is Table 10.

Table 10 Proposed safety requirements for safety functions

Hazardous Area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	-1	0	-1
SIL of the safety function that the monitoring or control unit is providing	-	SIL 2	SIL 3	-	SIL 1	SIL 2	-	SIL 1
Resulting equipment category (under ATEX) of the combination	category 1			category 2			category 3	
Note that a fault tolerance of "-1" implies that the equipment would be incendive in normal operation, without the intervention of the safety device								

Table 10 assumes that any feature of the certified electrical equipment which provides a level of fault tolerance will achieve a risk reduction equivalent to a SIL of 1. This is

consistent with the fact that SIL 1 represents the minimum integrity requirement of IEC 61508 for a system defined as being safety-related.

6 DETERMINATION OF EN954 CATEGORIES FOR SIMPLE SAFETY DEVICES

In section 4.2 above, it was concluded that simple safety devices should meet the EN 954 category, which achieves the relevant ATEX fault tolerance requirement. A suggested definition of "simple safety device" is one which is simple enough that all the failure modes can be identified.

The ATEX Directive (1) fault tolerance requirements can be summarised as follows:

- a fault tolerance of 2 is required by the ATEX Directive for the protection system of Category 1 equipment when the protection system is the sole means of protection against explosion;

- a fault tolerance of 1 is required by the ATEX Directive for the protection system of Category 2 equipment when the protection system is the sole means of protection against explosion;

- a fault tolerance of 0 is required by the ATEX Directive for the protection system of Category 3 equipment.

EN 954 has 5 categories for describing control systems:

- Category B has a fault tolerance of 0;
- Category 1 has a fault tolerance of 0;
- Category 2 has a fault tolerance of 0 but has automatic monitoring;
- Category 3 has a fault tolerance of 1, and
- Category 4 has:
  - a fault tolerance of 1 with automatic monitoring, **or**
  - a fault tolerance of 2 or more.

It therefore follows that the mapping between ATEX equipment categories and EN 954 categories for the safety devices is as given in Table 11. (Note that the addition of a safety device with a fault tolerance of zero to equipment with a fault tolerance of zero gives an overall fault tolerance of one.)

Table 11 EN 954 requirements for simple safety devices

Hazardous Area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	-1	0	-1
EN 954 category of the monitoring or control unit	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4
Resulting equipment category (under ATEX) of the combination	ATEX category 1			ATEX category 2			ATEX category 3	
Note that a fault tolerance of "-1" implies that the equipment would be incendive in normal operation, without the intervention of the safety device								

7 METHODOLOGY FOR TESTING, VALIDATION AND CERTIFICATION

7.1 Introduction

Task 5 of the SAFEC project entailed the determination of a methodology for testing, validation and certification. It is described in detail in Annex E. The objective was to develop a certification scheme for safety devices, which come within the scope of the SAFEC project, and which is suitable for inclusion in the standard being drafted by WG09. Task 4 of the project was concerned with the study of safety devices and this task developed a methodology for determining the SIL of a safety device. Such a methodology is needed by the certification scheme and could be included as an informative annex within the standard. The case studies to calculate the SILs of particular safety devices are not suitable for inclusion as worked examples, however, because the examples were for the purpose of calibration and therefore were concerned with simple safety devices rather than complex ones. Task 4 is described in detail in Annex D.

This section of the report discusses the reasons for the certification scheme, which has been chosen. Appendix 1 gives details of the target failure measures, certification scheme and methodology for determining SIL. It is proposed that the information in Appendix 1 be incorporated into the WG09 standard.

7.2 Requirements of certification scheme

The first problem is to identify safety devices. The ATEX Guidelines (25) indicate that the main identification aspect for a safety device is the **autonomous function** for avoiding explosion risk. A thermal fuse is therefore a safety device. The certification scheme theoretically has to be applicable to these simple safety devices. However, it makes no sense to develop a new certification scheme for simple safety devices. There are already standards available for these devices. Therefore, the new aspects of the certification scheme are mostly to be used for complex safety devices, but must have no contradiction to available standards for simple safety devices. Table 1 has been prepared to define the safety devices not specified by available standards based on Task 3 of this research project. This has been further developed into Table A1 in Appendix 1, which indicates whether a particular safety device should be certified according to existing CENELEC standards, EN 954 or IEC 61508.

Within Table A1, a first classification is made in the following way:

- Whether the technical aspects of the safety device are defined in existing standards for explosion protection (in some cases they are mentioned in existing standards, but no further definition is made, example see EN 50053-1 6.1.1).
- Whether other standards are applicable (advice is given if known, for example EN or prEN).
- Whether the safety device is normally certified as a component (advice is C),
- Whether the safety device is normally certified as equipment (advice is E, although it can be installed outside the explosion protected area),
- Whether the safety device is a protective system according to 94/9/EC (advice is P).

For simple safety devices no further assessment for the safety against faults is necessary Table A1 indicates if the safety against faults of the device typically can not be assessed only by the standards for explosion protection. It is possible to realise some simple safety functions for example with programmable logic controllers. In this case safety standards have to be used although they are not mentioned. The assessment for more complex electric / electronic or programmable electronic devices could be made by:

- EN 954-1: especially when all failure modes can be fully described,
- IEC 61508: especially when the failure modes can not be fully described (for example complex integrated circuits) and software is used.

The certification scheme for the functional safety of safety devices is independent of the certification scheme for the safety against potential ignition sources if the safety device is also in the scope of the ATEX Directive (1) as equipment. This is in general the same situation for gas measurement systems, for protection systems and safety devices.

A safety device can be based on several different technologies. The construction principle may be electrical / electronic or programmable electronic. In addition, mechanic, pneumatic, hydraulic and other technologies may be used. For example, a standard thermal protection relay, used for the protection of type EEx „e“ – engines, consists of a bimetal heating system and several mechanical elements. The mechanical components are responsible for the triggering of the relay if one phase is disconnected. The function and the reliability of the overload relay also depends on mechanical components. The application for example of IEC 61508 part 2 is not possible in that case. There must be a distinction between the certification scheme and the applicable standards for different technologies. The two standards EN 954-1 and IEC 61508 may not be the only standards for assessment.

The certification scheme is mainly intended for the certification of products in the scope of the ATEX Directive (1). However, the products are used under the scope of the 118A Directive (18). There may also be safety aspects which are the responsibility of the user and communicated from the manufacturer to the user via the “Information for use”. Aspects of the safe use of products may be taken into account in the certification scheme if these technical aspects are different from existing standards for the use of explosion protected equipment.

The technical requirements (essential safety requirements ESR) of the ATEX Directive (1) are based on existing technical standards for explosion protection in group I and group II. The ESRs are not fully described in the Directive. The authors of the Directive take the existing standards for explosion protection into account. Many aspects seem to be open but are mostly written clearly in the standards for explosion protection.

The aspects of using the products are defined in the 118A Directive (18). It is the ‘instructions for use’ which are the link between the manufacturer and the user. Therefore, the instructions are given an important role. With existing standards for

explosion protection, therefore products are certified with a view to existing standards for installation, maintenance, repair etc., and use.

A certification scheme for safety devices has to assess the required safety. Furthermore the certification scheme has to include all the information for use and special details necessary to decide about the users application. For example, a safety device is to be certified such that it can be used in an application with SIL 3. In this special application the safety device needs a manual periodic test every day. It cannot be used normally in explosion protection with standard test rates / maintenance rates. There has to be some information about proof intervals and maintenance rates if they are different from common used rates. If this is not possible for the application of the equipment, every parameter for diagnostics, periodic test etc. has to be defined in the certification under worst conditions and given to the user in the instruction to make sure that the equipment is used in a safe way and the necessary risk reduction is achieved in practical use for every application.

7.3 Selection of a concept for certification

Three possible concepts for certification were compared:

- A concept independent from technologies and application, based on EN 1441 (26).
- A concept based on a hierarchical structure of standards (A-, B- and C-type standards), based on EN 954 (16) and EN 1050 (27).
- A concept based on a life cycle structure, based on IEC 61508 (17).

It was concluded that the lifecycle approach of IEC 61508 is the most appropriate. The main disadvantage of the standard could seem to be the possibility of application only to electric, electronic and programmable electronic systems. This is wrong. It is possible to distinguish in IEC 61508 two main parts:

- The systematic description for the overall life cycle of a system not depending on a specific technology. This is located in the part 1 of IEC 61508
- The description of requirements based on safety integrity level (SIL) for electrical / electronic / programmable electronic safety-related systems. This is included in parts 2 - 7 of IEC 61508.

IEC 61508 describes the whole life cycle of equipment from concept to decommissioning or disposal. The validation and certification in general must be open for the application of different technologies and standards. This is possible in the life cycle scheme of IEC 61508. There is a possibility to use other standards. The verification process can take into account the different approaches of the applied standards.

Every life cycle has a corresponding part in existing explosion protection standards (for example life cycle 12 and 14: standards for installation and maintenance). For a certification, the SIL (step 9) and the steps 6, 7 and 8 have to be tested. It has to be checked whether the life cycles 12 - 14 can be fulfilled under the scope of explosion protection.

A safety device with other technologies can be certified according to step 10 with other standards. Table 11 has been provided by this project to define the allowable categories within EN 954-1 for particular applications within electrical equipment for use in potentially explosive atmospheres.

EN 954-1 gives no information about maintenance. Proof testing can be taken as a risk reduction facility but applied standards like EN 954-1 give no information about proof test interval and this will be required in the instructions for use, as required by the 118A Directive.

IEC 61508 contains a complete scheme for the handling of a product. This is an advantage to other possible schemes.

Tables which map the lifecycle approach of IEC 61508 to the requirements for safety devices for explosion protection are included within Annex E. A complete mapping was possible.

7.4 Certification scheme

Feedback from users and manufacturers, on the above proposal to base the certification scheme on IEC 61508, indicated that this would be too complex and time-consuming for simple systems, particularly given that there is no evidence that explosions have been caused by electrical equipment designed for use in potentially explosive atmospheres. It is therefore proposed that the certification scheme should be based on the following:

- For electrical equipment and safety devices, which are fully specified within CENELEC or other standards, certification should be against the provisions of the relevant standard.

- For electrical equipment incorporating simple safety devices, the safety devices should be specified in terms of the relevant EN 954-1 category. Certification that the device achieves this category should be against the requirements of EN 954.

- For electrical equipment incorporating complex/programmable safety devices, the safety function should be specified in terms of the IEC 61508 SIL. The necessary risk reduction can then be allocated between available safety systems, including the safety device. Certification that the safety device achieves its required level of risk reduction should be against the requirements of IEC 61508.

The proposed certification scheme is given in Appendix 1.

The following limitations apply to this certification scheme, in terms of the need to certify complex and programmable safety devices against the requirements of IEC 61508:

- Some parts of IEC 61508 are currently only available in draft and the whole IEC 61508 is not harmonised. However, the issue of the remaining parts of IEC 61508 is in process and there is an intention to achieve harmonisation.

- A common database of component reliabilities is needed for the application of IEC 61508. Without such a database, certification will have to use available sources of data, e.g. (28-29), but equal levels of safety within different European countries cannot be guaranteed. However, any alternative certification schemes would either need a similar database or would have to ignore reliability aspects of certification and thereby risk compromising safety.

8 CONCLUSIONS

1. Safety devices, as defined under the ATEX Directive (1) have an autonomous safety function. They include implementation in a number of technologies. However, those which need to be defined by the SAFEC project (because they are not already defined in existing CENELEC standards) are mainly electric/electronic/electronic programmable in nature and are defined by Table 1.

2. Control system standards have been reviewed in terms of their usefulness in defining the requirements of safety devices. A number of problems have been identified with the use of EN 954 because the defined categories are not hierarchical in terms of reliability/integrity. IEC 61508 is therefore preferred for complex or programmable safety devices.

3. Safety devices should be certified according to the following:

   - For electrical equipment and safety devices, which are fully specified within CENELEC or other standards, certification should be against the provisions of the relevant standard.

   - For electrical equipment incorporating simple safety devices, the safety devices should be specified in terms of the relevant EN 954-1 category. Certification that the device achieves this category should be against the requirements of EN 954.

   - For electrical equipment incorporating complex/programmable safety devices, the safety function should be specified in terms of the IEC 61508 SIL. The necessary risk reduction can then be allocated between available safety systems, including the safety device. Certification that the safety device achieves its required level of risk reduction should be against the requirements of IEC 61508.

4. Safety integrity level (SIL) as defined by IEC 61508 is a suitable target failure measure for definition of complex or programmable safety devices. However, it will also be necessary to define additional fault tolerance requirements to conform with the ATEX Directive.

5. SIL targets for safety functions and hence safety devices have been calibrated by considering individual risk criteria, accident statistics and the performance of existing safety devices. Good agreement was achieved between these different calibration methods. The results are presented in Table 10.

6. The safety categories of EN 954-1 are a suitable target failure measure for simple safety devices. Table 11 defines the required categories for different applications.

7. The following limitations apply to th need to certify complex/programmable safety devices against the requirements of IEC 61508:

- Some parts of IEC 61508 are currently only available in draft and the whole IEC 61508 is not harmonised. However, the issue of the remaining parts of IEC 61508 is in process and there is an intention to achieve harmonisation.

- A common database of component reliabilities is needed for the application of IEC 61508. Without such a database, certification will have to use available sources of data, e.g. (26-27), but equal levels of safety within different European countries cannot be guaranteed. However, any alternative certification schemes would either need a similar database or would have to ignore reliability aspects of certification and thereby risk compromising safety.

9 REFERENCES

1. Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, Official Journal of the European Communities, 19/4/94

2. EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements.

3. EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion.

4. EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p".

5. EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling "q".

6. EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure "d".

7. EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety "e".

8. EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety "i".

9. EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation “m” .

10. EN 50039 Electrical apparatus for potentially explosive atmospheres. Systems.

11. EN 50284 - Specific requirements for of construction for test and marking for electrical apparatus of equipment Group II category 1G

12. PREN 50303-Equipment intended for use in potentially explosive atmosphere Group 1 Category M

13. EN 60079-14 Electrical apparatus for explosive gas atmosphere : Installation

14. EN 60079-17 Electrical apparatus for explosive gas atmosphere : Maintenance

15. EN-60079-19 Electrical apparatus for explosive gas atmosphere : Repair and overhaul

16. EN 954-1 Safety of machinery - Safety-related parts of control systems

17. IEC 61508 Functional safety of electrical, electronic and programmable electronic safety-related systems

18. Directive 1999/92/EC of the European Parliament and of the council of 16 December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (15th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)

19. CENELEC TC31/WG09, Draft proposal for a European Standard, "Electrical Equipment of Potentially Explosive Atmospheres - Reliability of safety-related devices", 12.02.99

20. Area Classification Code for Petroleum Installations (Part 15 of the Institute of Petroleum Model Code of Safe Practice in the Petroleum Industry), Institute of Petroleum/John Wiley, 1990

21. The tolerability of risk from nuclear power stations, HSE/HMSO, 1992

22. Institute of Petroleum Electrical Committee, "A risk based approach to hazardous area classification", Portland Press, 1998

23. BIA, “Dokumentation Staubexplosionen, Analyse und Einzelfalldarstellung”, Report 11/97, 1997

24. A. W. Cox, F. P. Lees & M. L. Ang, “Classification of hazardous locations”, Institution of Chemical Engineers, 1990

25. ATEX Guidelines - Guidelines on the Application of Council Directive 94/9/EC of 23 March 1994 on the Approximation of the Laws of the Member States concerning Equipment and Protective Systems intended for Use in potentially explosive Atmospheres, Draft 3 February 1999

26. EN 1441:1997 Medical devices - Risk analysis

27. EN 1050 : 1997, "Safety of Machinery. Principles for Risk Assessment"

28. RDF 93, Recueil de données de fiabilité des composants électroniques *(Electronic component reliability data log)*

29. A.BIROLINI, Quality and reliability of technical Systems (Ed. Springer - Verlag)

30. Draft 5 (5/13/1996 - ISA technical report).

APPENDIX 1
DETAILED GUIDELINES FOR TESTING, VALIDATION AND CERTIFICATION

A1.1 Scope

This certification scheme applies to safety devices as defined by the ATEX Directive (1) and which are a part of electrical equipment for use in potentially explosive atmospheres. It does not apply to the certification of "equipment" as defined by the ATEX Directive.

A1.2 Overview

The method of certification depends on the complexity of the safety device. Three cases are identified:

1. For electrical equipment and safety devices, which are fully specified within CENELEC or other standards, certification should be against the provisions of the relevant standard.

2. For electrical equipment incorporating simple safety devices, the safety devices should be specified in terms of the relevant EN 954-1 category. Simple safety devices are those for which the failure modes are known. Certification that the device achieves this category should be against the requirements of EN 954.

3. For electrical equipment incorporating complex/programmable safety devices, the safety function should be specified in terms of the IEC 61508 SIL. The necessary risk reduction can then be allocated between available safety systems, including the safety device. Certification that the safety device achieves its required level of risk reduction should be against the requirements of IEC 61508.

Table A1 has been developed to indicate which types of safety device may fall under which of the three cases above. This will depend on the function of the safety device, the type of electrical equipment in which it is used and the technology of implementation. The first step in the certification is to determine which of the three cases apply.

For case 1, certification should be directly against the requirements of the CENELEC standard which applies. This is identified by a "X" in the column "EN 50014ff" in Table A1.

For case 2, certification should be against the requirements of EN 954 (which are not detailed here). However, the allowable EN 954 categories of safety device for use in different applications are covered in A1.3 below. This is identified by a "X" in the column "EN 954-1" in Table A1.

For case 3, certification is covered in A1.4 below. This is identified by a "X" in the column "IEC 61508" in Table A1.

Table A1 Safety devices defined in the existing European Standards for explosion protection

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
EN 1127-1	6.2.2.2	Gas-warning devices		E		X	EN	X	X
	6.2.2.2	Flow-control devices		E		X		X	X
	6.4.8	Lightning protection	C			X			
	6.5.3	Explosion pressure relieve devices			P		prEN		
	6.5.4	Explosion suppression devices			P		prEN	X	X
	6.5.5	Flame barriers (various systems)			P		prEN		
	6.5.5.2.1	Deflagration arrester			P		prEN		
	6.5.5.2.2	Flame arrester			P		prEN		
	6.5.5.2.3	Detonation arrester			P		prEN		
	6.5.5.2.4	Flashback preventer			P		prEN		
	6.5.5.3.2	Rapid-action valves			P		prEN		
	6.5.5.3.3	Rotary valves			P		prEN		
	6.5.5.3.5	Double valves with its controls			P		prEN	X	X
EN 50014	10.	Interlocking devices				X			
	18.2	Electrically or mechanically interlocked disconnectors with a suitable load breaking device	C			X			
	18.3	an interlock for disconnectors in switchgears				X			
	18.5	Short-circuit and earth fault relays		E		X	EN		
	18.6	doors and covers Interlocked with a disconnector				X			
	19.	Interlocking for enclosures containing fuses				X			
	20.1	plugs and sockets shall be interlocked	C			X			
	20.2	plugs and sockets witch breaks the rated current with delayed release		E		X			
	21.2	luminaries interlocked with automatically disconnecting all poles	C			X			
EN 50015 (Ex o)	4.3.1	Pressure relieve device (for sealed devices)				X			
	4.3.2	Breathing device				X			
	4.4	Devices to indicate the liquid level				X			
	4.5	Liquid level indicating device				X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
	4.9	Devices for draining the liquid				X			
	4.11	Manually only resettable protective device which causes interruption of the supply current		E		X	EN	X	X
EN 50016 (Ex p)	3.3	A safety device to limit the maximum internal overpressure	C			X			
	3.6.1	Interlocking devices disconnecting the power supply	C			X			
	3.6.2	Similar to 3.6.1	C			X			
	4.2	By bringing an auxiliary ventilation system into operation		E		X		X	X
	5.6	Safety devices such as time-delay relays and devices for monitoring the flow of protective gas		E		X		X	X
	5.7	The protection gas is air. Not exceed 25% of the LEL (it could be monitored with a gas analyser)				X			
	5.7	The protection gas is other than air. Not exceed 2% by volume (an oxygen analyser could be used)				X			
	5.7	The purging flow rate shall be monitored		E		X		X	X
	5.8	One or more automatic safety devices shall be provided to operate when the overpressure falls below the minimum value specified by the manufacturer		E		X		X	X
	6.2	Oxygen analysers		E		X	EN	X	X
	6.5	Two automatic safety devices shall be provided to operate when the overpressure falls below the prescribed value		E		X		X	X
	7	Supply of protective gas							
	10.2	The flow limiting device	C			X			
	12.	Flame arrestors	C			X			
	13.	Safety devices		E		X		X	X
	Annex A.A.1	Two independent firedamp detectors. Arranged to disconnect automatically the electricity supply.			P	X		X	X

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
	Annex A.A.2	Fitting of barriers	C			X			
EN 50017 (Ex q)	11.2	Electrical or thermal protective device for temperature limitation, non self-resetting	C			X			
	11.3	Current limiting device (resistor)				X			
	14.	associated power supply with limited ratings		E		X			
	10.	Protected against fault conditions such as short-circuit or thermal overload		E		X			
	11.2	Temperature limitation shall be achieved by an internal or external, electrical or thermal, protective device		E		X		X	
	11.2	When fuses are used as protective devices	C			X			
	11.3	Current limiting device	C			X			
EN 50018 (Ex d)	12.6	Suitable detection device enables the power supply to the enclosure to be disconnected, on the supply side, before possible decomposition of the insulating materials leads to dangerous conditions.	C			X			
	17.2.1	Quick acting doors or covers shall be mechanically interlocked with an isolator				X			
	18.1	Quick-acting switch in a flameproof enclosure, which breaks all poles of the lamp circuit before contact separation				X			
EN 50019 (Ex e)	4.7.4	Appropriate devices for winding protection		E		X		X	X
	5.1.4.3	Current dependent safety devices		E		X	EN	X	X
	5.1.4.4	Protection against overloads (e.g. motor stalled) with temperature sensors		E		X	EN	X	X
	5.1.4.5	Frequency and voltage converter, with the protecting device incorporated		E		X		X	X
	5.3	Electrically or mechanically				X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
		interlocked in order to avoid the separation of contacts in a hazardous zone							
	5.4	Current transformer	C			X			
	5.6.2.3	level indicating device				X			
	5.8.3	Electrical protecting device, limiting the heating effect due to abnormal earth fault and earth leakage currents: - for TT and TN systems a residual current protective device - for TI an insulator monitoring device		E		X	EN		
	5.8.8	Isolate all energized parts of the resistance heating device or unit				X			
	5.8.9	Sensing the temperature. Sensing that temperature and other parameters. Measuring one or more parameters other than temperature.		E		X			
EN 50020 (Ex i)	8.4	Resistors				X			
	8.5	Blocking capacitor				X			
	8.6 / 7.5.2	shunt safety assemblies				X			
	9.	diode safety barriers		E		X			
	7.5.3	series blocking diodes				X			
	8.	Transformers and damping windings	C			X			
	7.3	Fuses	C			X			
	6.6	Earth conductors				X			
	6.3.2	Plugs and sockets	C			X			
	6.4.12	Relays	C			X			
	8.8	Galvanically separating components	C			X			
	8.7/ 6.4.11	Wiring and connections				X			
EN 50021 (Ex n)	10.9.2.1	Supplied at varying frequency and voltage by a converter. Supply other than that derived from a converter. Non sinusoidal load (e.g. thyristors).		E			X	X	X
	11.	Fuses and fuse assemblies				X			
	12.1	Fuses and fuse assemblies				X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
	12.2.5.2	Glow type starters				X			
	12.2.5.3	Electronic starters and ignitors	C			X			
	12.2.5.5	Ballasts (electronic ballasts)	C			X			
	15.1.	Interlocked mechanically or electrically				X			
	16.3.2	Interlocked mechanically or electrically				X			
	16.4.2	Chargers for type 2 cells and batteries		E		X			
	21.2	Reliable means of limiting the voltage and current available to energy storing components or at any normally sparking contact, e.g. by the use of zener diodes and series resistors				X			
	21.7	Polarity reversal				X			
	21.8.2	Fuses				X			
	21.8.3	Shunt safety components such as diodes or voltage limiting devices				X			
EN 50028 (Ex m)	4.1.3	Fuse				X			
	4.1.5	wire wound resistor				X			
	4.1.5	plastic foil capacitor				X			
	4.1.5	paper capacitor				X			
	4.1.5	ceramic capacitor				X			
	4.1.5	opto-coupler				X			
	4.1.5	transformer				X			
	4.1.5	coil				X			
	4.1.5	motor windings				X			
	4.4	Temperature limitation: this can be achieved by a non self-resetting internal or external, electrical or thermal, protecting device.				X			
	4.2.3	Use of a duplicated, non self-resetting thermal protection devices, positioned as necessary throughout the circuit.							
	4.2.3	Other apparatus or associated apparatus having control over voltage and current limitation equivalent of that of a category “ib” circuit according to EN 50020, though not necessary at the same levels of voltage,		E		X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
		current or power.							
	4.2.5	Mechanical separation element. Separation elements consist of a partition wall, possibly combined with a flameproof joint or an air gap with natural ventilation.				X			
	4.5	The mechanical connection to the boundary shall be flameproof				X			
EN 50053-1	5.3.1	An exhaust ventilation system	C			X			
	5.3.2	The exhaust ventilation system shall be interlocked				X			
	5.4.5	Earthing and bonding				X			
	6.1.1	The high voltage supply shall be switched off in such a manner that it cannot be re-energised							
EN 50053-2	5.3.3	Explosion suppression system, an explosion relief, explosion barriers, or other explosion protection systems			P	X			
EN 50053-3	5.3.1	Ventilation system. Exhaust ventilation system.	C			X			
EN 50177	5.1.2.2	Device which automatically switches off the high voltage							
	5.1.3.2	Voltage discharges							
	5.2.1	An exhaust ventilation system	C			X			
	5.2.2	Interlocked with other equipment. Devices shall be installed to monitor the actual flow of the exhaust ventilation system air and arranged to interrupt immediately the high voltage supply if the volumetric flow falls ...							
	5.2.4	Explosion suppression or explosion relief venting			P	X			
	5.2.6	Interlocked so that the high voltage supply system will be switched off							
	5.2.10	Automatic local fire extinguishing systems.... switched off by automatic			P	X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
		means							
	5.3.1	Interlocking shall be provided to prevent the high voltage being applied							
	5.5	Earthing measures							
EN 50281-1-1	4.3	Fasteners				X			
	4.4	Interlocking devices				X			
	5.2.2	Interlocked with a suitable load breaking device	C			X			
	5.2.3	Any interlock				X			
	5.2.4	Interlocked with a disconnector				X			
	5.3	Enclosures containing fuses				X			
	5.4.1	Shall be interlocked				X			
	5.4.2	Breaks the rated current with delayed release		E		X			
	5.5.2	Automatically disconnecting all poles	C			X			
	6.3	Fasteners				X			
	6.4	Interlocking devices				X			
	7.2.2	Interlocked with a suitable load breaking device				X			
	7.2.3	Any interlock				X			
	7.3	Enclosures containing fuses shall be interlocked				X			
	7.4.1	Shall be interlocked				X			
	7.4.2	Breaks the rated current with delayed release	C			X			
	7.5.2	Automatically disconnecting all poles				X			
EN 50281-1-2	7.	System power limitation		E		X	EN	X	X
EN 50284	4.2.2	Associated apparatus e.g. Ex ia power supply		E		X			
	4.2.3	thermal protective devices, non self-resetting	C			X			
	4.2.3	associated power supply with limited ratings, similar to Ex ib, (safe with one fault)		E		X			
	4.2.3	Non self-resetting thermal protection devices, positioned as necessary throughout the circuit.				X			
	4.2.3	Apparatus or associated apparatus having control over voltage and current limitation				X			

Standard	Clause	Safety Device	Component	Equipment	Protective Systems	EN 50014ff	Possible other Standards	EN 954-1	IEC 61508
		equivalent of that of a category "ib" circuit according to EN 50020, though not necessary at the same levels of voltage, current or power							
	4.2.5	Mechanical separation element. Separation elements consist of a partition wall, possibly combined with a flameproof joint or an air gap with natural ventilation.				X			
	4.5	Mechanical connection to the boundary shall be flameproof				X			

A1.3 Conformity assessment procedure according to EN 954-1

The allowable categories of safety device for any given application are defined by Table A1.2.

Table A1.2 Definition of allowable EN 954 categories for safety devices

Hazardous Area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	-1	0	-1
EN 954 category of the monitoring or control unit	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4
Resulting equipment category (under ATEX) of the combination	ATEX category 1			ATEX category 2			ATEX category 3	
Note that a fault tolerance of "-1" implies that the equipment would be incendive in normal operation, without the intervention of the safety device								

Assessment of whether a particular device meets the requirements for a particular category should be carried out according to EN 954.

A1.4 Conformity assessment procedure according to IEC 61508

This follows the overall lifecycle given in Figure A1 (IEC 61508 Part 1 Figure 2).

A1.4.1 Conditions

For a conformity assessment procedure based on IEC 61508 minor changes have to be made for the application to safety devices.

- The boxes 1 - 4 are already fulfilled by existing standards for explosion protection and the work in Task 1 and Task 2 of the SAFEC project.

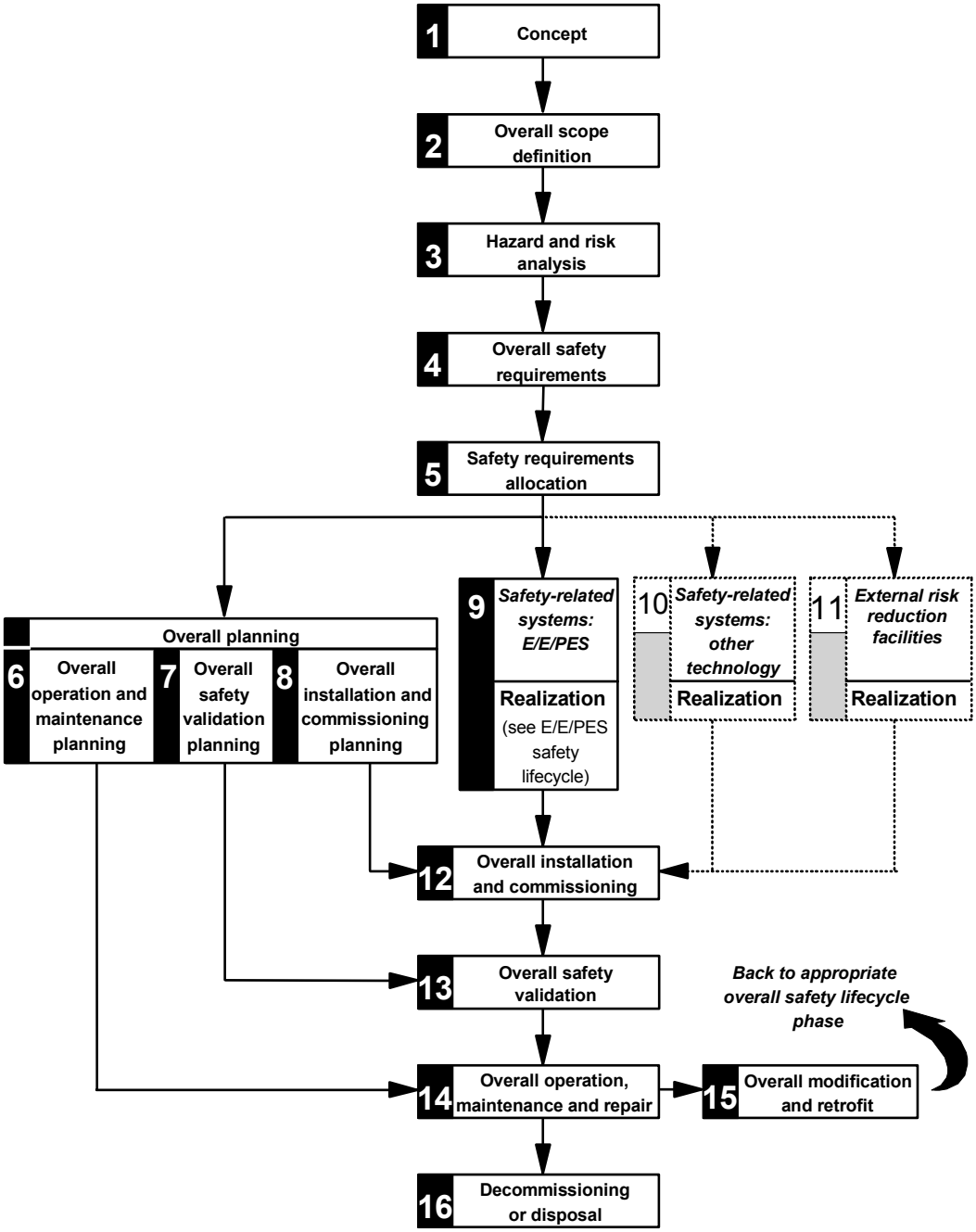
- The box 5 is mainly defined by existing standards for explosion protection (function) and Task 2 (safety integrity level).

The required safety integrity requirements for the overall safety function of preventing an explosion (box 4), depending on the hazardous zone, is defined by Table A3 (based on Table 9 in the main text).

Table A3 Proposed overall risk reduction requirements

Hazardous Zone	ATEX equipment categories	Target SIL requirement
0 or 20	1	SIL 3
1 or 21	2	SIL 2
2 or 22	3	SIL 1

If the safety requirements allocation (box 5) is such that the requirements are allocated between the fault tolerance of the equipment (without the safety device) and the safety device, then the SIL requirement for the safety device is as defined in Table A4 (based on Table 10 in the main text of this report).



NOTE 1 Activities relating to ***verification, management of functionalsafety*** and ***functional saftey assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure A1 The safety lifecycle from IEC 61508

Table A4 Proposed target risk reduction requirements for safety functions

Hazardous Area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	-1	0	-1
SIL of the safety function that the monitoring or control unit is providing	-	SIL 2	SIL 3	-	SIL 1	SIL 2	-	SIL 1
Resulting equipment category (under ATEX) of the combination	category 1			category 2			category 3	
Note that a fault tolerance of "-1" implies that the equipment would be incendive in normal operation, without the intervention of the safety device								

In addition, the fault tolerance requirements of the ATEX Directive shall be met. These are defined by Table A5 (same as Table 3)

Table A5 Fault tolerance requirements of the safety device as required by the ATEX Directive

ATEX category	Fault tolerance requirement
1	2
2	1
3	0

In any cases where more safety systems are available for safety requirement allocation, the manufacturer and the notified body would have to do the safety requirement allocation according to IEC 61508, Part 1, 7.6.

A1.4.2 Validation process

- The certification scheme itself is based on box 9, for electric / electronic or programmable electronic safety devices or on box 10, together with box 11 for other technologies.

Figures A2 and A3 (Figures 3 and 4 of IEC 61508 part 1) show the lifecycle realization phase including validation process.

- The notified bodies have to carry out the conformity assessment procedure according to boxes 9.1 to 9.6 for hardware and software. The assessment can include less or more the point 9.1 to 9.5. This is depending on the safety devices. The most important step is 9.6.

The tasks included in realization phase relate to the description in IEC 61508 Part 1. The objective of the requirements of this sub clause is to create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements.

The specific demands are contained in IEC 61508 Part 2 and 3. Further information can be obtained from IEC 61508 parts 2 and 3. A possible methodology for determining SIL for E/E/EP systems is given in the Informative Annex below.

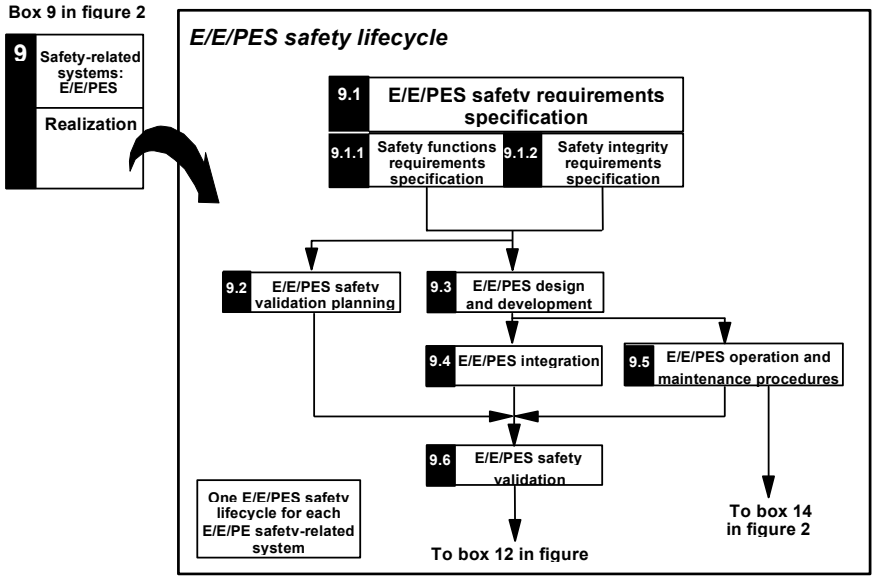


Figure A2 E/E/PES safety lifecycle (in realization phase)

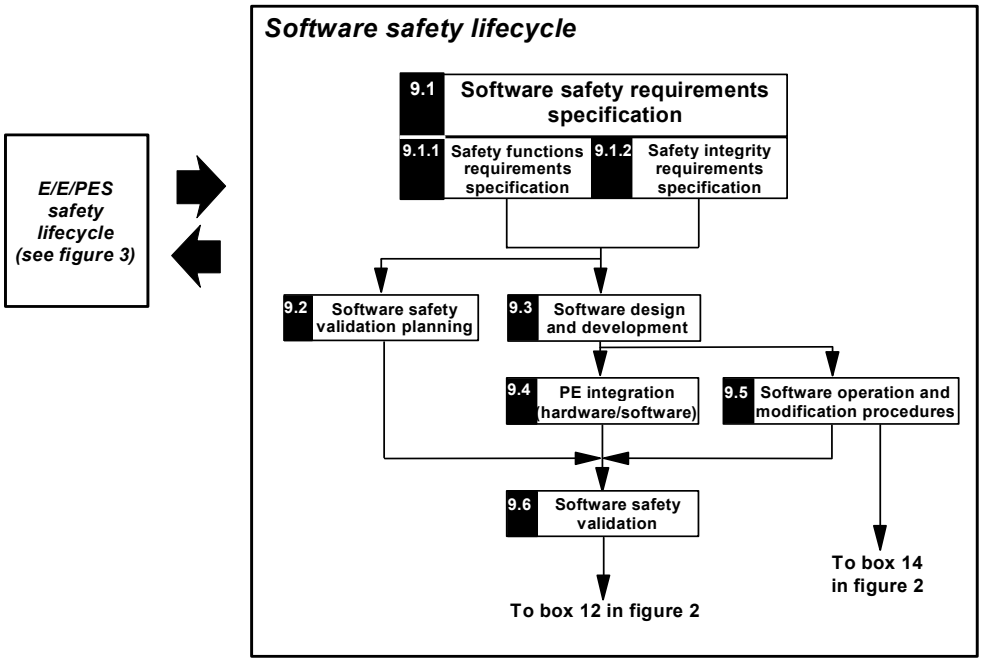


Figure A3 Software safety lifecycle (in realization phase)

A1.4.3 Validation process for other technologies and external risk reduction facilities

The validation for other technologies can be led by using EN 954-1. Specification of the validation process may use PrEN 954-2. Other standards are possible (for example DIN EN 61496-1 06/98).

The lack of information e.g. about proof intervals has to be covered by special procedures. The validation of an electrical / electronic or programmable electronic device with EN 954-1 needs separate calculation of reliability for circuits responsible for the validated safety function. The reliability of external risk reduction facilities should be handled similarly. The reliability calculations suggested by the Informative Annex will be appropriate.

A1.4.4 Validation of instructions for use

The notified bodies should ensure that, when particular maintenance procedures or proof test intervals are required to achieve the necessary safety integrity of the safety devices, that these are detailed in the instructions for use.

A1.5 Independence for validation / conformity assessment procedures

Tables A6 and A7 define the levels of independence which are changed by the ATEX Directive (1) to the two groups "notified bodies" and "manufacturers".

Table A6 - Responsibility for conformity assessment procedure of safety devices in use with electrical equipment or internal combustion engines

Zone of intended use (overall equipment category)	Safety integrity level			
	1	2	3	4
0 (1, M1)	-	Notified Body	Notified Body	Notified Body
1 (2, M2)	-	Notified Body	Notified Body	-
2 (3)	-	-	-	-

Table A7 - Responsibility for conformity assessment procedure of safety devices in use with non-electrical equipment

Zone of intended use (overall equipment category)	Safety integrity level			
	1	2	3	4
0 (1, M1)	-	Notified Body	Notified Body	Notified Body
1 (2, M2)	-	Manufacturer	Manufacturer	-
2 (3)	-	-	-	-

A1.6 INFORMATIVE ANNEX TO CERTIFICATION SCHEME METHODOLOGY FOR DETERMINING THE SIL OF A SAFETY DEVICE

The system's safety integrity level is assessed in accordance with the following procedure that breaks down the assessment into the five following stages with logical links :

- 1st stage : functional analysis,
- 2nd stage : failure rate prediction
- 3rd stage : failure modes, effects and criticality analysis,
- 4th stage : modelling of the system's various states,
- 5th stage : system safety integrity level assessment.

It should be noted that this assessment does not take into account :

- common mode failures,

- systematic errors,
- connection failures,
- errors linked to cabling,
- human errors.

1.6.1 First stage : functional analysis

The purpose of the functional analysis is to identify the functions to be fulfilled by the system. It is also intended to explain the system's operation by establishing a link between the hardware and software functions. This stage is the assessment's input point. It needs to be sufficiently accurate to identify failures with an impact on the system's safety.

Several functional analysis procedures may be used to explain the operation of automatic systems :

- functional block diagram procedure,
- SADT procedure,
- SA_RT procedure,
- etc.

A1.6.2 Second stage : failure rate prediction

The purpose of the failure rate prediction is not to assess the system's reliability. Calculations are only conducted for the components with a risk in relation to safety, in order to quantify the dangerous failure rate. To that end, a calculation makes it possible to assess an equivalent failure rate of the system. This calculation comprises : component failure rates, component stress, climatic environment, component quality, etc.

The failure rate prediction allows us to quantify the FMECA (**F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis - See 3rd stage) and to identify the contribution of the various failure modes to the system's unsafe situation.

Failure rate calculations are grounded on databases that supply a basic failure rate for each type of component. This basic failure rate is modulated according to corrective factors according to the environment and component.

A1.6.3 Third stage : failure modes effects and criticality analysis (FMECA)

After identifying the components fulfilling the functions (hardware and software), identified by the functional analysis, the failure modes and their effects on the system's operation must be analysed in the scope of this study. The purpose of this stage is to

analyse the failures to identify " dangerous " failure modes, and to quantify the probability of failure occurrence.

The **F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis (FMECA) is conducted at electronic component detail level for the safety device. The purpose of this analysis is :

- to identify the " dangerous " failure modes to assess the " dangerous " failure rates leading to the hazardous event, while assessing a coverage rate for the various tests;
- to identify the possible preventive maintenance provisions to be integrated to guarantee a safety integrity level in compliance with the defined goals.

Failures are classified in 4 classes :

- dangerous detected failures whose effects are on safety and availability (λ^{DD}),
- dangerous un-detected failures whose effects are only on safety (λ^{DU}),
- non-dangerous detected failures whose effects are only on availability (λ^{SD}),
- non-dangerous and undetected failures whose effects are only on availability (λ^{SU}).

(λ^{DU} = λ **D**angerous, **U**ndetected ; λ^{S} = λ **S**afe).

λ^{S} = Safe failure : i.e. a failure that results in system fallback (safe situation for safety).

λ^{DU} = Unsafe failure : failure whose consequence leads to a dangerous state from the standpoint of safety.

The following diagram (Figure A4) gives further details of this notion of distribution of failures according to their effect. The objective of this stage is to define the unsafe failure modes. References (28) and (29) are examples of sources of data for the failure mode distribution for various components.

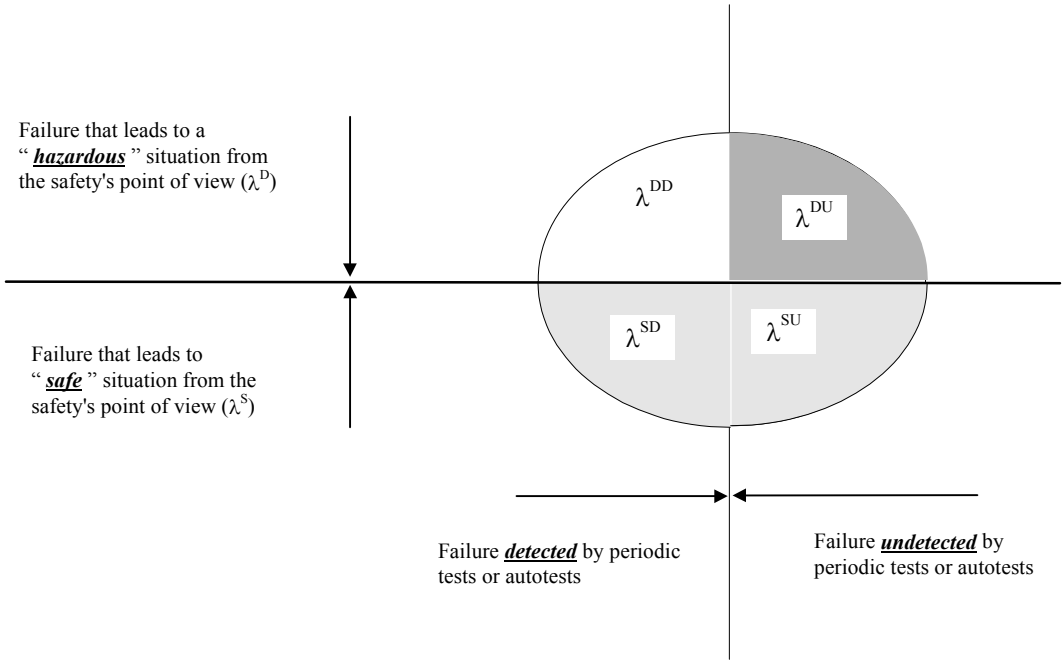


Figure A4 : Failure distribution according to their effect

A1.6.4 Fourth stage : modelling of the system's various states

There are three system types according to the various encountered systems :

[1] Failsafe systems

[2] Non-redundant systems

[3] Redundant systems

The system's dangerous failure probability calculation is different according to the various types of system.

Failsafe systems

Failsafe systems are systems in which the failure modes of all components of the system lead to a « safe state » in relation to safety. For these systems, there is no use in calculating the dangerous failure probability as the λ^{DU} dangerous failure rate does not exist

Non-redundant systems

Non-redundant systems are " simple " systems in which the safety function can be lost in the event of failure. Two states are possible : safe state or dangerous state. The calculation of the dangerous failure probability for the systems comes down to a specific reliability calculation depending on the dangerous failure rate (λ^{DU} - identified in FMECA) and with the same duration as the preventive maintenance operations.

Redundant systems

In the event of redundant systems, the safety function can be lost due to combinations of failures depending on the logic implemented within the safety system. There are several safety integrity level quantitative assessment procedures for such systems. The main drawback of the more traditional procedures such as the analysis by fault tree system, or the analysis by reliability block diagram, is that they do not always take into account the time aspect, test periodicity, coverage levels, as well as the repair rate.

The various failure and operating states can be modelled with MARKOV graphs, by integrating the time aspect of the preventive maintenance tests, the autotests as well as the coverage rate, as the electronic systems are subject to a failure law of exponential form with a constant failure rate.

A1.6.4.1 Influence of testability on safety

For safety purposes, the state of the resources must be known on a permanent basis to see if hidden (or dormant or latent) failures liable to mask the safety function exist. These dormant failures are only detected during periodic tests voluntarily conducted by the user.

A test policy is useless for failsafe systems as each failure leads to a " safe " position in relation to safety.

On the contrary, for systems that are neither failsafe nor autotestable and on which dangerous failures exist, a test policy to detect the " dangerous failures " (with a risk for safety) is required.

These tests must be conducted according to a periodicity grounded on the characteristics of the various elements constituting the system. Dangerous failures can be detected in two ways :

- Either by the test and autotests system of the safety system for detectable failures (λ^{DD}),
- Or during verification operations for non-detectable failures (λ^{DU}).

The PLC's reliability level is not increased by testability. It just makes it possible to ensure that resources are still available : to read the inputs and control the outputs, on the one hand, and to make sure that the processing modules are still functional, on the other hand. Only dangerous failure detection comes into play. It is possible to detect and switch to safe position in the event of failure, thanks to this test, and therefore to better guarantee safety. The following diagram shows the impact of testability on safety, and the impact of a state changeover test policy conducted every 24 hours or every 6 months on safety.

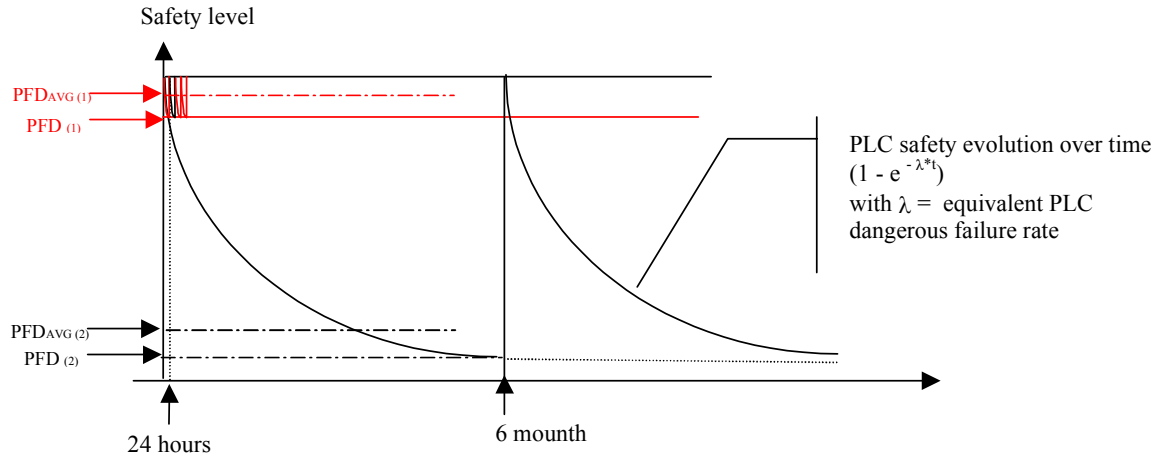


Figure A5 : Testability impact on safety

A1.6.4.2 Graph establishment

IEC 61508 (18) and reference (30) stipulate the procedure and various stages of system modelling. State graphs are represented below for each safety function. Modelling is achieved with " states " that the system is liable to enter. There are 3 states in most cases :

State 2 represented as follows : 

This state corresponds to the modelling of redundancy. In this state, all implemented resources are present and operate in a nominal manner.

State 1 represented as follows : 

This state corresponds to the modelling of redundancy downgraded by the dangerous failure of a hardware element on one of two channels. In this state, all implemented resources are not present. It is an undetected dangerous failure state. Safety is still guaranteed.

State 0 represented as follows : 

This state corresponds to the modelling of the loss of redundancy due to the dangerous failure of several hardware elements from the channels. In this state, safety is no longer guaranteed and in the event that the safety function is called upon, the system will not go to safe position.
The " P " probability of being in " 0 " state is designated by PFD(t) in the IEC 61508 standard. The meaning of PFD(t) value is the value defined in the previous paragraph.

A1.6.4.3 Assumptions

MARKOV graph modelling for the studied systems by INERIS was grounded on the following assumptions :

[1] failure rates (λ) and repair rates (μ) are assumed constant to make it possible to model and calculate the safety level with MARKOV graphs.

[2] The mission time (TI) corresponds to the intervals between the OFF LINE periodic test times. All test rates concerning the aptitude to detect state changeovers (μ_{PTi}) are stated for each arc of each graph.

[3] Inputs and outputs do not go to the safe state if the power supply is cut off.

[4] The common failure modes, and the systematic errors are assumed equal to those defined in reference (28). λ^D common mode failures or faults have the specificity of affecting all lines at the same time. The selected values are those defined in the same document.

A1.6.4.4 System modelling example

Two active redundancy systems are modelled as follows

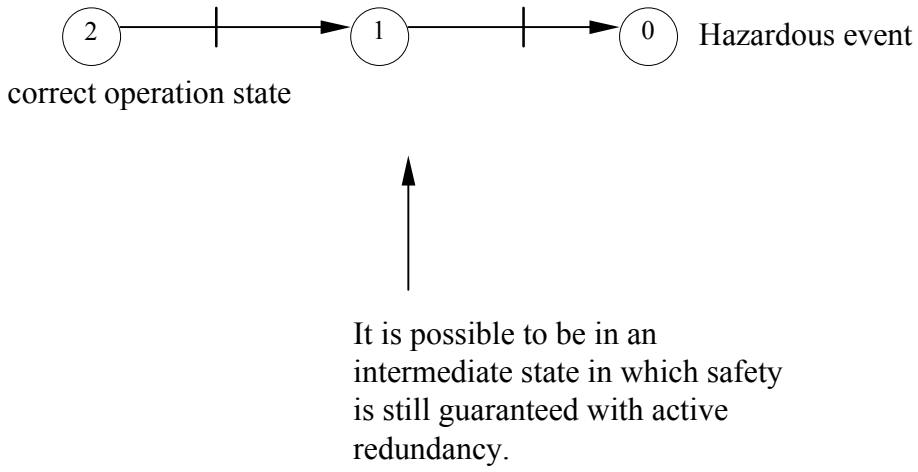


Figure A6 : Redundant system state modelling

This graph is equivalent to the following graph :

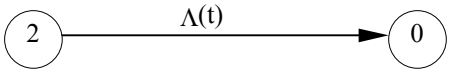


Figure A7 : Redundant system state reduced modelling

The " P " probability of being in a " 0 " state therefore depends on a failure rate that in turn depends on time T : $P = \Lambda(t) \times T$.
This example shows that the more time T increases and the more the probability of being at " 0 " state increases.

A1.6.5 Fifth stage : Safety integrity level assessment

The system's various states were modelled with the fourth stage. This stage consists of resolving the mathematical calculation and comparing the level achieved by the system with the classifications of the IEC 61508 standard.

The dangerous failure probability calculation (PFD) is a function of a system failure rate (function variable over time) and of a duration, in most cases. Therefore, the safety integrity level calculation is a specific reliability calculation in which safety is equal : either to the reliability during a time equal to that of the auto-test's overall time, or to that of the preventive maintenance intervals.

APPENDIX 2
DETAILS OF SAFEC PARTNERS

HEALTH AND SAFETY EXECUTIVE
Health and Safety Laboratory (HSL)
Harpur Hill
Buxton
Derbyshire
SK17 9JN
UK

Contacts:

Jill Wilday (Project co-ordinator)
Phone: +44 114 289 2156
Fax: +44 114 289 2160
E-mail: jill.wilday@hsl.gov.uk

Tony Wray (leader of Task 2)
Phone: +44 114 289 2481
Fax: +44 114 289 2468
E-mail: anthony.wray@hsl.gov.uk

The Health and Safety Laboratory (HSL) is an agency of the UK Government's Health and Safety Executive (HSE). It is based on two sites – one in Sheffield and the other in Buxton – and it employs nearly 400 people, many of whom are scientists or technical specialists. It primarily supplies HSE with the scientific and technical expertise needed to carry out its duties.

DEUTSCHE MONTAN TECHNOLOGIE GmbH (DMT)
Pro Tec Division
Beylingstrasse 65
D-44329 Dortmund
Germany

Contact:
Dr-Ing Franz Eickhoff
Phone: +49 231 24 91-234
Fax: +49 231 24 91 – 224
E-mail: Fr.Eickhoff@dmt.de

DMT runs laboratories in the fields of e.g. process control equipment with responsibility for safety, explosion protection, machinery, personal protective equipment and explosives. DMT is a notified body to the Commission according to several EC Directives, including the full range of the ATEX Directive 94/9/EC.

INSTITUT NATIONAL DE L'ENVIRONMENT INDUSTRIEL ET DES RISQUES (INERIS)
Parc Technologique
ALATA
BP No 2
60550 Verneouil-en-Halatte
France

Contacts:

M Stanislas Halama
Phone: +33 3 44 55 65 45
Fax: +33 3 44 55 67 04
E-mail: Stanislas.Halama@ineris.fr

M Eric Fae
Phone: +33 3 44 55 66 77
Fax: +33 3 44 55 66 88
E-mail: eric.fae@ineris.fr

INERIS is the national institute for industrial environment and risks. INERIS focusses on all chemical pollution and technical hazards except nuclear hazards. It contains six Science departments: measurement and analysis; toxicology/ecotoxicology; soil/subsoil ecosystems; explosion/fire; assessment. Modelling and analysis of hazards; and electrical and elctronic safety systems.

LABORATORIO OFICIAL MADARIAGA (LOM)
Area ATEX
Alenza 1
28003 Madrid
Spain

Contact:

Mr Eduardo Conde Lazaro
Phone: +34 91 3367009
Fax: +34 91 441 99 33
E-mail: econde@dse.upm.es

The Laboratorio Oficial J M Madariaga is a centre of the Madrid Polytechnic University (UPM). LOM is dedicated to testing, certification, studies and research on safety concerning explosions, explosive and other hazardous environments. Also, LOM is a Notified Body for testing and certification in accordance with the ATEX Directive 94/9/EC.

ANNEX A

DERIVATION OF TARGET FAILURE MEASURES

Author: Jill Wilday
Health and Safety Laboratory

SUMMARY

OBJECTIVES

The SAFEC project (contract SMT4-CT98-2255) has the overall objective to produce a harmonised system for subdivision of safety devices which are used in electrical equipment for use in potentially explosive atmospheres, together with a methodology for selecting the appropriate subdivision of safety device for any particular application.

Task 1, which is described in this report, has the objective of deriving target failure measures for the protective devices that are within the scope of the project. These can then be used by the later project Tasks in order to develop a methodology for the testing, validation and certification that the protective device meets the target failure measures and is therefore suitable for use in a particular ATEX category.

MAIN FINDINGS

(a) The use of target failure measures which are solely in terms of fault tolerance could lead to problems in ensuring safety, unless the details of the design are well specified in standards, because fault tolerance criteria give no information about the maximum allowable frequency of a fault.

(b) The target failure measures for safety devices in terms of IEC 61508 safety integrity levels (SIL), as proposed by CENELEC TC 31/WG09, are suitable for adoption by this project.

(c) Although the target failure levels proposed by TC31/WG09 were derived in terms of fault tolerance, they also seem sensible in terms of the reliability of achieving the safety function, for two example cases. However, these cases may not be within the scope of electrical equipment defined by the CENELEC standards in references [1] to [8]. The geometry of the CENELEC TC31/WG09 proposals may not be ideal in reliability terms.

MAIN RECOMMENDATIONS

(a) This report should be made available for comment from TC31/WG09 and from users and manufacturers of equipment.

(b) The proposed target failure measures should be reconsidered in the following ways at various stages in the project:

(i)the mapping of SIL onto the fault tolerance requirements of the ATEX Directive should be considered further in Task 2;

(ii)the possibility of producing an alternative mapping, which does not rely on fault tolerance allocation, from that proposed by CENELEC TC31/WG09, should be considered during Task 2;

(ii)the mapping of SIL, in terms of equipment reliability and whether faults give rise to continuous or intermittent ignition sources, should be considered during the study of safety devices in Task 4;
(iii)the practicality of using these target failure measures for testing, validation and certification should be confirmed in Task 5.

(c) If any improvements to the proposed target failure measures are identified during the course of the project, they should be made in liaison with TC31/WG09.

CONTENTS

1. INTRODUCTION

1.1 Background

Electrical apparatus which is intended for use in potentially explosive atmospheres sometimes relies on the correct operation of control or protective devices in order to maintain certain characteristics of the apparatus within acceptable limits. Examples of such devices are motor protection circuits (to limit temperature rise during stall conditions) and overpressurisation protection.

The approval and certification of electrical apparatus for potentially explosive atmospheres, therefore, requires that, where such control and protection devices are used, an assessment be made of their suitability for the intended purpose. This will need to be expressed in terms of some measure of confidence that the devices will be able to maintain a required level of safety at all times.

For many years, European industry has carried out hazardous area classification of its operating sites in order to identify areas in which potentially explosive atmospheres (due to flammable gas, vapour or dust) can exist at different frequency levels. Equipment for use in such potentially explosive atmospheres has been developed and is covered by the following CENELEC standards :

EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements[1].
EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion[2].
EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p"[3].
EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling "q"[4].
EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure "d"[5].
EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety "e"[6].
EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety "i"[7].
EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation "m"[8].
EN 50039 Electrical apparatus for potentially explosive atmospheres. Systems[9].
EN 50284 Electrical apparatus for potentially explosive atmospheres. Requirements for Zone 0 [10]
PrEN 50303 Electrical apparatus for potentially explosive atmospheres.. Requirements for M1 [11].
EN 60079-14 Installation[12]
EN 60079-17 Maintenance[13]
EN 60079-19 Repair[14]

Such electrical equipment is used within areas with potentially explosive atmospheres in order to reduce the likelihood of ignition of such atmospheres to an acceptably low level. The electrical equipment described in the standards above contains specific safety-related devices (e.g. motor protection, overpressurisation protection, thermal fuses etc.). Other safety-related devices such as gas detectors may also be used within potentially explosive atmospheres and contribute to the overall level of safety.

The EC ATEX Directive, 94/9/EC[15], has introduced Essential Safety Requirements for equipment. Those which particularly apply to safety-related devices associated with equipment for use in potentially flammable atmospheres are 1.5 and 2. The ATEX Directive also places requirements for risk evaluation of devices used for protection of electrical and electronic equipment used in potentially explosive atmospheres in order to determine their suitability for use in particular hazardous areas. However, the treatment of this aspect of electrical apparatus for potentially explosive atmospheres may not be adequate within existing standards for such apparatus and further guidance is needed to support the approval and certification process.

CENELEC identified the need for research to determine whether existing and proposed standards in the field of safety-related control systems are suitable for this purpose, and to develop a methodology which will provide the required support for the approval and certification process. Research proposals on this topic were invited under the Standardisation, Measurement and Testing (SMT) Programme and the SAFEC project proposal was selected for funding.

1.2 The SAFEC project

1.2.1 Objectives

The SAFEC project (contract SMT4-CT98-2255) has the overall objective to produce a harmonised system for subdivision of safety devices which are used in potentially explosive atmospheres, together with a methodology for selecting the appropriate subdivision of safety device for any particular application.

The specific objectives are:

- to draft a description of appropriate subdivisions of safety devices. (The appropriate subdivisions would be chosen so as to harmonise with those defined in existing European standards as discussed in 1.1 above);

- to define all safety devices which are used in the context of electrical equipment for use in potentially explosive atmospheres ('used safety devices'), and study their characteristics and performances in terms of the defined subdivisions;

- to draft a method for identifying when a particular subdivision should be used, taking account of the application and working environment for which the equipment is to be used;

- to determine the correspondence between the proposed subdivisions and the relevant essential safety requirements;

- to draft specific measuring methods, where necessary, paying special attention to the calibration methods and the reproducibility of the measurements;

- to take account of input from users and manufacturers of electrical equipment designed for use in potentially explosive atmospheres.

1.2.2 Project overview

The project is a 12 month project which began in January 1999. SAFEC has the following partners:

The Health and Safety Laboratory of the Health and Safety Executive (HSL) in the UK. HSL is the project coordinator.

The ProTec Division of the Deutsche Montan Technologie GmbH (DMT) in Germany.

The National Institute for Industrial Environment and Risks (INERIS) in France.

The Laboratorio Oficial J.M. Madariaga (LOM) in Spain.

The project is broken into six tasks or work packages as shown in Table 1.

The SAFEC project is being conducted with liaison with CENELEC Technical Committee 31, Working Group 9 (TC31/WG09) and with a number of industrial users and manufacturers of electrical apparatus for use in potentially explosive atmospheres. TC31/WG09 is developing a European Standard: "Electrical Equipment for Potentially Explosive Atmospheres: Reliability of safety-related devices". This European Standard will make links between the requirements of the ATEX Directive[15,17], CENELEC standards for electrical equipment for use in potentially explosive atmospheres[1-14, 16], the CEN standard EN 954[18] and the International Electrotechnical Commission standard IEC 61508[19]. It is intended that the results of the SAFEC project will assist in the development of the TC31/WG09 standard.

Table 1 SAFEC Project Tasks

Task	Description	Partner	Duration (months)	Completed by end of month
1	Derive target failure measures in discussions among partners and others.	all (led by HSL)	3	March 1999
2	Assess current control system standards with reference to target failure measures from Task 1.	HSL	5	July 1999
3	Consider devices currently used with reference to CENELEC standards.	LOM	3	May 1999
4	Study "used safety devices" identified in Task 3.	INERIS	4	September 1999
5	Determine methodology for testing, validation and certification.	DMT	4	September 1999
6	Draft final report including proposal for requirements to be incorporated in European Standard in the light of obtained results.	all (led by HSL)	3	December 1999

1.2.3 Scope

The scope of the SAFEC project is limited to:

a) Electrical apparatus which comes under the requirements of the ATEX Directive, i.e. the focus is on what can be done by the manufacturer of equipment which is for sale (rather than on what should be done by the user of equipment and covered under the 118A Directive[20]).

b) Electrical apparatus for use in flammable atmospheres for which safety devices are relevant. This includes Type e"" (increased safety)[6] and Type "p" (pressurisation)[3]. Any further types of electrical apparatus which fall within the scope will be defined during Task 3 of the project.

c) All types of safety devices. This includes those which are electrical, electronic or programmable electronic in nature. Some such devices may be relatively complex so that the type and consequence of failure may be indeterminate, e.g. because failures may result from latent systematic faults. Less complex safety devices are also included such as, for example, a switch which cuts off the power to flameproof equipment if it is opened; or thermal fuses (if provided by the manufacturer rather than by the user).

1.3 Objectives of SAFEC Task 1

Task 1 has the objective of deriving target failure measures for the protective devices that are within the scope of the project. These can then be used by the later project Tasks in order to develop a methodology for the testing, validation and certification that the protective device meets the target failure measures and is therefore suitable for use in a particular ATEX category.

2. REQUIREMENTS OF ATEX DIRECTIVE

2.1 Categories of electrical equipment

The ATEX Directive defines two Groups of application of electrical equipment, each of which has Categories of electrical equipment according to the level of protection required:

- Group I comprises mining applications where the flammable material is firedamp or flammable dust:

  - Category M1 means that the equipment is required to remain functional in an explosive atmosphere.

  - Category M2 equipment is intended to be de-energised in the event of an explosive atmosphere.

- Group II comprises other applications where equipment is to be used in a potentially explosive atmosphere:

  - Category 1 equipment is intended for use in Zone 0 and/or 20, where explosive atmospheres are present continuously, for long periods of time or frequently.

  - Category 2 equipment is intended for use in Zone 1 and/or 21, where explosive atmospheres are likely to occur.

  - Category 3 equipment is intended for use in Zone 2 and/or 22, where explosive atmospheres are less likely to occur, and if they do occur, do so infrequently and for only a short period of time.

2.2 Types of safety device

The ATEX Directive covers the following:

a) equipment;
b) protective systems;
c) components;
d) safety, controlling or regulating devices.

It is the safety, controlling or regulating devices which are the concern of this project. These will be parts of equipment or protective systems but, unlike components, they have an autonomous safety function.

Safety devices for equipment for use in explosive atmospheres could come under the requirements of the ATEX Directive even if the safety device is to be positioned outside the flammable area. This could give rise to different cases:

i) If the safety device is for use outside the flammable area, its safety function will be to prevent ignition of a flammable atmosphere by the equipment with which it is associated.

ii) If the safety device will be located inside the flammable atmosphere then it will also have a safety function to prevent the equipment from causing ignition. The potential causes of ignition within the equipment will have to be assessed including any introduced by the safety device. However, the safety device may have a different explosion protection concept applied to it than that applied to the electrical equipment. This may therefore be a more complex case.

2.3 Specified failure measures

The ATEX Directive specifies the level of protection required for each of the Categories of equipment in terms of the number of faults required to cause failure. The position is summarised by a Table in section 4.2.3 of the ATEX Guidelines[17], which is reproduced here as Table 2.

Table 2 Level of protection requirements of the ATEX Directive

Level of protection	Category		Performance of protection	Conditions of operation
	Group I	Group II		
Very high	M1		Two independent means of protection or safe even when two faults occur independently of each other. Relevant stresses must be withstood	Equipment remains functioning when explosive atmosphere present
Very High		1	Two independent means of protection or safe even when two faults occur independently of each other.	Equipment remains functioning in Zones 0,1,2 (G) and/or 20,21,22 (D)
High	M2		Suitable for normal operation and severe operating conditions.	Equipment de-energised when explosive atmosphere present.
High		2	Suitable for normal operation and frequently occurring disturbances or equipment where faults are normally taken into account.	Equipment remains functioning in Zones 1,2 (G) and/or 21, 22(D)
Normal		3	Suitable for normal operation	Equipment remains functioning in Zones 2 (G) and/or 22(D)

The above requirements relate to the equipment, rather than to a particular safety device which forms part of the equipment.

3. CONCEPTS FOR TARGET FAILURE MEASURE

3.1 Types of target failure measure

The following types of target failure measure are possible.

3.1.1 Fault tolerance

The target failure measures can be set in terms of the number of faults which must be tolerated by the system before failure occurs. In this context, failure would equate with the creation of an ignition source. However, a target in terms only of fault tolerance says nothing about the frequency of faults nor whether they would be apparent or not.

Table 2 above indicates that the ATEX Directive specifies criteria in terms of fault tolerance for equipment. Fault tolerance has historically been the criterion used for

intrinsically safe (IS) electrical apparatus[7]. The IS approach as been successful in preventing ignition of flammable atmospheres. However, in this case, the technology used for the design of IS circuits may be such that a particular (high) level of reliability (low fault frequency) is implied. The ATEX Directive criterion of tolerance of 2 faults for use in Zone 0 mirrors the IS criterion, but the implicit assumptions about low fault frequency may not necessarily follow for other technologies.

3.1.2 Reliability

Target failure measures could equally be set in terms of reliability (of achieving the safety function), e.g. the maximum frequency of occurrence of faults or the maximum probability of failure on demand. (For the purpose of this document, which is concerned only with failures to danger, and, in the absence of any alternative concise and convenient term, the term “reliability” will be used to refer only to those failures which result in the system in which they occur moving to a less-safe state). The target failure measure would then be quantitative. However, since the use of reliability criteria has not been the practice in the field of electrical apparatus for use in potentially explosive atmospheres, numerical criteria in terms of reliability have not (so far) been developed. It should be noted that it is the reliability of achieving the safety function on demand that is important, rather than the reliability of the equipment (which may tend to fail to safety).

The achievement of high reliability uses requires the use of redundancy and/or diversity of components. This will tend to give a measure of fault tolerance. The achievement of high reliability will also usually require periodic proof testing[14] to be carried out and may require diagnostics to be built into the system so that faults can be recognised when they occur. High reliability may also be achieved by the use of well-proven techniques.

3.1.3 Quality control

Reliability techniques can be used to reduce the frequency of random faults but do little to reduce the frequency of systematic faults. Such systematic faults tend to occur in software systems and include human error during the design and specification of hardware, and errors in the writing of control software. Formalised quality control systems can be used to reduce the likelihood that software errors will be present in the system.

3.2 Discussion

3.2.1 Problems with using fault tolerance alone

Mellish[21] has reviewed the use of the single fault philosophy in order to draw out the assumptions which it relies on. The single fault philosophy can be stated as: "In single

fault condition, there shall be no hazard" but this implies that double fault conditions can be ignored since, by implication a double fault will be unsafe.

IEC 60601[22] states in Appendix A:

> "...Equipment is required to remain safe in single fault condition. Thus one fault of a single protection means is allowed.
>
> "The probability of simultaneous occurrence of two single faults is considered small enough to be negligible.
>
> "This condition can only be relied upon if either:
>
> a) the probability of a single fault is small, because of sufficient design reserve, or the presence of a double protection prevents the development of a first single fault, or
>
> b) a single fault causes operation of a safety device (e.g. fuse, overcurrent release, safety catch etc.) which prevents occurrence of a safety hazard, or
>
> c) a single fault is discovered by an unmistakable and clearly discernible signal which becomes obvious to the operator, or
>
> d) a single fault is discovered and remedied by periodic inspection and maintenance which is prescribed in the instructions for use."

It follows that fault tolerance can only be used as a target failure measure if the reliability requirements given above are met. If the above requirements are not met, then a single fault could occur almost immediately the equipment is put into service and would not be diagnosed nor rectified. The likelihood of a second, unrelated fault occurring simultaneously with the first fault would then be relatively high and certainly too high to be negligible.

The use of fault tolerance as a target failure measure is making implicit assumptions about reliability and diagnostics (whether a fault will be found and remedied if it occurs). The point is also made by Mellish that a single fault includes any additional faults that would be directly caused by the first single fault, or that share a common cause with it, i.e. common cause or common mode failure must be taken into account and this is a reliability issue.

3.2.2 Types of target failure measure used in control standards

Since the safety devices within the scope of the project are control systems, it is appropriate to consider the target failure measures used by current and emerging

European and International control system standards for safety-related systems. One of the aims of the project is to produce a system of categorisation of safety devices which is consistent with other appropriate standards.

IEC 61508[19] uses a combination of all of the above concepts, as necessary, depending on the circumstances. The higher the level of protection required, the more concepts are used and the tighter the criteria which must be met. Safety integrity levels (SIL) are defined. A particular SIL has primary requirements in terms of the amount of risk reduction (reliability) and these are reproduced in Table 3. Additional requirements are also given in terms of fault tolerance, diagnostics and quality control.

Table 3 Reliability requirements of IEC 61508

SIL	Probability of failure on demand (for low demand rate operation)	Frequency of failure (per hour) for continuous operation
4	10^{-5} - 10^{-4}	10^{-9} -10^{-8}
3	10^{-4} - 10^{-3}	10^{-8} - 10^{-7}
2	10^{-3} - 10^{-2}	10^{-7} - 10^{-6}
1	10^{-2} - 10^{-1}	10^{-6} - 10^{-5}

EN 954[18] defines categories B, 1, 2, 3 and 4 for safety-related devices. However, EN 954 states that these categories are not intended to be used in any given order nor in any given hierarchy in respect of safety requirements.

Task 2 of the project is to look at these control standards in more detail.

3.2.3 Requirements for testing, validation and certification

The practicality of testing, validation and certification is another important factor to be taken into account in deciding which concepts should be used for target failure measures. Tasks 4 and 5 will consider this in more detail: Task 4 by studying a range of safety devices and Task 5 by developing a methodology for testing, validation and certification. These Tasks will provide information on:

a) the levels of complexity of safety devices which come within the scope of the project and hence which types of target failure measure may be appropriate, and

b) whether a practical methodology can be developed for all types of target failure measure.

At this stage in the project, it may not be necessary to assign numerical values to the possible types of target failure measure. It may be sufficient to know that they could be either in terms of number of faults which must be tolerated (which may allow a mapping

to the EN 954 categories) or in terms of a particular SIL (which includes aspects of reliability, fault tolerance and quality control). However, numerical values will need to be proposed by the end of the project.

4. TARGET FAILURE MEASURES PROPOSED IN TC31/WG09 DRAFT STANDARD

4.1 Description

Section 4 of the current draft[23] gives a Table which is reproduced here as Table 4.

Table 4 Proposed target failure measures in TC31/WG09 draft standard

Hazardous Area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Equipment (EUC) fault tolerance	2	1	0	1	0	-1	0	-1
safety category of monitoring or control unit	-	SIL 2	SIL 3	-	SIL 2	SIL 3	-	SIL 2
Resulting equipment category (under ATEX) of the combination	category M1/1			category M2/2			category 3	

In Table 4, it should be noted that:

A fault tolerance of -1 means that ignition sources would be present in the equipment under control (EUC) under normal operation, so that a demand is put on the safety device in normal operation.

The safety categories of the monitoring or control unit are in terms of the SIL levels defined in IEC 61508[19].

SIL2 means either a failure tolerance of 1 with 60% degree of detection or a failure tolerance of 0 with 90% degree of detection.

SIL3 means either a failure tolerance of 2 with 60% degree of detection or a failure tolerance of 1 with 90% degree of detection.

4.2 Discussion

4.2.1 Assumed derivation of target failure measures

It is important to note that the fault tolerance requirements given by the ATEX Directive (see Table 2) refer to the equipment, i.e. to the electrical apparatus for use in potentially explosive atmospheres as defined by references [1] to [14]. However, the SIL levels given by TC31/WG09 (see Table 4) refer to a safety device which is an integral part of the "equipment" as defined by the ATEX Directive.

Thus in Table 4:

> "Equipment (EUC)" in the second row is the "Equipment under control" in the sense of IEC 61508, i.e. it is that part of the total "equipment" (in the sense of ATEX) which does not include the safety device.
>
> "Monitoring or control unit" in the second row is the safety device.
>
> "Equipment" in the final row is as defined in the ATEX Directive.

This is further illustrated by Figure 1.

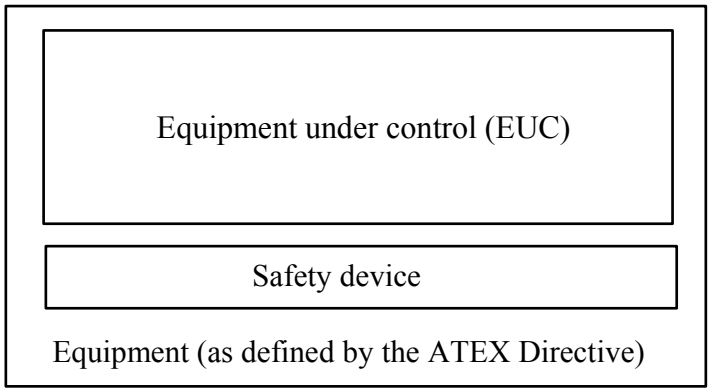


Figure 1 Definition of terms in Table 4

The required SILs for the safety devices are then found by subtracting the existing fault tolerance of the EUC from the required fault tolerance of the equipment (as defined by ATEX). This gives the number of faults which must be tolerated by the safety device. The SIL which requires that degree of fault tolerance (within the requirements of IEC 61508) has then been selected.

4.2.2 Comments

Since the SAFEC project aims to assist TC31/WG09 in the development of their standard, it will be important that both use the same target failure measures.

The choice of IEC 61508 SIL as the target failure measure in the TC31/WG09 draft standard has the advantage that SIL includes the concepts of reliability, fault tolerance and quality control as is appropriate to the application. As discussed in section 3 above, this combination should be better at ensuring safety than fault tolerance alone.

The mapping of SIL onto the ATEX requirements for different categories of equipment, which has been done by TC31/WG09, is in terms of fault tolerance alone. Although fault tolerance requirements for each SIL are specified in IEC 61508, these are somewhat incidental compared with the reliability requirements.

It would be interesting to check that the mapping shown in Table 4 is sensible in terms of reliability requirements. However, this is not readily done because the ATEX Directive does not specify reliability criteria for equipment and the reliability of the EUC part of electrical equipment is also unknown. An attempt is made in section 5 below to link the SIL requirements of the TC31/WG09 draft with major hazard risk criteria. This is most easily done for those cases in which the EUC has ignition sources under normal operation. It may also be possible, during Task 2 of the project, to comment on the mapping in terms of the reliability and fault tolerance requirements within IEC 61508. It may further be possible, during Task 4 of the project, to estimate the reliability of typical EUC for the safety devices studied. If either of these Tasks lead to a proposal that the mapping in the draft TC31/WG09 standard could be improved, this would be recommended to the Working Group.

Table 4 does not at present cater for the situation where more than one safety device exists on one EUC. This case could be handled by requiring that the SIL requirement in Table 4 is met be the combination of the installed safety devices.

The mapping shown in Table 4 assumes that it is reasonable to allocate fault tolerance between the EUC and the safety device in order to achieve an overall fault tolerance as specified by the ATEX Directive (Table 2). This does not necessarily follow. Reliability requirements can be allocated between different devices as described in IEC 61508[19] but fault tolerance is not necessarily related to reliability as discussed in 3.2.1 above. Table 4 suggests that a safety device fault tolerance lower than that implied in ATEX is possible. The validity of having anything other than a fault tolerance of 2, 1 and 0 for Categories 1, 2 and 3 respectively is questionable, regardless of whether that tolerance applied to the equipment as a whole or to its associated safety device(s). The validity or otherwise of allocating fault tolerance between the EUC and the safety device will be further explored within Task 2, which will look in detail at the application of existing control system standards to safety devices associated with electrical equipment for use in potentially explosive atmospheres.

It could follow from Table 4 that apparatus not meeting the appropriate explosion protection concept, e.g. industrial apparatus, could be used in flammable atmospheres provided a control system meeting a particular SIL were used. This is not intended in ATEX. ATEX requires established explosion protection concepts[1-8] to be used. When this established concept involves the possible use of a control system (e.g. increased safety and pressurisation) it should meet a specified integrity level. In the case of 'e' and 'p' which are Category 2 apparatus, any associated safety device should also be safe with a single fault. Table 3 therefore implies a wider scope than may be appropriate for the limited application of safety devices associated with electrical apparatus defined by references [1] to [8]. Task 3, which will define the types of safety devices, will confirm this.

5. TARGET FAILURE MEASURES IN TERMS OF RISK

5.1 Introduction

Quantitative risk criteria are usually in terms of the maximum tolerable frequency for a given level of accident consequence or severity. The ATEX Directive places requirements on manufacturers of equipment rather than on users and the manufacturer will not know the details of the application in which his equipment is to be used (but will know the zone where the equipment will be installed). The manufacturer therefore cannot make a detailed estimate of the consequences of an explosion and so must make worst case assumptions when designing the equipment.

At present, standards for hazardous area classification are not risk-based in that they also make worst case assumptions about the consequences of an explosion. However, attempts continue to be made to develop a risk-based hazardous area classification procedure[24,25]. This may in future allow risk (consequences) to be taken into account in defining the hazardous zone, and hence the required ATEX equipment category.

Another European collaborative project, RASE, is developing a methodology for risk assessment of unit operations and equipment in explosive atmospheres. RASE is focusing on risk of ignition for non-electrical ignition sources. The current draft risk assessment methodology[26] developed by this project does not address the issue of tolerability criteria. It is the intention of this section to develop such criteria.

5.2 Review of major hazard risk criteria

It can be assumed as a worst case that the explosion of a flammable atmosphere would constitute a "major accident" according to the Seveso Directive[27]. It is therefore appropriate to make use of major hazard criteria for risk tolerability which have been developed elsewhere.

5.2.1 UK individual risk criteria

The UK Health and Safety Executive has published guidance on the tolerability of risk[28,29]. This is in terms of the risk of death to an individual person. The framework illustrated in Figure 2 is introduced. There is a level of risk which is so high as to be intolerable and a lower level of risk which can be considered broadly acceptable because it is low in comparison with the background risk. Between these two levels is the ALARP region in which a risk is only tolerable if it has been reduced as low as is reasonably practicable. Cost/benefit analysis may be used to determine whether ALARP has been achieved.

HSE[28] states that a risk of death of 10^{-3} per year would be intolerable for a worker (whilst a risk of 10^{-4} per year would be intolerable for a member of the public). 10^{-3} per year corresponds to the risk which is tacitly accepted by workers in the riskiest occupations in the UK, e.g. deep sea diving. A risk of death of 10^{-6} per year would be considered broadly acceptable. Between 10^{-6} and 10^{-3} per year, the risk would be tolerable only if reduced as low as is reasonably practicable (ALARP).

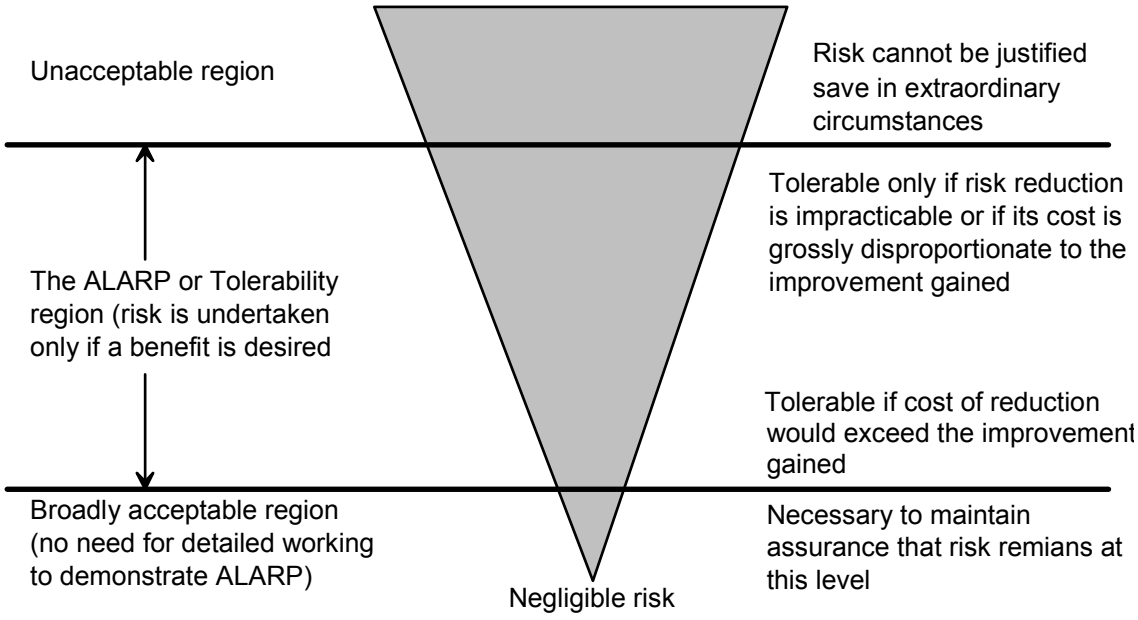


Figure 2 HSE framework for risk tolerability

5.2.2 Netherlands societal risk criteria

Societal risk criteria are presented in terms of a plot of frequency, F, (cumulative frequency of more than N fatalities) versus the number of fatalities, N. Those used in the Netherlands[30] are shown in Figure 3.

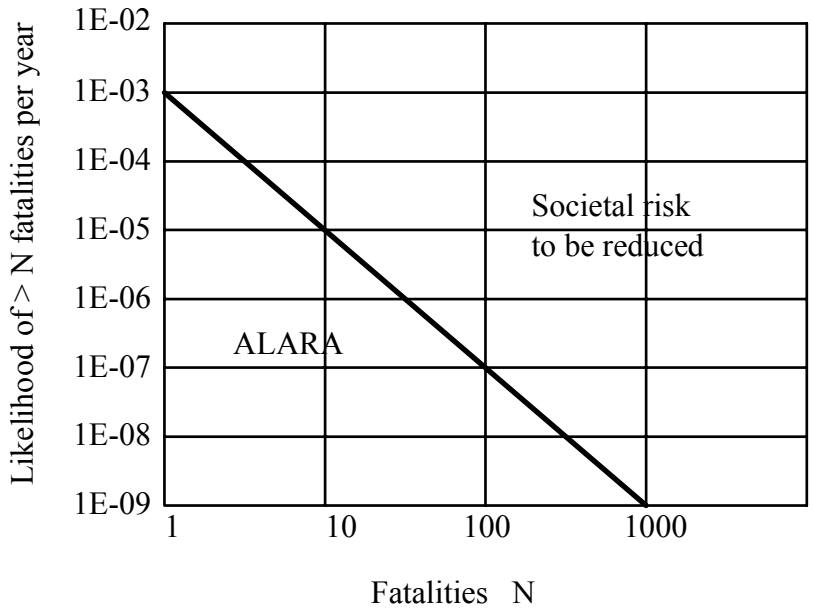


Figure 3 Netherlands societal risk criteria

5.2.3 "Short-cut risk assessment" criteria

The short-cut risk assessment methodology of Allum and Wells[31,32] defines a number of consequence (severity) bands and suggests quantitative tolerability criteria for each consequence level. This includes criteria for both individual and societal risk of death and risk of less severe consequences. Wells reviewed the risk criteria used by a number of industrial companies in developing these criteria. The criteria and consequence descriptions are shown in Table 5. In general, the acceptable frequency criteria are within the ALARP region for the criteria in 5.2.1 and 5.2.2 above.

5.2.4 Criteria used in development of IEC 61508

Bell and Reinert[33] gave an example of the use of the developing IEC 61508 in a major hazards context. They used a tolerability criterion of 10^{-4} per year.

Table 5 Short-cut risk assessment criteria

Severity	Description	Acceptable frequency (per year)
5	Catastrophic damage and severe clean-up costs On-site: loss of normal occupancy for three months Off-site: loss of normal occupancy for one month Severe national pressure to shut down Three or more fatalities to plant personnel Fatality of member of the public or at least five injuries Catastrophic damage and severe clean-up costs Damage to site of special scientific interest or historic building Severe permanent or long-term damage to the environment	10^{-5}
4	Severe damage and major clean-up Major effect on business with loss of occupancy up to three months Possible damage to public property Single fatality or injuries to more than 5 plant personnel A one in ten chance of a public fatality Short-term environmental damage over a significant area of land Severe media reaction	10^{-4}
3	Major damage and minor clean-up Minor effect on business but no loss of building occupancy Injuries to less than 5 plant personnel with one in ten chance of fatality Some hospitalisation of public Short-term environmental damage to water, land, flora or fauna Considerable media reaction	10^{-3}
2	Appreciable damage to plant No effect on business Reportable near-miss incident under CIMAH Regulations Injury to plant personnel Minor annoyance to public	10^{-2}
1	Near-miss incident with significant quantity released Minor damage to plant No effect on business possible injury to plant personnel No effect on public, possible smell	10^{-1}

5.2.5 Discussion

There is a large measure of agreement between the tolerability criteria reported above. Both the UK and the Netherlands are using an "as low as reasonably practicable" (ALARP) or "as low as reasonably achievable" (ALARA) principle. This means that, if it is reasonable to do so, more stringent tolerability criteria should be applied.

The maximum tolerable individual risk (N = 1) of 10^{-3} per year is the same for the UK and Netherlands criteria. The Netherlands societal risk criteria use a slope of -2 (on a log:log basis) which means that multiple fatality accidents are given a higher weighting than if there were the same number of fatalities in a series of smaller accidents. In their recent review for HSE[30], Ball and Floyd suggest that most psychological studies on

risk perception/tolerability show that a slope of -1 (i.e. non higher weighting of multiple fatalities) is more reasonable.

The criteria of Allum & Wells[31,32] and of Bell and Reinert[33] are values within the ALARP or ALARA regions of the national criteria. ALARP/ALARA can be applied only to specific applications on a case by case basis. For the purpose of deciding whether the SIL values proposed by TC31/WG09 are sensible in terms of reliability, the Allum and Wells criteria have the advantage of effectively being average ALARP/ALARA criteria.

5.3 Generic fault tree for ignition of potentially flammable atmosphere

The risk tolerability criteria discussed above are in terms of the consequences of an explosion. A fault tree, showing the logic of how such consequences arise, can be used to relate the tolerability criteria to the reliability of the protection system. Such a fault tree is shown in Figure 4.

The fault tree indicates that there may be several ignition sources present. Ignition source 1 (box (m)) has been assumed to be the item of electrical equipment. The fault tree has been further developed for this case to include the equipment under control (EUC) element of the equipment and the safety device (see Figure 1).

There are a number of boxes in the fault tree whose probability depends on the application. Since the application is known only to the user and not to the manufacturer, worst case assumptions will be made about these boxes. These assumptions are summarised in Table 6.

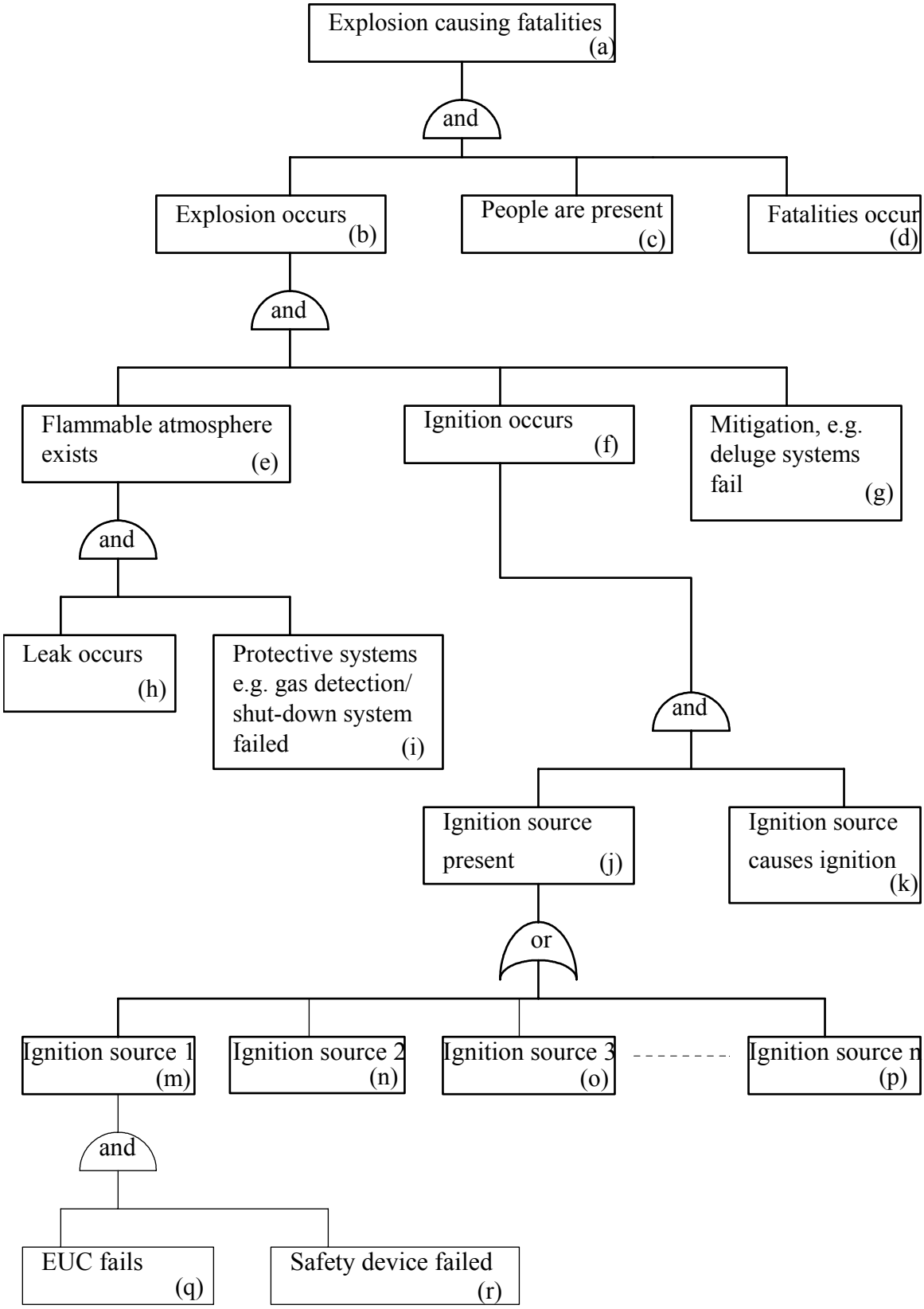


Figure 4 Generic fault tree for explosion

Table 6 Worst case assumptions about data for fault tree

Box	Description	Worst case probability	Comments
(c)	People are present	1	
(d)	Fatalities occur	1	
(g)	Mitigation, e.g. deluge systems, fail	1	These may not be present, or , if present, have unknown reliability
(i)	Protective systems, e.g. gas detection shut-down system failed	1	Again, these may not be present. Also, this box may be irrelevant as the probability/frequency for box (e) may be taken directly from the hazardous zone definition
(k)	Ignition source causes ignition	1	Use of an ignition probability of 1 ignores the fact that a spark energy may be insufficient to ignite some dusts.

5.4 Comparison with TC31/WG09 proposals

No information is available about the reliability of the EUC in achieving its fault tolerance. However, the cases in Table 4 for which the EUC produces an ignition source in normal operation will be considered. (However, this is a situation outside the scope of electrical apparatus built to the standards in references [1] to [8].) The worst case for this would be that the EUC produced a continuous ignition source in normal operation, i.e. the probability in box (q) of the fault tree is 1.

5.4.1 Zone 2 with fault tolerance of -1

For this case, the TC31/WG09 draft suggests a SIL of 2. For continuous operation, IEC 61508 defines the reliability in terms of a frequency of failure of 10^{-7} - 10^{-6} per hour. Using a conversion factor of 8760 hours per year, which is appropriate for continuously operating process plant, the failure frequency is 8.8×10^{-4} - 8.8×10^{-3} per year, or in round numbers 10^{-3} - 10^{-2} per year.

The ICI/RoSPA guide[34] and UK Institute of Petroleum Code of Practice [35] define Zone 2 as an area in which a flammable atmosphere exists for no more than 10 hours

per year. Thus, the maximum probability of a flammable atmosphere existing in Zone 2 is 10/8760 = 1.1 x 10^{-3}.
With these data the fault tree can be evaluated to give the maximum frequency of an explosion. However, the presence of other ignition sources must also be taken into account when evaluating the fault tree. This has been done by assuming that the equivalent of 10 other sources of ignition (with the same frequency of producing an ignition source) could be present.

The resulting frequency of an explosion =

1 (box (q) EUC fails and gives continuous ignition source)
x 8.8x10^{-4} to 8.8x10^{-3} per year (box (r) failure rate of safety device)
x 10 (boxes (m) to (p) accounting for other ignition sources)
x 1 (box (k) ignition source causes ignition)
x 1.1x10^{-3} (box (e) flammable atmosphere present in Zone 2)
x 1 (box (g) mitigation fails)
x 1 (box (c) people present)
x 1 (box (d) people killed)
= 0.97 x 10^{-6} - 10^{-5} per year

5.4.2 Zone 1 with fault tolerance of -1

For this case, the TC31/WG09 draft suggests a SIL of 3. For continuous operation, IEC 61508 defines the reliability in terms of a frequency of failure of 10^{-8} - 10^{-7} per hour. Using a conversion factor of 8760 hours per year, which is appropriate for continuously operating process plant, the failure frequency is 8.8x10^{-5} - 8.8x10^{-4} per year, or in round numbers 10^{-4} - 10^{-3} per year.

The ICI/RoSPA guide[34] and UK Institute of Petroleum Code of Practice[35] define Zone 1 as an area in which a flammable atmosphere exists for between 10 and 1000 hours per year. Thus, the maximum probability of a flammable atmosphere existing in Zone 1 is 1000/8760 = 0.11.

Again, the presence of other ignition sources must also be taken into account when evaluating the fault tree. This has again been done by assuming that the equivalent of 10 other sources of ignition (with the same frequency of producing an ignition source) could be present.

The resulting frequency of an explosion =

1 (box (q) EUC fails and gives continuous ignition source)
x 8.8x10^{-5} to 8.8x10^{-4} per year (box (r) failure rate of safety device)
x 10 (boxes (m) to (p) accounting for other ignition sources)
x 1 (box (k) ignition source causes ignition)
x 0.11 (box (e) flammable atmosphere present in Zone 2)

x 1 (box (g) mitigation fails)
x 1 (box (c) people present)
x 1 (box (d) people killed)
= 0.97 x 10^{-5} - 10^{-4} per year

5.4.3 Discussion

The results of the two calculations shown above are in the range 10^{-4} to 10^{-6} per year risk of an explosion which could cause single or multiple fatalities. These results seem quite consistent with the risk tolerability criteria which were discussed in 5.2 above. For the two cases calculated, the proposed SILs seem reasonable.

Two other observations can be made:

a) The TC31/WG09 recommendations (in Table 4) have a geometry in which, for the same degree of fault tolerance of the EUC, the SIL is increased by 1 in going from Zone 2 to Zone 1 or from Zone 1 to Zone 0. However, an increase in SIL of 1 means an increase in reliability by one order of magnitude (in terms of annual failure rate or probability of failure on demand) but a change in Zone from 2 to 1 implies (according to ICI/RoSPA and the UK Institute of Petroleum [34,35]) an increase in the likelihood of a flammable atmosphere by two orders of magnitude. This means that the SILs stated in the TC31/WG09 draft may perhaps be inconsistently onerous in Zone 2 and/or lax in Zone 0. It should, however, be noted that the definition of Zones in terms of quantitative probability of a flammable atmosphere existing is not included in European Standards nor in the ATEX Directive; these all use qualitative definitions (see 2.2 above).

b) The TC31/WG09 draft takes no account of whether an ignition source, if produced, would be continuous or rare. Less stringent requirements might be possible for ignition sources which would only occur occasionally following a fault. This approach has been proposed[36] to the working group dealing with EN 1127 may be investigated further within the EC RASE project.

The calculations shown in this section indicate that the SILs proposed by TC31/WG09 for the two cases which were looked at are sensible in terms of reliability. However, these cases were outside the scope of electrical apparatus defined by the standards in references [1] to [8] since these types of electrical apparatus would not give rise to sources of ignition in normal operation. Typical reliabilities of the EUC component of electrical equipment would need to be derived to check the proposed SILs in the other cases in Table 4 (which are more appropriate to the scope of this project). It might be possible to do this for a small number of case studies in Task 4 of the project. This would allow further conclusions to be reached about whether possible problem identified in (a) above requires any changes to be made to Table 4. It might also be possible for Task 4 to look at the types of fault which might occur and hence whether

the SIL criteria require further development to account for differences between faults causing continuous ignition sources and faults causing rare ignition sources.

6. ALTERNATIVE METHODS OF DECIDING SAFETY DEVICE SAFETY INTEGRITY LEVEL

Reservations have been expressed in section 5 above about the proposed TC31/WG09 mapping of SIL level for safety devices associated with different ATEX equipment categories for use in different hazardous zones. However, the use of target failure measures for safety devices in terms of a SIL requirement seems sound as it takes account of reliability as well as fault tolerance and systematic issues.

An alternative to Table 3 proposed by TC31/WG09, which assumes that fault tolerance can be allocated between the EUC and the safety device, would be a Table or Riskgraph which gives the SIL requirement in terms of such parameters as the hazardous zone, the consequences of failure of the safety device and perhaps the demand rate on the safety device. This would need to be calibrated. Task 2 will look further at the possibility of producing such a Table.

7. CONCLUSIONS

(a) The use of target failure measures which are solely in terms of fault tolerance could lead to problems in ensuring safety, unless the details of the design are well specified in standards, because fault tolerance criteria give no information about the maximum allowable frequency of a fault.

(b) The target failure measures for safety devices in terms of IEC 61508 safety integrity levels (SIL), as proposed by CENELEC TC 31/WG09, are suitable for adoption by this project.

(c) Although the target failure levels proposed by TC31/WG09 were derived in terms of fault tolerance, they also seem sensible in terms of the reliability of achieving the safety function, for two example cases. However, these cases may not be within the scope of electrical equipment defined by the CENELEC standards in references [1] to [8]. The geometry of the CENELEC TC31/WG09 proposals may not be ideal in reliability terms.

8. RECOMMENDATIONS

(a) This report should be made available for comment from TC31/WG09 and from users and manufacturers of equipment.

(b) The proposed target failure measures should be reconsidered in the following ways at various stages in the project:

- the mapping of SIL onto the fault tolerance requirements of the ATEX Directive should be considered further in Task 2;
- the possibility of producing an alternative mapping, which does not rely on fault tolerance allocation, from that proposed by CENELEC TC31/WG09, should be considered during Task 2;

- the mapping of SIL, in terms of equipment reliability and whether faults give rise to continuous or intermittent ignition sources, should be considered during the study of safety devices in Task 4;

- the practicality of using these target failure measures for testing, validation and certification should be confirmed in Task 5.

(c) If any improvements to the proposed target failure measures are identified during the course of the project, they should be made in liaison with TC31/WG09.

9. REFERENCES

1. EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements.

2. EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion.

3. EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p".

4. EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling "q".

5. EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure "d".

6. EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety "e".

7. EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety "i".

8. EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation "m"

9. EN 50039 Electrical apparatus for potentially explosive atmospheres. Systems.

10. EN 50284 - Specific requirements for of construction for test and marking for electrical apparatus of equipment Group 2 category 1G

11. PREN 50303-Equipment intended for use in potentially explosive atmosphere Group 1 Category M

12. EN 60079-14 Electrical apparatus for explosive gas atmosphere : Installation

13. EN 60079-17 Electrical apparatus for explosive gas atmosphere : Maintenance

14. EN-60079-19 Electrical apparatus for explosive gas atmosphere : Repair and overhaul

15. Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, Official Journal of the European Communities, 19/4/94

16. EN 1127-1 Explosive atmospheres - Explosion prevention and protection. Part 1: Basic concepts and methodology

17. "ATEX Guidelines. Guidelines on the application of Council Directive 94/9/EC of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres", ATEX/98/5, Draft, 22 September 1998

18. EN 954-1 Safety of machinery - Safety-related parts of control systems

19. IEC 61508 Functional safety of electrical, electronic and programmable electronic safety-related systems

20. COMMON POSITION (EC) No 13/1999 adopted by the Council on 22 december 1998 with a view to adopting Council Directive 1999/…/EC of … on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (1999/C55/06)

21. R G Mellish, "The single fault philosophy: how it fits with risk management", Medicial Devices Agency, UK

22. IEC 60601-1 (1988-12) Medical electrical equipment – Part 1: General requirements for safety

23. CENELEC TC31/WG09, Draft proposal for a European Standard, "Electrical Equipment of Potentially Explosive Atmospheres - Reliability of safety-related devices", 12.02.99

24. A W Cox, F P Lees & M L Ang, "Classification of Hazardous Locations", IChemE, 1990

25. Institute of Petroleum Electrical Committee, "A risk based approach to hazardous area classification", Portland Press, 1998

26. FSA, "The RASE Project. Explosive atmospheres: risk assessment of unit operations and equipment. Methodology on risk assessment of unit operations and equipment-updated version", December 1998

27. Council Directive 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances.

28. HSE, "The tolerability of risk from nuclear power stations", HMSO, 1992

29. Interdepartment Liaison Group on Risk Assessment, "The Use of Risk Assessment Within Government Departments", MISC 038, HSE Books, 1996

30. D J Ball & P J Floyd, "Societal risks: a report prepared for the Health and Safety Executive" 1998

31. G L Wells, "Hazard identification and risk assessment", IChemE, 1996

32. S Allum & G L Wells, "Short Cut Risk Assessment", Trans IChemE, Part B, Vol 71, 161-168, August 1993

33. R Bell and D Reinert, "Risk and system integrity concepts for safety-related control systems", Safety Science, 5, 283-308, 1992

34. "Electrical installations in flammable atmospheres. ICI Engineering Codes and Regulations, Group C (Electrical) Vol 1.5, ICI/RoSPA, 1972

35. Area Classification Code for Petroleum Installations (Part 15 of the Institute of Petroleum Model Code of Safe Practice in the Petroleum Industry), Institute of Petroleum/John Wiley, ISBN 0 471 92160 2, 1990.

36. A Tyldesley, "Ignition hazard assessment", proposal for inclusion in EN 1127

ANNEX B

ASSESSMENT OF CURRENT CONTROL SYSTEM STANDARDS

Author: A M Wray PhD
Health and Safety Laboratory

SUMMARY

This report describes the work associated with Task 2 of the SAFEC project. This project has the overall objective of producing a harmonized system for subdivision of the safety devices used in the Hazardous Zones associated with flammable atmospheres.

OBJECTIVES

Task 2: To look at current standards and assess them with regard to their use in defining the integrity of safety devices for use in flammable atmospheres.

MAIN FINDINGS

1) Two standards, which may be used to determine the integrity level of electrical/electronic safety-related control systems, have been identified. These are EN 954-1 and IEC 61508. IEC 61508 is the standard that provides the most appropriate means of determining, and prescribing, the integrity requirements of electrical and electronic protection systems for use in Hazardous Zones and also may be applied to programmable electronic systems.

2) Quantified risk and reliability assessments suggest that the safety integrity levels (SILs) specified in IEC 61508 should be allocated to protection systems used in Hazardous Zones. Suggested allocations are provided for each Hazardous Zone.

3) The ATEX Directive gives fault tolerance requirements. These must be applied in addition to the qualitative requirements of IEC 61508.

5) When determining the SIL of a protection system, all parts of that protection system must be considered. For example, the overall SIL of a pressurization system depends on the pressurized cabinet, its control system AND the reliability of the compressed air supply to it.

CONTENTS

1 Introduction

This report describes the work associated with Task 2 of the SAFEC project. This project has the objective of producing a harmonized system for subdivision of the safety devices used in the Hazardous Zones associated with flammable atmospheres. Details of the project can be found in Reference 6.

The objective of Task 2 is to look at current standards and assess them with regard to their use in defining the integrity of safety devices for use in flammable atmospheres. First, however, the author will examine the requirements of the ATEX Directive (Reference 1), whose requirements define the design of equipment used in potentially flammable atmospheres, in order to determine how these requirements will affect the use of current standards associated with the design and use of control systems.

Following this, the important aspects of the standards EN 954-1 (Reference 3) and IEC 61508 (Reference 4) will be considered in relation to their use in categorizing equipment for use in hazardous zones.

The author will then carry out calculations based on:

- individual risk;
- accident records, and
- the failure rate of a generic design of pressurization system.

The results of these will then be used, together with a proposal from Working Group 9 of CENELEC committee TC31 (Reliability of Safety-related Devices) in order to determine which safety integrity levels are appropriate for use in each Zone[1].

2 An interpretation of the ATEX Directive requirements

The Directive has not been written in precise and unambiguous English, so may be open to alternative interpretations. Because the interpretation of the Directive may be subjective, previous interpretations may have been over-influenced by particular standards, for example, BS EN 954-1[2]. Therefore, the author has re-examined the relevant requirements of the Directive with an open mind. Only those requirements relating to system integrity (i.e., not relating to functionality) have been considered.

The numbers in brackets, e.g., (1.5.1), refer to the relevant paragraph numbers within Reference 1.

---

[1] The analyses and recommendations given in this report relate to the integrity of the protection devices, i.e., their ability to carry out their intended protection functions. The use of EN 954-1 and IEC 61508 in enabling an estimate of the integrity of the protection devices to be made, do not take into account the sparking potential of the protection devices themselves and so give no indication of whether the protection devices may be installed inside or outside the hazardous area.

[2] EN 954-1 was published in the UK as BS EN 954-1 by BSI Standards. As the author used the latter, the standard will be referred to by its UK designation within this report.

2.1 The ATEX requirements

2.1.1 ANNEX I (Classification of categories)

2.1.1.1 Equipment-group I - Category M1

1) Category M1 equipment is required to remain functional, even in the event of rare incidents relating to equipment, with an explosive atmosphere present, and is characterized by means of protection such that:

- *either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection,*
- *or the requisite level of protection is assured in the event of two faults occurring independently of each other.*

2.1.1.2 Equipment-group I - Category M2

(This equipment is intended to be de-energized in the event of an explosive atmosphere.)

1) The means of protection relating to equipment in this category assures the requisite level of protection during normal operation and also in the case of more severe operating conditions, in particular those arising from rough handling and changing environmental conditions.

2.1.1.3 Equipment-group II - Category 1

1) Equipment in this category must ensure the requisite level of protection, even in the event of rare incidents relating to equipment, and is characterized by means of protection such that:

- *either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection,*
- *or, the requisite level of protection is ensured in the event of two faults occurring independently of each other.*

This requirement appears to direct that this type of equipment must tolerate:

- the failure of one redundant protection system (first bullet point). In this case, more than one fault may occur in that protection system, for example, as a result of additional knock-on faults resulting from the first fault. The author does not associate the term "independent" with diversity. Therefore, the two means of protection could be identical, but not interconnected, or
- two faults (second bullet point), if these faults occur in a single protection system. The criterion requires the operation of the protection system to tolerate two faults, where the second fault is neither initiated by the first fault nor results from the same common-cause as the first fault.

Neither requirement takes into account the proof-test interval of the equipment nor the failure rate of the channels/components which make up the equipment.

2.1.1.4 Equipment-group II - Category 2

1) The means of protection relating to equipment in this category ensure the requisite level of protection, even in the event of frequently occurring disturbances or equipment faults which normally have to be taken into account.

The author interprets this to mean that:

- the equipment must tolerate single faults, but
- the equipment need not tolerate certain single faults which do not "normally have to be taken into account".

This rather ambiguous, and potentially weak, requirement could be interpreted to mean that the equipment should tolerate single faults where these faults are considered to be credible; however, defining whether a component fault is credible or not is left to either the (subjective) opinion of the designer, or current custom and practice.

2.1.2 ANNEX II (Equipment requirements)

2.1.2.1 Requirements in respect of safety-related devices

1) As far as possible, failure of a safety device must be detected sufficiently rapidly by appropriate technical means to ensure that there is only very little likelihood that dangerous situations will occur. (1.5.1.)

Clearly, the aim of this requirement, which is system specific, is to define the maximum time between the occurrence of a fault and the equipment being brought into a safe state for a particular installation. This time will include:

- the time between a fault occurring and its detection, which will depend on, for example, the repetition rate of any automatic diagnostic functions (e.g., as carried out by programmable electronic systems [PES]);
- the time required to bring the system into a safe state following a detection of a fault. The requirement does not mention the time to bring the equipment into a safe state following the detection of a fault; presumably, this time is considered to be so small that it may be neglected.

The maximum available safe time between the occurrence of a fault and the equipment being brought into a safe state for a particular installation will depend on the time taken for, for example, an explosive concentration of gas to be reached and will be installation dependent. In many cases, this time will be based on a probabilistic assessment of the conditions at the time of the failure, leading to a probability of explosion based on: the failure rate; the shutdown time (or time taken for a second protection system to operate), and the probability of formation of an explosive atmosphere.

2) For electrical circuits the fail safe principle is to be applied in general. (1.5.1.)

This rather ambiguous requirement could imply:

- safety-related equipment should be designed to operate such that the most probable mode of failure of its components leads to a safe state. For example:
    - a control circuit should be designed such that de-energization causes shutdown, then an open-circuit connection, the most likely failure mode, would lead to a shutdown;
    - relays, whose predominant failure mode is to the de-energized state, should be arranged to cause shutdown on their de-energization;
    - dynamic operation should be employed, for example, a continuously changing signal should be used in preference to a DC level, because such a signal is unlikely to be produced by a component failure, etc., or
    - systems should have a level of fault tolerance.

3) Safety-related switching must in general directly actuate the relevant control devices without intermediate software command. (1.5.1)

The implication of this requirement is that safety devices, e.g., protective systems, should not be programmable, i.e., they may be electrical, electromechanical or electronic, but should not incorporate microprocessors in the control path.

The author has been informed that the intention is to forbid the use of programmable equipment to drive output devices, for example, via local area networks; however, the document is very ambiguous with respect to this point.

4) In the event of a safety device failure, equipment and/or protective systems shall, wherever possible, be secured. (1.5.2.)

The meaning of this requirement is not fully clear.

5) In the design of software-controlled equipment, protective systems and safety devices, special account must be taken of the risks arising from faults in the program. (1.5.8.)

This requirement leads to a realization that systematic faults may be present in software, and, hence, that measures should be taken to minimize the probability of such faults being present, for example, by the use of quality assurance techniques in the software lifecycle.

This requirement is in direct conflict with that at 3, above, unless the interpretation is as shown at 3, above.

2.1.2.2 Category M1 of equipment-group I

1) Equipment must be equipped with a means of protection such that:

- *either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection,*

- *or, the requisite level of protection is ensured in the event of two faults occurring independently of each other. (2.0.1.1)*

This requirement appears to direct that this type of equipment must tolerate:

- the failure of one redundant protection system (first bullet point). In this case, more than one fault may occur in that protection system, for example, as a result of additional knock-on faults resulting from the first fault. The author does not associate the term "independent" with diversity. Therefore, the two channels of protection could be identical, but not interconnected, or
- two faults (second bullet point), if these faults occur in a single protection system. The criterion requires the operation of the protection system to tolerate two faults, where the second fault is neither initiated by the first fault nor results from the same common-cause as the first fault.

Neither requirement takes into account the proof-test interval of the equipment nor the failure rate of the channels/components which make up the equipment.

2) Where necessary, this equipment must be equipped with additional special means of protection. (2.0.1.1)

This requirement appears to duplicate that at the first bullet point at 1, above.

2.1.2.3 Category 1 of equipment-group II

1) It must be equipped with a means of protection such that:

- *either, in the event of failure of one means of protection, at least an independent second means provides the requisite level of protection,*
- *or, the requisite level of protection is ensured in the event of two faults occurring independently of each other. (2.1.2.1).*

See the comments at 2.1.2.2.

2.1.2.4 Category 2 of equipment-group II

1) Equipment must be so designed and constructed as to prevent ignition sources arising, even in the event of frequently occurring disturbances or equipment operating faults, which normally have to be taken into account.

The author interprets this to mean that:

- the equipment must tolerate single faults, but
- the equipment need not tolerate certain single faults which do not "normally have to be taken into account".

This rather ambiguous, and open-ended, requirement could be interpreted to mean that the equipment should tolerate single faults where these faults are considered to be credible; however, defining whether a component fault is credible, or not, is left to either the (subjective) opinion of the designer, or current custom and practice.

2.2 Summary of the requirements

For the purpose of this summary, the equipment will be assumed to be used in an explosive atmosphere caused by a gas and not dust.

1) The time to detect a fault shall be small in order give a high probability of ensuring that equipment will be put into a safe state before a dangerous situation can occur.

2) The design should take the mode of failure of components into account and ensure that the most probable failure modes of the components lead to a safe state.

3) In general, safety-related systems should be mechanical, pneumatic, hydraulic, electromechanical, electrical or electronic but not programmable.

4) Software should be designed to minimize the probability of systematic faults.

5) For Category 1 equipment, if a single protection system is used, this should have a fault tolerance of two. If multiple protection systems are arranged in a redundancy configuration, the design should tolerate the failure of a single channel. Therefore, the component fault tolerance must be two (single-channel protection) and the channel failure tolerance should be at least one (multiple-channel protection).

6) Category 2 equipment should tolerate "normally taken into account" single faults - presumably faults considered to be credible by the designer[3].

7) There is no fault-tolerance requirement for Category 3 equipment.

8) There are no requirements for proof-test interval, fail-safe fraction[4], diagnostics, diagnostic coverage or component/equipment failure rates. In this respect, the ATEX Directive appears to assume that the failure rate of a fault tolerant system is likely to be low over the lifetime of the equipment. This may be difficult to justify without further qualification.

2.3 Discussion of the requirements

The Directive leaves a lot of questions unanswered and is open to interpretation. For example, a requirement that a protection system should tolerate a protection-system failure seems, at first sight, to be excellent; however, the effects of this requirement will depend on many factors that are not defined and which could lead to very wide variations in system integrity for a particular level of fault tolerance. These include:

- the failure rate of the components. Two protection systems could be used in order to meet the requirements of the Directive for Category 1 equipment. However, these could be so unreliable that a well designed single protection system could achieve a lower overall failure rate;

---

[3] This examination looks only at the Directive; however, it should be noted that standards describing the faults that may be excluded are available.

[4]That fraction of the failure rate of a component which will result in a safe system failure

- whether automatic diagnostics are used. A system could incorporate automatic diagnostics with a high repetition rate. If the coverage of the diagnostics were, for example, 90%, the effective rate of potentially dangerous failures (or probability of failure on demand) for the protection system could be reduced by a factor of 10;
- the repetition rate of any automatic diagnostics. The probability of failure on demand will depend on the repetition rate of the diagnostics. A short interval between diagnostic tests will lead to a lower probability of failure on demand;
- whether manual proof tests are carried out. Manual proof testing could be used to detect failures in one channel of a redundancy system, for example;
- the period between manual proof tests (the proof test interval). As with automatic diagnostics, a low proof test interval will lead to a lower probability of failure on demand. The period between manual proof tests is an important parameter in determining the failure-to-danger rate of any system, but especially one which operates on demand, and
- which components are considered to have credible failures. Information on the failure rate of components is required to make a judgement on whether the failure of a component should be considered to be credible or not - in making the decision that a fault is, or is not, credible, an assumption about the reliability is being made. The belief that the use of the concept of fault tolerance avoids a need for a knowledge of reliability, is, in fact, a delusion. To avoid the subjective uncertainty associated with deciding which component faults are incredible requires a definitive and comprehensive list of such component faults.

It should be clear that the integrity of any system with a fault tolerance greater than 0 will be dependent on the automatic diagnostic and manual proof tests (including the intervals between them) carried out on the system. Therefore, a requirement for a particular level of fault tolerance is an incomplete requirement for defining system integrity. For example, consider a system designed to have a fault tolerance of 1. If that system is never tested, eventually a fault **will** occur. The system now has a fault tolerance of 0 and this situation will remain until a test, that will identify the fault, is carried out and the system is repaired.

All that can be stated regarding a system with a fault tolerance of 1 is that its integrity is likely to be higher than that of a system with a fault tolerance of 0 and likely to be lower than that with a fault tolerance of 2. However, even this limited statement assumes that the proof-test interval and the failure rate of the components/channels is approximately the same in all cases.

Therefore, if system integrity is to be defined using fault tolerance as a measure, the allowable range of component failure rates, proof test interval, coverage of automatic diagnostics and their repetition rate, and the means of preventing common-cause failures must, in addition, be defined.

The author's overall opinion is that the requirements of the Directive have tried to cover each of the parameters that would be considered in a quantitative risk assessment; however, it:

- considers these parameters individually as if they are independent. Unfortunately, they are not;
- does not take into account the effects of testing (manual and automatic) on the system integrity, and
- in trying to measure integrity in terms of fault tolerance, fails to take into account the considerable effect that testing and component failure rates can have on system integrity.

3 Comments on the TC31/WG9 proposal (Reference 2)

The following comments take into account the interpretation of the ATEX Directive described above and the author's use of both BS EN 954 and IEC 61508 in the assessment of safety-related control systems.

Table 1 reproduces the table and accompanying comments at Section 4 of Reference 2.

Table 1: The table in Section 4 of Reference 2

Hazardous area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Equipment (EUC) Fault tolerance	2	1	0	1	0	-1.00[1]	0	-1
Safety category of monitoring or control unit	-	SIL2[2]	SIL3	-	SIL2	SIL3	-	SIL2
Resulting equipment category[3][4] of the combination	Category M1/1			Category M2/2			Category 3	

[1] ignition sources under normal operation

[2] according to IEC 61508

[3] according to RL/94/9/EC

[4] comment:

SIL2 means either a failure tolerance 1 with 60% degree of detection or a failure tolerance 0 with 90% degree of detection
SIL3 means either a failure tolerance 2 with 60% degree of detection or a failure tolerance 1 with 90% degree of detection

The reader will notice a number of inconsistencies with other documents when observing Table 1, which has been reproduced as closely as possibly to the original. These are:

1) The safety integrity levels described in IEC 61508 appear to have been selected according to the fault tolerance associated with them. In fact, IEC 61508 does NOT determine SILs according to fault tolerance. Instead, following the application of quantitative and qualitative measures, fault tolerance criteria are applied in order to determine a ceiling for the SIL of any particular system. This is used as an additional measure in order to ensure that the SIL, calculated as a result of, for example, false assumptions, or misinterpretations, is not unrealistic and takes into account component complexity (i.e., Type A and Type B components). Clearly, the fault tolerance criteria of IEC 61508 should not be used as a means of estimating integrity, i.e., these criteria should not be mapped directly to the SIL. Hence, the comment below Table 1 must be considered to be void.

2) The ATEX directive requires a fault tolerance of two, for a single-channel protection system, or a channel failure tolerance of 1 for protection systems arranged in a redundancy configuration.

3) IEC 61508 is based on both quantitative analysis (to ensure an adequately low failure-to-danger rate due to random hardware faults) and qualitative measures (to ensure that the number of systematic faults is adequately low so as not significantly to affect the random hardware failure rate). Determining the SIL inappropriately, i.e., by improper reverse engineering based on an existing system, could lead to a random hardware failure rate that is not consistent with the safety requirements.

4) The SILs described in IEC 61508 apply to safety functions, not individual pieces of hardware. A SIL could, for example, define the probability of failure of a particular function (several of which could be carried out by one, or more, items of hardware and each item of hardware could be involved with one, or more, safety functions). Reference 2 implies that the SILs apply to the protection systems themselves.

5) IEC 61508 takes a scientific approach to SIL determination, based the reduction in risk resulting from each protective function. Although a SIL could be assigned arbitrarily, as in Table 1, from, for example, the consequence of failure, this would lead to a quantified failure rate requirement based on arbitrary rather than scientific arguments.

6) Reference 2 does not differentiate between the fault tolerance required by the ATEX Directive for a single-channel protection system and the channel failure tolerance for protection systems arranged in a redundancy configuration.

Whilst the author does not wish to dispute the contents of the table produced by TC31/WG9 (Table 1) nor the Working Group's right to choose those particular contents, he considers that the justification of the SIL chosen for each element in the table to be somewhat tenuous.

4 Comments on the available standards

There are two standards which provide guidance on the design of control systems for use in safety-related applications:

- EN 954-1 [published as BS EN 954-1 in the UK (Reference 3)], and
- IEC 61508 (Reference 4).

These will now be discussed.

4.1 BS EN 954-1 (Reference 3)

The author has used BS EN 954 in the assessment of a number of safety-related systems and has identified the following problems with its use:

1) The standard does not have an underlying principle which follows from start to finish. Instead, there is a large number of minor requirements and 'give aways'. For example, the fundamental requirements of the various categories are simple to follow and relate to fault tolerance. However, having established the requirements for Category 3, for example, one finds that it is not necessary to detect all single faults but only some. (See Table Guide to the categories for safety-related parts of control systems from BS EN 954-1, in Reference 3.)

2) The principles of BS EN 954-1 are based on fault tolerance. This, at first sight, seems to be a very simple way of defining the integrity of the safety functions. However, there are many component failures which, in combination, could lead to the hazard and many of these failures are unlikely, highly unlikely or even incredible. The standard allows incredible component failures to be excluded; however, the decision to exclude such failures from the analysis is a subjective task, making what appears, at first sight, to be a simple and objective methodology both difficult and subjective. In this respect, the standard, in effect, replaces reliability calculation with subjective judgement.

3) Because the requirements of BS EN 954 are somewhat vague, for example, in determining which faults may be excluded from an assessment, the independence of any validation may be compromized because of the need for the independent assessor to exclude exactly the same components as the designer.

4) BS EN 954-1 gives no means of assessing or ensuring the integrity of software.

5) BS EN 954-1 mentions maintenance, but does so very weakly. In any safety-related protection system (which may be called to operate only infrequently), regular manual proof testing (in the absence of automatic diagnostics) is an important factor in maintaining the integrity, which will vary approximately linearly with the frequency of the manual proof checks.

6) BS EN 954-1 is a design standard, so does not give advice on the manufacture of the system being designed. A well-designed system that is sloppily manufactured could have a reduced integrity. (For example, a multi-channel system, whose wiring has been designed to be kept separate in order to avoid common-cause failures, could have the wiring strapped together as a single loom leading to a significant potential for common-cause failures.) Surprisingly, advice is given regarding maintenance at Clause 9. (It

should be noted that the validation stage, e.g., type testing, cannot account for variations between manufactured items resulting from, for example, a poorly specified manufacturing stage.)

7) By assuming that subsystems are single components and applying the fault exclusion principle, it is possible to determine a Category without the need for complex calculation. However, the failure rate of a complex subsystem may be considerably higher than that of a single component. Therefore, the Category of a dual-channel subsystem cannot be considered equivalent to a dual-channel system at the component level, e.g., an interlock based on 2 relays cannot be compared with one based on two complex PLCs, even if both interlocks achieve Category 3. Hence, two systems, each having the same Category, may be considered to be equivalent only if they use the same technology and a comparable number of components.

8) The Categories in BS EN 954-1 are not hierarchical. A number of factors will considerably distort the hierarchy of Categories. (Although the standard clearly states otherwise, it is inconceivable that the hierarchy was not developed on the basis that a monotonic relationship exists between the integrity and the Category.) For example:

- the standard is based on system behaviour in the presence of faults. Modern technology allows the incorporation of sophisticated automatic diagnostics with a coverage approaching 100%. A single-channel system with sophisticated diagnostics may have a higher integrity than a crude multi-channel system. Although the standard allows incredible faults to be excluded, it does not give advice on how this problem should be addressed.
- a highly reliable system, based on simple technology (e.g., a scotch) and (because of its single-channel status) having a Category of 1, may in practice have an integrity comparable, or even higher than, that of a Category 4 system employing a complex and, therefore, difficult-to-assess technology.

9) The categories used to define the integrity of a system are based on fault tolerance. This is an arbitrary means of defining the probability of failure on demand and takes no account of the frequency of such failures, which could be vastly different for alternative technologies. The methodology gives a meaningful result only if all components use the same technology.

10) Because of the subjective means of determining the required Category described in Informative Annex B, it is not very difficult to justify a change of the Category by one either up or down in order to suit other agendas.

11) BS EN 954-1 relates to components and not safety functions. Therefore, a safety function carried out by a large number of components or a single component could be allocated the same Category; however, the safety function carried out by the single component could have a significantly higher integrity.

12) In the author's opinion, BS EN 954-1 was developed for relay-based systems as existed in the 1970s, an application for which it would have been ideal as it is simple to apply, and it would have led to in improvement in the safety standards at that time. Unfortunately, the standard has been overtaken by the technologies used in safety-related systems and it would be difficult to take into account: sophisticated automatic

diagnostics; the use of systems which include different technologies having vastly different failure modes and reliabilities, and the use of software. The feature of the standard is its underlying simplicity; however, even in its present form, this simplicity has begun to be lost. If attempts are made to take these deficiencies into account, the simplicity of the standard will be completely lost, and it would be better to go directly to a standard designed to address these deficiencies from the outset.

4.2 IEC 61508 (Reference 4)

IEC 61508, Reference 4, is a much later standard than BS EN 954-1, having been only recently published. IEC 61508 takes a scientific approach to the determination of integrity by taking into account:

1) the quantified reliability of the safety function[5]. The failure-to-danger rate of the functions carried out by a safety-related system must be less than that which would lead to an unacceptable hazard rate. The quantified analysis of a system deals with the random hardware failure rate;

2) the qualitative reliability. The techniques used to design, maintain, etc., the system throughout its lifecycle must be sufficient to ensure that the rate of systematic failures is less than the random hardware failure rate, and

3) the architectural constraints, based on fault tolerance and fail-to-safety characteristics[6]. These put a ceiling on the safety integrity level (SIL) that can be claimed for any particular system in order to ensure that uncertain reliability calculations, e.g., where reliability data are sparse, do not lead to an inflated SIL.

As a generic standard, IEC 61508 can be applied to safety-related systems of any complexity based on electrical or electronic or programmable electronic technology. However, the focus of the standard is on programmable electronic technology. In the case of low complexity, non-programmable technology, many of the requirements will be fulfilled by normal engineering practice (see Annex A).

4.3 Summary of the standards with respect to the ATEX Directive

1) IEC 61508 takes a scientific approach to safety integrity and covers all types of electronic safety-related systems, whereas BS EN 954-1 cannot be applied to programmable systems.

---

[5]For the purpose of this document, which is concerned only with failures to danger, and in the absence of any alternative concise and convenient term, the term reliability will be used to refer only to those failures which result in the system in which they occur moving to a less-safe state.

[6]The characteristics of certain components predominantly to fail to a particular state on failure. This can be exploited by ensuring that this state leads to, for example, a safe shut-down. In complex systems, this property can be emulated using automatic diagnostics.

2) IEC 61508 gives a more certain determination of integrity than does BS EN 954-1, which is based on fault tolerance.

3) IEC 61508 uses fault tolerance only to determine a ceiling for the SIL that can be claimed for a system and even then uses this only in conjunction with diagnostic coverage (or fail-safe fraction).

4) BS EN 954 is based on fault tolerance; however, it does not have a category corresponding directly to the fault tolerance requirement of 2 of the ATEX Directive. BS EN 954 has 4 categories for describing control systems:

- Category 1 has a fault tolerance of 0;
- Category 2 has a fault tolerance of 0 but has automatic monitoring;
- Category 3 has a fault tolerance of 1, and
- Category 4 has:
  - a fault tolerance of 1 with automatic monitoring, **or**
  - a fault tolerance of 2.

5) BS EN 954 was intended for machinery control systems and does not take into account the complexities of some systems. For example, it would be difficult, using BS EN 954, to take the failure rate of a compressed-air supply into account when determining the integrity of a pressurization system.

6) IEC 61508 (or industry-specific standards that will be based on it) is likely to be the dominant standard for future safety-related design and assessment.

7) IEC 61508 allows the integrity of systems containing programmable electronics to be determined and, as a result, will allow the integrity of these systems to be determined in the future when they eventually become widespread in this type of application. The use of BS EN 954 may stifle the use of programmable systems in the future in areas where their flexibility and diagnostic capabilities could lead to improved safety.

8) The principles of reliability encompassed by IEC 61508 can be applied equally to low-complexity systems as to programmable systems; however, for low-complexity systems, the emphasis will be on the reliability aspects as the systematic aspects will be straightforward, requiring very little more than a consideration of conventional design practices.

9) It will be realised that either standard could be used to determine the integrity of equipment intended for a hazardous atmosphere; but:

- IEC 61508 would provide a better indication of system integrity; however,
- neither standard would fully provide the ATEX requirements of fault tolerance which, although possibly inappropriate, are required by legislation to be followed by any standard appropriate to equipment for use in hazardous zones.

Therefore, it is the author's opinion that any industry-specific standard should be based on IEC 61508 but have an additional requirement, based on fault tolerance, which will ensure that the fault tolerance requirements of the ATEX Directive are met.

5 The target SIL for systems used in Hazardous Zones

IEC 61508 sets targets for, and determines the integrity of, systems in terms of Safety Integrity Levels (SILs). These incorporate the qualitative and quantitative requirements discussed in Section 4.2. To design a system using IEC 61508, a target SIL must first be determined by risk assessment, or other means, e.g., industry-specific standards. This section will describe a number of diverse calculations used by the author to estimate the target SILs appropriate for each of the Hazardous Zones. These will then be used to determine target SILs for recommendation for use in each of the zones.

A SIL could arbitrarily be assigned as has already been discussed in Section 2 (See Table 1). Whilst this assignment may be perfectly valid, the author regards the route used to determine the assignment in Table 1 to have very tenuous justification.

Table 1 can be rewritten as shown in Table 2. This table assumes that a system is available that has been certified for use in a particular zone. For example, suppose a pressurized cabinet is used with a system in order to allow the use of the system in a more onerous zone. Table 2 may be used to indicate the target SIL of the pressurization system, including any function leading to a shutdown if pressurization fails.

Table 2: Reformatted form of Table 1: SIL of the protection system			
Zone for which the EUC has been designed (ATEX category)	Zone of intended use (overall equipment category)		
	0 (1)	1 (2)	2 (3)
0 (1)	N/A[1]	N/A	N/A
1 (2)	SIL2	N/A	N/A
2 (3)	SIL3	SIL2	N/A
-[2]	SIL4[3]	SIL3	SIL2

[1] N/A: Not applicable – additional protection is unnecessary.

[2] The equipment is considered to provide an ignition source during normal use so corresponds to the equipment fault tolerance of –1 in Table 1. For this row, the protection (e.g., pressurization) system must provide, in its own right, the entire integrity for explosion protection.

[3] This entry is not present in Table 1, but has been added to give symmetry to the table.

Whilst Table 2 may be provide a satisfactory determination of the SIL, there is no satisfactory justification that, for example:

- SIL4 will provide an adequate level of integrity for a protection system allowing the use in a Zone 0 of a system that has not been certified for use in a Hazardous Zone, or
- SIL3 is inadequate under the same circumstances.

Hence, the table requires calibration.

Table 2 does not encompass the (additional) fault-tolerance requirements of the ATEX Directive. These are shown in Table 3.

Table 3: Fault tolerance requirements of the protection system			
Zone for which the EUC has been designed (ATEX Category)	Zone of intended use		
	0	1	2
0 (1)	N/A	N/A	N/A
1 (2)	0	N/A	N/A
2 (3)	1	0	N/A
-	2	1	0

It will be noted in Table 3 that:

- a fault tolerance of 2 is required by the ATEX Directive for the protection system of Category 1 (Zone 0) equipment when the protection system is the sole means of protection against explosion;
- a fault tolerance of 1 is required by the ATEX Directive for the protection system of Category 2 (Zone 1) equipment when the protection system is the sole means of protection against explosion;
- a fault tolerance of 1 is required of the protection system where the protection system is intended to raise the category of the equipment under protection from Category 3 to Category 1, leading to the overall equipment having a fault tolerance of 2, and
- in those cases, where a fault tolerance of 0 is required, an additional (to the protection system) second means of protection is provided because the equipment has already been certified for use in a lower-risk zone, therefore, no additional fault tolerance requirements are placed on the protection system by the ATEX Directive. This is because the addition of a second means of protection, by default, increases the fault tolerance by 1. [The operation of two systems, each having a fault tolerance of zero, in parallel leads to an overall fault tolerance of 1.] Therefore, no additional fault tolerance requirements are placed on the additional means of protection.
- N/A means not applicable – an additional protection system is not required.

5.1 Probability of an explosive vapour being present

The probability of a flammable gas being present in a particular zone is normally defined in a qualitative way, e.g., continuous, frequent or less frequent. Reference 7 provides a convenient quantitative definition of the zones in terms of the time that flammable gas would be expected to be present. This is:

- Zone 0: >1000 hours per year;
- Zone 1: <=1000 but >10 hours per year, and
- Zone 2: <=10 hours per year.

It should be noted that these values have not been well accepted in all industrial sectors so, although they have been considered by CENELEC working groups, they have not been incorporated in standards.

The worst case for Zones 0 and 2 (continuous and 10 hours, respectively) can be assumed. However, the span of Zone 1 covers a factor of 100, which causes a number of difficulties. For example:

- if a worst-case value were chosen, this would lead to equipment used in environments corresponding to the lower end of Zone 1 being overspecified by a factor of up to 100, alternatively

- if a (logarithmic) mean value were chosen, equipment used in environments corresponding to the upper end of Zone 1, could be underspecified, leading to a potentially unacceptable level risk.

Therefore, **for the purposes of the calculations in this report**, Zone 1 will be divided into two equal zones each covering a factor of 10 leading to the values shown in Table 4. In all cases, the probability of occurrence corresponds to the **worst-case probability** for the particular zone.

Table 4: Probability of an explosive vapour being present

Zone	Quantitative assumption (hrs/yr)	Probability of occurrence (%)
0	>1000	100
1H	<1000 and >100	10
1L	<100 and >10	1
2	<10	0.1

The subdivision of Zone 1 into two equal (on a logarithmic scale) width sub-zones leads to :

- it being reasonable to assume a worst case value for the probability of a flammable gas being present in each zone, and
- the probabilities being separated by a factor of 10. This corresponds to the spacing between the safety integrity levels (SILs) used in IEC 61508.

5.2 Determination of the ALARP level of risk

The procedures described in this section were intended to provide independent routes for estimating the ALARP level of risk associated with the hazardous zones. The primary aim is to determine the ALARP level quantitatively, **so qualitative requirements (e.g., fault tolerance, etc.) have not been taken into account**.

5.2.1 From individual risk

The HSE document *Tolerability of risk from nuclear power stations*, Reference 5, indicates that a probability of death of 10^{-3} per year is intolerable for a worker and 10^{-4} per year is intolerable for a member of the public. In the other direction, a probability of death of 10^{-6} would be considered to be acceptable. (Also see Reference 6.)

Based on these overriding criteria, we can determine a coarse estimate of the system integrity, as defined in terms of the Safety Integrity Levels (SILs) described in IEC 61508, as shown in Table 5.

Table 5: Coarse estimate of system integrity based on Reference 5					Unit
Probability of death to be achieved	1,000	100	10	1	per 10^6 yrs
Number of workers/members of the public present[1]	0.3	0.3	0.3	0.3	
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 0	0.57	0.057	0.006	0.0006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 1H	5.7	0.57	0.06	0.006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 1L	57	5.7	0.57	0.06	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 2	570	57	5.7	0.57	per 10^6 hrs
SIL required to achieve target[2], Zone 0	SIL2	SIL3	SIL4	SIL5[3]	
SIL required to achieve target, Zone 1H	SIL1	SIL2	SIL3	SIL4	
SIL required to achieve target, Zone 1L	SIL1[4]	SIL1	SIL2	SIL3	
SIL required to achieve target, Zone 2	SIL1[5]	SIL1[6]	SIL1	SIL2	

Notes to Table 5:

[1] Section 5.2.3 estimates the SIL of pressurization systems. A large number of these systems is used to provide protection to visual display units and personal computers, which generally have an operator nearby. Therefore, although the probability of death occurring as a result of a general explosion may be as low as 1%, the probability of death from an explosion resulting from the failure of a pressurization system could be much greater than this. It was agreed at the 26/8/99 joint meeting of SAFEC and TC31 that 20 deaths per 100 explosions involving pressurization systems should be assumed. Because later sections of this report concentrate on pressurization systems, Table 5 has been made compatible in order to allow comparison.

[2] This is the SIL of the overall safety function and includes all protection measures/devices.

[3] SIL5 is outside the range of achievable SILs considered by IEC 61508; however, SIL 5 has been used here in order to make the table more meaningful.

[4, 5 and 6] SIL1 represents the minimum integrity requirement of IEC 61508 for a system defined as being safety-related; therefore, SIL1 must apply to these positions.

It will be seen that:

1) Table 5 defines the overall SIL of the safety function and is based on Table 3 of Part 1 of IEC 61508. This table applies to the high-demand mode of operation, i.e., systems in continuous operation and would not necessarily apply to, for example, a shutdown system, which is normally dormant and comes into operation only when flammable gas is detected, i.e., when a demand is made on the system. The safety function is that function preventing an explosion if flammable gas becomes present. A continuous source of ignition is assumed;

2) to achieve a probability of death of 10^{-6} requires >SIL4 for Zone 0. This is outside the range of achievable SILs described in IEC 61508. Therefore, based on Table 3 of Part 1 of IEC 61508, a probability of death of 10^{-6} may not be achievable for Zone 0 with current electrical/electronic technologies;

3) the table may be used to define both a floor and a ceiling for the overall SIL definition;

4) it is assumed that, on average, one person is killed for every 3 explosions involving pressurized protection systems. (See Note 1 to Table 5.) Because each SIL has a span covering a factor of 10, and the failure frequencies fall approximately in the centre of these ranges, an error of nearly a factor of 3 in either direction will not affect the SIL that is obtained;

5) the SILs for Hazardous Zones will be expected to be in the ranges:

- Zone 0 - SIL3 to SIL5[7];
- Zone 1H - SIL2 to SIL4;
- Zone 1L - SIL1 to SIL3, or
- Zone 2 - SIL1 to SIL2;

6) if the middle of this range is assumed (i.e., corresponding to the shaded column of Table 5, containing SILs of SIL4, SIL2 and SIL1), this table is not very dissimilar to the bottom row of Table 2. For the bottom row of Table 2, the protection system provides the entire protection from explosion; therefore, this row can be compared directly with the SILs obtained in Table 5. The dissimilarity between Table 2 and the shaded column of Table 5 arises as a result of the overall span of Zone 1 being a factor of 100 and, as Table 2 is based on fault tolerance, this factor is not taken into account, and

7) a probability of death of 10^{-5}/yr, as is proposed as the criterion for acceptable risk in Reference 8, is not unreasonable.

5.2.2 From accident records

Discussion with a UK manufacturer of pressurization systems has indicated that about 18,000[8] such systems have been put into service in the UK over the past 20 years.

---

[7]SIL 5 is outside the range of achievable SILs considered by IEC 61508. SIL 5 has been used here ONLY for illustrative purposes.

Assuming a life expectancy in the region of 8 years, this suggests an average of about 6,000 systems have been in use over this time.

The author is not aware of any explosions resulting from the failure of a pressurization system. Therefore, this sets a lower limit on the integrity of pressurization systems over the past 20 years, as shown in Table 6, below. The values in Table 6 were calculated on the assumption that, if no explosions occur over N operating hours, the probability of an explosion occurring in the next N operating hours is 0.5.

Table 6: SIL indications from accident records	Assumed zone of operation[1]			Units
	Zone 1H	Zone 1L	Zone 2	
Period of study	20	20	20	years
Number of systems in use in the UK over this period	6,000	6,000	6,000	
Total operating period	1,051,920,000	1,051,920,000	1,051,920,000	system-hours
Probability of gas presence[2]	0.032	0.0032	0.00032	
Operating period with gas present	33,661,440	3,366,144	336,614	"gas" hours
Number of known explosions	0	0	0	
Indicated dangerous failure rate for each system	0.015	0.15	1.5	per 10^6 hrs
Indicated SIL for the overall safety system[3]	SIL3	SIL2	SIL1	

Notes to Table 6:

[1] The data in each of the columns have been calculated on the basis that all systems were used in the single specified zone.

[2] It would be inappropriate to use the worst-case probabilities for the presence of flammable gas in the calculations in this particular table, as we must use an estimate of the actual probability. Without any prior knowledge of the distribution of this probability, the logarithmic mean of the range of probabilities covered by each (sub) zone has been used. This is: Zone 1H - 3.2%; Zone 1L - 0.32% and Zone 2 - 0.032%.

[3] This is the average SIL of the total configuration of safety-related systems. The pressurization control system (e.g., purge and shutdown systems) will contribute to this SIL together with other systems, e.g., the air supply.

---

[8]Determined from the number of systems supplied by the manufacturer and its share of the UK market.

Table 6 suggests that the integrity of existing pressurization systems is:

- SIL1, if they have been mainly used in Zone 2;
- SIL2, if they have been mainly used at the lower end of Zone 1, or
- SIL3, if they have been mainly used at the upper end of Zone 1. However, as the probability of gas in the majority of Zone 1 environments will probably lie near the lower end of the zone (i.e., Zone 1L as shown in Table 6) with few at the upper end (shown as Zone 1H), Table 6 should not be considered to indicate that existing pressurization systems are able to achieve SIL3.

The author understands that pressurization systems are used:

- in Zone 1 with continuously sparking equipment. In this case, the equipment is tripped if pressurization were to fail and an alarm is given.
- to protect Zone 2-type equipment in Zone 1. In this case, if pressurization were to fail an alarm is given.
- to protect continuously sparking equipment in Zone 2. In this case, if pressurization were to fail an alarm is given.

Therefore, the equipment may be used in either Zone 1 or Zone 2. However, when used in Zone 1, it may provide only an additional means of protection. Nevertheless, the evidence strongly suggests that the **overall**[9] integrity of existing pressurization systems is at least SIL1.

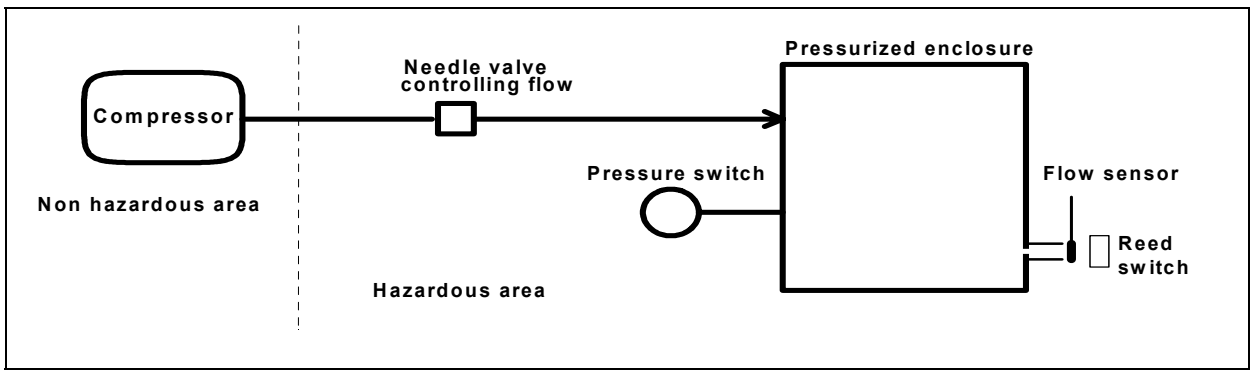
5.2.3 From an examination of a protection system

To facilitate the identification of data and, hence, allow calculations to be made, this section will consider only one system type - pressurization systems. The actual system chosen for examination is not intended to use state-of-the-art techniques and is of a very simple but generic design and, hence, not specific to any particular manufacturer.

Design of the generic system

The system to be considered is shown in Figure 1.

Figure 1: Generic design for a pressurization system: Air-flow diagram



The design shown in Figure 1 is such that:

1) the needle valve is used to set the rate of flow of air into the pressurized enclosure to a predetermined value.

2) the flow sensor is a simple bar magnet mounted on a leaf spring. When the flow exceeds a predetermined rate (which is less than that set by the needle valve) the bar magnet is moved towards the reed switch. This closes contacts of the reed switch. Other types of sensor in common use include orifice plates with differential-pressure switches, the latter including semiconductor sensing elements or simple diaphragm switches.

3) the contacts of the pressure switch close when the pressure in the cabinet exceeds a predetermined value (e.g., 0.5mb). The actual pressure within the enclosure is determined by:

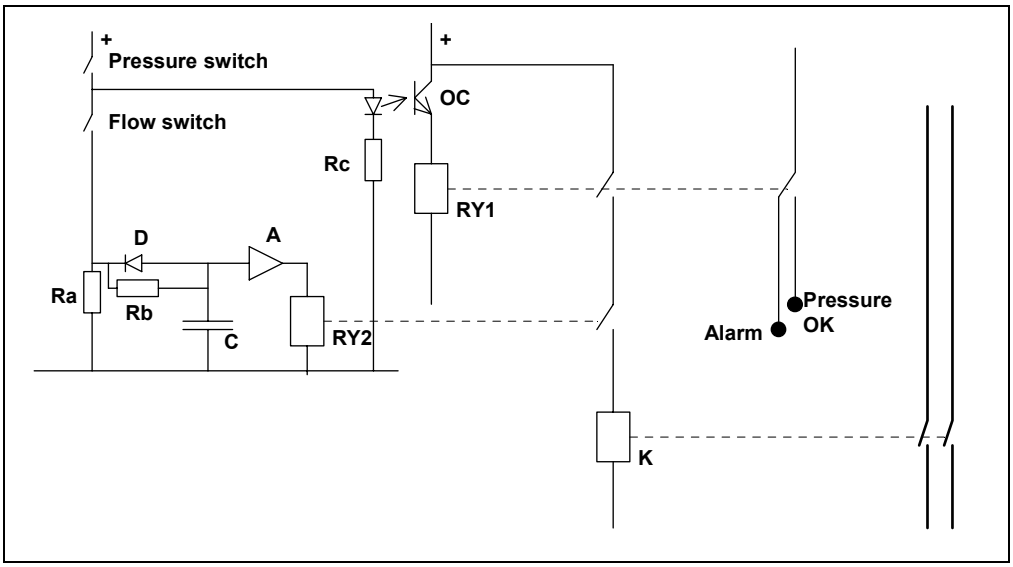
- the air pressure from the compressor;
- the setting of the needle valve, and
- the orifice plate or other constriction on the outlet of the enclosure.

4) during purging, the flow rate through some types of enclosure may be increased in order to speed up the purging process. This is not a safety-related function, so will not be considered in this simplistic design.

5) the compressor is outside the hazardous zone.

The electrical circuit of the system to be considered is as shown in Figure 2.

Figure 2: Generic design for a pressurization system: Electrical diagram



[9] The calculated integrity takes into account ALL protection systems, including the pressurization system.

The circuit in Figure 2 shows that:

1) the pressure switch controls Relay RY1 such that, when pressure in the enclosure is above the pre-set level, Relay RY1 is energized.

2) the flow switch operates via a purge timer. C charges via Rb when the flow switch is closed, the purging period being complete when amplifier A reaches its discrimination level and energizes Relay RY2. If the flow switch opens, Capacitor C is discharged quickly via diode D and Ra.

3) if pressure is available within the cabinet and the purge period has been completed, Contactor K is energized. The contacts of Contactor K are in series with the power supply to the equipment in the pressurized enclosure.

4) the system under consideration will de-energize the equipment in the enclosure if pressurization fails.

Therefore, the system carries out two functions:

- Function 1: to turn off the equipment within the pressurized enclosure if the pressurization fails. The author understands that this function may not be used, depending on the application; however, for the purpose of this assessment, it will be assumed that this function is utilized. This will be referred to as Function 1.
- Function 2: to purge the enclosure prior to power being allowed to the equipment within it. This will be referred to as Function 2.

5.2.3.1 Component failure analysis of the generic system

Because of the simplicity of the generic circuit, a failure modes and effects analysis and its description has not been considered to be necessary. Instead, the failure modes of the components that will lead to a failure towards danger will first be identified. These will then be used to determine the failure-to-danger rate of the functions carried out.

Table 7 shows the failure rates of the components. These were obtained from Reference 9. Comments are given as to any assumptions that were made.

Table 7: Dangerous component failures of the generic design			
Component	**Failure mode**	**Comment**	**Failure rate** per 10^6hrs
Compressor	Loss of air supply	Likely to lead to shutdown of entire process but this cannot be assumed. Also, a redundant compressor is likely to be used. Assume middle of range for single compressor.	200
Needle valve	Blockage/failure to closed state	20/10^6hrs but assume 5% to blocked	1
Pressure switch	Contact-closed	5/10^6hrs but assume 10% to closed	0.5
Flow sensor	Contact-closed	Not differential pressure sensor. Assume same as reed relay.	0.2
Enclosure	Loss of integrity	Maintenance error or external damage. Must be systematic.	0
Resistor Ra	Open circuit/resistance increase[1]	0.004/10^6hrs. Assume 50% to drift	0.002
Resistor Rb	Short circuit/reduced resistance	Not credible	0
Diode D	Short circuit	0.04/10^6hrs. Assume 15% to short-circuit	0
Capacitor C	Reduced capacitance	Type unknown. Assume aluminium electrolytic.	0.3
Discriminator A	Output high	Bipolar linear	0.12
Relay RY2	Energized state	Crystal can. 10% failure to open.	0.01
Opto-coupler OC	On state	0.3/10^6hrs but assume 50% to ON	0.15
RY1	Energized state	Armature. 10% failure to open.	0.03
Contactor K	Energized state	4/10^6hrs but assume 10% failure to open	0.4

[1] Although this will not directly cause the function to fail, it will prevent the capacitor from discharging between purge cycles, so could lead to a failure if repeated purging were required.

5.2.3.2 Quantitative analysis: Function 1

The failure rate of Function 1 will now be considered.

Table 8: Determination of failure rate of the shutdown circuit			
Component	**Failure mode**	**Failure rate, etc.**	**Unit**
Contactor K	Energized state. Assumes power circuit correctly fused.	0.400	per 10^6hrs
Pressure switch	Contact closed	0.500	per 10^6hrs
Circuit board	Ignored as de-energized = safe state	0.000	per 10^6hrs
RY1	Energized state	0.030	per 10^6hrs
Opto-coupler OC	On state	0.150	per 10^6hrs
Resistor Rc	Ignored as open circuit = safe state, and short circuit will lead to safe failure of OC	0.000	per 10^6hrs
Flow sensor	Contact closed	0.2	per 10^6hrs
Resistor Ra	To open circuit	0.002	per 10^6hrs
Diode D Capacitor C	Failure irrelevant to Function 1	0	per 10^6hrs
Discriminator A	Output high	0.12	per 10^6hrs
Relay RY2	Energized state	0.01	per 10^6hrs
Overall failure rate: Function 1 (λ_1)[1]		0.420	per 10^6hrs
Proof test interval, T (six months)		4,383	hours
Probability of failure on demand (PFD=λ_1T/2)		9.2	$*10^{-4}$
Safety integrity level of Function 1 based on PFD		SIL3[2]	

[1] Takes into account the two independent paths (via RY1 and RY2) for turning off contactor K. A β-factor of 0.03 has been used. Because only Contactor C is common to the two paths, its failure rate dominates the overall failure rate. It has been assumed that either the flow sensor or the pressure switch will indicate a loss or pressurization, i.e., there is a diverse means of identifying a loss of pressurization.

[2] This SIL has been determined only quantitatively and does not take the various qualitative requirements of IEC 61508 into account.

Loss of Function 1 will not lead to a failure of the pressurized enclosure unless it is associated with a simultaneous failure of the air supply. The failure rate of the air supply is determined in Table 9.

Table 9: Determination of rate of air-loss events

Component	Failure mode	Failure rate per 10^6hrs
Compressor	Loss of air supply	200
Needle valve	Blockage/failure to closed state	1
Enclosure	Loss of integrity	0.00[1]
Overall failure rate of the pressurization		201

[1] As the probability of the integrity of the enclosure being compromised is low compared to the failure rate of the compressor, an assumption of 0 for the former will not significantly affect the eventual outcome of the calculation.

This leads to an overall failure rate of the pressurized enclosure (i.e., loss of pressurization with equipment in the enclosure powered) as shown in Column 2 of Table 10. On the basis of a probability of death of 10^{-5} per year, as shown in the shaded column of Table 5, this system would be appropriate for protecting uncertified equipment only in Zone 2. However, the overall probability of a pressurization failure with the power applied is proportional to the failure rate of the air supply, so an increase in the availability of compressed air will lead to a corresponding increase in the integrity of the safety function. For example, in practice, the air supply may:

- be a redundancy system in order to achieve a high availability for use by other systems in the plant associated with production, or
- lead to a shutdown of the plant if the air supply fails. Therefore, minimizing the probability of subsequent leakage of flammable substances.

The effect of improving the reliability of the air supply by a factor of 10 is shown in the shaded column of Table 10. Therefore, an analysis of the failure rate of the air supply would be a significant factor in the consideration of the acceptability of this equipment for use, for example, for the protection of uncertified equipment in Zone 1.

Table 10: Determination of the hazard rate associated with Function 1			
Component	**Item**	**Item**	**Unit**
Probability of failure on demand: Function 1 ($P=\lambda_1 T/2$)	9.2	9.2	$*10^{-4}$
Failure rate of air supply[1] (λ_2)	201	20	per 10^6 hrs
Failure rate of pressurization with power applied ($P*\lambda_2$)	0.18	0.02	per 10^6 hrs
Safety integrity level of overall protection function[2]	SIL2	SIL3	

[1] The overall failure rate is proportional to the failure rate of the air supply. If the air supply were backed up or leads to the plant being put into a safe state when it fails, the overall failure rate will decrease. The third (shaded) column illustrates the use of a more reliable air supply.

[2] These SILs have been determined **only** quantitatively and do not take the various qualitative requirements of IEC 61508 into account.

5.2.3.3 Quantitative analysis: Function 2

Table 11: Determination of failure rate of purging-delay function			
Component	**Failure mode**	**Failure rate, etc.**	**Unit**
Contactor K	Energized state. Assumes power circuit correctly fused.	0.400	per 10^6hrs
RY2	Energized state	0.030	per 10^6hrs
Discriminator A	Output high	0.120	per 10^6hrs
Capacitor C	Reduced capacitance	0.300	per 10^6hrs
Circuit board	Ignored as de-energized = safe state	0.000	per 10^6hrs
Diode D	Short circuit	0.006	per 10^6hrs
Resistor Rb	Short circuit/reduced resistance	0.000	per 10^6hrs
Resistor Ra	Open circuit/increased resistance	0.002	per 10^6hrs
Flow sensor AND Pressure sensor	Contacts-closed - □-factor of 0.05 assumed	0.050	per 10^6hrs
Overall failure rate: Function 2 (□)		0.908	per 10^6hrs
Proof test interval, T (six months)		4,383	hours
Probability of failure on demand (□T/2)		1.99	$*10^{-3}$
Safety integrity level of Function 2		SIL2	

Because the frequency of access to the pressurized cabinet is likely to be significantly less than the proof test interval, at first sight it may be assumed that failures of the purging function are unlikely to be revealed by the proof tests. However, this does not take into account:

- there may be no gas present when the pressurized cabinet is opened, and
- the person opening the pressurized cabinet will be able to smell the flammable gas (unless this is, for example, hydrogen) at a level well below the lower explosive limit.

If these are taken into account, a demand on the purging function (i.e., when the cabinet has been opened in the presence of flammable gas) occurs less often than the proof tests as is shown in Table 12, which determines the explosion rate from the failure rate of the purging function.

Table 12: The effect of Function 2 on the explosion rate								Unit
Zone of use	2	2	2	1L	1L	1L	1H	
Probability of flammable gas being present	0.1	0.1	0.1	1	1	1	10	%
Probability of cabinet being opened when flammable gas is present[1]	1	10	100	1	10	100	10	%
Period between openings of cabinet	1	1	1	1	1	1	1	days
Frequency of opening of the cabinet with flammable gas present. This is the actual demand rate on the purging function.	0.42	4.2	42	4.2	42	417	417	per 10^6hrs
Probability of failure on demand of the purging function	2	2	2	2	2	2	2	* 10^{-3}
Frequency of explosions assuming a continuous ignition source.	0.001	0.01	0.08	0.01	0.08	0.83	0.83	per 10^6hrs
Probability of personnel being present[2]	1	1	1	1	1	1	1	
Rate of deaths	0.007	0.07	0.7	0.07	0.7	7	7	per 10^3yrs

Table 13: Changes required to achieve a rate of death of 10^{-5}/year[4]								
PFD[3] of the pressurization system	2.7	0.27	0.03	0.27	0.03	0.003	0.003	* 10^{-3}
SIL equivalent to the row above.	SIL2	SIL3	SIL4	SIL3	SIL4	>SIL4	>SIL 4	
Probability[5] of cabinet being opened when flammable gas is present	1.4			0.14			0.014	%

Notes to Tables 12 and 13

[1] The person opening the pressurized cabinet is unlikely to do so if flammable gas is present. Unless the gas is H_2, the person will recognize the presence of gas from its smell at far below the lower explosive limit. A range of values is shown.

[2] Someone must open the pressurized enclosure - it is assumed that only one person is present.

[3] This row shows the probability of failure on demand required of the purge control system in order to achieve a death rate of 10^{-5}/year with all of the other contributing factors remaining as shown in Table 12.

[4] The columns in Table 13 correspond to the columns immediately above in Table 12.

[5] This row shows the probability of cabinet being opened when flammable gas is present (i.e., the probability of someone failing to smell the flammable gas or opening the cabinet despite smelling flammable gas) that would be required to achieve a death rate of 10^{-5}/year with all other contributing factors remaining the same as shown in Table 12.

The human nose can detect most gases at levels well below their lower explosive limit and it is considered unlikely that a pressurized enclosure would be opened if gas were smelled. Therefore, a value of 100%, for the probability of a cabinet being opened when flammable gas is present, is considered to be unreasonable except in the case of hydrogen. The entries in the shaded columns assume that this probability is 10%, a value that is not considered to be unreasonable, but nevertheless may differ significantly from the true value. This leads to the values shown in the shaded columns, which show probabilities of death of:

- $7 * 10^{-5}$per year for Zone 2;
- $7 * 10^{-4}$ per year for Zone 1l, and
- $7 * 10^{-3}$ for Zone 1H.

Because of the large uncertainty in the assumptions used in this analysis, these results should be treated with great caution.

The apparent freedom from explosions suggests that existing systems, as represented by the generic design considered in this report, provide an adequate level of safety. This suggests that factors which have not been taken into account in the calculations shown

in Table 12 are providing additional means of protection. Such factors could include the human element (i.e., avoidance of opening a pressurized enclosure if gas is smelled) being significantly better than has been assumed, additional data that are being provided by additional sensors being heeded or the probability of a spark, being generated by equipment considered to be continuously sparking, being less than one.

Table 13 indicates that the probability of a person opening a pressurized enclosure may in practice be 1.4% for Zone 2, 0.14% for Zone 1L or 0.014% for Zone 1H. In view of the large uncertainties in the calculation in this section of this report due to the assumptions that have been necessary, the reader is recommended not to place any reliance on the values indicated in either Tables 12 or 13; however, the indication that the human element, or other factors, may play a significant part in the avoidance of explosions should be noted.

5.2.4 ALARP level of risk: summary

1) The ALARP level must fall within the ranges shown in Table 5.

2) Reference 8 proposes that a risk of 10^{-5} deaths per year is a reasonable target risk. This lies within the ranges shown in Table 5.

3) The absence of explosions resulting from the failure of existing pressurization systems strongly suggests that their integrity is at least SIL1.

4) A risk of 10^{-5} deaths per year leads to an overall SIL requirement of 4, 3, 2 & 1 for Zones 0, 1H, 1L & 2, respectively. The division of Zone 1 into an upper and a lower zone was made for only illustrative purposes within this report. In the absence of such a division, it would be inappropriate to use other than the SIL for the upper division for the undivided Zone 1 as any other approach would be unsafe. Therefore, the SILs appropriate to Zones 0, 1 and 2 are SIL4, SIL3 and SIL1.)Table 2 (the author's understanding of the recommendations of TC31/WG9) is compatible with a risk of death of not less than 10^{-5} per year. However, because Table 2 is based on only fault tolerance, it does not take the very wide span of Zone 1 into account. As a result, the calculations suggest that Table 2 errs towards a higher level of safety than may be considered appropriate for Zone 2.

6) The quantitative estimation of the SIL for the generic design of control system for a pressurized cabinet suggests that its shutdown function has an integrity of SIL3. However, when considered in conjunction with its associated air supply, for which a worst-case assumption (i.e., no redundancy) has been made in respect of its reliability, the overall integrity becomes SIL 2. If the use of a more reliable air supply had been assumed, the analysis could have indicated SIL3. (This calculation is based only on reliability and does NOT take into account the qualitative requirements of IEC 61508, which may limit the SIL that can be claimed.)

7) The quantitative estimation of the SIL for the generic design of control system for a pressurized cabinet suggests that its purging function has a SIL of 2.

8) Pressurization systems are currently used:

- in Zone 1 with continuously sparking equipment. In this case, the equipment is tripped if pressurization were to fail and an alarm is given. The generic shutdown system discussed in Section 5.2.3, may be able to achieve SIL3 if used with a reliable air supply as shown in Table 2 for this type of use; however, the generic purging system is unlikely to do so.
- to protect Zone 2-type equipment in Zone 1. In this case, if pressurization were to fail, an alarm is given. The generic shutdown system discussed in Section 5.2.3, could in practice achieve SIL2 as shown in Table 2 for this type of use.
- to protect continuously sparking equipment in Zone 2. In this case, if pressurization were to fail an alarm is given. The generic shutdown system discussed in Section 5.2.3, could be used to sound an alarm which could achieve SIL2 as shown in Table 2 for this type of use.

9) The analysis indicates that, in determining the target SIL, one must consider other systems which may lead to demands on the protection system. Such demands would be ignored by any methodology which classifies integrity in terms of fault tolerance, e.g., BS EN 954-1. Only by using a quantified scientific approach as set out in IEC 61508, will these demands appropriately be taken into account. For example, one must consider:

- the reliability of the air supply, in the case of the shutdown function, and
- the required frequency of purging, in the case of the purging function.

10) The results of the calculations described in Section 5 of this report do not disagree significantly with the SIL requirements shown in Table 2, which the accident data suggest are currently being achieved. (Note that the SILs shown in Table 2 are for the entire system, not, for example, just the pressurization control system.)

11) The calculations used to determine the above were based purely on a quantified analysis - none of the qualitative requirements of IEC 61508, e.g., fault tolerance, have been considered.

6 Conclusions

1) Two standards, which may be used to determine the integrity level of electrical/electronic safety-related control systems, have been identified. These are EN 954-1 (Reference 3) and IEC 61508 (Reference 4). IEC 61508 is the standard which provides the most appropriate means of determining, and prescribing, the integrity requirements of electrical and electronic protection systems for use in Hazardous Zones and also may be applied to programmable electronic systems.

2) Quantified risk and reliability assessments indicate that the safety integrity levels specified in IEC 61508 should be allocated to protection systems used in Hazardous Zones according to Table 14.

3) The ATEX Directive gives fault tolerance requirements. These must be applied in addition to the qualitative requirements of IEC 61508. Where such fault tolerance requirements exist, these are shown in square brackets in Table 14.

Table 14: Target SIL determination and fault tolerance requirements for protection systems used in Hazardous Zones			
Zone for which the EUC has been designed (ATEX category)	Zone of intended use (overall equipment category)		
	0 (1)	1 (2)	2 (3)
0 (1)	N/A	N/A	N/A
1 (2)	SIL2 [0]	N/A	N/A
2 (3)	SIL3 [1]	SIL2 [0]	N/A
-	SIL4 [2]	SIL3 [1]	SIL1 [0]

4) When determining the SIL of a protection system, all parts of that protection system must be considered. For example, the overall SIL of a pressurization system depends on the pressurized cabinet, its control system AND the reliability of the compressed air supply to it. The SILs quoted in Table 14 apply to the ENTIRE protection system, or configuration of protection systems.

7 References

1) Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, Official Journal of the European Communities, 19/4/94

2) European Standard, Electrical equipment for potentially explosive atmospheres, Reliability of safety-related devices, 1. Draft proposal 1999-xx-yy, TC31-WG9, CENELEC, 12/02/1999.

3) BS EN 954-1: 1997, Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design., BSI Standards, ISBN 0 580 27466 7.

4) IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, 1998.

5) The tolerability of risk from nuclear power stations, HSE/HMSO, 1992.

6) Determination of safety categories of Electrical devices used in Potentially Explosive Atmospheres: Report on Task 1: Derivation of target failure measures, SAFEC project, Contract SMT4-CT98-2255, 1999.

7) Area Classification Code for Petroleum Installations (Part 15 of the Institute of Petroleum Model Code of Safe Practice in the Petroleum Industry), Institute of Petroleum/John Wiley, ISBN 0 471 92160 2, 1990.

8) A risk-based approach to hazardous area classification, Institute of Petroleum, London, November 1998, ISBN 0 85293 238 3.

9) Reliability, maintainability and risk - Practical methods for engineers, Fourth edition, David J. Smith, Butterworth Heinemann, 1993, ISBN 0 7506 0854 4.

10) Private communication: Analysis of data contained in BIA (Berufsgenossenschaftliches Insitut Fer Asbeitssicherheit) Report 11/97 Dokumentation Staubexplosionen, Analyse und Einzelfalldarstellung, Dr. –Ing. Franz Eickhoff, Deutsche Montan Technologie GmbH, Dortmund, 1999.

8 Acknowledgements

Mr A M Owler and Mr P MacAulay, Expo-Telektron Safety Systems, for the supply of information on pressurization systems.

ANNEX A

The essential principles of IEC 61508

by

Simon Brown, Health & Safety Executive, Magdalen House, Bootle

Background

This note arises from discussion at the SAFEC project meeting, Madrid, 3-4 November, 1999, where it was agreed to produce a note explaining the essential principles of IEC 61508 and the application of the standard to systems of different complexity. Many of the safety devices under consideration within this project are of low complexity and there is concern that IEC 61508 is not an appropriate standard to use for the classification of such devices.

Introduction

The aim of IEC 61508 is to provide a route whereby safety-related systems can be implemented using electrical or electronic or programmable electronic technology in such a way that an acceptable level of functional safety is achieved. The strategy of the standard is first to derive the safety requirements of the safety-related system from a hazard & risk analysis and then to design the safety-related system to meet those safety requirements taking into account all possible causes of failure including random hardware faults, systematic faults in both hardware and software and human factors.

Scope of IEC 61508

The scope of IEC 61508 is safety-related systems based on electrical / electronic / programmable electronic technology. In broad terms, a safety-related system can be considered to be any system which carries out a safety function so as to prevent, or mitigate, a hazardous situation. The original focus of the standard was on systems based on programmable electronic technology, which tend to be complex in the sense that they are likely to have a multitude of failure modes and their freedom from designed-in, or systematic, faults cannot be proven by testing alone. It is therefore necessary to take a methodical approach at every stage of the lifecycle to minimise, as far as possible, the

introduction of such systematic faults. The uncertainty associated with the failure characteristics of programmable systems means that it is not usually appropriate to rely solely on the more traditional "fail-safe", or fault tolerance approach to safety design.

The scope of IEC 61508 was extended, during the development of the standard, to include safety-related systems based on electrical and electronic technology. This was in order to provide a unified approach. Complex systems based on these technologies can be as prone to systematic faults as programmable systems, so it seemed that a common approach was needed.

IEC 61508 acknowledges that, for 'low complexity' E/E/PE safety-related systems, certain requirements specified in the standard may be unnecessary and exemption from such requirements is possible. A 'low complexity' system is defined by IEC 61508 as one "where the failure modes of each individual component are well defined, and where the behaviour under fault conditions may be completely determined". This will normally mean that systems which include programmable components such as microprocessors, even if the microprocessor is part of a device have an apparently simple function (such as a temperature sensor), should not be classified as being of 'low complexity' (although it might be possible to claim 'low complexity' for a microprocessor which is well proven-in-use).

So, the standard, as written, is essentially intended for application to programmable electronic systems, although it can be applied to 'low complexity' electrical or electronic systems, in which case certain requirements would be regarded as unnecessary, but it does not state which of the requirements would be regarded as unnecessary.

It is also worth noting that IEC 61508 addresses 'systems'. Whilst almost anything can be regarded as a "system", it would be both unwise and unnecessary to attempt to apply all the principles of IEC 61508 to a very simple device such as a fuse or a thermal or current relay for motor protection.

Essential principles of IEC 61508

The following are considered to be the essential principles of IEC 61508:

a) Use of a structured systematic 'safety lifecycle', including verification, validation and independent assessment as a framework for the management of all activities from specification, through design, integration, installation. operation, use and maintenance. (IEC 61508-1).

This is necessary to ensure that all activities relating to functional safety are carried out as planned, with a clear record of the 'inputs' and 'outputs' at each phase of the lifecycle. This enables the processes of verification (checking the outputs of each phase are as intended) and validation (checking that the end result is consistent with the specified requirements). This is particularly aimed at minimising the number of systematic faults built into the safety-related system. Given that, with low-complexity systems, systematic faults are likely to be self-evident, or are revealed during testing, it

is thought that a formalised safety-lifecycle framework would not be a beneficial (or indeed profitable) approach to the development of a low complexity system.

b) Derivation of the target probability of failure on demand (or failure rate) of safety functions from a hazard analysis and risk assessment, taking into account the contributions to safety provided by other technology safety-related systems and other (external) risk reduction facilities. (IEC 61508-1).

The aim of this is that the target performance of the safety-related system, in terms of likelihood of failure, should be adequate taking into account the nature of the hazards and the probability of the hazards resulting in actual hazardous situations, *in the absence of the safety-related system*. This method for deriving performance requirements is appropriate whatever the level of complexity of the safety-related system. It should be noted that IEC 61508 accepts that the performance requirements can be derived using quantitative *or* qualitative methods.

c) Limitation of SIL according to hardware fault tolerance (redundancy) (IEC 61508-2)

The safety integrity level (SIL) of a safety function is limited (no matter what the reliability claimed) by hardware fault tolerance in combination with safe failure fraction (the fraction of faults which are either detected by automatic diagnostics or are 'safe-by-design'). The so-called "architectural constraints" are detailed in IEC 61508-2 and are applicable to systems whatever the complexity. This means, for example, that in order to claim that a safety function is SIL3, then, for a complex system having no redundancy, then a safe failure fraction of at least 99% is required.

d) Quantified estimation of probability of failure of safety functions. (IEC 61508-2)

It is a requirement that probability of failure of safety functions due to random hardware failures is estimated. This is akin to a reliability analysis and requires some knowledge of the reliability of the individual hardware components, or good knowledge of the failure rate of the equipment in use. Note that this does not necessarily mean that the reliability of components is known to a high degree of accuracy. It might be acceptable, for example, to undertake a 'worst case' analysis based on reasonable assumptions. This quantitative analysis is required whatever the level of complexity.

e) Techniques and measures for the avoidance of failures (IEC 61508-2, IEC 61508-3)

The aim is, as far as possible, to avoid any design faults which could lead to dangerous failures during use of the equipment. This is particularly important for complex systems, and for software. In the main, the techniques and measures recommended by IEC 61508 in this respect are those of what would be regarded as good engineering practice. For example, use of guidelines and standards, project management, documentation, structured specification & design. Equipment which has been adequately 'proven-in-

use' in accordance with IEC 61508-2, does not need to be compliant with these requirements.

f) Requirements for the control of systematic faults (IEC 61508-2, IEC 61508-3)

These requirements are particularly aimed at programmable electronic systems where it is possible to incorporate design features (such as program sequence monitoring by use of watchdog timers) that make the equipment tolerant against residual design faults in both hardware and software and operator mistakes. These requirements would not usually be applicable to low complexity, non-programmable systems. Equipment which has been adequately 'proven-in-use' in accordance with IEC 61508-2, does not need to be compliant with these requirements.

g) Requirements for system behaviour on detection of a fault (IEC 61508-2)

These requirements specify the action that should taken following detection of a fault in the safety-related system. Faults may be detected by diagnostic tests, proof tests or by any other means. The aim is to ensure continued safe operation. If that is not possible, then the equipment should be shutdown to a safe state. The requirements are applicable whatever the level of complexity of the safety-related system, and to electrical or electronic or programmable electronic systems.

Conclusions

The following requirements of IEC 61508 are considered to be applicable whatever the level of complexity, and whether the technology is electrical, electronic or programmable electronic:

- *Derivation of the target probability of failure on demand (or failure rate) of safety functions from a hazard analysis and risk assessment, taking into account the contributions to safety provided by other technology safety-related systems and other (external) risk reduction facilities. (IEC 61508-1)*

- *Limitation of SIL of safety functions according to hardware fault tolerance (redundancy) (IEC 61508-2)*

- *Quantified estimation of probability of failure of safety functions based on the reliability of the hardware of the safety-related system. (IEC 61508-2)*

- *Requirements for system behaviour on detection of a fault (IEC 61508-2)*

The other requirements of IEC 61508 are aimed at minimising the likelihood of systematic faults and are particularly applicable when programmable electronic technology is used. For low complexity, non-programmable technology, it is considered that no more than good engineering practice would be required to satisfy these requirements.

ANNEX C

IDENTIFICATION OF "USED SAFETY DEVICES"

AUTHORS: *Pablo Reina Peral*
Eduardo Conde Lázaro

LABORATORIO OFICIAL MADARIAGA
C/Alenza, 1 y 2. 28003 Madrid. SPAIN.

CONTENTS

5. INTRODUCTION

In Europe, the operating sites of industry where an explosive atmosphere is or may be present, are usually divided in zones according to the expected frequency and duration of the explosive atmosphere. Electrical equipment intended for use in such areas is designed with special measures to reduce the likelihood of ignition of the explosive atmosphere; the different types of protection of electrical equipment are covered by CENELEC standards (see references).

Such equipment sometimes relies on the correct operation or control of protecting devices, like motor protection devices, in order to maintain certain characteristics of the apparatus within acceptable limits. Other safety-related devices such as gas detectors may also be used within potentially explosive atmospheres and contribute to the overall level of safety.

The approval and certification of electrical apparatus for potentially explosive atmospheres, therefore, requires that, where such safety devices are used, an assessment be made of their suitability for the intended purpose.

2. OBJECTIVE

The SAFEC project has the overall objective to produce a harmonised system for subdivision of safety devices which are used in electrical equipment for use in potentially explosive atmospheres, together with a methodology for selecting the appropriate subdivision of safety device for any particular application.

Task 3, which is described in this report, is aimed at the identification of the safety devices currently used as control and protection devices for electrical apparatus intended for use in potentially explosive atmospheres. The safety devices should be identified and related, when it is possible, to the CENELEC standards which define them.

3. SCOPE

The scope of the SAFEC project is limited to:

a) electrical apparatus which comes under the requirements of the ATEX Directive, i.e. the focus is on what can be done by the manufacturer of the equipment which is for sale (rather than by the user).
b) electrical apparatus for use in flammable atmospheres for which safety devices are relevant. Examples of this are type “e” (increased safety) and type “p” (pressurisation). More types are defined in this report.
c) all types of safety devices. This includes those which are electrical, electronic or programmable electronic in nature. Some such devices may be relatively complex so that the type and consequence of failure may be indeterminate. Less complex safety devices are also included such as, for example, a switch which cuts off the power of

the flameproof equipment if it is opened, or thermal fuses (if provided by the manufacturer).

The project is then focused on safety, controlling and regulating devices. These are parts of equipment or protective systems, and have an autonomous safety function.

The ATEX Directive, in the annex II, clause 1.5 defines the requirements for the safety devices.

The directive 94/09/EC requires, that safety devices must function independently of any measurement or control devices required for operation. As far as possible, failure of a safety device must be detected sufficiently rapidly by appropriate technical means to ensure that there is only little likelihood that dangerous situations will occur.

For electrical circuits the fail-safe principal is to be applied in general.

Safety-related switching must in general directly actuate the relevant control devices without intermediate software command.

In the event of a safety device failure, equipment and/or protective systems shall, wherever possible, be secured.

Emergency stop controls of safety devices must, as far as possible, be fitted with restart lockouts. A new start command may take effect on normal operation only after the restart lockouts have been intentionally reset.

Where control and display units are used, they must be designed in accordance with ergonomic principals in order to achieve the highest possible level of operating safety with regard to the risk of explosion.

In so far as they relate to equipment used in explosive atmospheres, devices with a measuring function must be designed and constructed so that they can cope with foreseeable operating requirements and special conditions of use. Where necessary, it must be possible to check the reading accuracy and serviceability of devices with a measuring function. The design of devices with a measuring function must incorporate a safety factor which ensures, that the alarm threshold lies far enough outside the explosion and/or ignition limits of the atmosphere to be registered, taking into account, in particular, the operating conditions of the installation and possible aberrations in the measuring system.

If the design of software controlled equipment, protective systems and safety devices, special account must be taken of the risks arising from faults in the programme.

4. REVIEW OF CENELEC STANDARDS RELATING TO SAFETY DEVICES

In the different CENELEC standards, mentioned above to the different protection types, there are numerous references to safety devices, when the apparatus relies on the correct operation of such devices. This section includes a list of the references found throughout the standards (the review tries to be as complete as possible but it may not be exhaustive, and so, some references may not appear below).

Below, a review of the safety devices mentioned in each standard is described, relating each device to the clause of the text in which the reference has been found. The references found in text are not reproduced textually in the report. Most of the times, only a fragment of the standard clause has been extracted. When similar or equal safety devices are mentioned several times through a particular standard, the repeated references have been omitted.

Note: In the standards, sometimes, the level of safety achieved by measures that imply the use of safety devices, e.g. disconnectors or interlocking devices, can also be achieved by marking safety warnings such as "DO NOT OPEN WHEN ENERGIZED". At other times the marking of such safety warnings is obligatory, e.g. EN 50014 6.2. - "DO NOT OPEN WHEN AN EXPLOSIVE GAS ATMOSPHERE MAY BE PRESENT".

4.1 "EN 50014". GENERAL REQUIREMENTS

- **10. Interlocking devices.**

  Interlocking devices used to maintain a type of protection shall be so constructed that their effectiveness cannot readily be defeated by the use, for example, of a screwdriver or pliers.

- **15. Connection facilities for earthing or bonding conductors**
- **18. Switchgear:**

  - 18. 2 Disconnectors (which are not designed to be operated under the intended load) shall be *electrically or mechanically interlocked with a suitable load breaking device.*

  - 18.3 When the switchgear includes a disconnector, *an interlock* between it and the cover or door of the switchgear shall allow the cover or door to be opened only when the separation of the disconnector contacts is effective.

  - 18.5 For group I, *short-circuit and earth fault relays* of swithgear shall latch out after actuation.

  - 18.6 doors and covers giving access to interior of enclosures containing remotely operated circuits with switching contacts that can be made or broken by non

manual influences *shall be interlocked with a disconnector* which prevents access to the interior unless it has been operated to disconnect unprotected internal circuits.

- **19. Fuses**

  - *enclosures containing fuses shall be interlocked* for the insertion and removal of replaceable elements, etc..

- **20. Plugs and sockets**

  - 20.1 *shall be interlocked* so that they cannot be separated when the contacts are energized

  - 20.2 some kinds of plugs and sockets (see standard) shall not comply with the requirements of 20.1 if they comply with:

    - the plug and socket *breaks the rated current with delayed release* (*temporization relay*).

- **21. Luminaires**

  - 21.2 covers giving access to the lampholder shall be *interlocked* with a device *automatically disconnecting all poles* of the lampholder when the opening of the cover begins.

4.2.“EN 50015”. OIL INMERSION “o”

- **4.3.1**. Apparatus which is sealed shall be provided with a *pressure relief device*, that shall be set and sealed by the manufacturer of the liquid filled apparatus to operate at least at 1,1 times the pressure above the liquid level at the maximum permissible protective liquid level.

- **4.3.2** Apparatus which is not sealed shall be provided with a *breathing device* complete with a suitable drying agent, so that gas or vapour which may evolve from the liquid in normal service can readily escape.

- **4.4** Means shall be provided to guard against accidental loosening of external and internal fasteners, as well as of *devices to indicate the liquid level*, plugs and other parts for filling or draining the liquid.

- **4.5** A protective *liquid level indicating device* shall be provided, ...

- **4.9** *Devices for draining the liquid* shall be provided with an effective sealing device, and shall be secured by fasteners that are shrouded or secured against unauthorised removal.

- **4.11** Non sealed enclosures shall be provided with an oil expansion facility and be equipped with a *manually only resettable protective device which causes interruption of the supply current* if there is an internal fault in the liquid-filled enclosure such as would create evolution of gas from the protective liquid.

4.3."EN 50016". PRESSURIZED APPARATUS "p"

- **3.3**. *a safety device* shall be fitted by the manufacturer *to limit the maximum internal overpressure* to a level below that which could adversely affect the type of protection

- **3.6.1** For group I *interlocking devices* shall be provided, for cases of static pressurization, *disconnecting the power supply* when the doors and covers are opened,…

- **3.6.2** For group II, similar to 3.6.1

- **4.2** If during normal service the temperature of any internal surfaces exceeds the maximum value permitted in EN 50014, appropriate means shall be taken to ensure that, if pressurization ceases, any explosive atmosphere that may exist cannot reach the heated surface before they have cooled below the permitted maximum value, …, *e.g. by bringing an auxiliary ventilation system into operation*, etc..

- **5 Safety provisions and devices**

- **5.6** *Safety devices such as time-delay relays and devices for monitoring the flow of protective gas*, shall be provided to ensure that pressurised electrical apparatus cannot be energized until it has been purged by a quantity of protective gas,…

- **5.7** where the protection gas is air, the flammable gas concentration after purging shall not exceed 25% of the LEL (it could be monitored with a *gas analyzer*).

- **5.7** where the protection gas is other than air, oxygen concentration after purging shall not exceed 2% by volume (an *oxygen analyzer* could be used).

- **5.7** The *purging flow rate shall be monitored* at the outlet of the pressurized enclosure

- **5.8** *One or more automatic safety devices* shall be provided to *operate when the overpressure falls below the minimum value specified by the manufacturer*. Also when given by the manufacturer, *safety devices shall be* provided to operate when the protective gas flow rate falls below the prescribed value. (The purpose for which

the safety device is used, e.g. to disconnect power or to sound *an alarm*, or other means to ensure safety, is the responsibility of the user).

- **6. Safety provisions and devices for static overpressure**

- **6.2** The protection gas shall be inert. The oxygen concentration after filling shall be less than 1%. (*Oxygen analyzers*).

- **6.5** *Two automatic safety devices* shall be provided to operate *when the overpressure falls below the prescribed value*

- **7.** *Supply of protective gas*

- **10.2** Containment systems with limited release. The flow shall be limited by flow limiting devices, fitted outside the pressurized enclosure. *The flow limiting device* may be or not a part of the material.

- **12. Note**. The use of *flame arrestors* could be necessary to avoid an ignition source within the containment system back into the plant

- **13 Hot internal surfaces**. If the pressurized enclosure contains any surface having a temperature which exceeds the ignition temperature of the flammable substance released from the containment system, the sample flow into the containment system shall be cut off automatically following the operation of the *safety devices* specified in 5.8

- **ANEX A. A.1** When the gas protection inlets in the supply ducts are placed in classified zones, the following precautions shall be taken:

    - *two independent firedamp detectors*, independently, shall be fitted at the discharge side of the fan or compressor, each *arranged to disconnect automatically the electricity supply* if firedamp concentration is higher than 10% of the LIE

- **ANEX A. A.2** Ducts for exhausting the protection gas should preferably have their outlets in a non-hazardous area, etc… Otherwise consideration should be given to the *fitting of barriers* (to guard against the ejection of ignition capable sparks or incandescent particles).

4.4.“EN 50017”. POWDER FILLING “q”

- **10**. Each powder filled electrical apparatus, part of electrical apparatus Ex shall be *protected against fault conditions such as short-circuit or thermal overload* so that the permissible limit temperature is not exceeded, etc…

- **11.2** *Temperature limitation shall be achieved by an internal or external, electrical or thermal, protective device*. The device shall not be self-resetting.

- **11.2** when *fuses are used as protective devices*, the fusing shall be of the enclosed type in glass or ceramic

- **11.3** Power supply prospective short circuit current. If a *current limiting device* is necessary to limit the prospective current to a value not greater than the rated breaking capacity of the fuse, this device shall be a resistor according to 11.1…

- **14.** Associated power supply with limited ratings

4.5."EN 50018". FLAMEPROOF ENCLOSURES "d"

- **12.6** However if the above-mentioned materials (insulating materials subjected to electrical stresses capable of causing arcs in air such as circuit-breakers, contactors, isolators, etc...) do not pass this test (see standard) they may be used if…, or if a *suitable detection device enables the power supply to the enclosure to be disconnected, on the supply side, before possible decomposition of the insulating materials leads to dangerous conditions*. The presence and effectiveness of such a device shall be verified by the testing station.

- **17.2.1 Switchgear.** *Quick acting doors or covers shall be mechanically interlocked with an isolator* so that the isolator can only be closed when the doors or covers ensure the properties of the flameproof enclosure.

- **18.1 Lampholders and lampcaps.** Devices preventing lamps working loose, required in EN 50014, may be omitted for threaded lampholders *provided by a quick-acting switch in a flameproof enclosure, which breaks all poles of the lamp circuit before contact separation.*

4.6."EN 50019". INCREASED SAFETY "e"

- **4.7.4** the windings will be protected with *appropriate devices* ensuring that the maximum temperature is not exceeded. These devices can be installed in the winding or externally.

- **5.1.4.3** protection against non permitted overheating with *current dependent safety devices*.

- **5.1.4.4** *protection against overloads* (e.g. motor stalled) *with temperature sensors* in the windings

- **5.1.4.5** motors fed from a variable *frequency and voltage converter*, shall be tested together with the specified converter, and with the *protecting device* incorporated.

- **5.3** lampholders and lampcaps with its own power supply

    - the commutation devices, producing sparks in normal operation, including relays like the "reed" type producing sparks in hermetic enclosures, *shall be electrically or mechanically interlocked in order to avoid the separation of contacts in a hazardous zone*.

- **5.4 Measuring transformers and instruments**. Ammeters circuits fed by *a current transformer*.

- **5.6.2.3** Batteries. All the elements requiring the maintenance of the electrolyte level shall be provided with a *device indicating* that the *level* is within the permitted values. (or electrolyte flow if there is recirculation).

- **5.8.3** The resistance heating devices shall be constructed with *an electrical protecting device*, *limiting the heating effect due to abnormal earth fault and earth leakage currents*:

    - **f**or TT and TN systems a *residual current protective device* should be used.

    - for TI an *insulator monitoring device* should be used to disconnect the supply whenever the insulation resistance is not greater than 50 Σ/V of rated voltage.

- **5.8.8** The resistance heating device or unit shall be prevented from exceeding the limit temperature when energized. This shall be ensured by a *protective system* according to 5.8.9 consisting of one or more electrical protective devices which at a predetermined surface temperature, *isolate all energized parts of the resistance heating device or unit*.

- **5.8.9** The protection shall be achieved by

    - *sensing the temperature* of the resistance heating device

    - or by *sensing that temperature and other parameters (e.g. level, or flow*)

    - or by *measuring one or more parameters other than temperature*

4.7."EN 50020". INTRINSICAL SAFETY "i"

- **6.3.1** Separation between terminals for intrinsically safe circuits from non-intrinsically safe circuits, can be separated by insulating partitions or earthed metal partitions
- **6.4.13** Coils of relays connected to an intrinsically safe circuit...

- **6.5** Protection against the reversal of polarity. This may be achieved with a single diode
- **6.6** Earth conductors, connections and terminals. Sometimes the maintenance of this type of protection depends on these devices.
- **6.7** where fuses are used to protect other components, 1,7 In shall be assumed to flow continuosly
- **7.4.5** current limiting devices for batteries in associated apparatus
- **7.4.8** external contacts for charging batteries. To prevent short-circuit or the delivery of ignition-capable energy, blocking diodes or infallible resistors shall be placed in the charging circuits.
- **7.5.2** Shunt voltage limiters: diodes, diode connected transistors, thyristors, zener diodes
- **7.5.3** Series current limiters: blocking diodes
- **8.1.2** The input circuit of mains transformers intended for supplying intrinsically safe circuits shall be protected by fuses or by a suitable circuit breaker**.** Also an embedded thermal fuse or other thermal device shall be used for overheating protection.
- **8.3** Damping windings to minimize the effect of inductance
- **8.4** Current limiting resistors
- **8.5** Blocking capacitors
- **8.6.1** Safety shunts. Where diodes or shunt diodes are used as shunt components in an infallible shunt safety assembly they shall form at least two parallel paths of diodes.
- **8.6.2** Safety shunts
  - for limitation of discharge from energy storing devices such as inductors or piezoelectric devices
  - for limitation of voltage to energy storing devices such as capacitors
- **8.6.3** Galvanic separation components. Isolating elements other than transformer and relays shall be considered, e.g. optocouplers.
- **9** Diode safety barriers: shunt diodes or diode chains protected by fuses or resistors or a combination of these. The barriers are interface between intrinsically safe circuits and non-intrinsically safe circuits.

4.8.“EN 50028”. ENCAPSULATION “m”

- **4.4** *Temperature limitation*: this can be achieved by a *non self-resetting internal or external, electrical or thermal, protecting device*.

4.9.“EN 50284”. Special requirements for construction, test and marking of electrical apparatus of equipment group II, category 1 G

- **4.2.2** associated apparatus to category 1 equipment

- **4.2.3** where a fault of an internal component may lead to failure of the encapsulation system due to increasing temperature, protection shall be ensured by the use of *a duplicated, non self-resetting thermal protection devices, positioned as necessary throughout the circuit.*

- **4.2.3** where protection is dependent on application of correct voltage to the connections to the apparatus, all connections shall be to *other apparatus or associated apparatus having control over voltage and current limitation equivalent of that of a category "ib" circuit according to EN 50020, though not necessary at the same levels of voltage, current or power*.

- **4.2.5** apparatus, which is mounted across the boundary wall to the hazardous area requiring category 1 equipment and contain electrical circuits not intrinsically safe category "ia", shall comply at least with one of the standardised types of protection. Additionally, they shall contain *a mechanical separation element* inside the apparatus to seal off the electrical circuits of the apparatus from the explosive atmosphere. In the case, the type of protection fails, the separation element shall also prevent flame propagation through the apparatus into the hazardous area of the application.

  Separation elements consist of a partition wall, possibly combined with a flameproof joint or an air gap with natural ventilation.

  Note: The requirements and performance of the separation wall, the flameproof joint and the air gap with natural ventilation are described in the standard.

- **4.5** Apparatus according to 4.2.5 (see above) mounted across the boundary wall of a hazardous area requiring category 1, shall avoid ignition caused by the apparatus of the atmosphere external to that requiring category 1 equipment. Hence *the mechanical connection to the boundary shall be flameproof* in such a way that in the case of an atmospheric propagation from outside into the hazardous area requiring category 1 equipment is excluded.

4.10."EN 50281-1-2". Electrical apparatus for use in the presence of combustible dust. Part 1-2: Electrical apparatus protected by enclosures. Selection, installation and maintenance

7. The special requirements for Zone 20 can be met *by a system power limitation*, with or without inherent temperature control, which shall be investigated under simulated working conditions.

4.11."EN 50281-1-1". Electrical apparatus for use in the presence of combustible dust. Part 1-1: Electrical apparatus protected by enclosures. Construction and testing

4.1.2. (Cat 1&2) Enclosures which can be opened more quickly than the time necessary, to allow incorporated capacitors to discharge to a value of residual energy of ....
4.3. (Cat 1&2) *Fasteners*: parts necessary to achieve a specified degree of dust ingress protection...
4.4. (Cat 1&2) *Interlocking devices* used to maintain a specified degree of dust protection...
4.8. (Cat 1&2) Connection facilities for earthing and bonding conductors
5.2. Switchgear (cat 2)
- **5.2.2**. Disconnectors (which are not designed to be operated under the intended load) shall be electrically or mechanically *interlocked with a suitable load breaking device*, or...
- **5.2.3.** *Any interlock* between such disconnector and the cover or door of the switchgear shall allow this cover or door to be opened only when the separation of the disconnector contacts is effective.
- **5.2.4.** doors and covers giving access to interior of enclosures containing remotely operated circuits with switching contacts that can be made or broken by non manual influences *shall be interlocked with a disconnector* which prevents access to the interior unless it has been operated to disconnect unprotected internal circuits.

5.3. Fuses (cat 2)
- *enclosures containing fuses shall be interlocked* for the insertion and removal of replaceable elements, etc..

5.4. Plugs and sockets (cat 2)
- **5.4.1** *shall be interlocked* so that they cannot be separated when the contacts are energized
- **5.4.2** some kinds of plugs and sockets (see standard) shall not comply with the requirements of 5.4.1 if they comply with:
- the plug and socket *breaks the rated current with delayed release* (*temporization relay*).

5.5. Luminaires (cat 2)
- **5.5.2** covers giving access to the lampholder shall be *interlocked* with a device *automatically disconnecting all poles* of the lampholder when the opening of the cover begins.

6.3. (Cat 3) *Fasteners*: parts necessary to achieve a specified degree of dust ingress protection...
6.4. (Cat 3) *Interlocking devices* used to maintain a specified degree of dust protection...
6.8. (Cat 3) Connection facilities for earthing and bonding conductors
7.2. Switchgear (cat 3)
- **7.2.2.** Disconnectors (which are not designed to be operated under the intended load) shall be electrically or mechanically *interlocked with a suitable load breaking device*, or...
- **7.2.3.** *Any interlock* between such disconnector and the cover or door of the switchgear shall allow this cover or door to be opened only when the separation of the disconnector contacts is effective.

7.3. Fuses (cat 3)

- *enclosures containing fuses shall be interlocked* for the insertion and removal of replaceable elements, etc..

7.4. Plugs and sockets (cat 3)

- **7.4.1** *shall be interlocked* so that they cannot be separated when the contacts are energized
- **7.4.2** some kinds of plugs and sockets (see standard) shall not comply with the requirements of 7.4.1 if they comply with:
- the plug and socket *breaks the rated current with delayed release* (*temporisation relay*).

7.5. Luminaries (cat 3)

- **7.5.2** covers giving access to the lampholder shall be *interlocked* with a device *automatically disconnecting all poles* of the lampholder when the opening of the cover begins.

4.12."EN 50177". Automatic electrostatic spraying installations for flammable coating powder

5.1.2.2. Provisions shall be made *for a device which automatically switches off the high voltage*, when the electrical supply current rises to a non-admissible level, discharges the spraying system and interrupts any further supply of spraying material.

5.1.3.2 Any parts under high voltage shall be discharged within 2 seconds to a discharge energy not exceeding 350 mJ before gaining access *(voltage discharges).*

5.2.1 ... *An exhaust ventilation system* shall be provided so that the average concentration of powder in air is not exceeding 50% of the LEL....

5.2.2 ... The exhaust ventilation system shall be *interlocked with other equipment* so that neither the high voltage supply can be switched on nor spraying material be fed as long as the exhaust system does not properly operate. *Devices shall be installed to monitor* the actual flow of the exhaust ventilation system air *and arranged to interrupt* immediately the high voltage supply if the volumetric flow falls ...

5.2.4. Where necessary to prevent danger in the case of an enclosed spray cabin it shall be equipped *with either explosion suppression or explosion relief venting* to discharge to an area where it will not be dangerous to personnel or other means offering equivalent safety.

5.2.6. For systems of type C, any access to the spraying area intended for use by personnel shall be *interlocked so that the high voltage supply system will be switched off* in the event of any access being opened

5.2.10. For spraying devices of type B and C and powder collection units shall be fitted with *automatic local fire extinguishing systems*.... As soon as it starts operating, the high voltage supply system and the coating powder feed shall be *switched off by automatic means.*

5.3.1. *Interlocking shall be provided to prevent the high voltage being applied* in types of system in accordance with 5.1.3 (type C) causing dangerous situations for personnel.

5.5. ***Earthing measures***

4.13"EN 50176" Automatic electrostatic spraying installations for flammable liquid spraying material

5.1.2.2 Similar to the device mentioned in 5.1.2.2. of EN 50177
5.1.3.2 Similar to the device mentioned in 5.1.3.2. of EN 50177
5.2.1 Similar to the device mentioned in 5.2.1. of EN 50177
5.2.2 Similar to the device mentioned in 5.2.2. of EN 50177
5.2.8. Similar to the device mentioned in 5.2.10 of EN 50177
5.3.1 Similar to the device mentioned in 5.3.1. of EN 50177
5.5. Similar to the device mentioned in 5.5. of EN 50177

4.14 "EN 50053-1" Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic paint spray guns with an energy limit of 0,24 mJ and their associated apparatus

5.3.1 ... *An exhaust ventilation system* shall be provided so that the average concentration of flammable vapour or mist is below 25% of the LEL....
5.3.2 *the exhaust ventilation system shall be interlocked* with the electrostatic spraying equipment, so that electrostatic spraying cannot be carried out unless the exhaust ventilation is in operation.
5.4.5 ***earthing and bonding***
6.1.1 Before starting to clean the gun or carrying out any other work in the spraying area *the high voltage supply shall be switched off in such a manner that it cannot be re-energised* by operating the trigger of the spray gun.

4.15 "EN 50053-2" Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic powder spray guns with an energy limit of 5 mJ and their associated apparatus

5.3.1. Similar to the device mentioned in 5.3.1. of EN 50053-1, but for a LEL of 50% (see standard).
5.3.2. Similar to the device mentioned in 5.3.2. of EN 50053-1
5.3.3. The powder collection unit should for example be fitted with *an explosion suppression system, an explosion relief, explosion barriers, or other explosion protection systems*, designed to reduce the effects of an explosion to a safe level.
5.5. Earthing and bonding
6.1.1 Similar to the device mentioned in 6.1.1 of EN 50053-1

4.15 "EN 50053-3" Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic flock spray guns with an energy limit of 0,24 mJ or 5 mJ and their associated apparatus

5.3.1 The average concentration of flock in air shall be maintained always below 50% of the LEL, if necessary by a *ventilation system*...

When spraying is carried out in association with adhesives, then *an exhaust ventilation system* to ensure concentration of flammable gases below 25% of the LEL is required.

5.3.2. Similar to the device mentioned in 5.3.2. of EN 50053-1
5.3.3. Similar to the device mentioned in 5.3.3. of EN 50053-2
5.5. Earthing and bonding
6.1. Similar to the device mentioned in 6.1.1. of EN 50053-1

4.16 "EN 50021" Electrical apparatus for potentially explosive atmospheres – Type of protection "n"

10.9.2.1 Motors intended to be *supplied at varying frequency and voltage by a converter* shall be tested for this duty as a unit in association with the converter...
Motors intended to be connected *to a supply other than that derived from a converter*, but which is non-sinusoidal, shall be tested ...
Generators intended to be connected to a *non sinusoidal load (e.g. thyristors)* shall be tested...

11. ***Fuses and fuse assemblies***

12.1 Luminaries. Lamps with *internal ignitors* can cause uncontrolled voltages that can damage ballasts or electronic ignitors...
12.2.5.2 Auxiliaries for luminaries. ***Glow type starters***
12.2.5.3 Auxiliaries for luminaries. ***Electronic starters and ignitors***
12.2.5.5 Auxiliaries for luminaries. ***Ballasts (electronic ballasts)***
15.1 Plugs and sockets for external connections: they shall *be interlocked mechanically or electrically* or otherwise designed so that they cannot be separated when the contacts are energised and the contacts cannot be energised with plug and socket separated.
16.3.2 ***Chargers for type 1 cells and batteries.***
16.4.2 ***Chargers for type 2 cells and batteries***
21.2 Associated energy-limited apparatus. The apparatus shall contain ***a reliable means of limiting the voltage and current available to energy storing components or at any normally sparking contact, e.g. by the use of zener diodes and series resistors....***
21.7 ***Protection against polarity reversal*** for energy limited apparatus, for example with *a single diode*
21.8.2 *Fuses* to protect other components and to limit the current flowing in energy-limited circuits

21.8.3 ***Shunt safety components*** such as ***diodes or voltage limiting devices...***

4.17 "EN 60079-14" Electrical apparatus for explosive gas atmospheres. Part 14: Electrical installations in hazardous areas (other than mines)

6.2.3 Type IT system

- Insulation monitoring device, indicate the first earth fault.
- Safety isolating transformers for SELV and PELV.

7 Electrical protection

For rotating electrical machinery
- Overload protective device
- Time lag protective monitoring all three phases
- Device for direct temperature control
- Warning device as an alternative to automatic disconnection

8.1 Emergency switch-off

- Emergency switch off electrical device

11.2.1 Overload protection

- Inverse-time delay overload protective devices

11.4 Resistance heating device

- residual current device (RCD), limit the heating effect due to abnormal earth-fault and earth-leakage currents

12.3 Installation for zone 0

- Surge protection device

13.1 Ducting

- Device to guard against the ejection of ignition-capable sparks or particles (spark and particle barriers)

4.18 "EN 1127-1" Explosion prevention and protection
Part 1: Basic Concepts and methodology.

6.2.2.2 Gas warning devices

6.2.2.2 Flow-control devices

6.4.8 Lightning protection
6.5.3 Explosion pressure relieve devices

6.5.4 Explosion suppression

- Explosion suppression systems.

6.5.5.2.1 Deflagration arrester
6.5.5.2.2 Flame arrester
6.5.5.2.3 Detonation arrester
6.5.5.2.4 Flashback preventer

Flow control valves

6.5.5.2.5 Extinguishing barrier

6.5.5.3.2 Rapid-action valves
6.5.5.3.3 Rotary valves
6.5.5.3.5 Double valves with its controls

4.19 "EN 50054" Electrical apparatus for the detection and measurement of combustible gases. General requirements and test methods

- Externally adjustable means of setting either one or more alarm set points.

5. SUMMARY OF GENERIC SAFETY DEVICES

In this section a summary of safety devices is described. The devices have been taken from different sources: CENELEC standards, draft proposal "Reliability of safety related devices" from TC31-WG09, LOM database, catalogues of equipment from different manufacturers, etc. Each item includes an indication whether the safety devices are already specified in existing CENELEC standards or whether the safety device would need to be handled by the standard that is being developed by CENELEC TC31/WG9:

- ➔ Motor protection; specially for type ‘e’: thermal and current relays, PT100, switches. (existing CENELEC standards)

- ➔ Overload monitoring devices for ‘e’ motors, which models the temperature-time characteristic. (existing CENELEC standards)

- ➔ Thermal protection devices and electronic control units for heating systems. (existing CENELEC standards)

- ➔ Overvoltage protection. (existing CENELEC standards)

- ➔ Monitoring units for concentration of flammable gases, oxygen or inert gas levels, e.g. gas detectors, limit detectors for end of line. (existing CENELEC standards)

- ➔ Systems for transmission and data acquisition (SCADA) for safety purposes, e.g. mining power shut-off in Group 1. (existing national standards and code of practice).

- ➔ PLC (programmable logic control) units, including the application software, for safety purposes. (to be covered by WG9 standard)

- ➔ Level indicators and switches for liquids used to provide safety for submersible equipment. (to be covered by WG9 standard)

- ➔ Protection relays for no load operation of submersible pumps e.g. monitoring of the power factor (cos φ) during normal operation. (to be covered by WG9 standard)

- ➔ Adjustable protection elements of AC converters for ‘p’, ‘e’, ‘d’. ‘n’ type motors (current limitation, overload protection, thermal limitation, etc...). (to be covered by WG9 standard)

- ➔ Devices controlling flow, temperature and/or level of cooling (liquid or gas) for ‘d’, ‘p’ and ‘e’ motors. (to be covered by WG9 standard)

- ➔ Control devices for bearings in big rotating machines. Lubrication and temperature control devices. (to be covered by WG9 standard)

- ➔ Pressure monitoring systems for ‘p’ type. Air and/or protective gas supply for the same type of protection; including e.g. detectors, auxiliary ventilation systems, if required. (to be covered by WG9 standard)

- ➔ In belt transportation systems, devices for controlling the alignment and slip of the belt. (to be covered by WG9 standard)

- ➔ For bucket elevators anti-runback devices and belt speed meters to detect belt slip. Also control of bearings. Detectors of feed rate to avoid overloads. (to be covered by WG9 standard)

➔ Interlocking devices, may be electrical switchgear or mechanical devices used for safety purposes.

Annex 3 includes useful information about currently used safety collected from commercial catalogues that can be found in the market.

6. CONCLUSIONS

- A review of available information of devices currently used in explosive atmospheres and the standards applicable to them has been carried out, with the objective of establishing a guide list of the safety devices that should be studied or considered within the SAFEC project.

Anyhow, the list is neither definitive nor exhaustive, and so, other devices from different sources, different considerations of the standards or different conceptions of use of the device may lead to changes in the review.

- In some cses it may be difficult to differentiate components and safety devices. This has to be carefully considered, because otherwise a large number of components could be considered as safety devices (for example safety barriers separating intrinsically from non intrinsically circuits).

- The same device can have different safety or protecting levels depending on the particular situation in which it is applied (for example, a thermocouple the signal of which can be used just for monitoring temperature or to activate a disconnecting switch).

7. REFERENCES

1. EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements.

2. EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion.

3. EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p".

4. EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling "q".

5. EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure "d".

6. EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety "e".

7. EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety "i".

8. EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation “m” [8].

9. EN 50284 Special requirements for construction, test and marking of electrical apparatus of equipment group II, category 1 G

10. EN 50281-1-2 Electrical apparatus for use in the presence of combustible dust. Part 1-2: Electrical apparatus protected by enclosures. Selection, installation and maintenance

11. EN 50281-1-1 Electrical apparatus for use in the presence of combustible dust. Part 1-1: Electrical apparatus protected by enclosures. Construction and testing

12. EN 50177 Automatic electrostatic spraying installations for flammable coating powder

13. EN 50176 Automatic electrostatic spraying installations for flammable liquid spraying material

14. EN 50053-1 Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic paint spray guns with an energy limit of 0,24 mJ and their associated apparatus

15. EN 50053-2 Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic powder spray guns with an energy limit of 5 mJ and their associated apparatus

16. EN 50053-3 Requirements for the selection, installation and use of electrostatic spraying equipment for flammable materials. Part 1. Hand-held electrostatic flock spray guns with an energy limit of 0,24 mJ or 5 mJ and their associated apparatus

17. EN 50021 Electrical apparatus for potentially explosive atmospheres – Type of protection “n”

18. EN 60079-14 Electrical apparatus for explosive gas atmospheres.
    Part 14: Electrical installations in hazardous areas (other than mines)

19. EN 50054 Electrical apparatus for the detection and measurement of combustible gases. General requirements and test methods

20. ATEX Directive.

21. EN 1127-1 Explosive atmospheres - Explosion prevention and protection. Part 1: Basic concepts and methodology

22. ATEX Directive.

23. IEC 61508 Functional safety of electrical, electronic and programmable electronic safety-related systems

24. Directive 1999/92/EC of the European Parliament and of the Council of 16 December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (15th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)

25. CENELEC TC3 I/WG09, Draft proposal for a European Standard, "Electrical Equipment of Potentially Explosive Atmospheres - Reliability of safety-related devices", 12.02.99.

26. “Determination of safety categories of electrical devices used in potentially explosive atmospheres”. Technical annex. Annex 1 of SAFEC Project.

27. Guide to Dust Explosion Prevention and Protection. Part 2-Ignition, prevention, containment, inerting, suppression and isolation. C. Schofield and J.A. Abbott. The Institution of Chemical Engineers. (1988 Edition).

28. Laboratorio Oficial Madariaga internal database of Ex electrical equipment.

29. Commercial catalogues of equipment used in potentially explosive atmosphere

ANNEX 3

EXAMPLES

TABLES OF CURRENTLY USED SAFETY DEVICES FOR EXPLOSIVE ATMOSPHERES

Device	Description
ction circuit breakers	They are suitable both for use with explosion-protected motors (types EEx d and EEx e) and also for system protection. The circuit breaker is equipped with a fixed setting, fast short-circuit trip and thermal over current trip.
tor starters	Motor protection switches are used for direct-on-line starting and overload protection of motors. They are fitted with an adjustable thermal over current release and an electro-magnetic fast-acting short circuit release. They are suitable and approved for the protection of Ex e and Ex d motor
rupters / motor switches	Load and motor switch
bases	
rcuit breaker (m.c.b.)	The miniature circuit breakers are current limiting circuit breakers and have non-adjustable thermal and electromagnetic trips.
ge circuit breaker	It has an earth fault current detector.
ction relays	
motor protection	It is used for monitoring the temperature of electrical machines and other apparatus
ter units	They transmit binary signals from intrinsically safe control circuits to non intrinsically safe signal circuits
arrester-over voltage	Due to its non-linear resistance it gives a low residual voltage, even with heavy current surges
s	Enclosures integrating various functions, e.g. Diodes, resistors, small fuses and small relays.
ers	Different starters assemblies optionally provided with line fuses, main isolators, and control circuit fuses.

Device	Description
distribution panels with es	Fuses and m.c.b. distribution panels. Panels completely wired to terminals. It has a main switch, main fuses, m.c.b., contactors, thermal relays
e controller and limiter tor	Capillary tube thermostats are suitable for monitoring and controlling temperatures of solids, liquids or gases. It has mechanical or electrical interlock
rotected control panels zed type of protection	This control is used to maintain a positive pressure into the enclosures
nit for installations of ection pressurized Ex p	This device controls the flow of inert gas into the enclosure. The air supply unit consists of a pressure regulator with attached manometer, a solenoid valve, and a fine control valve.
for installations using apparatus-protection	This unit provides the pressure control unit differential pressure with switch intrinsically safe power supply to the control switch and the pressure control switch; receive and process the switch signals from the differential pressures switches; control of the purging phase timing; actuation of the air-supply unit solenoid valve;....
nit for installations of ressurized apparatus	This protection is crucial during the purge phase. The inert gas flow must be monitored during this operation.
k, heater plate	For anti-condensation heating of enclosures
ly unit	The power supply unit serves as an I.S. isolator for data transfer between the terminal and an automation system and provides the power necessary to operate the terminal.
transmitters for Pt 100 hermometers	It converts the input measure value into a linearly-proportional standardized signal. The power supply and the input and output circuits are all galvanically isolated fron each other.
nsmiters for les	The units are intended for operation as temperature transmitters for IEC and DIN thermocouples
itters	Temperature transmitter

Device	Description
ters for standardized signals	The apparatus serves as an intermediate unit for the transmission of pneumatic measurement signals from a sensor, to an electrical instrumentation/process control system
ters for standardized	This transmitter is intended for the conversion of a standardized electrical signal to a standardized pneumatic signal
oximity switches	It can control relays or contactor. It can be used to open the voltage source if we are opening an enclosure.
or binary signal	In telemetering and control circuits using binary signals, relays can be used for the transmission of the information and instruction.
detector for d signals	It is used for the purpose of signalling and indicating limiting values.
with contact-break	This element can be used for switching, controlling and regulating in Ex-areas, for example, for disconnecting voltage source when opening an enclosure.
witches	It could be used in valves, thermostats, push switches, servo components, level meters and switching gear.
or for valves	This modules is used in a situation involving pneumatic actuators for valves, and it needs the aid of limit switches.
ric proximity swicth / oto-electric proximity	It could be used in environments that preclude the use of conventional sensors. It could be used as switching operation or transmit information
nitor DC	This module operating voltage for over or undervoltage. In both cases the built-in relay de-energizes.
esistor	For monitoring switching contacts, open circuit monitoring
ng diode	Suppressors for electrical and electronic control systems, for the prevention of overvoltage in inductive loads.
iode modules	Signal isolation in lamp testing

Device	Description
ge limiter	Measuring and control or data processing from transient voltage surges
t	This device acts as a suppressor on contacts, coils, solenoids and inductive circuits
y	It is suitable for switching load current circuits up to 12 A
er	IS circuits
	isolate IS-circuits and non-IS-circuits
power supply unit	It is used for supplying transmitters and the transmission of measured signals
or / repeater; Output olator	This module isolates intrinsically safe circuits from non intrinsically safe circuits at the same time that ensuring the electrical isolation of the analogue signal.
ce 4x4 ... 20 mA input	This module enables 4x4 .. 20mA analoge signals to be connected with a CAN bus
nterface 4x4 ... 20 mA	This module enables 4x4 .. 20mA analoge signals to be connected to the interbus-S bus
tector system	It is a safety system designed to give an alarm when a little leakage is collected inside the sump of a tank or a storing deposit.
egrity monitor	This device continuously monitors a bonding conductor and warns of any significance change in resistance or large current being conducted, for example monitoring of the safety earth in a barrier system
ystem	It is a system that can be used to transmit a large number of process signals between field units installed in a hazardous area and an automation system. Field devices such initiator contacts, resistance thermometer (Pt 100), thermocouples, transmitters, actuators and solenoid valves can be connected directly to its I/O units
e	Configuration, diagnosis and communication software for field bus system.
safe digital multiplexer	

Annex D

Study of ‘ Used Safety Devices’

Authors :

E. FAÉ - S. HALAMA

INERIS

CONTENTS

FIGURES

TABLES

1. SCOPE OF THE DOCUMENT– LIMITS OF THE STUDIES

1.1 SCOPE OF THE DOCUMENT

The SAFEC project (contract SMT4-CT98-2255) has the overall objective to produce a harmonised system for subdivision of safety devices which are used in potentially explosive atmospheres (see references [1] to [8]), together with a methodology for selecting the appropriate subdivision of safety device for any particular application (see reference [9]).

This report describes the work associated with Task 4 of the SAFEC project whose objective is to study used safety devices identified in task 3, and assess them with regard to their use in flammable atmospheres. This report will deal with the following aspects :

[1] Safety requirements of IEC 61508 standards.

[2] Risk analysis – hazardous event definition.

[3] Safety level assessment procedure.

[4] Application of safety integrity level assessment procedure.

[5] Conclusions.

1.2 LIMITS OF THE STUDY

The ATEX Directive covers the following :

[1] Equipment.

[2] Protective systems.

[3] Components.

[4] Safety, controlling or regulating devices.

It is the safety, controlling or regulating devices which are the concern of this project. These will be parts of equipment or protective systems but, unlike components, **they have an autonomous safety function.**

Only safety devices are studied. Studies that assess the explosion risk resulting from a failure of the safety device and from the presence of an explosive atmosphere are the subject of previous tasks 1 and 2.

2. SAFETY REQUIREMENTS OF IEC 61508 STANDARD

IEC 61508 standard (see reference [10]) consists of the following parts, under the general title " Functional safety of electrical/ electronic/programmable electronic safety-related systems " :

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PESs)) that are used to perform safety functions.

Systems intended to fulfil safety functions must meet the following main requirements, in order to be graded in accordance with the safety integrity levels of the IEC 61508 standard (see reference [10]). The main requirements are :

[1] System development cycle requirements around a safety life cycle and in terms of related documentation (part 1 and 2 of reference [10]).

[2] Qualitative and quantitative technical requirements in the presence of faults (parts 1 and 2 of reference [10]).

[3] Technical requirements in relation to software design and validation (part 3 of reference [10]).

Only the validation of the qualitative and quantitative technical requirements in the presence of faults, will be studied in the following for the types of devices identified below.

2.1 SAFETY SYSTEM GRADING - CLASSIFICATION

IEC 61508 requirements are graded according to 6 classes from " a, SIL 1 to SIL 4, b " in which " a " corresponds to " no specific safety requirements ".

These requirements are linked to defect behaviour qualitative requirements and quantitative requirements in terms of fault accumulation and probability of safety function loss.

Safety systems defined in the IEC 61508 standard are graded according to 2 safety related system types :

- Safety related control systems, systems ensuring a check of the monitored parameter (e.g. : motor or relay output) that may enter a dangerous state if the control system fails. **ONLY THESE SAFETY DEVICES ARE UNDER THE SCOPE OF THE SAFEC PROJECT**
- Safety related protection systems, systems designed to react when the checked element is subject to certain conditions, liable to be dangerous. These safety systems operate in order to reduce the risk or prevent hazardous events.

2.2 ARCHITECTURAL CONSTRAINTS ON HARDWARE SAFETY INTEGRITY

In the context of hardware safety integrity, the highest safety integrity level that can be claimed for a safety function is limited by the hardware fault tolerance and safe failure fraction of the subsystems that carry out that safety function. The following tables specify the highest safety integrity level that can be claimed for a safety function which uses a subsystem taking into account the hardware fault tolerance and safe failure fraction (see annex C of IEC 61508 standard, part 2).

The requirements of these tables shall be applied to each subsystem carrying out a safety function and hence every part of the E/E/PE safety related system. With respect to these requirements,

- a hardware fault tolerance of " N " means that " N+1 " faults could cause a loss of the safety function. In determining the hardware fault tolerance, no account shall be taken of other measures that may control the effects of faults such as diagnostics, and
- where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault.

A subsystem can be regarded as **type A** if, for the components required to achieve the safety function, the failure modes of all constituent components are well defined; the behaviour of the subsystem under fault conditions can be completely determined; there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

A subsystem shall be regarded as **type B,** if for the components required to achieve the safety function, the failure mode of at least one constituent component is not well defined; or the behaviour of the subsystem under fault conditions cannot be completely determined; or there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

The architectural constraints of either the following tables shall apply to each subsystem carrying out a safety function, so that the hardware fault tolerance requirements shall be achieved for the whole of the E/E/PE safety-related system.

Following tables will be applicable to E/E/PE safety-related systems comprising both type A and type B subsystems.

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Table 1 : Hardware safety integrity : architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Table 2 : Hardware safety integrity : architectural constraints on type B safety-related subsystems

2.3 Quantitative requirements of IEC 61508

Quantitative requirements of the IEC 61508 international standard are established in terms of probability for the safety system to no longer ensure the safety function for which it was designed.

The standard sets goals according to the safety system's operation :

- operation mode on request,
- continuous operation mode.

The " on request " operation refers to the use of safety systems for which the frequency of demands is lower than the periodic test frequency. The IEC 61508 standard's quantitative requirements are as follows :

Safety integrity level (SIL)	" On request " operation mode (dangerous failure probability per year)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 3 : Quantitative requirements of IEC 61508

2.4 COMMENTS ON IEC 61508 AND SIL LEVELS

In IEC 61508 part 1 chapter 7.6.2.10, it is written that *" an architecture that is comprised of only a single E/E/PE safety related system of safety integrity level 4 shall be permetted only if :*

There has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the safety integrity failure measure ;

Or, there has been extensive operating experience of the components used as part of the E/E/PE safety-related system (...), and the is sufficient harware failure data obtained for components used as part of the E/E/PE safety-related system (...).

In general, in process industries, when a safey integrity level of SIL 4 is required for a safety function, the risk reduction is provided by the three following devices :

- other technology safety-related systems **AND**
- E/E/PE safety-related system **AND**
- external risk reduction facilities.

When a risk reduction can be provided only with a E/E/PE safety-related system (also called Safety Instrumented System SIS), engineers decide to change the design because the risk level is too high.

In addition, the highest safety level claim for safety devices such as safety PLC according to IEC 61508 is SIL 3.

2.5 DIFFERENCES BETWEEN HARDWARE FAULT TOLERANCE OF IEC 61508 AND OF ATEX STANDARDS

The requirements of hardware fault tolerance of IEC 61508 are defined to their consequence regarding the loss of the safety function. The IEC 61508 requirements regarding fault tolerance and SIL calculations give some construction principles (see chapter 2.2 and 2.3). Those requirements are a measurement of the effectiveness of a safety-related device.

The requirements of hardware fault tolerance of ATEX standards are defined to their consequence regarding the explosion hazard. The ATEX standards requirements regarding fault tolerance are construction principles that have to be applied to the electrical apparatus in order to guarrante that the consequence of the failure will not be a spark or an over heating.

2.6 DIFFERENCES BETWEEN IEC 61508 SAFETY - RELIABILTY AND OF ATEX STANDARDS INFAILLIBLE COMPONENTS

According to EN 50020 and EN 50028 (see references [7] and [8]), if some construction principles are met (for example if the component is working lower than the 2/3 of its maximum characteristics, …), then the component is considered as infaillible.

According to IEC 61508, the safety-level of a safety-device is a part of the reliability of

this device (see Figure 2 : Failure distribution according to their effect). In reliability standards and databases (such as CNET (see reference [12]), MIL HDBK 217, …), used for the calculation of the Safety Integrity Level of E/E/PE safety-related system, the concept of infaillible component is not considered.

3. RISK ANALYSIS – HAZARDOUS EVENT DEFINITION

The following types of failures or faults must be considered to grade the safety systems or components with respect to ATEX and IEC 61508 standard requirements :

- Failures that are " without consequence " on the safety function and that may cause either the ignition or non-ignition of the explosive atmosphere. The ATEX standards cover these types of failures or faults.
- Failures whose consequence on the safety function is a " loss of safety function " and that can cause either the ignition or the non-ignition of the explosive atmosphere. The ATEX standards cover these types of failures or faults. In addition, in the event of safety function loss, the consequence is indirect and requires an external initiating action. Consequences may be :
    - Either an explosion in the event of contact between an explosive atmosphere and the system due to a failure of the safety device. As an example, one can mention the case of a temperature or pressure probe that would have failed to fulfil its function and whose failure prevents the safety function. Such a safety device could correspond to what the IEC 61508 standard refers to as the " safety related control systems ".
    - Or another consequence, or another hazard depending on the safety system's application and use. As an example, one can mention the case of a level detector (petrol or LPG (Liquid Petroleum Gas) storage tank filling) that may result in tank overflowing. Those type of safety device could correspond to what the IEC 61508 standard refers to as " safety related protection systems ". Those devices are not in the scope of this study.

Various failure cases and related consequences are presented below :

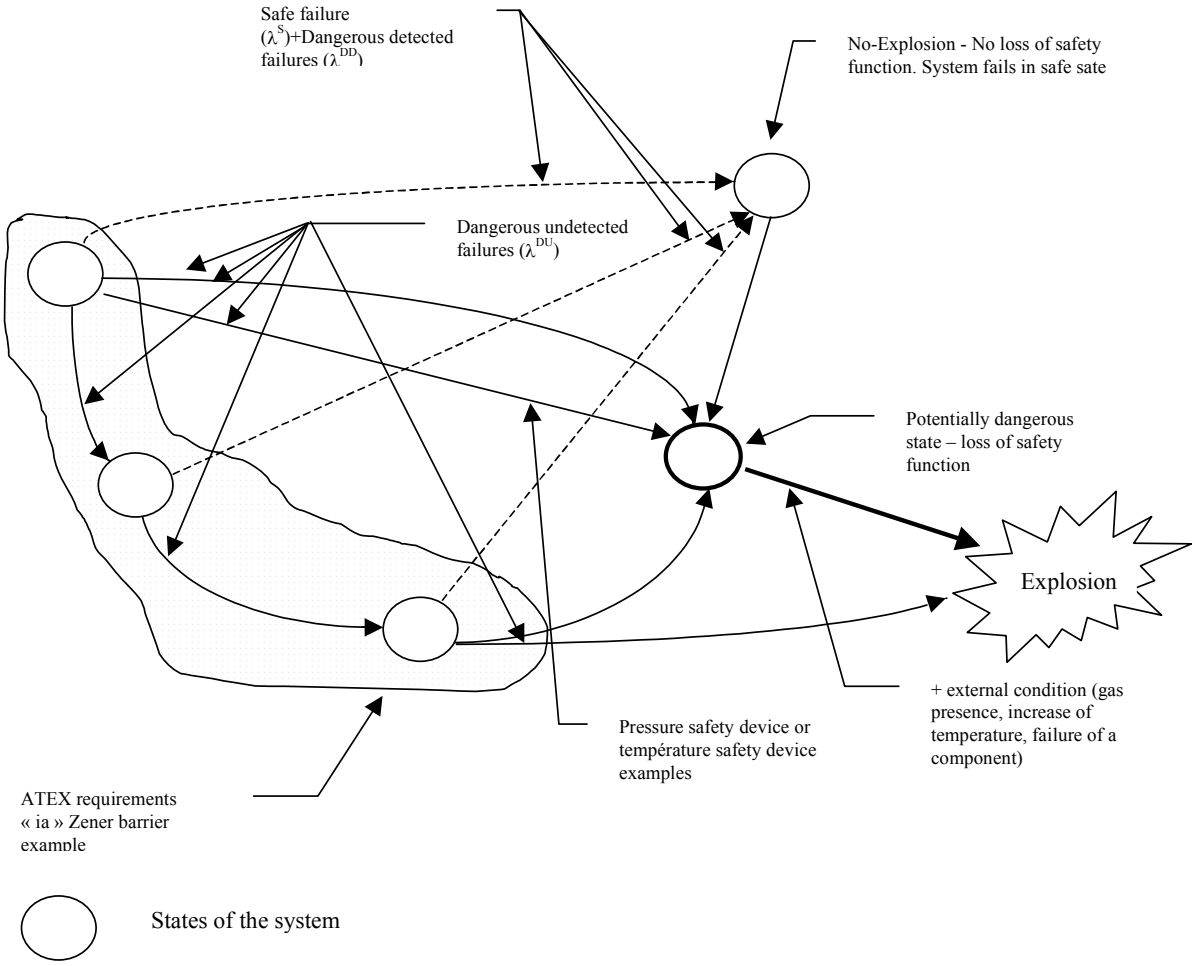


Figure 1 : Safety device failure effects

4. SAFETY LEVEL ASSESSEMENT PROCEDURE

The system's safety integrity level is assessed in accordance with the following procedure that breaks down the assessment into the five following stages with logical links :

- 1st stage : functional analysis,
- 2nd stage : failure rate prediction
- 3rd stage : failure modes, effects and criticality analysis,
- 4th stage : modelling of the system's various states,
- 5th stage : system safety integrity level assessment.

This procedure is defined in reference [11], which is confidential.

4.1 ASSUMPTIONS

This assessment does not take into account :

- common mode failures,
- systematic errors,
- connection failures,
- errors linked to cabling,
- human errors.

4.2 FIRST STAGE : FUNCTIONAL ANALYSIS

The purpose of the functional analysis is to identify the functions to be fulfilled by the system. It is also intended to explain the system's operation by establishing a link between the hardware and software functions. This stage is the assessment's input point. It is sufficiently accurate to identify failures with an impact on the system's safety.

Several functional analysis procedures may be used to explain the operation of automatic systems :

- functional block diagram procedure,
- SADT procedure,
- SA_RT procedure,
- etc.

4.3 SECOND STAGE : FAILURE RATE PREDICTION

4.3.1 Purpose

The purpose of the failure rate prediction is not to assess the system's reliability. Calculations are only conducted for the components with a risk in relation to safety, in order to quantify the dangerous failure rate. To that end, a calculation makes it possible to assess an equivalent failure rate of the system. This calculation comprises : component failure rates, component stress, climatic environment, component quality, etc.

The failure rate prediction allows us to quantify the FMECA (**F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis - See 3rd stage) and to identify the contribution of the various failure modes to the system's unsafe situation.

4.3.2 Calculation assumptions

Failure rate calculations are grounded on databases that supply a basic failure rate for each type of component. This basic failure rate is modulated according to corrective factors according to the environment and component.

The databases (for information) are :

- MIL HDBK 217 (Military Handbook);

- CNET,

- etc.

The database used by INERIS for the failure rate calculations is the CNET RDF 93 rev. 2/95 database (see reference [12]). Calculations are conducted with the RAM Commander version 6.1 software. The selected calculation assumptions are as follows :

- temperature or pressure measurement device environment : GM; + 40 °C (fixed on a track, motor, …),
- power supply shut off device environment : GF; + 40 °C,
- temperature or pressure measurement device component quality : “ non-CECC ” or equivalent; stress rate inferior or equal to 50%; CMS machine assembly,
- power supply shut off device component quality : “ CECC ” or equivalent; stress rate inferior or equal to 50%; assembly on card “ components to be punched ” manual assembly.

4.3.3 Experience of returns

There is experience of returns to the company manufacturing the low level detection system. These systems are mainly installed to detect petroleum product levels in tankers.

By comparing the number of devices returned to the manufacturer with the pool of installed devices and by assuming :

- a balanced distribution between detected failures and undetected failures,
- a reliability according to the constant failure rate exponential law.

We obtain a failure rate grounded on the returns experience " sixfold " lower than the predicted failure rate. This can be explained by :

- certain devices are probably being stored for availability reasons,
- failing devices are probably not systematically returned in the event of fault (guarantee period expired, …).

In the following safety integrity level calculations, the selected value is that of the predicted reliability.

In addition, this " sixfold " ratio between the predicted values and measured values is less than the order of magnitude range of failure rates within a safety integrity level as defined by the IEC 61508 standard.

4.4 THIRD STAGE : FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS (FMECA)

After identifying the components fulfilling the functions (hardware and software), identified by the functional analysis, the failure modes and their effects on the system's operation must be analysed in the scope of this study. Certain standards formalise this type of study (MIL STD 1629, …), others give values to distribute the components' failure modes (CNET, manufacturer data, …).

The purpose of this stage is to analyse the failures to identify " dangerous " failure modes, and to quantify the probability of failure occurrence.

The **F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis (FMECA) is conducted at electronic component detail level for the safety device. The purpose of this analysis is :

- to identify the " dangerous " failure modes to assess the " dangerous " failure rates leading to the hazardous event, while assessing a coverage rate for the various tests;
- to identify the possible preventive maintenance provisions to be integrated to guarantee a safety integrity level in compliance with the defined goals.

Failures are classified in 4 classes :

- dangerous detected failures whose effects are on safety and availability (λ^{DD}),
- dangerous un-detected failures whose effects are only on safety (λ^{DU}),
- non-dangerous detected failures whose effects are only on availability (λ^{SD}),
- non-dangerous and undetected failures whose effects are only on availability (λ^{SU}).

(λ^{DU} = λ **D**angerous, **U**ndetected ; λ^{S} = λ **S**afe).

λ^{S} = Safe failure : i.e. a failure that results in system fallback (safe situation for safety),

λ^{DU} = Unsafe failure : failure whose consequence leads to a dangerous state from the standpoint of safety.

The following diagram give further details of this notion of distribution of failures according to their effect.

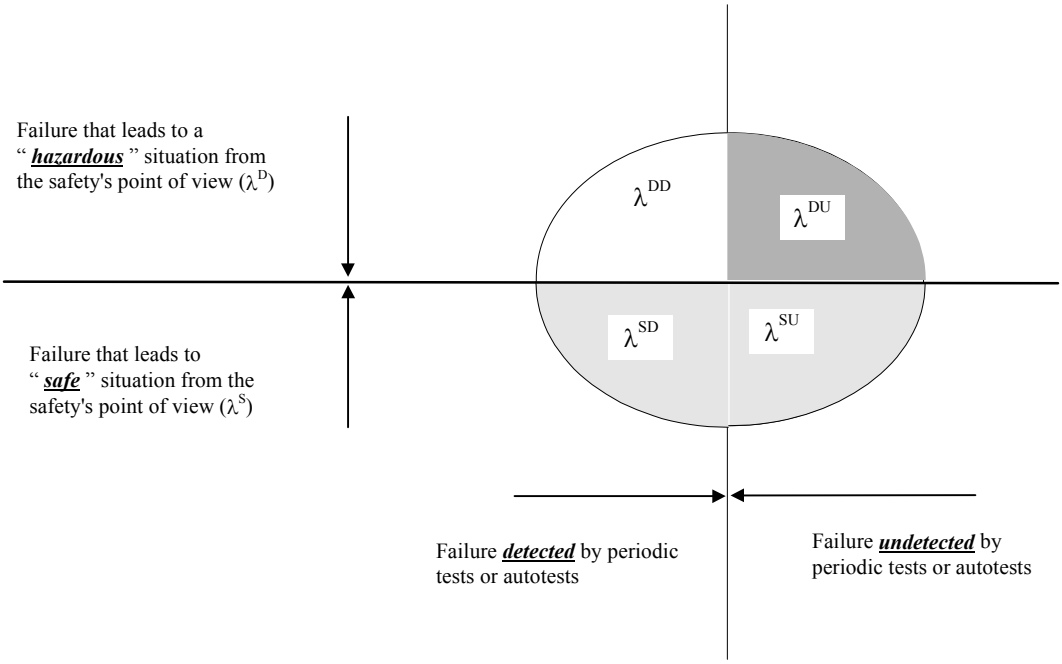


Figure 2 : Failure distribution according to their effect

References [12] and [13] state the failure mode distribution for various components.

4.5 FOURTH STAGE : MODELLING OF THE SYSTEM'S VARIOUS STATES

There are three system types according to the various encountered systems :

[1] Failsafe systems

[2] Non-redundant systems

[3] Redundant systems

The system's dangerous failure probability calculation is different according to the various types of system.

4.5.1 Failsafe systems

Failsafe systems are systems in which the failure modes of all components of the system lead to a " safe state " in relation to safety. For these systems, there is no use in calculating the dangerous failure probability as the λ^{DU} dangerous failure rate does not exist

4.5.2 Non-redundant systems

Non-redundant systems are " simple " systems in which the safety function can be lost in the event of failure. Two states are possible : safe state or dangerous state. The calculation of the dangerous failure probability for the systems comes down to a specific reliability calculation depending on the dangerous failure rate (λ^{DU} - identified in FMECA) and with the same duration as the preventive maintenance operations.

4.5.3 Redundant systems

In the event of redundant systems, the safety function can be lost due to combinations of failures depending on the logic implemented within the safety system. There are several safety integrity level quantitative assessment procedures for such systems. The main drawback of the more traditional procedures such as the analysis by fault tree system, or the analysis by reliability block diagram, is that they do not always take into account the time aspect, test periodicity, coverage levels, as well as the repair rate.

The various failure and operating states can be modelled with MARKOV graphs, by integrating the time aspect of the preventive maintenance tests, the autotests as well as the coverage rate, as the electronic systems are subject to a failure law of exponential form with a constant failure rate.

4.5.3.1 Influence of testability on safety

For safety purposes, the state of the resources must be known on a permanent basis to see if hidden (or dormant or latent) failures liable to mask the safety function exist. These dormant failures are only detected during periodic tests voluntarily conducted by the user.

A test policy is useless for failsafe systems as each failure leads to a " safe " position in relation to safety.

On the contrary, for systems that are neither failsafe nor autotestable and on which dangerous failures exist, a test policy to detect the " dangerous failures " (with a risk for safety) is required.

These tests must be conducted according to a periodicity grounded on the characteristics of the various elements constituting the system. Dangerous failures can be detected in two ways :

- Either by the test and autotests system of the safety system for detectable failures (λ^{DD}),
- Or during verification operations for non-detectable failures (λ^{DU}).

The PLC's reliability level is not increased by testability. It just makes it possible to ensure that resources are still available : to read the inputs and control the outputs, on the one hand, and to make sure that the processing modules are still functional, on the other hand. Only dangerous failure detection comes into play. It is possible to detect and switch to safe position in the event of failure, thanks to this test, and therefore to better guarantee safety. The following diagram shows the impact of testability on safety, and the impact of a state changeover test policy conducted every 24 hours or every 6 months on safety.

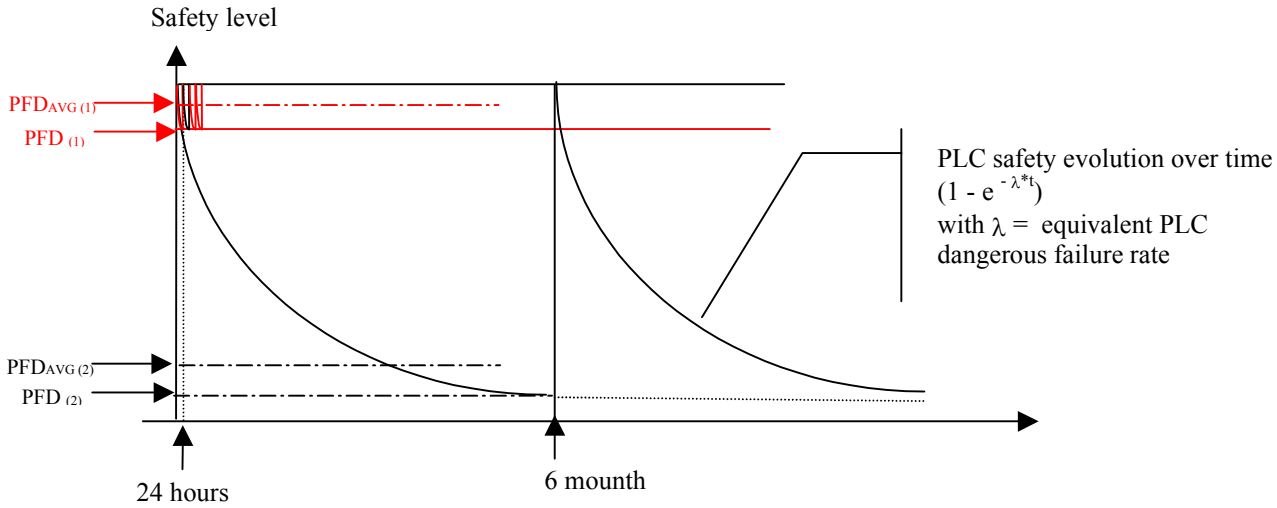


Figure 3 : Testability impact on safety

On this figure is shown that PFD is the probability of failure and PFD_{AVG} is the average probability of failure which is aproximately the half of PFD (see PFD $_{(1)}$) for safety systems with short period state changeover test, and the third of PFD (see PFD $_{(2)}$) for safety systems with long period state changeover test. This difference is due, for electronic systems, to a constant failure rate (λ) and to the reliability calculation with the exponential law.

4.5.3.2 Graph establishment

References [10] and [14] stipulate the procedure and various stages of system modelling. State graphs are represented below for each safety function. Modelling is achieved with " states " that the system is liable to enter. There are 3 states in most cases :

State 2 represented as follows  :

This state corresponds to the modelling of redundancy. In this state, all implemented resources are present and operate in a nominal manner.

State 1 represented as follows : 

This state corresponds to the modelling of redundancy downgraded by the dangerous failure of a hardware element on one of two channels. In this state, all implemented resources are not present. It is an undetected dangerous failure state. Safety is still guaranteed.

State 0 represented as follows  :

This state corresponds to the modelling of the loss of redundancy due to the dangerous failure of several hardware elements from the channels. In this state, safety is no longer guaranteed and in the event that the safety function is called upon, the system will not go to safe position.

The " P " probability of being in " 0 " state is designated by PFD(t) in the IEC 61508 standard. The meanning of PFD(t) value is the value defined in the previous paragraph.

4.5.3.3 Assumptions

MARKOV graph modelling for the studied systems by INERIS was grounded on the following assumptions :

[1] failure rates (λ) and repair rates (μ) are assumed constant to make it possible to model and calculate the safety level with MARKOV graphs.

[2] The mission time (TI) corresponds to the intervals between the OFF LINE periodic test times. All test rates concerning the aptitude to detect state changeovers (μ_{PTi}) are stated for each arc of each graph.

[3] Inputs and outputs do not go to the safe state if the power supply is cut off.

[4] The common failure modes, and the systematic errors are assumed equal to those defined in reference [14]. λ^D common mode failures or faults have the specificity of affecting all lines at the same time. The selected values are those defined in the same document.

4.5.4 System modelling example

Two active redundancy systems are modelled as follows

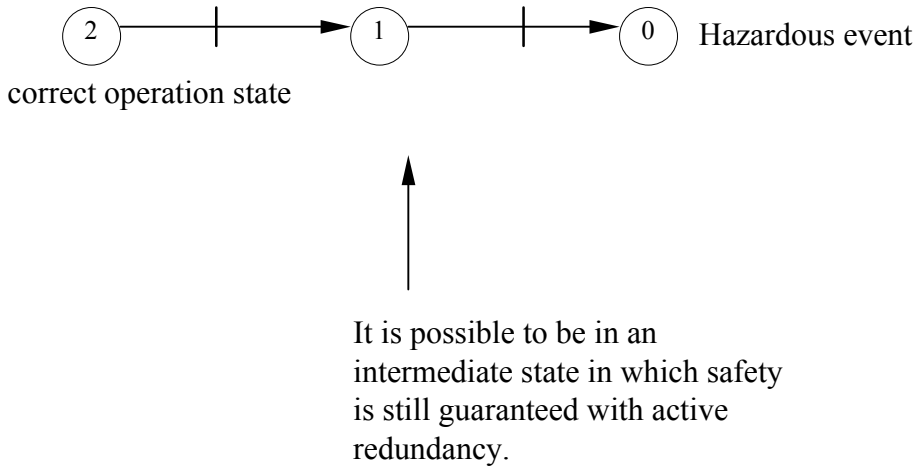


Figure 4 : Redundant system state modelling

This graph is equivalent to the following graph :

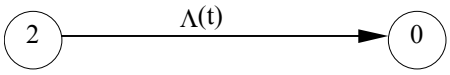


Figure 5 : Redundant system state reduced modelling

The " P " probability of being in a " 0 " state therefore depends on a failure rate that in turn depends on time T : $P = \Lambda(t) \times T$.

This example shows that the more time T increases and the more the probability of being at " 0 " state increases.

4.6 FIFTH STAGE : SAFETY INTEGRITY LEVEL ASSESSMENT

The system's various states were modelled with the fourth stage. This stage consists of resolving the mathematical calculation and comparing the level achieved by the system with the classifications of the IEC 61508 standard.

The dangerous failure probability calculation (PFD) is a function of a system failure rate (function variable over time) and of a duration, in most cases. Therefore, the safety integrity level calculation is a specific reliability calculation in which safety is equal : either to the reliability during a time equal to that of the auto-test's overall time, or to that of the preventive maintenance intervals.

5. APPLICATION OF SAFETY INTEGRITY LEVEL ASSESSEMENT PROCEDURE

5.1 CASE STUDY OF DIODE SAFETY BARRIER

5.1.1 Description and functional analysis

Diode safety barriers are assemblies incorporating shunt diodes or diode chains (including zener diodes) protected by fuses or resistors or a combination of these.

The diodes, zener diodes in the example of figure 6, limit the voltage applied to an intrinsically safe circuit and a following infallible current limiting resistor limits the current which can flow into the circuit. These assemblies are intended for use as interfaces between intrinsically safe circuits and non-intrinsically safe circuits.

The diode safety barrier is manufactured as an individual apparatus rather than a part of a larger apparatus and, as it contains both intrinsically safe circuits and non-intrinsically safe circuits, the barrier is an associated apparatus and shall be :

- either protected by an alternative type of protection listed in EN 50014 [1] for use in the appropriate explosive gas atmosphere,
- or situated outside the explosible atmosphere.

Besides, the barrier shall comply with requirements of EN 50020 [7] which specify in particular for safety devices that the assembly must contain :

- three diodes or three diode chains for category " ia " (safe with two faults),
- two diodes or two diode chains for category " ib " (safe with one fault).

The choice of category " ia " for an intrinsically safe apparatus allows the use of such an electrical apparatus in hazardous areas where explosive gas atmosphere is present continuously or for long periods.

The choice of category " ib " for an intrinsically safe apparatus allows the use of such an electrical apparatus in hazardous areas where explosive gas atmosphere is likely to occur in normal operation.

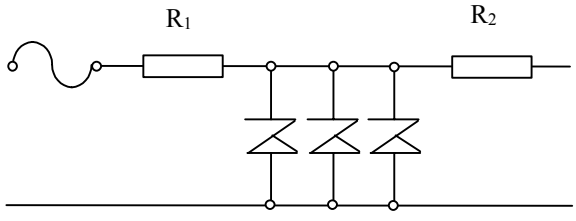


Figure 6 : zener barrier

5.1.2 Failure rate prediction

Results of the calculation for a low power (1.5 W) Zener diode give a failure rate of $\lambda = 2.4*10^{-9}$/hr grounded on assumptions defined in paragraph 4.3.

5.1.3 FMECA

5.1.3.1 ATEX classification

According to ATEX requirements this failure mode is impossible because :

- According to EN 50020, during normal operation, a component can't fail if it works under the 2/3 of its maximum characteristics. This component is considered as an unfaillible component.
- According to EN 50020 if a zener diode fails to short-circuit during the transient period, the fuse can blow if the maximum current is over 1.7 of the nominal current of the fuse. In this case the maximum power dissipated by the diode is lower than its maximum power characteristics, and the safety function of the safety barrier is guarranted. If the maximum current is lower than 1.7 nominal current, then the power dissipated in the diode is lower than its maximum power characteristics.
- During worst functionning (maximum input voltage up to 250 Volts applied to the barrier inputs), the fuse will blow in a very short time (usually lower than 1 milli-second) and the consequence of this worst functionning is a " safe state ", so the safety barrier has to be changed, and there is no hazard. In addition, during the short time of the blowing of the fuse, the functionning power rate of the components (Zener diodes and resistors) complies with the 2/3 rules of their maximum characteristics. So the Zener diode have a low probability to get a short circuit because of the worst functionning of the associated electrical circuit connected to the barrier inputs.

5.1.3.2 IEC 61508 / CNET classification

According to reliability of the CNET standard (see reference [12]) and of other reliabiity standards, a component has several *failures modes* which not take into account the working conditions of the component. Only the failure rate take into account the working conditions of the component.

The CNET's database gives the following failure mode for a low power Zener diode (1.5 W) :

- 10% for voltage drifts
- 20% for open circuit and
- 70% for short-circuit.

5.1.3.2.1 Safe state

The loss of the safety function leading to a safe position regarding safety is achieved if one of the three diodes is short-circuited.

5.1.3.2.2 Dangerous state

The hazardous event in relation to the explosion would be the loss of intrinsic safety characteristics i.e. the following failure mode : " open circuit on the 3 diodes ".

Safety level assessment

5.1.3.3 Dangerous state

Modelling by MARKOV graph is not required for this type of system, and the safety level calculation (3 diodes in open circuit) comes down to a specific reliability calculation in which the probability of event occurrence is equal to *Q(t)* = 1 - *R(t)* with :

- $\theta = \frac{1}{\lambda} * \sum_{i=1}^{3} \frac{1}{i}$
- then $\theta = \frac{1}{\lambda} * \left[1 + \frac{1}{2} + \frac{1}{3}\right] = \theta = \frac{11}{6 * \lambda} = \frac{1}{\lambda_{EQ}}$ for the loss of 3 diodes in open circuit (C.O.)
- hence $\lambda_{EQ} = \frac{6 * \lambda}{11}$ and
- $R(t) = e^{-(\lambda_{EQ}) * t}$

With a failure distribution assumption of 20% for the open system failure mode and 70% for the short-circuit failure mode, and a failure rate for a low power Zener diode (1.5 W) of $\lambda = 2.4*10^{-9}$/hr, we obtain a λ^{DU} of $4.8*10^{-10}$/hr for one diode, a λ_{EQ} for the 3 diodes of $2.6*10^{-10}$/hr.

The results of the calculations for the dangerous state (loss of intrinsic safety characteristics) are :

- Probability for the dangerous state for one year duration without tests : $1 - R(t) = 1 - e^{-(\lambda_{EQ}) * t} = \mathbf{2.28*10^{-6}}$.
- Probability for the dangerous state for ten years duration without tests : $1 - R(t) = e^{-(\lambda_{EQ}) * t} = \mathbf{2.28*10^{-5}}$

5.2 These are the " worst cases " assumptions for the SIL calculations

5.2.1.1 Safe state

The consequence of the failure of one of the three diodes in " short circuit " is a safe state because the fuse will blow in a very short time (usualy lower than 1 milli-second) and during this blowing the functionning rate of the component (zener diodes and resistors) complies with the 2/3 rules of their maximum characteristics.

With the same failure distribution assumptions and failure rate, the probability of this event is $Q(t) = 1 - R(t)$ with :

- $R(t) = e^{-[\sum \lambda i] * t}$

- and $R(t) = e^{-(3*\lambda i)*t}$
- Probability of safety function loss leading to a safe state for one year duration : $1 - R(t) = e^{-(3*\lambda i)*t} = 4.4*10^{-5}$
- Probability of safety function loss leading to a safe state for ten years duration : $1 - R(t) = e^{-(3*\lambda i)*t} = 4.4*10^{-4}$

5.2.2 IEC 61508 quality requirement observance examination

For the safe states, there is no need to check the Zener barrier because this unit will be replace by a new one to keep the well functionning of the safety-function.

The Zener diode safety barrier is a device for which 20% of failures lead to the hazardous event. This architecture can tolerate two failures and has a failsafe fraction of 80%.

This Zener diode safety barrier reachs the SIL 4 level qualitative and quantitative requirements for a one year period (and for a period of 10 years) without periodic test for a safety related protection system.

In theory, the Zener diode safety barrier reachs the SIL 4 qualitative and quantitative requirements for a period of 43 years. After this period, the Zener diode safety barrier reachs the SIL 3 quantitative requirements. This result must not be taken into account because the calculations basis are not valid after a period of ten years for electronic components (after this period, the failure rate is not constant).

5.3 CASE STUDY OF SAFETY LEVEL DETECTION SAFETY DEVICE

A system already " ia " intrinsic safety certified formed the subject of an assessment by INERIS in accordance with requirements of standard IEC 61508.

5.3.1 Functional analysis

We represent the case of a safety low level detection system installed in a tank containing liquid or liquefied hydrocarbons. The system is constituted of one detector connected to a processing unit to detect a low level in order to shut off the electric power.

5.3.2 Failure rate prediction

Grounded on assumptions mentioned in paragraph 4.3, the calculation results give a failure rate of $\lambda = 4*10^{-6}$/h for the detector, and of $\lambda = 1.1*10^{-6}$/h for the processing unit.

5.3.3 FMECA

The hazardous event in relation to safety for the safety level detection system is the loss of low level detection. The system's dangerous failure rate was calculated grounded on the detailed FMECAs. Results are as follows :

- A dangerous failure rate of $2*10^{-6}$/h for the detector i.e. an FSF of 49%
- A dangerous failure rate of $1.5*10^{-7}$/h for the processing unit, i.e. an FSF of 85%
- i.e. for the full system, an FSF under 60%

5.3.4 Safety level assessment

MARKOV graph modelling is not required, and the safety level calculation comes down to a specific reliability calculation in which the probability of occurrence of this event is $Q(t) = 1 - R(t) = 1 - (e^{-\lambda_d * t} * e^{-\lambda_{pu} * t})$.

By assuming a dangerous failure rate for the detector of $2*10^{-6}$/h and $1.5*10^{-7}$/h for the processing unit, we obtain the following values for a year :

Safety function loss of low level detection of $1.7*10^{-2}$

5.3.5 IEC 61508 requirement observance examination

If a processing unit design in simple chain tolerance to " 0 " failures is selected and if the following values are selected for the overall safety level detection system : a failsafe fraction (FSF) inferior to 60% and a PFD of $1.7*10^{-2}$, the safety level detection system can be graded as safety related control system, and is compliant with the SIL 1 level qualitative and quantitative requirements for a one year term and for operation on demand.

5.4 CASE STUDY OF PRESSURE AND TEMPERATURE SAFETY DEVICES

5.4.1 Functional analysis

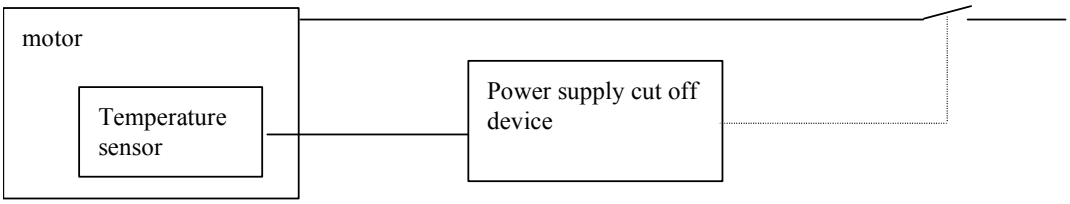


Figure 7 : Motor protection device

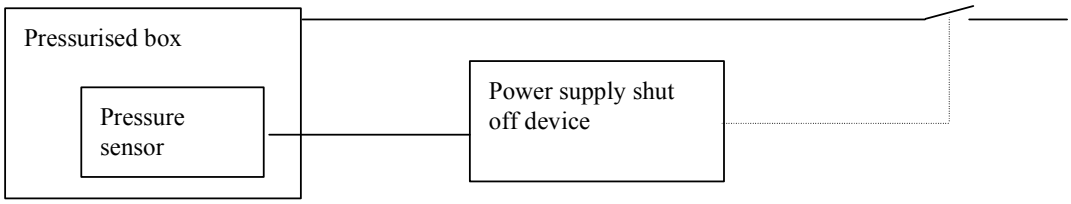


Figure 8 : Pressurised box protection device

5.4.2 Failure rate prediction

With the assumptions defined in paragraph 4.3, the results of the calculations give the following failure rate :

- Temperature sensor $\lambda = 5*10^{-9}$/h and
- Power supply shut off device $\lambda = 1.1*10^{-6}$/h

5.4.3 FMECA

Both architectures are similar. The safety function loss leads to an explosion risk under explosive atmosphere in both cases. The safety function loss occurs in the event of pressure sensor or power supply shut off device dangerous failure for the first architecture. The safety function loss occurs in the event of temperature sensor **or** power supply shut off device dangerous failure for the second architecture.

The detailed FMECAs at component level were conducted on a low level detection system in the event of LPG storage (see the values of chapter 5.3) in simple chain. Assuming a similar architecture for the power supply shut off device, the dangerous failure rate is $1.5*10^{-7}$/hr i.e. an FSF of 85%.

5.4.4 Safety level assessment

If a power supply shut off device design in simple chain based on discrete electronics is selected, the MARKOV graph modelling is not required, and the safety level calculation comes down to a specific reliability calculation in which the probability of occurrence of

this event is equal to $Q(t) = 1 - R(t)$ with $R(t) = e^{-[\sum \lambda i]*t}$

By assuming a failure rate of $5*10^{-9}$/hr for the temperature sensor, a dangerous failure distribution of 100%, and a dangerous failure rate for the power supply shut off device of $1,5*10^{-7}$/hr, we obtain the following values for a year :

Safety function loss leading to an explosion risk $R(t) = e^{-(\sum \lambda_i)*t} = 1.35*10^{-3}$

5.4.5 IEC 61508 requirement observance examination

If the power supply shut off device design in simple chain tolerance to " 0 " failure, a failsafe fraction of 85% and a PFD of $1.35*10^{-3}$ are selected, the device must meet the SIL 2 level quality and quantity requirements for operation on demand for a year and for a safety related protection system.

6. CONCLUSIONS

6.1 MAIN DIFFERENCES BETWEEN ATEX STANDARDS AND IEC 61508

There are differences between hardware fault tolerance of IEC 61508 and of ATEX standards. The requirements of hardware fault tolerance of IEC 61508 are defined to their consequence regarding the loss of the safety function. Those requirements are a measurement of the effectiveness of a safety-related device.

The requirements of hardware fault tolerance of ATEX standards are defined to their consequence regarding the explosion hazard.

According to some ATEX standards, if some construction principles are met, then the component is considered as infaillible. In IEC 61508 and reliability standards and databases the concept of infaillible component is not considered.

6.2 CLASSIFICATION OF ATEX SAFETY DEVICES ACCORDING TO IEC 61508

IEC 61508 standard requirements (see reference [10]) are :

- System development cycle requirements around a safety life cycle and in terms of related documentation (Part 1).
- Qualitative and quantitative technical requirements in presence of faults (Parts 1 and 2).
- Technical requirements in relation to software design and validation (Part 3).

INERIS only checked the qualitative and quantitative technical requirements in the presence of faults which were taken into account. The system's overall safety validation by functional safety tests, behaviour tests on defect and tests related to sizing and compliance with the environmental parameters were not conducted by INERIS. Similarly, INERIS did not check whether the requirements of the system's development cycle around a safety life cycle was taken into account and did not check the related documentation.

There are two types of failures according to the consequences for safety, in accordance with the qualitative and quantitative technical requirements in the presence of faults, set out in the IEC 61508 standard. These failures are :

- Safe failures, i.e; failures whose consequences lead to system fallback (safe situation in relation to safety),
- Dangerous failures, i.e. failures resulting in a dangerous state in relation to safety.

In accordance with the ATEX standards, failures are graded according to their effect in relation to the ignition of explosive atmospheres. These types of failures or faults correspond to the loss of safety function as defined in the IEC 61508 standard.

Ours conclusions concerning the safety devices' grading used in applications liable to form an explosive atmosphere are as follows :

- Safety devices must meet the requirements of applicable standards (see reference documents [1] to [9]).
- The only purpose of grading safety devices in accordance with the IEC 61508 standard requirement is to assess their capacity to guarantee the safety function for which they were designed during the time.
- Devices can be graded in accordance with the ATEX standard requirements and to those of the IEC 61508 standard if the effect of dangerous failures and safe failures as defined in the IEC 61508 standard correspond to the failures as defined in the ATEX standard, and that the failures can lead to the ignition of explosive atmospheres.

There are two main types of configurations :

- Configurations in which the undetected dangerous failure of a safety device does not directly lead to an explosion (e.g. case of a temperature measurement device and of an electric motor power supply shut off device in the event of overheating). In this case, the probability of explosion occurrence is subject to : motor overheating AND failure of the safety devices AND presence of an explosive atmosphere. This type of situation could correspond to what the IEC 61508 standard refers to as the " **safety related protection systems** ". These are the devices under the scope of the SAFEC project.
- Configurations in which an undetected dangerous failure of the safety device does not lead to an explosion but to another hazard (case of the level detection system). This case could correspond to what the IEC 61508 standard refers to as the " **safety related control systems** ". These devices are not under the scope of the SAFEC project because their use is under the knowledge and under the responsability of the end user. (A level detection system would fall into the first category if it was used as part of a submersible pump, such that ignition could occur if the level dropped below the level of the pump).

These conclusions only encompass safety devices used in applications under explosive atmospheres studied in paragraph 4 of this document, and with an autonomous safety function.

These conclusions are only valid if preventive maintenance is conducted. The purpose of these preventive maintenance operations is to detect, when it's possible, component failures leading to a dangerous state.

7. REFERENCES

[1] EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements[1].

[2] EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion[2].

[3] EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p"[3].

[4] EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling "q"[4].

[5] EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure "d"[5].

[6] EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety "e"[6].

[7] EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety "i"[7].

[8] EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation "m"[8].

[9] Reports on task 1 and 2 of the SAFEC project

[10] CEI 61508 - version FDIS of 1998-07-31
Functional Safety : safety-related systems (part 1 to 7)

[11] LSSE - 95.14 dated April 1995 (document confidential to INERIS)
(Analysis and assessment procedure for the safety and availability levels of safety automations by Markovian modelling)

[12] RDF 93
Recueil de données de fiabilité des composants électroniques *(Electronic component reliability data log)*

[13] A.BIROLINI
Quality and reliability of technical Systems (Ed. Springer - Verlag)

[14] " Draft 5 (5/13/1996 - ISA technical report ").

Annex E

Determination of a methodology for testing, validation and certification

Partner: Deutsche Montan Technologie GmbH
Fachstelle für leittechnische Einrichtungen mit Sicherheitsverantwortung
Beylingstr. 65, D - 44329 Dortmund

Authors: Dr. Franz Eickhoff
Dr. Michael Unruh

Content

Figures and Tables

1 Introduction

1.1 Working task

This working task is a part of the research project SMT4-CT98-2255 Determination of safety categories of electrical devices used in potentially explosive atmospheres. The task has the following content:

- **Task 5: Determination of a methodology for testing, validation and certification**
  A methodology allowing the testing, validation and certification of safety devices shall be developed. This shall take into account the target failure measures developed in Task 1, the currently available standards assessed in Task 2 and the 'used safety devices' identified in Task 3. A preliminary report with proposals for standardization shall be produced at the end of this task. This report shall be distributed for comments to users, manufacturers and experts involved in European standardisation groups from at least 6 EU countries. Comments received shall be considered in the final report produced in Task 6.

1.2 Definition of safety devices and applicable technologies

The aim of this task is the development of a procedure for certification of safety-related systems or safety devices used in the area of explosion protection.

The first problem is to identify safety devices. The definition of the ATEX Guidelines [2] may be helpful and shall be used for further definitions.

> ***"4.1.2Which kinds of products are covered by directive 94/9/EC?***
> *To be within the scope of the directive, a product has to be:*
> ***equipment**, as defined in Article 1.3.(a); or*
> *a **protective system**, as defined in Article 1.3.(b); or*
> *a **component**, as defined in Article 1.3.(c); or*
> ***a safety, controlling or regulating device** as defined in Article 1.2.*
> *.....*
> *d) Safety, controlling or regulating devices as defined in Article 1.2.*
> *The two main issues of Article 1.2 are,*
> *i) that **safety devices**, **controlling devices** and **regulating devices**, if they contribute to or are required for the safe functioning of equipment or protective systems with respect to the risks of explosion are **subject to the directive**;*
> *ii) that devices are covered **even if** they are situated **outside the potentially explosive atmosphere**.*
> *For such devices, the essential requirements shall only be applied so far as they are necessary for the **safe and reliable** functioning and operation of those devices with respect to the risk of explosion (ANNEX II, Preliminary observation B)*
> *The **definition** in i) leads to the following consequences:*
> *1. Devices other than safety, controlling and regulating devices are not covered. (However, a device of any kind, contributing to or required for the safe functioning, could be considered a safety device);*
> *2. **All devices**, including safety, controlling and regulating devices**, neither contributing** to **nor required** for the safe functioning with **respect to the explosion risk are not covered**;*

*3. Even **safety, controlling and regulating devices** contributing to or required for the safe functioning but **with respect to risks other than the explosion risk are not covered;***

For further illustration some examples:
*Examples for **devices falling under Article 1.2:***

- *A power supply feeding an intrinsically safe (EEx i) measurement system used for monitoring process parameters;*
- *A pump, pressure regulating device, backup storage device, etc. ensuring sufficient pressure and flow for feeding a hydraulically actuated safety system (with respect to the explosion risk);*
- *Overload protective devices for electric motors of type of protection EEx e 'Increased Safety';*
- *Controllers, in a safe area, for an environmental monitoring system consisting of gas detectors distributed in a potentially explosive area, to provide executive actions if dangerous levels of gas are detected;*
- *Controllers for sensors temperature, pressure, flow, etc, located in a safe area, for providing information used in the control of electrical apparatus, used in production or servicing operations in a potentially explosive area;*

*Examples for **devices not falling under Article 1.2:***

- *Switchgear, numeric controllers, etc. not related to any safety functions (with respect to the explosion risk); because of 2) above;*

***Item ii)** states that devices, as defined above, are subject to the directive, even when outside the potentially explosive atmosphere.*
For safety and economic reasons it will be preferable in most cases to install such devices in a non-hazardous area. However, sometimes it might be necessary to place such devices within a potentially explosive atmosphere. In such cases, although the directive does not explicitly say so, these devices can also be designated as equipment. Two situations can be identified:

- *If the device has its **own potential source of ignition** then, in addition to the requirements resulting from Article 1.2, the **requirements for equipment** will apply;*
- *If the device does not have its own potential source of ignition then the device will not be regarded as equipment but of course the requirements resulting from Article 1.2 will still apply."*

1.2.1 Conclusions from the ATEX-Guidelines

The main identification aspect for a safety device is the **autonomous function** for avoiding explosion risk. A thermal fuse is therefore a safety device. The certification scheme theoretically has to be applicable to these simple safety devices. However, is makes no sense to use it for simple safety devices. There are already standards available for these devices. Therefore, the certification scheme is mostly used for complex safety devices (see examples for safety devices [2]), but must have no contradiction to available standards for simple safety devices. This is mentioned in the work of TC 31 WG 09. A reference table is prepared to define the safety devices not covered by available standards based on Task 3 of this research project [13].

- **The certification scheme has to be applicable to simple and complex safety devices. The certification scheme is used more for complex safety devices or safety systems.**

The certification scheme for the functional safety of safety devices is independent on the certification scheme for the safety against potential ignition sources if the safety device is also in the scope of the RL 94/9/EC as equipment. This is in general the same situation for gas measurement systems, for protection systems and safety devices:

a) they can be equipment if the scope of the 94/9/EG,
b) they can have a safety function in the scope of 94/9/EG.

- **The two items can have strong relations to each other, but they have different features. In the scope of this research project is only feature b).**

A safety device can be based on several different technologies. The construction principle may be electrical / electronic or programmable electronic. In addition, mechanic, pneumatic, hydraulic and other technologies may be used.

- **Example for different technologies**
  A standard thermal protection relay used for the protection of type EEx „e“ – engines consists of a bimetal heating systems and several mechanical elements. The mechanical components are responsible for the triggering of the relay if one phase is disconnected. The function and the reliability of the overload relay also depend on mechanical components. The application for example of IEC 61508 part 2 is not possible in that case.

There must be a distinction between the certification scheme and the applicable standards for different technologies. The two standards EN 954-1 and IEC 61508 may not be the only standards for assessment.

- **The certification scheme has to be open to different technologies.**

The certification scheme is mainly used for the certification of products in the scope of 94/9/EC. The products are used under the scope of the 1999/92/EC directive [3]. Aspects of the safe use of products may be taken into account in the certification scheme if these technical aspects are different from existing standards for the use of explosion protected equipment.

- **The certification scheme has assessed the equipment to the ESR of the 94/9/EG. The scheme has to give the required information for the safe use under the directive 1999/92/EC.**

2 Requirements

2.1 Requirements of directives 94/9/EC and 1999/92/EC

The technical requirements (essential safety requirements ESR) of 94/9/EC are included in ANNEX II [1]. These requirements are based on existing technical standards for explosion protection in group I and group II. The ESR are not fully described in the directive. The authors take the existing standards for explosion protection into account. Many aspects seem to be open but most times written clearly in the standards for explosion protection (ANNEX 13 of [2]).

The aspects of using the products are defined in directive 1999/92/EC [3]. It is the instruction which is the link between the manufacturer and the user. Therefore, the instructions are given an important role. (ANNEX II of [1]):

> *"1.0.6. Instructions*
> *(a) All equipment and protective systems must be accompanied by instructions, including at least the following particulars:*
> *- a recapitulation of the information with which the equipment or protective system is marked, except for the serial number (see 1.0.5.), together with any appropriate additional information to facilitate maintenance (e.g. address of the importer, repairer, etc.);*
> ***- instructions for safe:***
> ***- putting into service,***
> ***- use,***
> ***- assembling and dismantling,***
> ***- maintenance (servicing and emergency repair),***
> ***- installation,***
> ***- adjustment;***
> *- where necessary, an indication of the danger areas in front of pressure-relief devices;*
> *- where necessary, training instructions;*
> ***- details which allow a decision to be taken beyond any doubt as to whether an item of equipment in a specific category or a protective system can be used safely in the intended area under the expected operating conditions****;*
> *- electrical and pressure parameters, maximum surface temperatures and other limit values;*
> ***- where necessary, special conditions of use, including particulars of possible misuse which experience has shown might occur;***
> *- where necessary, the essential characteristics of tools which may be fitted to the equipment or protective system."*

The instruction also is mentioned in the new EN 50014 [15].

With existing standards for explosion protection, therefore products are certified with a view to existing standards for installation, maintenance, repair etc., and the use. The information link between the manufacturer and the user is the instruction.

A certification scheme for safety devices has to assess the required safety. Furthermore the certification scheme has to include all the information for instruction for safe, etc. ... and special details necessary to decide about the users application.

- **Example:**
  A safety device is certified that it can be used in an application with SIL 4. In this special application the safety device needs a manual periodic test every day. It cannot be used normally in explosion protection with standard test rates / maintenance rates. There has to be some information about proof intervals and maintenance rates if they are different from common used rates.

If this is not possible for the application of the equipment, every parameter for diagnostics, periodic test etc. has to be defined in the certification under worst conditions and given to the user in the instruction to make sure that the equipment is used in a safe way and the necessary risk reduction is achieved in practical use for every application.

2.2 Summary of demands from 94/9/EC and 1999/92/EC

The certification for functional safety of safety devices has to assess the safety requirements. The certification has to distinguish all relevant parameters for the instruction given to the user.

3 Selection of concept for certification

Three possible concepts for certification are compared:
- A concept independent from technologies and application.
- A concept based on a hierarchical structure of standards (A-, B- and C-type standards).
- A concept based on a life cycle structure.

For these different concepts examples are given. The advantages and disadvantages are pointed out.

3.1 Concept of EN 1441 [9]

The EN 1441 is based on a basic risk assessment scheme (see Figure 1, an example taken from [10]).

The hazards in the steps for example are hardware or software faults or even wrong handling in several situations like manufacturing, transportation, storage and use. For every product, all the possible hazards can be identified systematically. Special applications can be taken into account. The result is a hazard list for the product. New products have to fulfil this list.

The scheme is open to every application, but the result will be very special to one type of product. It is an advantage for the use with medical products. The advantage for the application to electronic detonators was shown in a CEN working group [10]. A result which is special for one kind of product is the main disadvantage for the application to the wide range of safety devices.

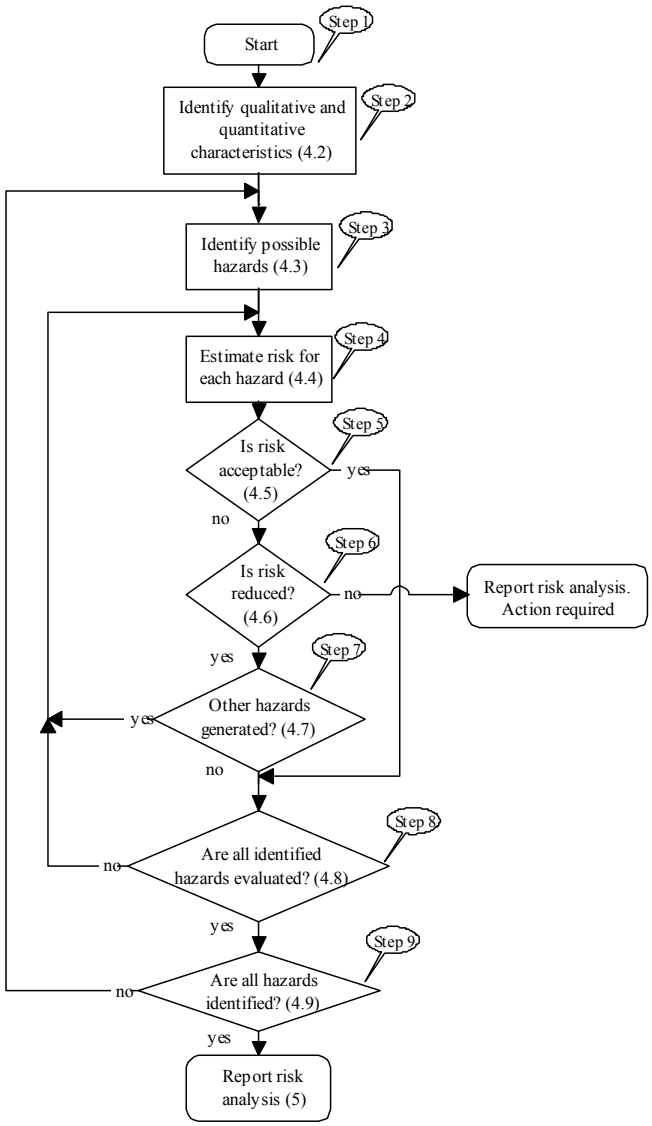


Figure 1 Risk assessment and test scheme based on EN 1441

3.2 Concept of harmonised standards under the scope of directive 98/37/EC

The harmonised standards related to 98/37/EC are separated in three levels:
- A-Type: General principles, e. g. EN 1050 Risk assessment,
- B-Type: Basic principles, e. g. EN 954-1 Safety related parts of control system [7],
- C-Type: standards for special products.

These standards are based on the application to machinery. The application of one standard has to take into account several other standards.

EN 954-1 is commonly used with EN 1050 together. Furthermore, some product standards are applicable for a special product. Some of the problems with application of EN 954-1 described in Task 2 are based on this concept of breaking up the standard.

The main advantage of these standards is the application to many technologies; the main disadvantage is that these standards are not applicable to programmable systems.
There is another disadvantage, which should not be missed: the standards are written as standards for manufactures. The standards like EN 954 -1 normally give no information about installation, maintenance and repair (see Task 2 [11]). The intended use of the product is covered by the risk analysis of the manufacturer. The manufacturers have to give this information for safety use to the user below 98/37/EC as if they have to give it below 94/9/EC. This is not especially written in the standards. The manufactures have to do give all relevant information to the user.

3.3 Concept of IEC 61508

IEC 61508 is the counterpart of several harmonized standards in comparison to the harmonised standards of directive 98/37/EC. The main disadvantage of the standard seems to be the possibility of application only to electric, electronic and programmable electronic systems. This is wrong. It is possible to distinguish in IEC 61508 two main parts:

a) The systematic description for the overall life cycle of a system not depending on a specific technology.
b) The description of requirements based on safety integrity level (SIL) for electric / electronic / programmable electronic safety-related systems.

For an overview see Figure 2.The part a) is located in the part 1 of IEC 61508. The part b) is included in part 2 - 7 of IEC 61508.

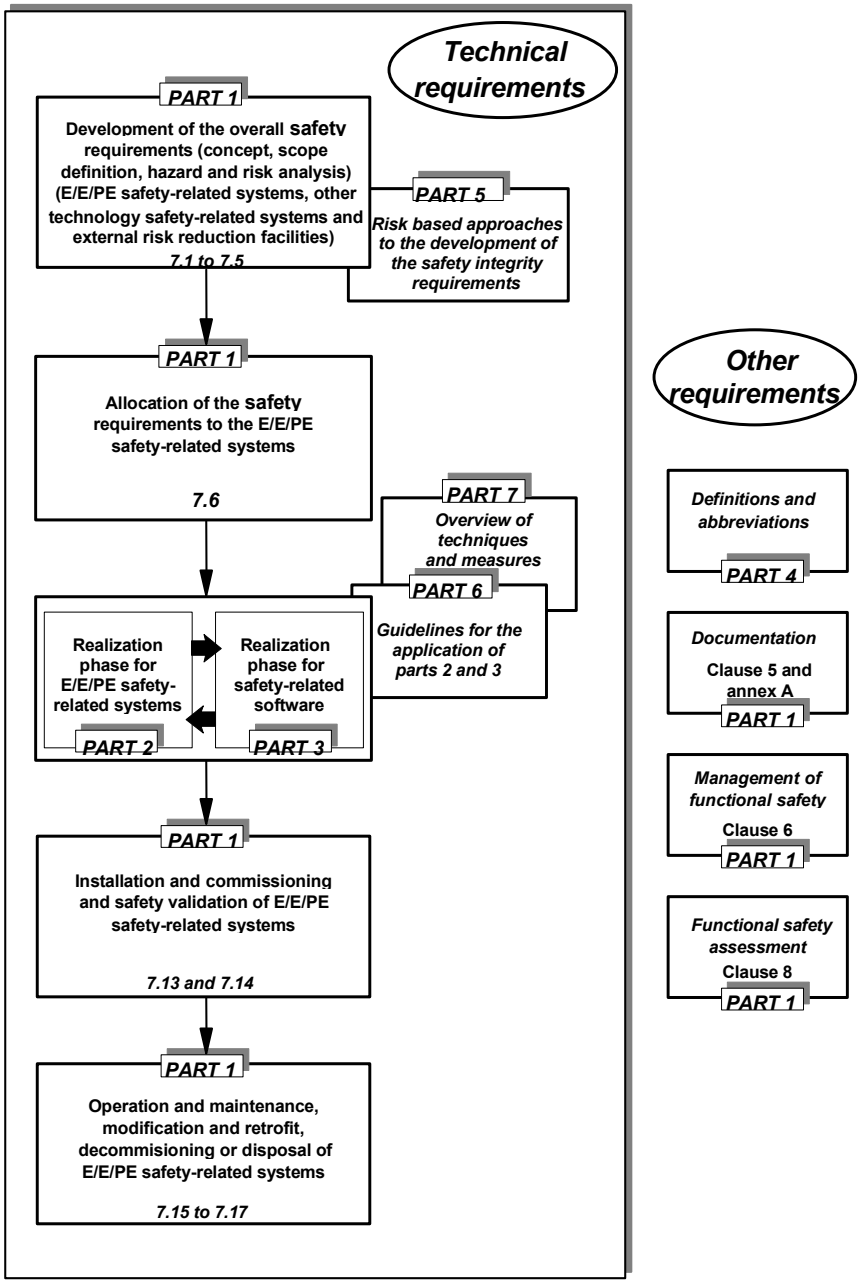
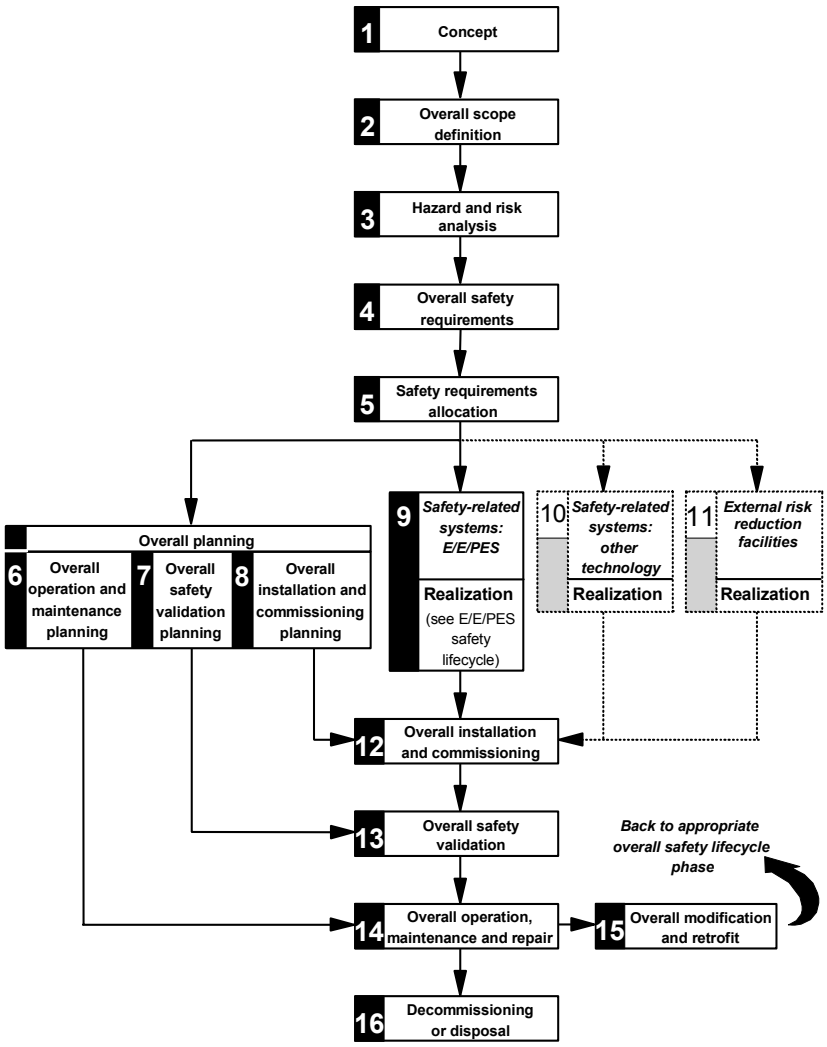


Figure 2 Overall framework of the IEC 61508 (IEC 61508 Part 1 Figure 1)

The IEC 61508 describes the whole life cycle of equipment from concept to decommissioning or disposal (see Figure 3).

The validation and certification in general must be open for the application of different technologies and standards (see 1.2.1). This is possible in the life cycle scheme of IEC 61508 (see Figure 3). There is a possibility to use other standards. The verification process can take into account the different approaches of the applied standards.



NOTE 1 Activities relating to ***verification, management of functionalsafety*** and ***functional saftey assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure 3 Overall safety lifecycle (IEC 61508 Part 1 Figure 2)

Every life cycle has a corresponding part in existing explosion protection standards (for example life cycle 12 and 14: standards for installation and maintenance).

For a certification, the SIL (step 9) and the steps 6, 7 and 8 have to be tested. It has to be checked whether the life cycles 12 - 14 can be fulfilled under the scope of explosion protection.

A safety device with other technologies can be certified according to step 10 with other standards. A reference table will be necessary, for example, between EN 954-1 levels and the safety integrity level of IEC 61508. This is not available because the references depend on the application and the technology.

A problem between IEC 61508 and EN 954-1 is mentioned in Task 2. The safety level steps in EN 954-1 are not hierarchically structured. The IEC 61508 and the zone definition for explosion protection are linear structured. Furthermore, depending on application a safety level in EN 954-1 can lead to different levels in IEC 61508

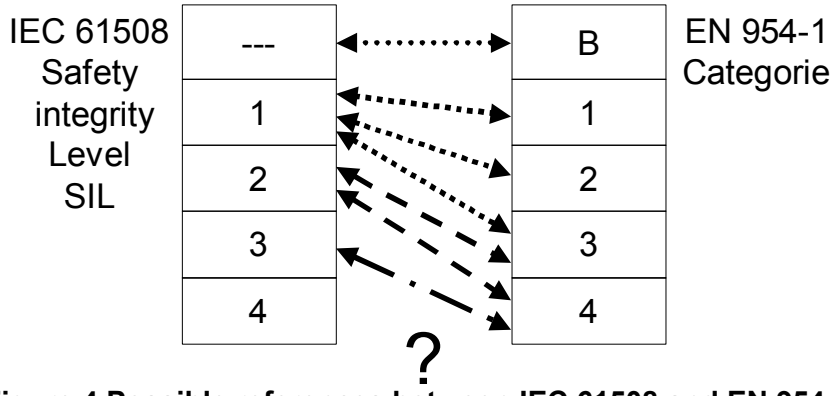


Figure 4 Possible references between IEC 61508 and EN 954

EN 954-1 gives no information about maintenance. The problems defined in Task 2 can be handled in step 11 or in step 6. Proof testing can be taken as a risk reduction facility if the applied standards like EN 954-1 give no information. The other possibility is to include such problems in step 6, but there the requirements of explosion protection to operation and maintenance should be placed.

IEC 61508 contains a complete scheme for the handling of a product. This is an advantage to other possible schemes. In the next chapter, an assignment is made from the lifecycle to the area of explosion protection. A complete correlation is possible (see part 3.4).

3.4 Assignment of IEC 61508 lifecycles to the area of explosion protection

The lifecycles of IEC 61508 can be divided into three parts.
1. This table contains lifecycles where the preconditions are given by existing standards for explosion protection (Table 1).
2. This table contains the cycles with relation to the certification process (Table 2).
3. This table contains the use of the product (Table 3).

To give some information Table 1 of IEC 61508 Part 1 is shown. It is divided into the three parts. This is mentioned above.

ecycle Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Concept	7.2.1: To develop a level of understanding of the EUC and its environment (physical, legislative etc) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	EUC and its environment (physical, legislative etc).	7.2.2	All relevant information necessary to meet the requirements of the sub clause.	Information acquired in 7.2.2.1 to 7.2.2.6.	- 94/9/EC - EN 60079-10 - existing stand for explosion protection: EN 50014, ...
Overall scope definition	7.3.1: To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc).	EUC and its environment.	7.3.2	Information acquired in 7.2.2.1 to 7.2.2.6.	Information acquired in 7.3.2.1 to 7.3.2.5.	- 94/9/EC - EN 60079-10 - existing standards fo explosion protection: E 50014, ...
Hazard and risk analysis	7.4.1: To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse; To determine the event sequences leading to the hazardous events determined; To determine the EUC risks associated with the hazardous events determined.	The scope will be dependent upon the phase reached in the overall, E/E/PES and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will comprise the EUC, the EUC control system and human factors.	7.4.2	Information acquired in 7.3.2.1 to 7.3.2.5.	Description of, and information relating to, the hazard and risk analysis.	- 94/9/EC - existing stand for explosion protection: EN 50014, ...

ecycle Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Overall safety require-ments	7.5.1: To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.	EUC, the EUC control system and human factors.	7.5.2	Description of, and information relating to, the hazard and risk analysis.	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	- 94/9/EC - existing stand for explosion protection: EN 50014, ... - Task 1[11] - Task 2 [11]
Safety require-ments allocatio n	7.6.1: To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities; To allocate a safety integrity level to each safety function.	EUC, the EUC control system and human factors.	7.6.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Information and results of the safety requirements allocation.	- existing stand for explosion protection: EN 50 014, ... - Task 1[11] - Task 2 [11]

1- Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - preconditions by existing standards

cycle phase Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	Special for saf devices, exam
Overall operation and maintenance planning	7.7.1: To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.7.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for operating and maintaining the E/E/PE safety-related systems.	- 94/9/EC A II, 1.0.6 Instructior - EN 60079 [18] - EN 60 079 [20]
Overall safety validation planning	7.8.1: To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.8.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan to facilitate the validation of the E/E/PE safety-related systems.	- 94/ 9/EG Annex II, Instructior - EN 60079 [18]
Overall installation and commission-ing planning	7.9.1: To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.	EUC and the EUC control system; E/E/PE safety-related systems.	7.9.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.	- 94/ 9/EG Annex II, Instructior - EN 60 079 - EN 50281

cycle phase Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	Special for saf devices, exam
E/E/PE safety-related systems: realization	7.10.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).	E/E/PE safety-related systems.	7.10.2 and parts 2 and 3	Specification for the E/E/PES safety requirements.	Confirmation that each E/E/PE safety-related system meets the E/E/PES safety requirements specification.	- 94/9/EC A II - IEC 61508 2 and 3
Other technology safety-related systems: realisation	7.11.1: To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other technology safety-related systems.	7.11.2	Other technology safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each other technology safety-related systems meets the safety requirements for that system.	- 94/9/EG A II - EN 954 Pa and 2
External risk reduction facilities: realization	7.12.1: To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).	External risk reduction facilities.	7.12.2	External risk reduction facilities safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each external risk reduction facility meets the safety requirements for that facility.	- 1999/92/E - Special pr cedures

- Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - lifecycles in re to certification process

cycle Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	special fo safety de examples
Overall installation and commis-sioning	7.13.1: To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	7.13.2	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.	Fully installed E/E/PE safety-related systems; Fully commissioned E/E/PE safety-related systems.	- 1999 - EN 6 14 - EN 5 1-2
Overall safety validation	7.14.1: To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.	EUC and the EUC control system; E/E/PE safety-related systems.	7.14.2	Overall safety validation plan for the E/E/PE safety-related systems; Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements; Safety requirements allocation.	Confirmation that all the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.	- 1992

cycle Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	special fo safety de examples
Overall operation, maintenan ce and repair	7.15.1: To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.	EUC and the EUC control system; E/E/PE safety-related systems.	7.15.2	Overall operation and maintenance plan for the E/E/PE safety-related systems.	Continuing achievement of the required functional safety for the E/E/PE safety-related systems; Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems.	- 94/9/ Anne 1.0.3 Spec chec and main e cond 1.0.6 Instr - 1992 - EN 6 14 - EN 6 17 - prEN 6007
Overall modificatio n and retrofit	7.16.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.	EUC and the EUC control system; E/E/PE safety-related systems.	7.16.2	Request for modification or retrofit under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems, both during and after the modification and retrofit phase has taken place; Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems.	- 94/9/ Anne - 1999 - EN 6 14 - EN 5 1-2

cycle Title	Objectives	Scope	Requirements sub clause	Inputs	Outputs	special fo safety de examples
Decommis sioning or disposal	7.17.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	EUC and the EUC control system; E/E/PE safety-related systems.	7.17.2	Request for decommissioning or disposal under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems both during and after the decommissioning or disposal activities; Chronological documentation of the decommissioning or disposal activities.	-

- Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - lifecycles rega to the use of products

3.4.1 Conclusion for IEC 61508

IEC 61508 is applicable for the certification of safety devices under the scope of the 94/9/EC [1]. The approach of IEC 61508 covers the scope of 94/9/EC and 1999/92/EC. IEC 61508 allows the use of not explicitly mentioned technologies for validation. The ESR can be covered by validation following IEC 61508.

There may be some differences for instance if a thermal control device is used for the control of electrical equipment or for the protection of non-electrical equipment because in 94/9/EC the certification procedure is different.

3.5 Summary

Every concept has advantages and disadvantages. With the use of EN 1441 or EN 954-1 many things have to be added to get a certification scheme for safety devices in the area of explosion protection.

IEC 61508 gives a complete concept for the certification of safety devices. The disadvantage is application only for specific technologies. The concept on the other hand is open for use of standards with other technologies. IEC 61508 only has to adapt to the use with safety devices for explosion protection.

4 Conformity assessment procedure according to IEC 61508

4.1 Conditions

For a conformity assessment procedure based on IEC 61508 minor changes have to be made for the application to safety devices.

- The boxes 1 - 4 are already fulfilled by existing standards for explosion protection and the work in Task 1 and Task 2 [11].

- The box 5 is mainly defined by existing standards for explosion protection (function) and Task 2 (safety integrity level).

The safety integrity level for a purge control system is defined. Even the safety integrity level for a thermal protection system can easily be defined.
For example, a type “e” engine is not suitable for zone 1 without a thermal protection system. So this safety device is needed. It has to be added and the safety function “thermal protection” has to fulfil SIL 2.
In other cases, the manufacturer and the notified body have to do the safety requirement allocation according to IEC 61508, Part 1, 7.6.

4.2 Validation process

- The certification scheme itself bases on the box 9, Figure 3 for electric / electronic or programmable electronic safety devices or on box 10, Figure 3 together with box 11 for other technologies.

Figure 5 and Figure 6 shows lifecycle realization phase including validation process.

- The notified bodies have to carry out the conformity assessment procedure according to boxes 9.1 to 9.6 for hardware and software. The assessment can include less or more the point 9.1 to 9.5. This is depending on the safety devices. The most important step is 9.6.

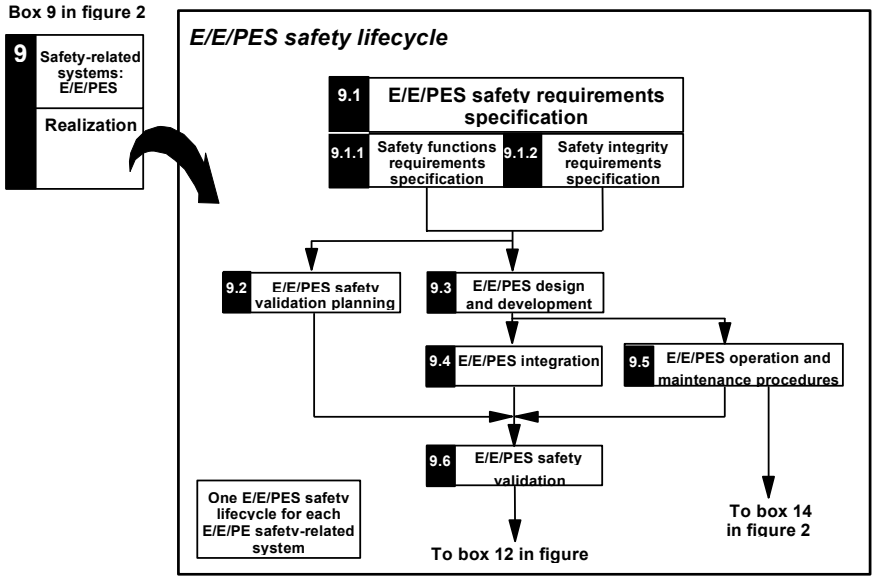


Figure 5 E/E/PES safety lifecycle (in realization phase) (IEC 61508 part 1, figure 3)

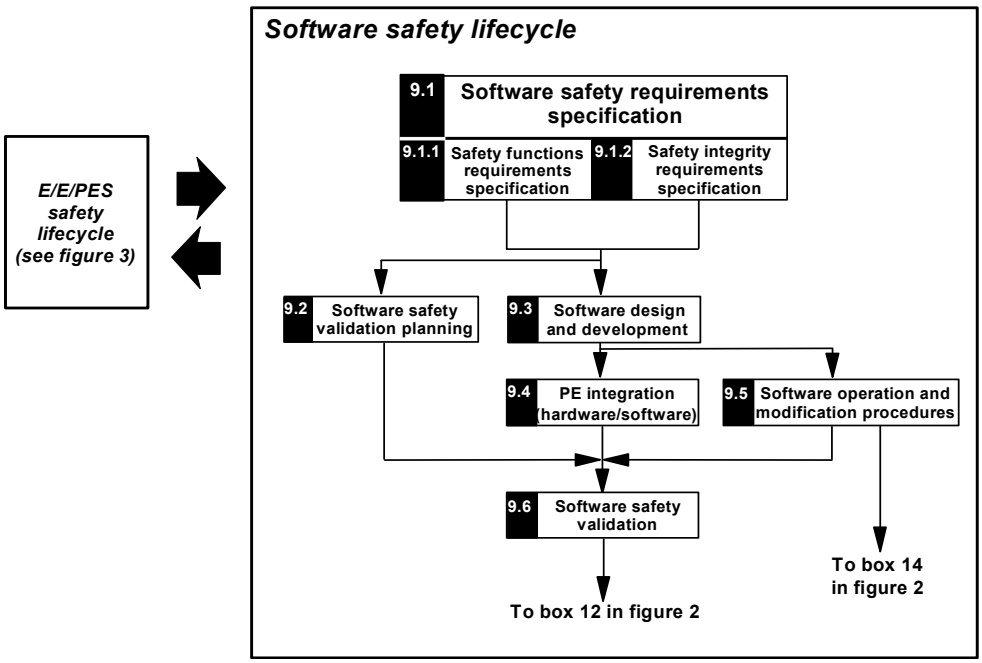


Figure 6 Software safety lifecycle (in realization phase) (IEC 61508 part 1, figure 4)

The tasks included in realization phase relate to the description in IEC 61508 Part 1. The following lifecycle / task has to be fulfilled [4]:

> *7.10 Realisation: E/E/PES*
> *NOTE This phase is box 9 of figure 3 and boxes 9.1 to 9.6 of figures 4 and 5.*
>
> *7.10.1 Objective*
> *The objective of the requirements of this sub clause is to create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements). See parts 2 and 3.*
>
> *7.10.2 Requirements*
> *The requirements that shall be met are contained in parts 2 and 3.*

The specific demands are contained in IEC 61508 Part 2 and 3. Further information can get from IEC 61508 parts 2 and 3.

4.3 Special demands with other standards in validation process

For other technologies, IEC 61508 includes the following recommendation:

7.11 Realization: other technology
NOTE: This phase is box 10 of figure 3.

7.11.1 Objective
The objective of the requirements of this sub clause is to create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.

7.11.2 Requirements
The specification to meet the safety functions requirements and safety integrity requirements for other technology safety-related systems is not covered in this standard.
NOTE: Other technology safety-related systems are based on a technology other than electrical/electronic/programmable electronic (for example hydraulic, pneumatic etc). The other technology safety-related systems have been included in the overall safety lifecycle, together with the external risk reduction facilities, for completeness (see 7.12).

The validation for other technologies can be led by using EN 954-1. Specification of the validation process is urgent necessary (see Task 2). PrEN 954-2 e.g. can be used. Other standards are possible (for example DIN EN 61496-1 06/98).

The lack of information e.g. about proof intervals has to be covered by special procedures. The validation of a electrical / electronic or programmable electronic devices with the EN 954-1 needs separate calculation of reliability for circuits responsible for the validated safety function.

This additional validation may be allocated to the lifecycles **Overall safety validation planning** (box 6, Figure 3) or to **External risk reduction facilities** (box 11, Figure 3). IEC 61508 part 1, Chapter 7.12 give some further information.

7.12 Realisation: external risk reduction facilities
NOTE: This phase is box 11 of figure 3.

7.12.1 Objective
The objective of the requirements of this sub clause is to create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities.

7.12.2 Requirements
The specification to meet the safety functions requirements and safety integrity requirements for the external risk reduction facilities is not covered in this standard.
NOTE The external risk reduction facilities have been included in the overall safety lifecycle, together with the other technology safety-related systems for completeness (see 7.11).

4.4 Special information for instruction

Furthermore, the notified bodies have to proof the results of the E 7 E / PES safety validation (lifecycle 9.6). The overall planning (lifecycles shown in box 6 - 8 (Figure 3)) has to proof according to the directive 1999/92 and the existing standards if special information must given in the instruction for the use of safety devices.

4.5 Actual problems with IEC 61508

A problem for application of IEC 61508 – 2 is that the standard is only available a draft and the whole IEC 61508 is not harmonised. The EN 954-1 is available as a harmonised standard. Therefore, standardisation committees for example in the type EEx “p” standard refer to EN 954-1 for validation. Even the committee for gas measurement systems do this.
The IEC 61508 needs for application a reliable database. There are several databases in use (Task 2, Task 4). Today no common database exists. Like in other standards for explosion protection, this common database must be established before certification can bases on IEC 61508 alone.

The authors do certification for some pressurized system controller according EN 954-1. The systems were suitable for application in category 3. Category 3 was recommend in an earlier draft for pressurised systems.

The controllers were also validated applying IEC 61508 - 2. Special attention was given to the dangerous undetected faults. The probability for dangerous undetected faults was calculated to give special information in the instruction if necessary. Two databases had been used ([22], [23]). The probability for failure in low demand mode of operation was low enough to fulfill safety integrity level 3. Because of a lack for proof testing the controllers are only suitable for a SIL 2 application (because of architectural constraints 61508 – 2, 7.4.5). This is the recommended SIL for pressurised system controller in Task 2. The result from EN 954-1 and IEC 61508 fits in this special application.

4.6 Independence for validation / conformity assessment procedures

IEC 61508 gives recommendation for level of independence for validation. This is shown in the following passage taken from the IEC 61508.

> *8.2.12 Unless otherwise stated in application sector international standards, the minimum level of independence of those carrying out the functional safety assessment shall be as specified in tables 4 and 5. The recommendations in the tables are as follows.*
>
> - *HR: the level of independence specified is highly recommended as a minimum for the specified consequence (table 4) or safety integrity level (table 5). If a lower level of independence is adopted then the rationale for not using the HR level should be detailed.*
> - *NR: the level of independence specified is considered insufficient and is positively not recommended for the specified consequence (table 4) or safety integrity level (table 5). If this level of independence is adapted then the rationale for using it should be detailed.*
>
> *-: the level of independence specified has no recommendation for or against being used.*
> *NOTE 1 Prior to the application of table 4, it will be necessary to define the resulting categories taking into account current good practices in the application sector. The consequences are those that would arise in the event of failure, when required to operate, of the E/E/PE safety-related systems.*
> *NOTE 2 Depending upon the company organisation and expertise within the company, the requirement for independent persons and departments may have to be met by using an external organisation. Conversely, companies which have internal organisations skilled in risk assessment and the application of safety-related systems, which are independent of*

and separate (by ways of management and other resources) from those responsible for the main development, may be able to use their own resources to meet the requirements for an independent organization.
NOTE 3 See 3.8.10, 3.8.11 and 3.8.12 of part 4 for definitions of independent person, independent department and independent organisation respectively.

8.2.13 In the context of tables 4 and 5, either HR[1] or HR[2] is applicable (not both), depending on a number of factors specific to the application. If HR[1] is applicable then HR[2] should be read as no requirement; if HR[2] is applicable then HR[1] should be read as NR (not recommended). If no application sector standard exists, the rationale for choosing HR[1] or HR[2] should be detailed. Factors that will tend to make HR[2] more appropriate than HR[1] are:

- *lack of previous experience with a similar design;*
- *greater degree of complexity;*
- *greater degree of novelty of design;*
- *greater degree of novelty of technology;*
- *lack of degree of standardisation of design features.*

8.2.14 In the context of table 4, the minimum levels of independence shall be based on the safety function, carried out by the E/E/PE safety-related system, that has the highest safety integrity level.

Minimum level of Independence	Safety integrity level			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	-	-	HR[2]	HR
NOTE See 8.2.12 (including notes), 8.2.13 and 8.2.14 for details on interpreting this table.				

Table 4 - Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9 - includes all phases of E/E/PES and software safety lifecycles (see Figure 3, Figure 5 and Figure 6))

IEC 61508 is not written to a special scope of application. The tables given by IEC 61508 part 1 have to change in respect to the regulations of 94/9/EC CHAPTER II Conformity assessment procedures, Article 8. Under the scope of the directive 94/9/EC, the table have to be divided into two parts, because the certification of electrical and non-electrical equipment is different ([1], Chapter II, Article 8)

Zone for which the EUC has been designed (ATEX category)	Zone of intended use (overall equipment category)		
	0 (1)	1 (2)	2 (3)
0 (1)	N/A	N/A	N/A
1 (2)	SIL2 [fault tolerance 0]	N/A	N/A
2 (3)	SIL3 [fault tolerance 1]	SIL2 [fault tolerance 0]	N/A
-	SIL4 [fault tolerance 2]	SIL3 [fault tolerance 1]	SIL1 [fault tolerance 0]

Table 5 - Target SIL determination for protection systems used in Hazardous Zones (Task 2 [11], Table 14)

In reference to the results of Task 2 the levels of independence are changed by the 94/9/EC to the two groups "notified bodies" and "manufactures". Therefore, the Table 4 changed to Table 6 and Table 7.

Zone of intended use (overall equipment category)	Safety integrity level			
	1	2	3	4
0 (1, M1)	-	Notified Body	Notified Body	Notified Body
1 (2, M2)	-	Notified Body	Notified Body	-
2 (3)	-	-	-	

Table 6 - Responsibility for conformity assessment procedure of safety devices in use with electrical equipment or internal combustion engines

Zone of intended use (overall equipment category)	Safety integrity level			
	1	2	3	4
0 (1, M1)	-	Notified Body	Notified Body	Notified Body
1 (2, M2)	-	Manufacturer	Manufacturer	-
2 (3)	-	-	-	

Table 7 - Responsibility for conformity assessment procedure of safety devices in use with non-electrical equipment

5 Summary

For the conformity assessment procedure, several standards are available. The most general standard is the IEC 61508. Because there is a large number of very different safety devices identified in Task 3 [13] it is important to take a general standard. This should be the IEC 61508, because this standards covers although the production and the use of electrical / electronic / programmable electronic systems. This is an important fact because for safety devices the two areas defined by the directives 94/9/EC [1] and 1999/92/EC [3] cannot be separated.

The IEC 61508 is open for the use of other standards for the validation of safety devices. This is even an important fact. For example, the EN 50 016 [16] recommends the use of the EN 954-1 for the validation of the used safety devices. This is done even in other standards or drafts [24].

The IEC 61508 can be regarded as a standard for the basic procedure and as "generic standard" for safety devices. In some cases "products standards" can be used if they are recommended from the specific standardisation committee. This is nearly the same principle like in the directive 89/336/EC for electromagnetic compatibility (“generic standards” 50082-xx together with test standards IEC 61000-4-xx and “product standards” with test standards IEC 61000-4-xx).

Common database is urgently needed (reliability of used components) for application of IEC 61508-2 in certification of safety devices. Without such a data base a certification in the scope of 94/9/EG in an equal safety level in different European countries cannot be achieved.

Furthermore today certification of safety devices is only possible according to harmonized standards like EN 954-1 or according to the directive 94/9/EC itself.

6 References

[1] Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, 394L0009

[2] ATEX Guidelines - Guidelines on the Application of Council Directive 94/9/EC of 23 March 1994 on the Approximation of the Laws of the Member States concerning Equipment and Protective Systems intended for Use in potentially explosive Atmospheres, Draft 3 February 1999

[3] Directive 1999/92/EC of the European Parliament and of the Council of 16 December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (15th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)

[4] IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems - Part 1: General requirements, 1998-12

[5] Draft IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[6] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 1998-12

[7] EN 954-1: 1997, Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design

[8] prEN 954-2:1998, Safety of machinery - Safety-related parts of control systems - Part 2: Validation

[9] EN 1441:1997 Medical devices - Risk analysis

[10] Draft EN xxxxx Explosives for civil uses - Detonators and relays , Part 27 Definitions, methods and requirements for electronic initiation systems

[11] Determination of safety categories of electrical devices used in potentially explosive atmospheres: Report on Task 1: Derivation of Target Failure Measures

[12] Determination of safety categories of electrical devices used in potentially explosive atmospheres: Report on Task 2: Assessment of Current Control System Standards, SAFEC project, Contract SMT4-CT98-2255, A. M. Wray, Engineering Control Group, Health & Safety Executive, 01/2000

[13] Determination of safety categories of Electrical devices used in Potentially Explosive Atmospheres: Report on Task 3:, Identification of “Used Safety Devices”, SAFEC project, Contract SMT4-CT98-2255, E. Conde, LABORATORIO OFICIAL MADARIAGA (LOM), November 1999

[14] Determination of safety categories of Electrical devices used in Potentially Explosive Atmospheres: Report on Task 4:, Study of “Used Safety Devices”, SAFEC project, Contract SMT4-CT98-2255, E. Faé, S. Halama, Institut National De L'Environnement Industriel Et Des Risques (INERIS), November 1999

[15] EN 50014:1999 Electrical apparatus for potentially explosive atmospheres - General requirements

[16] EN 50016:1995 Electrical apparatus for potentially explosive atmospheres - Pressurised apparatus "p"

[17] EN 50281-1-2:1999 Electrical apparatus for use in the presence of combustible dust - Part 1-2: Electrical apparatus protected by enclosure - Selection, installation and maintenance

[18] EN 60079-10:1996 Electrical apparatus for explosive atmospheres - Part 10: Classification of hazardous areas

[19] EN 60079-14:1997 Electrical apparatus for potentially explosive atmospheres - Electrical installations in hazardous areas (other than mines)

[20] EN 60079-17:1997 Electrical apparatus for potentially explosive atmospheres - Inspection and maintenance of electrical installations in hazardous areas (other than mines)

[21] prEN60079-19:1992 Installation of electrical apparatus in hazardous areas; Repair and overhaul for apparatus used in explosive atmospheres (other than mines)

[22] SN 29000 Teil 1 - 14, Ausfallraten Bauelemente, Erwartungswerte, Allgemeines, Siemens AG, 11.1991

[23] Reliability, Maintainability and Risk, Practical methods for engineers, David J. Smith, Butterworth Heinemann, Fifth Edition

[24] Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen; Requirements on the functional safety of fixed gas detection systems, First draft**,** 15.12.1999

[25] TC31-WG9, CENELEC, Electrical equipment for potentially explosive atmospheres, Reliability of safety-related devices, 1. Draft proposal 1999-xx-yy, 12/02/1999.