DETERMINATION OF SAFETY CATEGORIES OF ELECTRICAL DEVICES USED IN POTENTIALLY EXPLOSIVE ATMOSPHERES (SAFEC)

Contract SMT4-CT98-2255

FINAL REPORT

Co-ordinator: A J Wilday (Health and Safety Laboratory, UK)

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

Project duration: January 1999 – May 2000

Date of report: 10 July 2000

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:

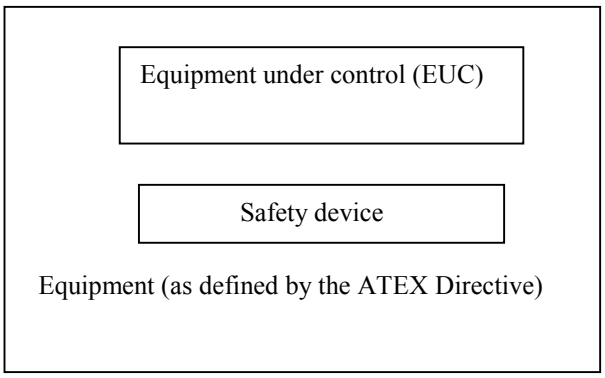
- Category 1 equipment is intended for use in Zone 0 and/or 20, where explosive atmospheres are present continuously, for long periods of time or frequently.

- 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).

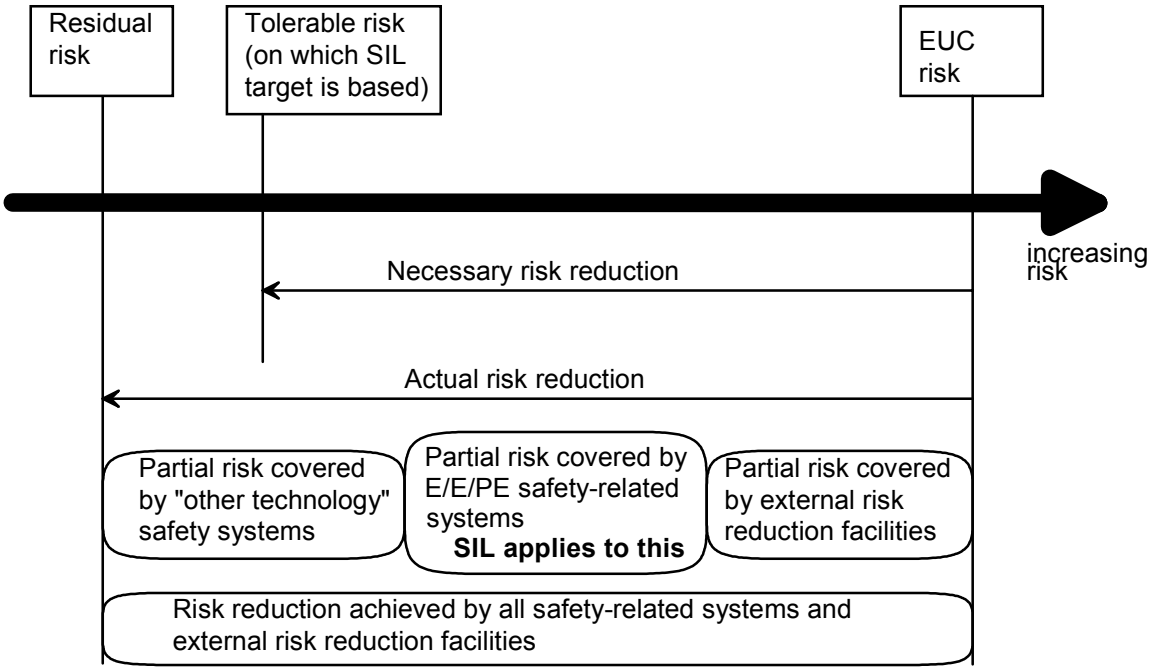


Figure 2 Risk concepts from IEC 61508

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.

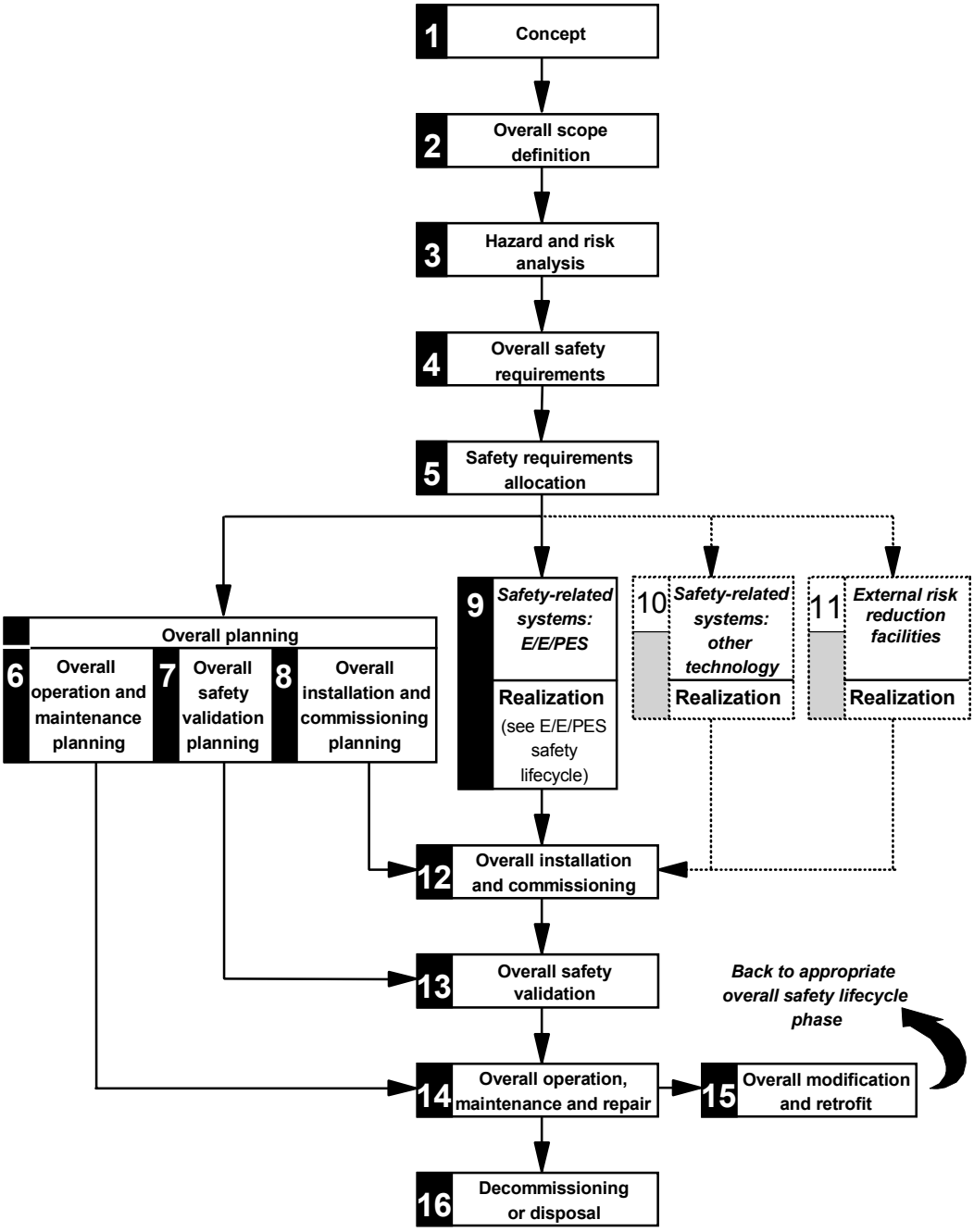
- The box 5 is mainly defined by existing standards for explosion protection (function) and Task 2 (safety integrity level).

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.

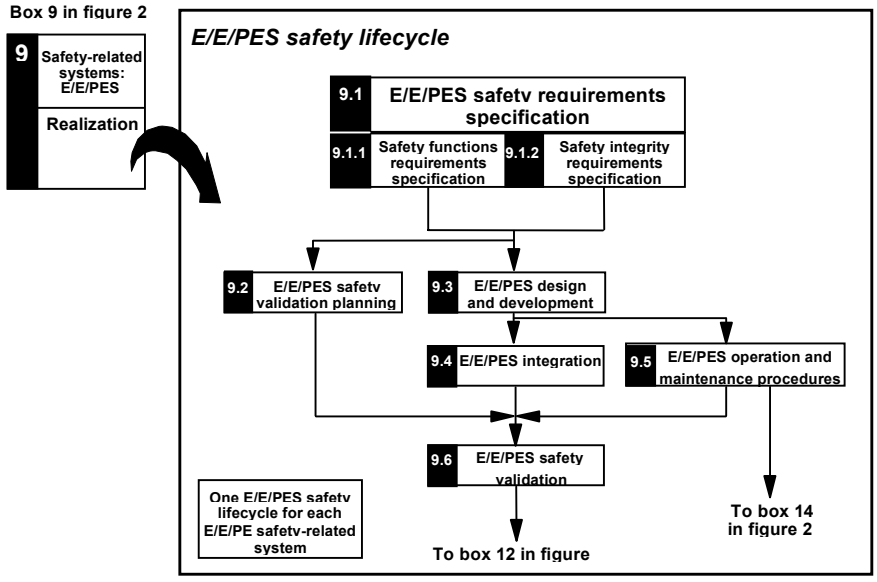


Figure A2 E/E/PES safety lifecycle (in realization phase)

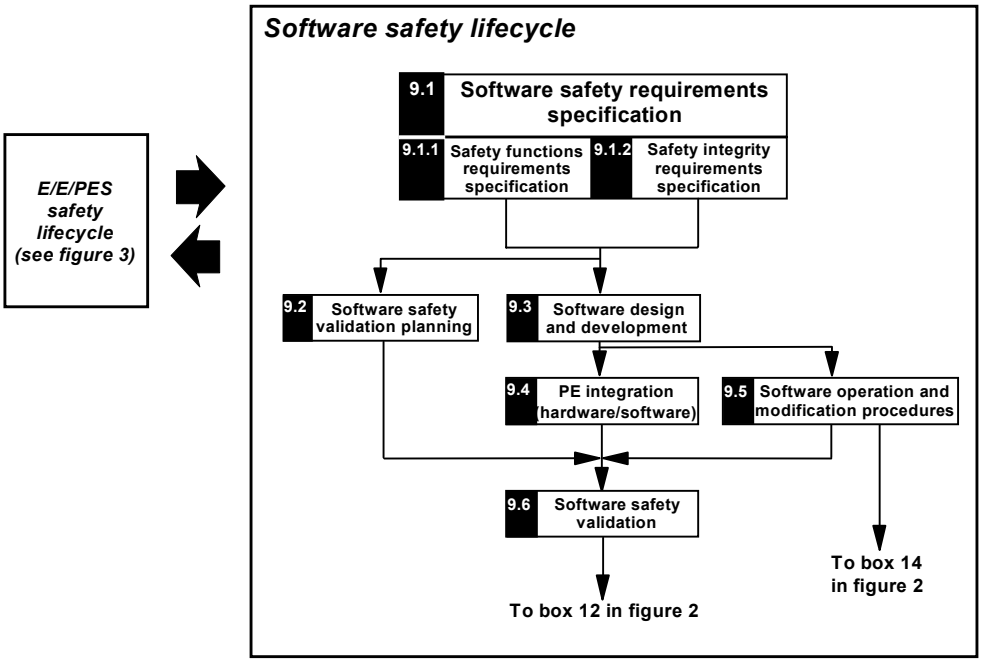


Figure A3 Software safety lifecycle (in realization phase)

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.

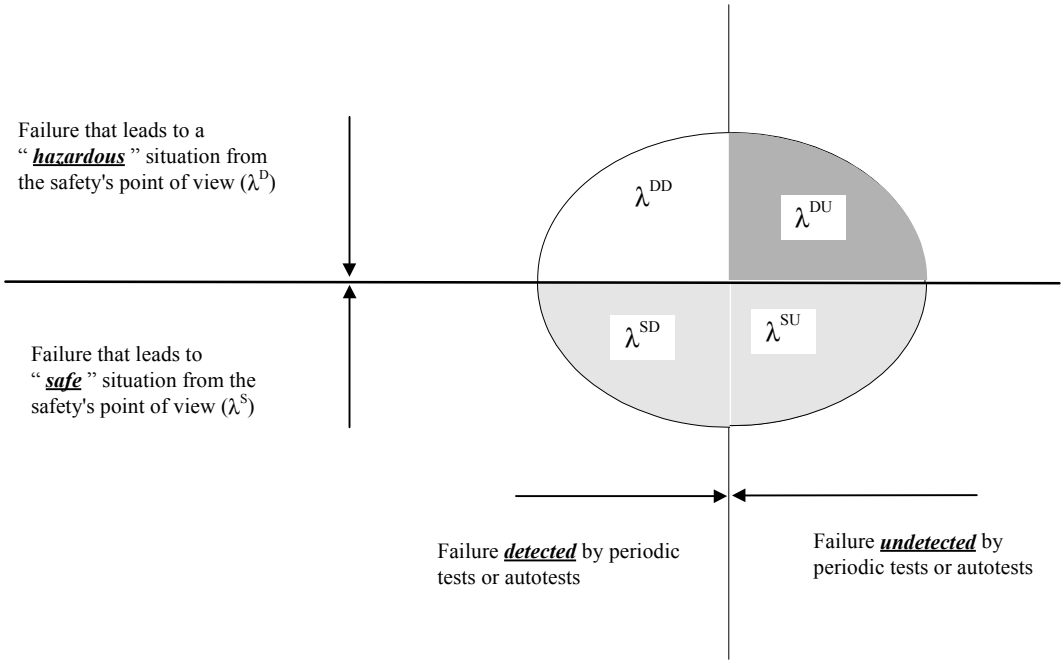


Figure A4 : Failure distribution according to their effect

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.

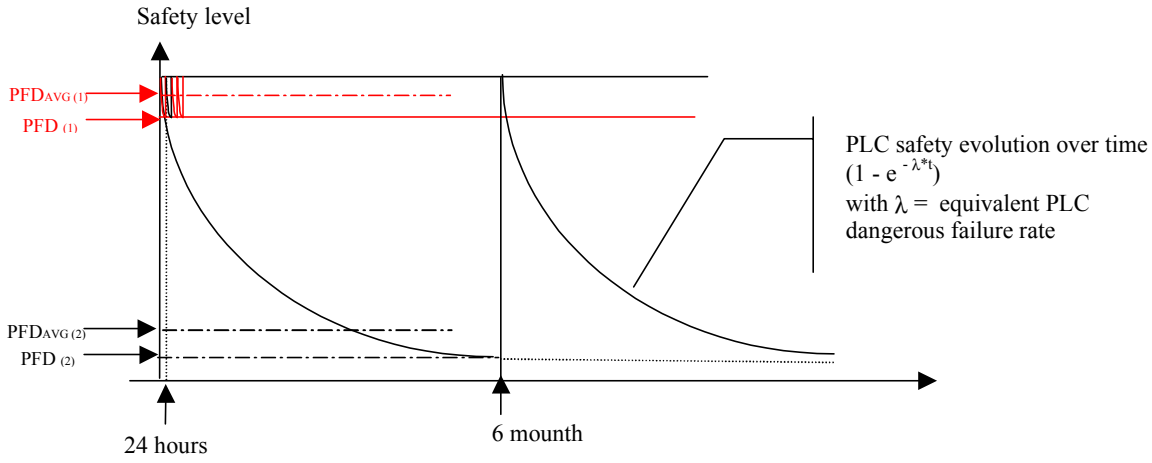


Figure A5 : Testability impact on safety

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

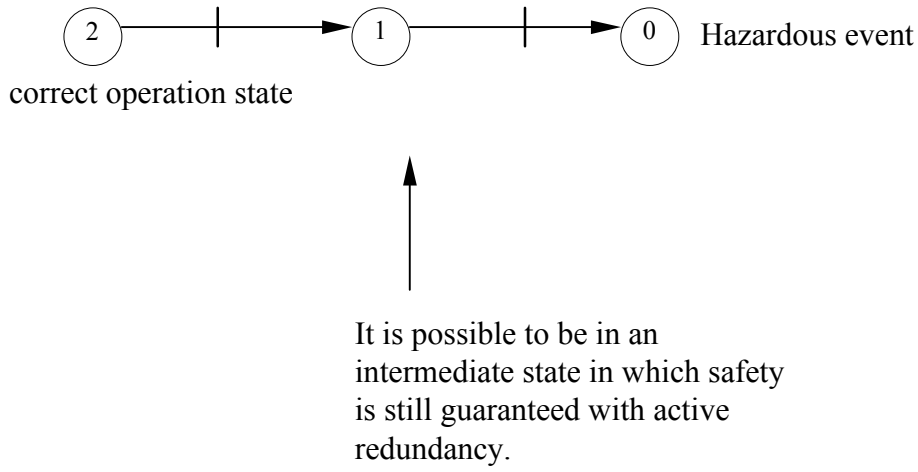


Figure A6 : Redundant system state modelling

This graph is equivalent to the following graph :

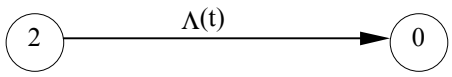


Figure A7 : Redundant system state reduced modelling

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.