ANNEX A

DERIVATION OF TARGET FAILURE MEASURES

Author: Jill Wilday
Health and Safety Laboratory

SUMMARY

OBJECTIVES

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

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

MAIN FINDINGS

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

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

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

MAIN RECOMMENDATIONS

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

1.1 Background

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

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

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

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

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

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

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

1.2 The SAFEC project

1.2.1 Objectives

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

The specific objectives are:

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

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

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

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

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

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

1.2.2 Project overview

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

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

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

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

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

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

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

Table 1 SAFEC Project Tasks

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

1.2.3 Scope

The scope of the SAFEC project is limited to:

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

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

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

1.3 Objectives of SAFEC Task 1

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

2. REQUIREMENTS OF ATEX DIRECTIVE

2.1 Categories of electrical equipment

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

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

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

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

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

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

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

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

2.2 Types of safety device

The ATEX Directive covers the following:

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

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

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

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

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

2.3 Specified failure measures

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

Table 2 Level of protection requirements of the ATEX Directive

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

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

3. CONCEPTS FOR TARGET FAILURE MEASURE

3.1 Types of target failure measure

The following types of target failure measure are possible.

3.1.1 Fault tolerance

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

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

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

3.1.2 Reliability

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

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

3.1.3 Quality control

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

3.2 Discussion

3.2.1 Problems with using fault tolerance alone

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

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

IEC 60601[22] states in Appendix A:

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

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

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

3.2.2 Types of target failure measure used in control standards

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

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

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

Table 3 Reliability requirements of IEC 61508

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

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

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

3.2.3 Requirements for testing, validation and certification

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

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

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

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

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

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

4.1 Description

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

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

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

In Table 4, it should be noted that:

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

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

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

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

4.2 Discussion

4.2.1 Assumed derivation of target failure measures

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

Thus in Table 4:

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

This is further illustrated by Figure 1.

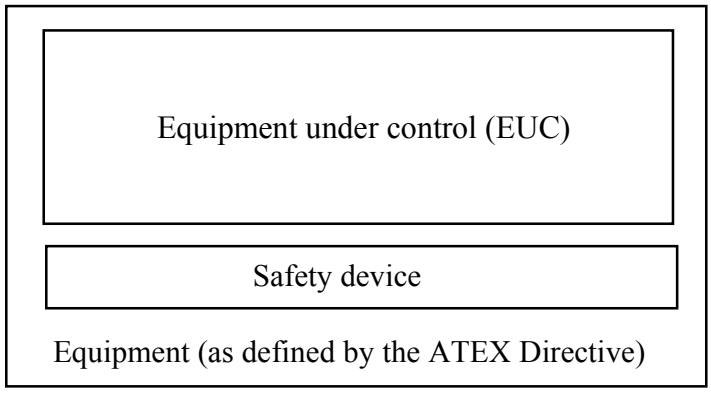

Figure 1 Definition of terms in Table 4

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

4.2.2 Comments

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

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

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

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

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

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

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

5. TARGET FAILURE MEASURES IN TERMS OF RISK

5.1 Introduction

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

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

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

5.2 Review of major hazard risk criteria

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

5.2.1 UK individual risk criteria

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

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

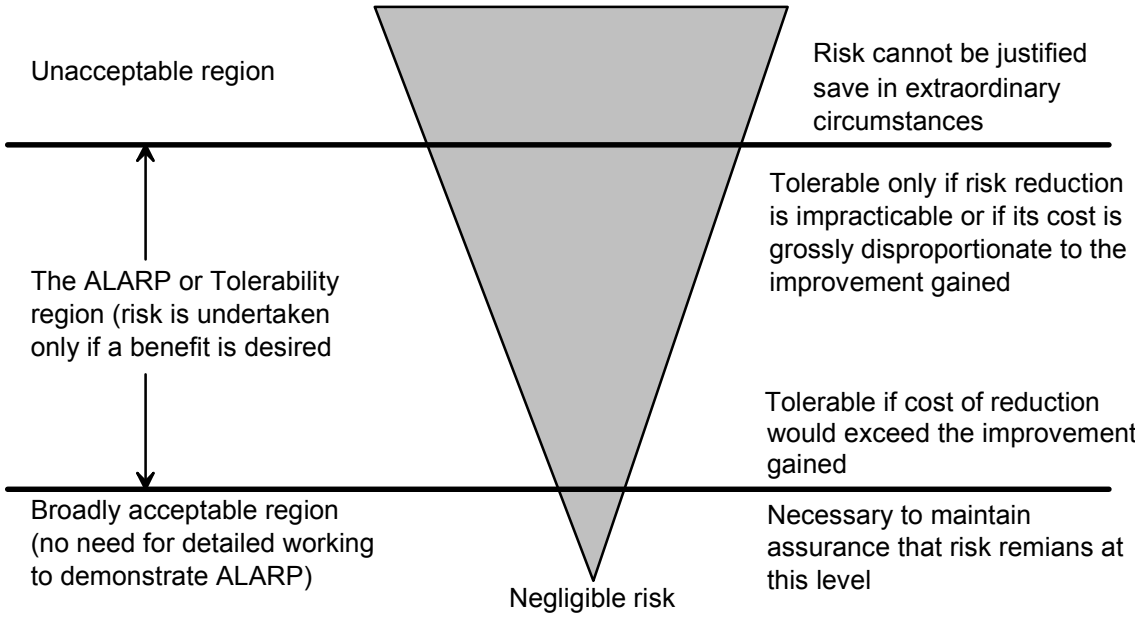

Figure 2 HSE framework for risk tolerability

5.2.2 Netherlands societal risk criteria

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

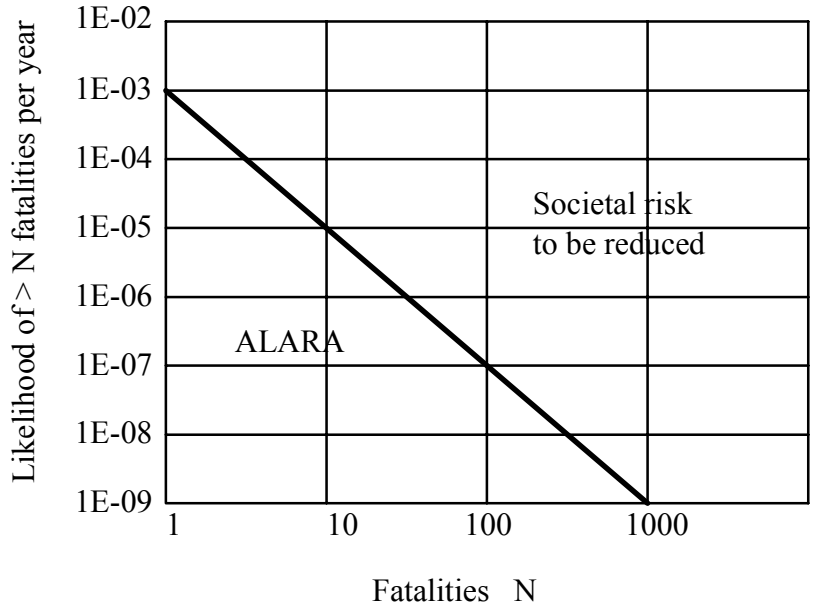

Figure 3 Netherlands societal risk criteria

5.2.3 "Short-cut risk assessment" criteria

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

5.2.4 Criteria used in development of IEC 61508

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

Table 5 Short-cut risk assessment criteria

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

5.2.5 Discussion

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

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

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

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

5.3 Generic fault tree for ignition of potentially flammable atmosphere

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

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

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

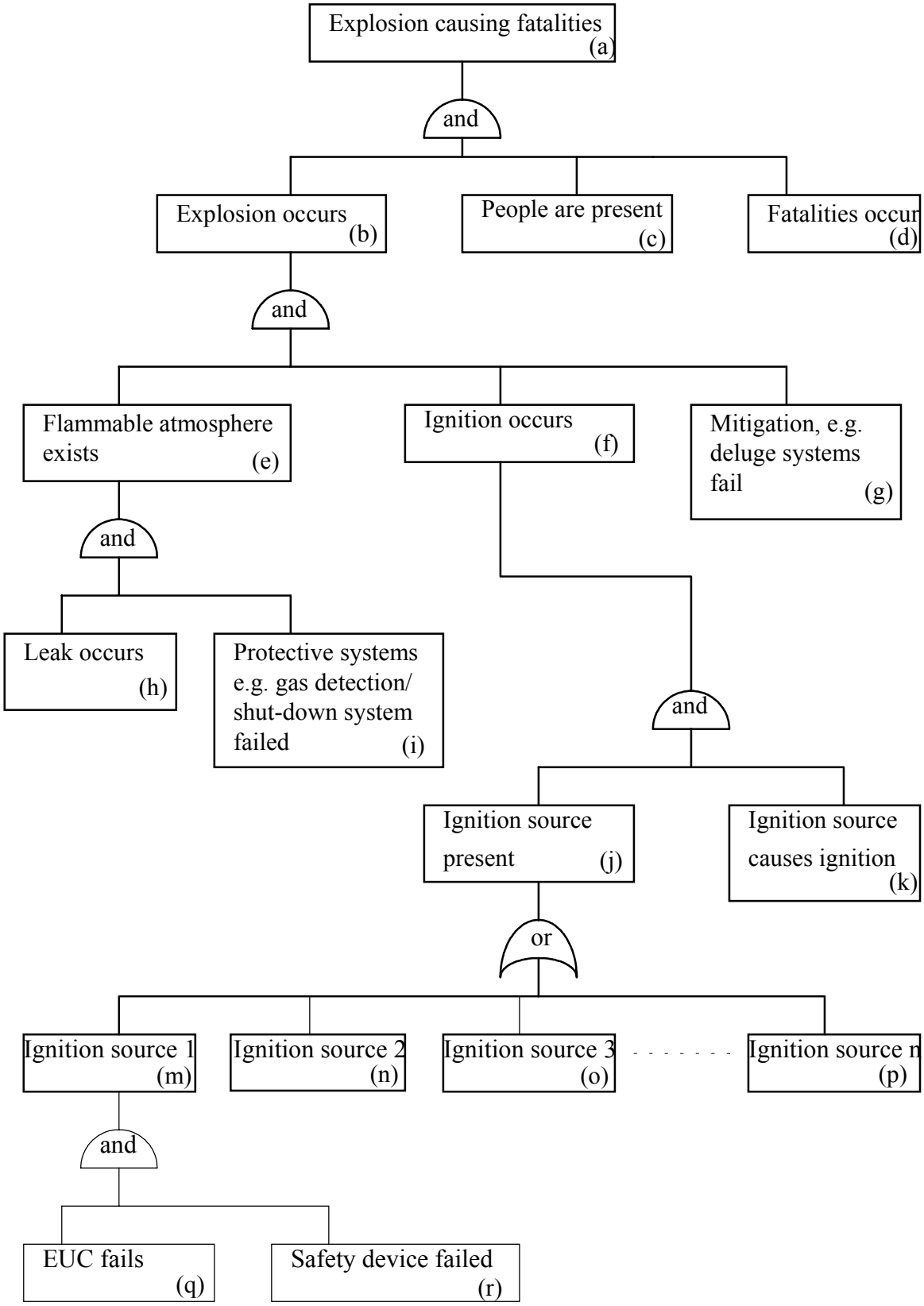

Figure 4 Generic fault tree for explosion

Table 6 Worst case assumptions about data for fault tree

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

5.4 Comparison with TC31/WG09 proposals

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

5.4.1 Zone 2 with fault tolerance of -1

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

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

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

The resulting frequency of an explosion =

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

5.4.2 Zone 1 with fault tolerance of -1

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

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

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

The resulting frequency of an explosion =

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

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

5.4.3 Discussion

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

Two other observations can be made:

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

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

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

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

6. ALTERNATIVE METHODS OF DECIDING SAFETY DEVICE SAFETY INTEGRITY LEVEL

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

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

7. CONCLUSIONS

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

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

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

8. RECOMMENDATIONS

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

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

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

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

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

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

9. REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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