ANNEX B

ASSESSMENT OF CURRENT CONTROL SYSTEM STANDARDS

Author: A M Wray PhD
Health and Safety Laboratory

SUMMARY

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

OBJECTIVES

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

MAIN FINDINGS

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

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

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

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

CONTENTS

1 Introduction B4
2 An interpretation of the ATEX Directive requirements B4
2.1 The ATEX requirements B5
2.1.1 ANNEX I (Classification of categories) B5
2.1.1.1 Equipment-group I - Category M1 .... B5
2.1.1.2 Equipment-group I - Category M2 .... B5
2.1.1.3 Equipment-group II - Category 1 .... B5
2.1.1.4 Equipment-group II - Category 2 .... B6
2.1.2 ANNEX II (Equipment requirements) B6
2.1.2.1 Requirements in respect of safety-related devices B6
2.1.2.2 Category M1 of equipment-group I B7
2.1.2.3 Category 1 of equipment-group II B8
2.1.2.4 Category 2 of equipment-group II B8
2.2 Summary of the requirements B9
2.3 Discussion of the requirements B9
3 Comments on the TC31/WG9 proposal (Reference 2) B11
4 Comments on the available standards B13
4.1 BS EN 954-1 (Reference 3) B13
4.2 IEC 61508 (Reference 4) B15
4.3 Summary of the standards with respect to the ATEX Directive B15
5 The target SIL for systems used in Hazardous Zones B17
5.1 Probability of an explosive vapour being present B19
5.2 Determination of the ALARP level of risk B20
5.2.1 From individual risk B20
5.2.2 From accident records B22
5.2.3 From an examination of a protection system B24
5.2.3.1 Component failure analysis of the generic system B26
5.2.3.2 Quantitative analysis: Function 1 .... B28
5.2.3.3 Quantitative analysis: Function 2 .... B31
5.2.4 ALARP level of risk: summary B34
6 Conclusions B35
7 References B36
8 Acknowledgements B36

Annex A The essential principles of IEC 61508 .... B37

1 Introduction

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

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

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

The author will then carry out calculations based on:

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

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

2 An interpretation of the ATEX Directive requirements

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

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

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

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

2.1 The ATEX requirements

2.1.1 ANNEX I (Classification of categories)

2.1.1.1 Equipment-group I - Category M1

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

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

2.1.1.2 Equipment-group I - Category M2

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

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

2.1.1.3 Equipment-group II - Category 1

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

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

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

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

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

2.1.1.4 Equipment-group II - Category 2

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

The author interprets this to mean that:

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

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

2.1.2 ANNEX II (Equipment requirements)

2.1.2.1 Requirements in respect of safety-related devices

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

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

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

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

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

This rather ambiguous requirement could imply:

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

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

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

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

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

The meaning of this requirement is not fully clear.

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

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

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

2.1.2.2 Category M1 of equipment-group I

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

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

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

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

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

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

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

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

2.1.2.3 Category 1 of equipment-group II

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

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

See the comments at 2.1.2.2.

2.1.2.4 Category 2 of equipment-group II

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

The author interprets this to mean that:

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

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

2.2 Summary of the requirements

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

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

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

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

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

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

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

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

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

2.3 Discussion of the requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1: The table in Section 4 of Reference 2

Hazardous area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Equipment (EUC) Fault tolerance	2	1	0	1	0	- 1.00[1]	0	-1
Safety category of monitoring or control unit	-	SIL2[2]	SIL3	-	SIL2	SIL3	-	SIL2
Resulting equipment category[34] of the combination	Category M1/1			Category M2/2			Category 3	

[1] ignition sources under normal operation

[2] according to IEC 61508

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

[4] comment:

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

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

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

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

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

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

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

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

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

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

4 Comments on the available standards

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

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

These will now be discussed.

4.1 BS EN 954-1 (Reference 3)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2 IEC 61508 (Reference 4)

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

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

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

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

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

4.3 Summary of the standards with respect to the ATEX Directive

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 The target SIL for systems used in Hazardous Zones

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

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

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

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

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

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

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

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

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

Hence, the table requires calibration.

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

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

It will be noted in Table 3 that:

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

5.1 Probability of an explosive vapour being present

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

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

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

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

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

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

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

Table 4: Probability of an explosive vapour being present

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

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

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

5.2 Determination of the ALARP level of risk

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

5.2.1 From individual risk

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

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

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

Notes to Table 5:

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

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

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

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

It will be seen that:

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

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

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

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

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

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

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

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

5.2.2 From accident records

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

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

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

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

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

Notes to Table 6:

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

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

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

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

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

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

The author understands that pressurization systems are used:

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

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

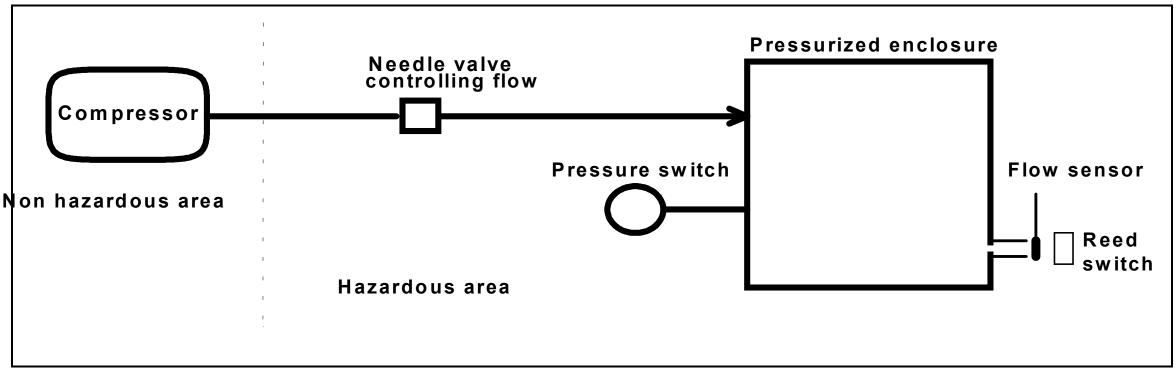
5.2.3 From an examination of a protection system

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

Design of the generic system

The system to be considered is shown in Figure 1.

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



The design shown in Figure 1 is such that:

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

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

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

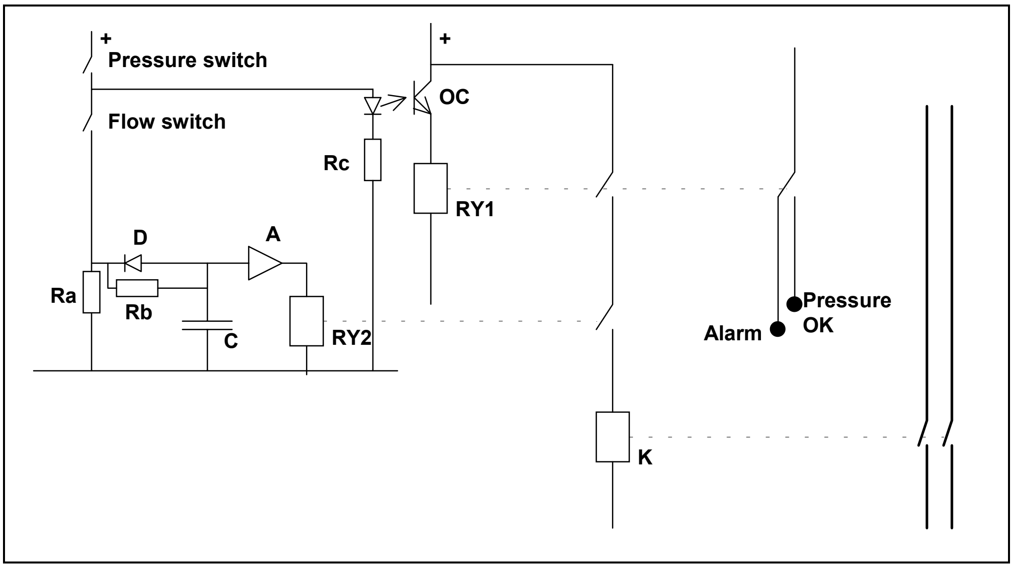
- the air pressure from the compressor;
- the setting of the needle valve, and
- the orifice plate or other constriction on the outlet of the enclosure.

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

5) the compressor is outside the hazardous zone.

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

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



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

The circuit in Figure 2 shows that:

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

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

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

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

Therefore, the system carries out two functions:

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

5.2.3.1 Component failure analysis of the generic system

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

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

Table 7: Dangerous component failures of the generic design

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

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

5.2.3.2 Quantitative analysis: Function 1

The failure rate of Function 1 will now be considered.

Table 8: Determination of failure rate of the shutdown circuit

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

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

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

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

Table 9: Determination of rate of air-loss events

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

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

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

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

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

Table 10: Determination of the hazard rate associated with Function 1

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

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

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

5.2.3.3 Quantitative analysis: Function 2

Table 11: Determination of failure rate of purging-delay function

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

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

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

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

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

Table 13: Changes required to achieve a rate of death of 10^{-5}/year[4]

PFD[3] of the pressurization system	2.7	0.27	0.03	0.27	0.03	0.003	0.003	* 10^{-3}
SIL equivalent to the row above.	SIL2	SIL3	SIL4	SIL3	SIL4	>SIL4	>SIL4	
Probability[5] of cabinet being opened when flammable gas is present	1.4			0.14			0.014	%

Notes to Tables 12 and 13

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

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

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

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

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

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

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

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

The apparent freedom from explosions suggests that existing systems, as represented by the generic design considered in this report, provide an adequate level of safety. This suggests that factors which have not been taken into account in the calculations shown in Table 12 are providing additional means of protection. Such factors could include the human element (i.e., avoidance of opening a pressurized enclosure if gas is smelled) being significantly better than has been assumed, additional data that are being provided by additional sensors being heeded or the probability of a spark, being generated by equipment considered to be continuously sparking, being less than one.

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

5.2.4 ALARP level of risk: summary

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

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

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

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

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

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

8) Pressurization systems are currently used:

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

- to protect Zone 2-type equipment in Zone 1. In this case, if pressurization were to fail, an alarm is given. The generic shutdown system discussed in Section 5.2.3, could in practice achieve SIL2 as shown in Table 2 for this type of use.

- to protect continuously sparking equipment in Zone 2. In this case, if pressurization were to fail an alarm is given. The generic shutdown system discussed in Section 5.2.3, could be used to sound an alarm which could achieve SIL2 as shown in Table 2 for this type of use.

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

- the reliability of the air supply, in the case of the shutdown function, and

- the required frequency of purging, in the case of the purging function.

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

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

6 Conclusions

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

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

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

Table 14: Target SIL determination and fault tolerance requirements for protection systems used in Hazardous Zones

Zone for which the EUC has been designed (ATEX category)	Zone of intended use (overall equipment category)		
	0 (1)	1 (2)	2 (3)
0 (1)	N/A	N/A	N/A
1 (2)	SIL2 [0]	N/A	N/A
2 (3)	SIL3 [1]	SIL2 [0]	N/A
-	SIL4 [2]	SIL3 [1]	SIL1 [0]

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

7 References

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

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

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

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

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

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

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

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

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

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

8 Acknowledgements

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

ANNEX A

The essential principles of IEC 61508

by

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

Background

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

Introduction

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

Scope of IEC 61508

The scope of IEC 61508 is safety-related systems based on electrical / electronic / programmable electronic technology. In broad terms, a safety-related system can be considered to be any system which carries out a safety function so as to prevent, or mitigate, a hazardous situation. The original focus of the standard was on systems based on programmable electronic technology, which tend to be complex in the sense that they are likely to have a multitude of failure modes and their freedom from designed-in, or systematic, faults cannot be proven by testing alone. It is therefore necessary to take a methodical approach at every stage of the lifecycle to minimise, as far as possible, the introduction of such systematic faults. The uncertainty associated with the failure characteristics of programmable systems means that it is not usually appropriate to rely solely on the more traditional “fail-safe”, or fault tolerance approach to safety design.

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

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

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

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

Essential principles of IEC 61508

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

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

This is necessary to ensure that all activities relating to functional safety are carried out as planned, with a clear record of the ‘inputs’ and ‘outputs’ at each phase of the lifecycle. This enables the processes of verification (checking the outputs of each phase are as intended) and validation (checking that the end result is consistent with the specified requirements). This is particularly aimed at minimising the number of systematic faults built into the safety-related system. Given that, with low-complexity systems, systematic faults are likely to be self-evident, or are revealed during testing, it is thought that a formalised safety-lifecycle framework would not be a beneficial (or indeed profitable) approach to the development of a low complexity system.

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

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

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

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

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

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

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

The aim is, as far as possible, to avoid any design faults which could lead to dangerous failures during use of the equipment. This is particularly important for complex systems, and for software. In the main, the techniques and measures recommended by IEC 61508 in this respect are those of what would be regarded as good engineering practice. For example, use of guidelines and standards, project management, documentation, structured specification & design. Equipment which has been adequately ‘proven-in-use' in accordance with IEC 61508-2, does not need to be compliant with these requirements.

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

These requirements are particularly aimed at programmable electronic systems where it is possible to incorporate design features (such as program sequence monitoring by use of watchdog timers) that make the equipment tolerant against residual design faults in both hardware and software and operator mistakes. These requirements would not usually be applicable to low complexity, non-programmable systems. Equipment which has been adequately 'proven-in-use' in accordance with IEC 61508-2, does not need to be compliant with these requirements.

g) Requirements for system behaviour on detection of a fault (IEC 61508-2)

These requirements specify the action that should taken following detection of a fault in the safety-related system. Faults may be detected by diagnostic tests, proof tests or by any other means. The aim is to ensure continued safe operation. If that is not possible, then the equipment should be shutdown to a safe state. The requirements are applicable whatever the level of complexity of the safety-related system, and to electrical or electronic or programmable electronic systems.

Conclusions

The following requirements of IEC 61508 are considered to be applicable whatever the level of complexity, and whether the technology is electrical, electronic or programmable electronic:

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

- *Limitation of SIL of safety functions according to hardware fault tolerance (redundancy) (IEC 61508-2)*

- *Quantified estimation of probability of failure of safety functions based on the reliability of the hardware of the safety-related system. (IEC 61508-2)*

- *Requirements for system behaviour on detection of a fault (IEC 61508-2)*

The other requirements of IEC 61508 are aimed at minimising the likelihood of systematic faults and are particularly applicable when programmable electronic technology is used. For low complexity, non-programmable technology, it is considered that no more than good engineering practice would be required to satisfy these requirements.