Annex E

Determination of a methodology for testing, validation and certification

Partner: Deutsche Montan Technologie GmbH
Fachstelle für leittechnische Einrichtungen mit Sicherheitsverantwortung
Beylingstr. 65, D - 44329 Dortmund

Authors: Dr. Franz Eickhoff
Dr. Michael Unruh

Content

Figures and Tables

1 Introduction

1.1 Working task

This working task is a part of the research project SMT4-CT98-2255 Determination of safety categories of electrical devices used in potentially explosive atmospheres. The task has the following content:

- **Task 5: Determination of a methodology for testing, validation and certification**
  A methodology allowing the testing, validation and certification of safety devices shall be developed. This shall take into account the target failure measures developed in Task 1, the currently available standards assessed in Task 2 and the 'used safety devices' identified in Task 3. A preliminary report with proposals for standardization shall be produced at the end of this task. This report shall be distributed for comments to users, manufacturers and experts involved in European standardisation groups from at least 6 EU countries. Comments received shall be considered in the final report produced in Task 6.

1.2 Definition of safety devices and applicable technologies

The aim of this task is the development of a procedure for certification of safety-related systems or safety devices used in the area of explosion protection.

The first problem is to identify safety devices. The definition of the ATEX Guidelines [2] may be helpful and shall be used for further definitions.

> ***"4.1.2Which kinds of products are covered by directive 94/9/EC?***
> *To be within the scope of the directive, a product has to be:*
> ***equipment**, as defined in Article 1.3.(a); or*
> *a **protective system**, as defined in Article 1.3.(b); or*
> *a **component**, as defined in Article 1.3.(c); or*
> ***a safety, controlling or regulating device** as defined in Article 1.2.*
> .....
> *d) Safety, controlling or regulating devices as defined in Article 1.2.*
> *The two main issues of Article 1.2 are,*
> *i) that **safety devices**, **controlling devices** and **regulating devices**, if they contribute to or are required for the safe functioning of equipment or protective systems with respect to the risks of explosion are **subject to the directive**;*
> *ii) that devices are covered **even if** they are situated **outside the potentially explosive atmosphere**.*
> *For such devices, the essential requirements shall only be applied so far as they are necessary for the **safe and reliable** functioning and operation of those devices with respect to the risk of explosion (ANNEX II, Preliminary observation B)*
> *The **definition** in i) leads to the following consequences:*
> *1. Devices other than safety, controlling and regulating devices are not covered. (However, a device of any kind, contributing to or required for the safe functioning, could be considered a safety device);*
> *2. **All devices**, including safety, controlling and regulating devices**, neither contributing** to **nor required** for the safe functioning with **respect to the explosion risk are not covered**;*

*3. Even **safety, controlling and regulating devices** contributing to or required for the safe functioning but **with respect to risks other than the explosion risk are not covered;***

For further illustration some examples:
*Examples for **devices falling under Article 1.2:***

- *A power supply feeding an intrinsically safe (EEx i) measurement system used for monitoring process parameters;*
- *A pump, pressure regulating device, backup storage device, etc. ensuring sufficient pressure and flow for feeding a hydraulically actuated safety system (with respect to the explosion risk);*
- *Overload protective devices for electric motors of type of protection EEx e 'Increased Safety';*
- *Controllers, in a safe area, for an environmental monitoring system consisting of gas detectors distributed in a potentially explosive area, to provide executive actions if dangerous levels of gas are detected;*
- *Controllers for sensors temperature, pressure, flow, etc, located in a safe area, for providing information used in the control of electrical apparatus, used in production or servicing operations in a potentially explosive area;*

*Examples for **devices not falling under Article 1.2:***

- *Switchgear, numeric controllers, etc. not related to any safety functions (with respect to the explosion risk); because of 2) above;*

***Item ii)** states that devices, as defined above, are subject to the directive, even when outside the potentially explosive atmosphere.*
For safety and economic reasons it will be preferable in most cases to install such devices in a non-hazardous area. However, sometimes it might be necessary to place such devices within a potentially explosive atmosphere. In such cases, although the directive does not explicitly say so, these devices can also be designated as equipment. Two situations can be identified:

- *If the device has its **own potential source of ignition** then, in addition to the requirements resulting from Article 1.2, the **requirements for equipment** will apply;*
- *If the device does not have its own potential source of ignition then the device will not be regarded as equipment but of course the requirements resulting from Article 1.2 will still apply."*

1.2.1 Conclusions from the ATEX-Guidelines

The main identification aspect for a safety device is the **autonomous function** for avoiding explosion risk. A thermal fuse is therefore a safety device. The certification scheme theoretically has to be applicable to these simple safety devices. However, is makes no sense to use it for simple safety devices. There are already standards available for these devices. Therefore, the certification scheme is mostly used for complex safety devices (see examples for safety devices [2]), but must have no contradiction to available standards for simple safety devices. This is mentioned in the work of TC 31 WG 09. A reference table is prepared to define the safety devices not covered by available standards based on Task 3 of this research project [13].

- **The certification scheme has to be applicable to simple and complex safety devices. The certification scheme is used more for complex safety devices or safety systems.**

The certification scheme for the functional safety of safety devices is independent on the certification scheme for the safety against potential ignition sources if the safety device is also in the scope of the RL 94/9/EC as equipment. This is in general the same situation for gas measurement systems, for protection systems and safety devices:

a) they can be equipment if the scope of the 94/9/EG,
b) they can have a safety function in the scope of 94/9/EG.

- **The two items can have strong relations to each other, but they have different features. In the scope of this research project is only feature b).**

A safety device can be based on several different technologies. The construction principle may be electrical / electronic or programmable electronic. In addition, mechanic, pneumatic, hydraulic and other technologies may be used.

- **Example for different technologies**
  A standard thermal protection relay used for the protection of type EEx „e“ – engines consists of a bimetal heating systems and several mechanical elements. The mechanical components are responsible for the triggering of the relay if one phase is disconnected. The function and the reliability of the overload relay also depend on mechanical components. The application for example of IEC 61508 part 2 is not possible in that case.

There must be a distinction between the certification scheme and the applicable standards for different technologies. The two standards EN 954-1 and IEC 61508 may not be the only standards for assessment.

- **The certification scheme has to be open to different technologies.**

The certification scheme is mainly used for the certification of products in the scope of 94/9/EC. The products are used under the scope of the 1999/92/EC directive [3]. Aspects of the safe use of products may be taken into account in the certification scheme if these technical aspects are different from existing standards for the use of explosion protected equipment.

- **The certification scheme has assessed the equipment to the ESR of the 94/9/EG. The scheme has to give the required information for the safe use under the directive 1999/92/EC.**

2 Requirements

2.1 Requirements of directives 94/9/EC and 1999/92/EC

The technical requirements (essential safety requirements ESR) of 94/9/EC are included in ANNEX II [1]. These requirements are based on existing technical standards for explosion protection in group I and group II. The ESR are not fully described in the directive. The authors take the existing standards for explosion protection into account. Many aspects seem to be open but most times written clearly in the standards for explosion protection (ANNEX 13 of [2]).

The aspects of using the products are defined in directive 1999/92/EC [3]. It is the instruction which is the link between the manufacturer and the user. Therefore, the instructions are given an important role. (ANNEX II of [1]):

> *"1.0.6. Instructions*
> *(a) All equipment and protective systems must be accompanied by instructions, including at least the following particulars:*
> *- a recapitulation of the information with which the equipment or protective system is marked, except for the serial number (see 1.0.5.), together with any appropriate additional information to facilitate maintenance (e.g. address of the importer, repairer, etc.);*
> ***- instructions for safe:***
> ***- putting into service,***
> ***- use,***
> ***- assembling and dismantling,***
> ***- maintenance (servicing and emergency repair),***
> ***- installation,***
> ***- adjustment;***
> *- where necessary, an indication of the danger areas in front of pressure-relief devices;*
> *- where necessary, training instructions;*
> ***- details which allow a decision to be taken beyond any doubt as to whether an item of equipment in a specific category or a protective system can be used safely in the intended area under the expected operating conditions****;*
> *- electrical and pressure parameters, maximum surface temperatures and other limit values;*
> ***- where necessary, special conditions of use, including particulars of possible misuse which experience has shown might occur;***
> *- where necessary, the essential characteristics of tools which may be fitted to the equipment or protective system."*

The instruction also is mentioned in the new EN 50014 [15].

With existing standards for explosion protection, therefore products are certified with a view to existing standards for installation, maintenance, repair etc., and the use. The information link between the manufacturer and the user is the instruction.

A certification scheme for safety devices has to assess the required safety. Furthermore the certification scheme has to include all the information for instruction for safe, etc. ... and special details necessary to decide about the users application.

- **Example:**
  A safety device is certified that it can be used in an application with SIL 4. In this special application the safety device needs a manual periodic test every day. It cannot be used normally in explosion protection with standard test rates / maintenance rates. There has to be some information about proof intervals and maintenance rates if they are different from common used rates.

If this is not possible for the application of the equipment, every parameter for diagnostics, periodic test etc. has to be defined in the certification under worst conditions and given to the user in the instruction to make sure that the equipment is used in a safe way and the necessary risk reduction is achieved in practical use for every application.

2.2 Summary of demands from 94/9/EC and 1999/92/EC

The certification for functional safety of safety devices has to assess the safety requirements. The certification has to distinguish all relevant parameters for the instruction given to the user.

3 Selection of concept for certification

Three possible concepts for certification are compared:
- A concept independent from technologies and application.
- A concept based on a hierarchical structure of standards (A-, B- and C-type standards).
- A concept based on a life cycle structure.

For these different concepts examples are given. The advantages and disadvantages are pointed out.

3.1 Concept of EN 1441 [9]

The EN 1441 is based on a basic risk assessment scheme (see Figure 1, an example taken from [10]).

The hazards in the steps for example are hardware or software faults or even wrong handling in several situations like manufacturing, transportation, storage and use. For every product, all the possible hazards can be identified systematically. Special applications can be taken into account. The result is a hazard list for the product. New products have to fulfil this list.

The scheme is open to every application, but the result will be very special to one type of product. It is an advantage for the use with medical products. The advantage for the application to electronic detonators was shown in a CEN working group [10]. A result which is special for one kind of product is the main disadvantage for the application to the wide range of safety devices.

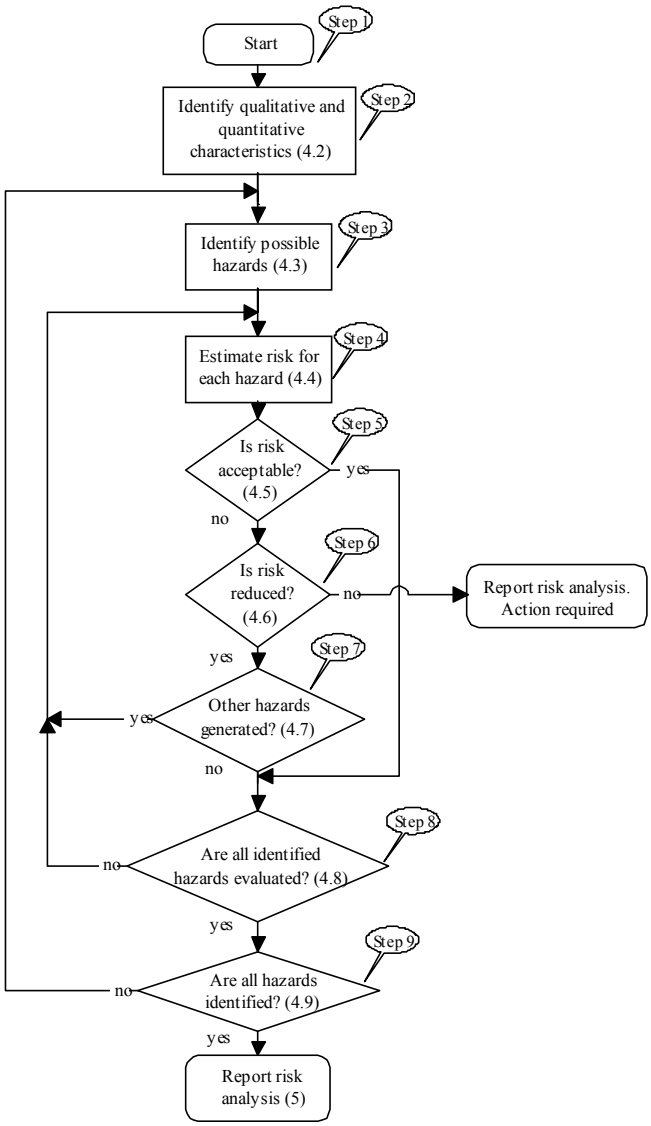


Figure 1 Risk assessment and test scheme based on EN 1441

3.2 Concept of harmonised standards under the scope of directive 98/37/EC

The harmonised standards related to 98/37/EC are separated in three levels:
- A-Type: General principles, e. g. EN 1050 Risk assessment,
- B-Type: Basic principles, e. g. EN 954-1 Safety related parts of control system [7],
- C-Type: standards for special products.

These standards are based on the application to machinery. The application of one standard has to take into account several other standards.

EN 954-1 is commonly used with EN 1050 together. Furthermore, some product standards are applicable for a special product. Some of the problems with application of EN 954-1 described in Task 2 are based on this concept of breaking up the standard.

The main advantage of these standards is the application to many technologies; the main disadvantage is that these standards are not applicable to programmable systems.
There is another disadvantage, which should not be missed: the standards are written as standards for manufactures. The standards like EN 954 -1 normally give no information about installation, maintenance and repair (see Task 2 [11]). The intended use of the product is covered by the risk analysis of the manufacturer. The manufacturers have to give this information for safety use to the user below 98/37/EC as if they have to give it below 94/9/EC. This is not especially written in the standards. The manufactures have to do give all relevant information to the user.

3.3 Concept of IEC 61508

IEC 61508 is the counterpart of several harmonized standards in comparison to the harmonised standards of directive 98/37/EC. The main disadvantage of the standard seems to be the possibility of application only to electric, electronic and programmable electronic systems. This is wrong. It is possible to distinguish in IEC 61508 two main parts:

a) The systematic description for the overall life cycle of a system not depending on a specific technology.
b) The description of requirements based on safety integrity level (SIL) for electric / electronic / programmable electronic safety-related systems.

For an overview see Figure 2.The part a) is located in the part 1 of IEC 61508. The part b) is included in part 2 - 7 of IEC 61508.

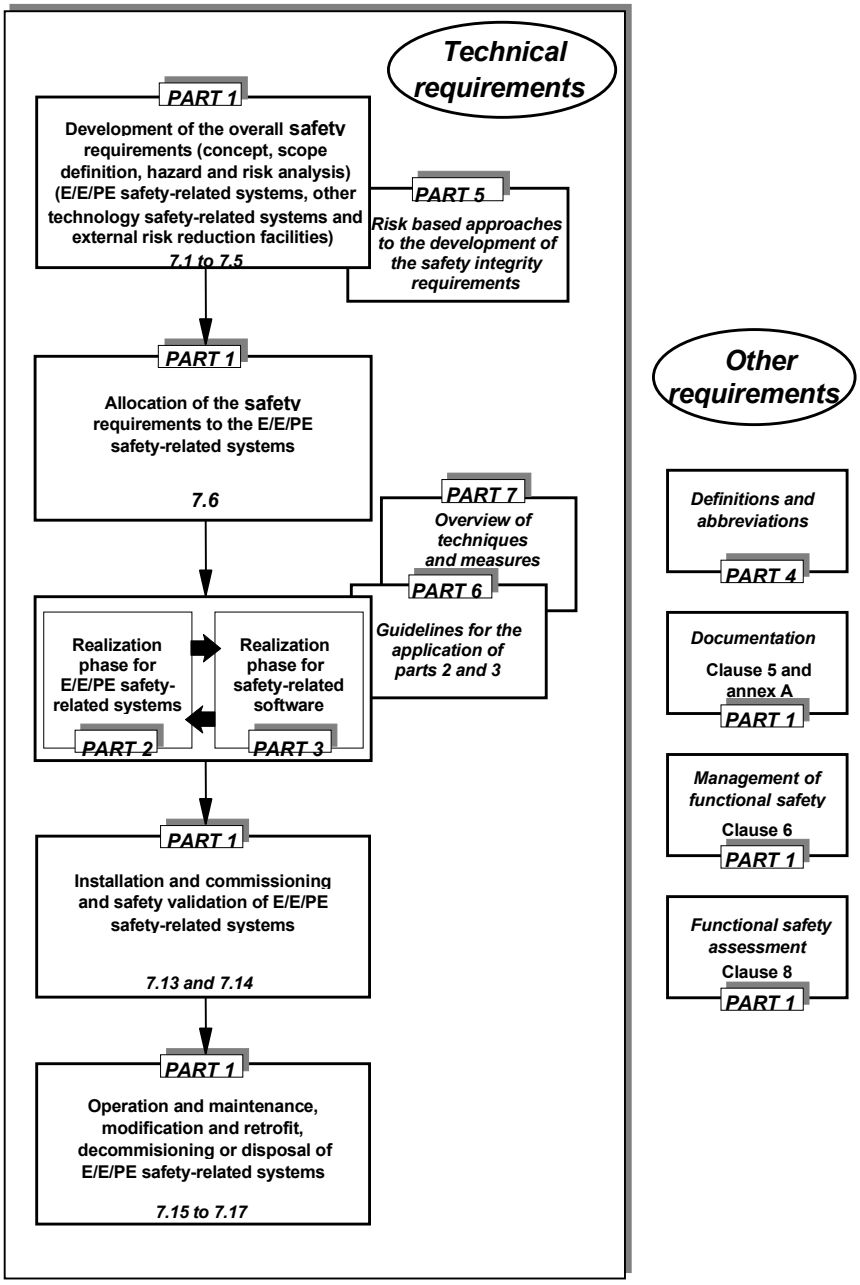
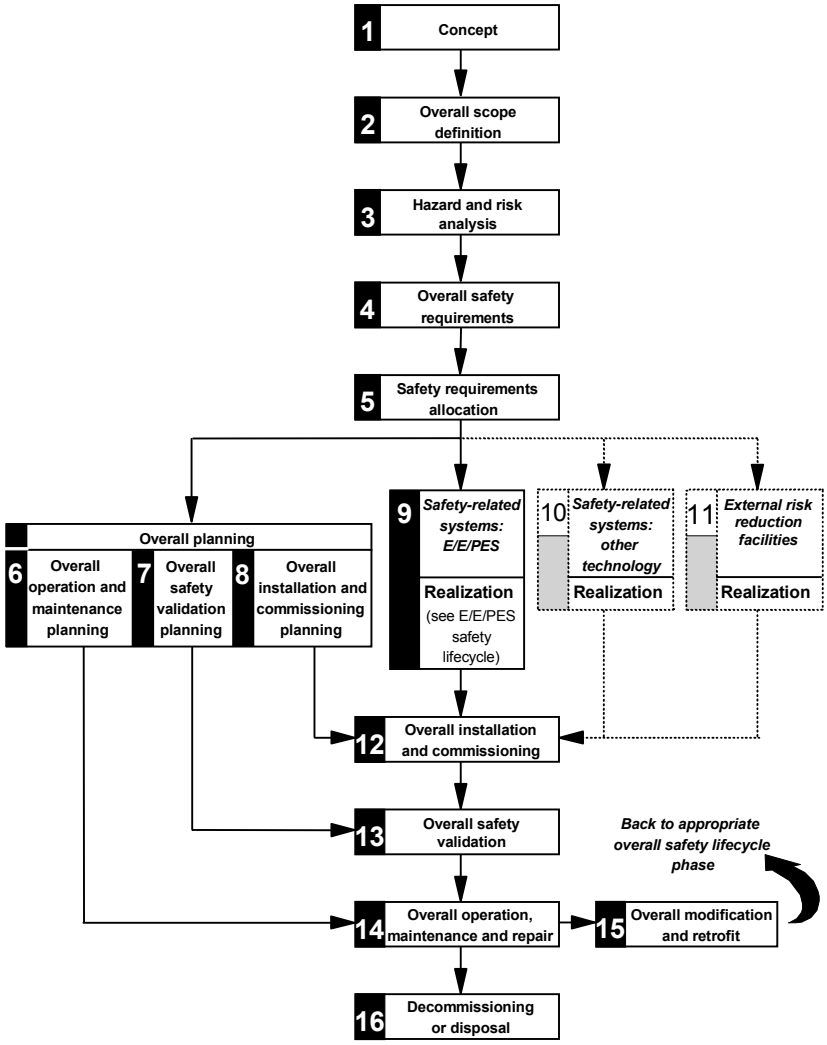


Figure 2 Overall framework of the IEC 61508 (IEC 61508 Part 1 Figure 1)

The IEC 61508 describes the whole life cycle of equipment from concept to decommissioning or disposal (see Figure 3).

The validation and certification in general must be open for the application of different technologies and standards (see 1.2.1). This is possible in the life cycle scheme of IEC 61508 (see Figure 3). There is a possibility to use other standards. The verification process can take into account the different approaches of the applied standards.



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

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

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

Figure 3 Overall safety lifecycle (IEC 61508 Part 1 Figure 2)

Every life cycle has a corresponding part in existing explosion protection standards (for example life cycle 12 and 14: standards for installation and maintenance).

For a certification, the SIL (step 9) and the steps 6, 7 and 8 have to be tested. It has to be checked whether the life cycles 12 - 14 can be fulfilled under the scope of explosion protection.

A safety device with other technologies can be certified according to step 10 with other standards. A reference table will be necessary, for example, between EN 954-1 levels and the safety integrity level of IEC 61508. This is not available because the references depend on the application and the technology.

A problem between IEC 61508 and EN 954-1 is mentioned in Task 2. The safety level steps in EN 954-1 are not hierarchically structured. The IEC 61508 and the zone definition for explosion protection are linear structured. Furthermore, depending on application a safety level in EN 954-1 can lead to different levels in IEC 61508

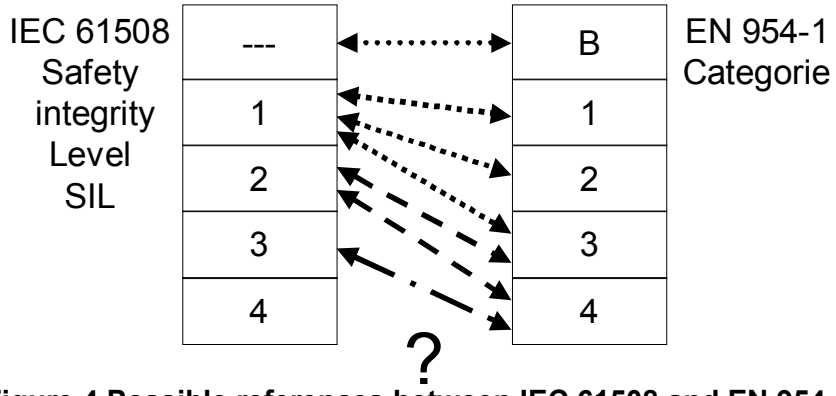


Figure 4 Possible references between IEC 61508 and EN 954

EN 954-1 gives no information about maintenance. The problems defined in Task 2 can be handled in step 11 or in step 6. Proof testing can be taken as a risk reduction facility if the applied standards like EN 954-1 give no information. The other possibility is to include such problems in step 6, but there the requirements of explosion protection to operation and maintenance should be placed.

IEC 61508 contains a complete scheme for the handling of a product. This is an advantage to other possible schemes. In the next chapter, an assignment is made from the lifecycle to the area of explosion protection. A complete correlation is possible (see part 3.4).

3.4 Assignment of IEC 61508 lifecycles to the area of explosion protection

The lifecycles of IEC 61508 can be divided into three parts.
1. This table contains lifecycles where the preconditions are given by existing standards for explosion protection (Table 1).
2. This table contains the cycles with relation to the certification process (Table 2).
3. This table contains the use of the product (Table 3).

To give some information Table 1 of IEC 61508 Part 1 is shown. It is divided into the three parts. This is mentioned above.

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Figure 3 box number	Title						
1	Concept	7.2.1: To develop a level of understanding of the EUC and its environment (physical, legislative etc) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	EUC and its environment (physical, legislative etc).	7.2.2	All relevant information necessary to meet the requirements of the sub clause.	Information acquired in 7.2.2.1 to 7.2.2.6.	- 94/9/EC - EN 60079-10 - existing standards for explosion protection: EN 50014, ...
2	Overall scope definition	7.3.1: To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc).	EUC and its environment.	7.3.2	Information acquired in 7.2.2.1 to 7.2.2.6.	Information acquired in 7.3.2.1 to 7.3.2.5.	- 94/9/EC - EN 60079-10 - existing standards for explosion protection: EN 50014, ...
3	Hazard and risk analysis	7.4.1: To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse; To determine the event sequences leading to the hazardous events determined; To determine the EUC risks associated with the hazardous events determined.	The scope will be dependent upon the phase reached in the overall, E/E/PES and software safety lifecycles (since it may be necessary for more than one hazard and risk analysis to be carried out). For the preliminary hazard and risk analysis, the scope will comprise the EUC, the EUC control system and human factors.	7.4.2	Information acquired in 7.3.2.1 to 7.3.2.5.	Description of, and information relating to, the hazard and risk analysis.	- 94/9/EC - existing standards for explosion protection: EN 50014, ...

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Figure 3 box number	Title						
4	Overall safety require-ments	7.5.1: To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.	EUC, the EUC control system and human factors.	7.5.2	Description of, and information relating to, the hazard and risk analysis.	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	- 94/9/EC - existing standards for explosion protection: EN 50014, ... - Task 1[11] - Task 2 [11]
5	Safety require-ments allocatio n	7.6.1: To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities; To allocate a safety integrity level to each safety function.	EUC, the EUC control system and human factors.	7.6.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Information and results of the safety requirements allocation.	- existing standards for explosion protection: EN 50 014, ... - Task 1[11] - Task 2 [11]

Table 1- Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - preconditions given by existing standards

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	Special for safety devices, examples
Figure 2 box number	Title						
6	Overall operation and maintenance planning	7.7.1: To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.7.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for operating and maintaining the E/E/PE safety-related systems.	- 94/9/EC Annex II, 1.0.6 Instructions - EN 60079-14 [18] - EN 60 079-17 [20]
7	Overall safety validation planning	7.8.1: To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.	EUC, the EUC control system and human factors; E/E/PE safety-related systems.	7.8.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan to facilitate the validation of the E/E/PE safety-related systems.	- 94/ 9/EG Annex II, 1.0.6 Instructions - EN 60079-14 [18]
8	Overall installation and commission-ing planning	7.9.1: To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.	EUC and the EUC control system; E/E/PE safety-related systems.	7.9.2	Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.	- 94/ 9/EG Annex II, 1.0.6 Instructions - EN 60 079-14 - EN 50281-1-2

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	Special for safety devices, examples
Figure 2 box number	Title						
9	E/E/PE safety-related systems: realization	7.10.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).	E/E/PE safety-related systems.	7.10.2 and parts 2 and 3	Specification for the E/E/PES safety requirements.	Confirmation that each E/E/PE safety-related system meets the E/E/PES safety requirements specification.	- 94/9/EC Annex II - IEC 61508 Part 2 and 3
10	Other technology safety-related systems: realisation	7.11.1: To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other technology safety-related systems.	7.11.2	Other technology safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each other technology safety-related systems meets the safety requirements for that system.	- 94/9/EG Annex II - EN 954 Part 1 and 2
11	External risk reduction facilities: realization	7.12.1: To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).	External risk reduction facilities.	7.12.2	External risk reduction facilities safety requirements specification (outside the scope and not considered further in this standard).	Confirmation that each external risk reduction facility meets the safety requirements for that facility.	- 1999/92/EC - Special pro-cedures

Table 2- Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - lifecycles in relation to certification process

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Figure 2 box number	Title						
12	Overall installation and commis-sioning	7.13.1: To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.	EUC and the EUC control system; E/E/PE safety-related systems.	7.13.2	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.	Fully installed E/E/PE safety-related systems; Fully commissioned E/E/PE safety-related systems.	- 1999/92/EC - EN 60079-14 - EN 50281-1-2
13	Overall safety validation	7.14.1: To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.	EUC and the EUC control system; E/E/PE safety-related systems.	7.14.2	Overall safety validation plan for the E/E/PE safety-related systems; Specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements; Safety requirements allocation.	Confirmation that all the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.	- 1992/92/EC

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Figure 2 box number	Title						
14	Overall operation, maintenance and repair	7.15.1: To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.	EUC and the EUC control system; E/E/PE safety-related systems.	7.15.2	Overall operation and maintenance plan for the E/E/PE safety-related systems.	Continuing achievement of the required functional safety for the E/E/PE safety-related systems; Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems.	- 94/9/EC Annex II, 1.0.3 Special checking and maintenance conditions, 1.0.6 Instructions - 1992/92/EC - EN 60079-14 - EN 60079-17 - prEN 60079-19
15	Overall modification and retrofit	7.16.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.	EUC and the EUC control system; E/E/PE safety-related systems.	7.16.2	Request for modification or retrofit under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems, both during and after the modification and retrofit phase has taken place; Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems.	- 94/9/EC Annex II - 1999/92/EC - EN 60 079-14 - EN 50281-1-2

Safety lifecycle phase		Objectives	Scope	Requirements sub clause	Inputs	Outputs	special for safety devices, examples
Figure 2 box number	Title						
16	Decommissioning or disposal	7.17.1: To ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	EUC and the EUC control system; E/E/PE safety-related systems.	7.17.2	Request for decommissioning or disposal under the procedures for the management of functional safety.	Achievement of the required functional safety for the E/E/PE safety-related systems both during and after the decommissioning or disposal activities; Chronological documentation of the decommissioning or disposal activities.	-

Table 3 - Overall safety lifecycle: overview - correlation to explosion protection (IEC 61508 Part 1 Table 1) - lifecycles regarding to the use of products

3.4.1 Conclusion for IEC 61508

IEC 61508 is applicable for the certification of safety devices under the scope of the 94/9/EC [1]. The approach of IEC 61508 covers the scope of 94/9/EC and 1999/92/EC. IEC 61508 allows the use of not explicitly mentioned technologies for validation. The ESR can be covered by validation following IEC 61508.

There may be some differences for instance if a thermal control device is used for the control of electrical equipment or for the protection of non-electrical equipment because in 94/9/EC the certification procedure is different.

3.5 Summary

Every concept has advantages and disadvantages. With the use of EN 1441 or EN 954-1 many things have to be added to get a certification scheme for safety devices in the area of explosion protection.

IEC 61508 gives a complete concept for the certification of safety devices. The disadvantage is application only for specific technologies. The concept on the other hand is open for use of standards with other technologies. IEC 61508 only has to adapt to the use with safety devices for explosion protection.

4 Conformity assessment procedure according to IEC 61508

4.1 Conditions

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

- The boxes 1 - 4 are already fulfilled by existing standards for explosion protection and the work in Task 1 and Task 2 [11].

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

The safety integrity level for a purge control system is defined. Even the safety integrity level for a thermal protection system can easily be defined.
For example, a type “e” engine is not suitable for zone 1 without a thermal protection system. So this safety device is needed. It has to be added and the safety function “thermal protection” has to fulfil SIL 2.
In other cases, the manufacturer and the notified body have to do the safety requirement allocation according to IEC 61508, Part 1, 7.6.

4.2 Validation process

- The certification scheme itself bases on the box 9, Figure 3 for electric / electronic or programmable electronic safety devices or on box 10, Figure 3 together with box 11 for other technologies.

Figure 5 and Figure 6 shows lifecycle realization phase including validation process.

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

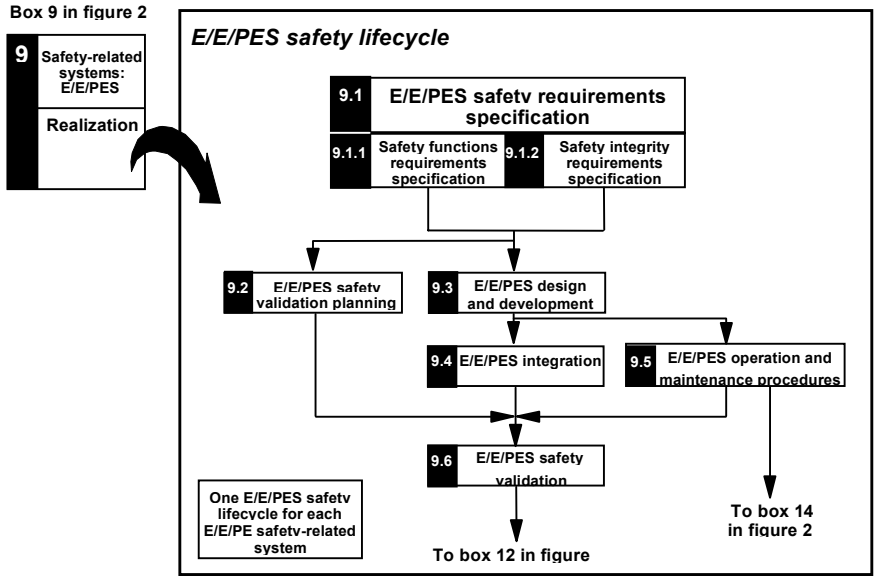


Figure 5 E/E/PES safety lifecycle (in realization phase) (IEC 61508 part 1, figure 3)

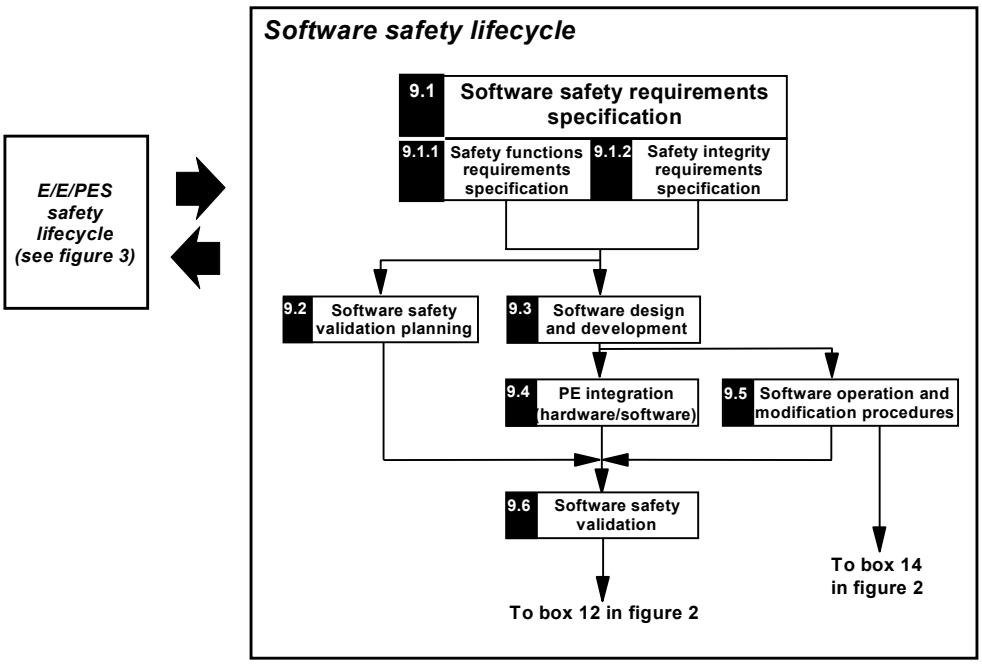


Figure 6 Software safety lifecycle (in realization phase) (IEC 61508 part 1, figure 4)

The tasks included in realization phase relate to the description in IEC 61508 Part 1. The following lifecycle / task has to be fulfilled [4]:

> *7.10 Realisation: E/E/PES*
> *NOTE This phase is box 9 of figure 3 and boxes 9.1 to 9.6 of figures 4 and 5.*
>
> *7.10.1 Objective*
> *The objective of the requirements of this sub clause is to create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements). See parts 2 and 3.*
>
> *7.10.2 Requirements*
> *The requirements that shall be met are contained in parts 2 and 3.*

The specific demands are contained in IEC 61508 Part 2 and 3. Further information can get from IEC 61508 parts 2 and 3.

4.3 Special demands with other standards in validation process

For other technologies, IEC 61508 includes the following recommendation:

7.11 Realization: other technology
NOTE: This phase is box 10 of figure 3.

7.11.1 Objective
The objective of the requirements of this sub clause is to create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.

7.11.2 Requirements
The specification to meet the safety functions requirements and safety integrity requirements for other technology safety-related systems is not covered in this standard.
NOTE: Other technology safety-related systems are based on a technology other than electrical/electronic/programmable electronic (for example hydraulic, pneumatic etc). The other technology safety-related systems have been included in the overall safety lifecycle, together with the external risk reduction facilities, for completeness (see 7.12).

The validation for other technologies can be led by using EN 954-1. Specification of the validation process is urgent necessary (see Task 2). PrEN 954-2 e.g. can be used. Other standards are possible (for example DIN EN 61496-1 06/98).

The lack of information e.g. about proof intervals has to be covered by special procedures. The validation of a electrical / electronic or programmable electronic devices with the EN 954-1 needs separate calculation of reliability for circuits responsible for the validated safety function.

This additional validation may be allocated to the lifecycles **Overall safety validation planning** (box 6, Figure 3) or to **External risk reduction facilities** (box 11, Figure 3). IEC 61508 part 1, Chapter 7.12 give some further information.

7.12 Realisation: external risk reduction facilities
NOTE: This phase is box 11 of figure 3.

7.12.1 Objective
The objective of the requirements of this sub clause is to create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities.

7.12.2 Requirements
The specification to meet the safety functions requirements and safety integrity requirements for the external risk reduction facilities is not covered in this standard.
NOTE The external risk reduction facilities have been included in the overall safety lifecycle, together with the other technology safety-related systems for completeness (see 7.11).

4.4 Special information for instruction

Furthermore, the notified bodies have to proof the results of the E 7 E / PES safety validation (lifecycle 9.6). The overall planning (lifecycles shown in box 6 - 8 (Figure 3)) has to proof according to the directive 1999/92 and the existing standards if special information must given in the instruction for the use of safety devices.

4.5 Actual problems with IEC 61508

A problem for application of IEC 61508 – 2 is that the standard is only available a draft and the whole IEC 61508 is not harmonised. The EN 954-1 is available as a harmonised standard. Therefore, standardisation committees for example in the type EEx “p” standard refer to EN 954-1 for validation. Even the committee for gas measurement systems do this.
The IEC 61508 needs for application a reliable database. There are several databases in use (Task 2, Task 4). Today no common database exists. Like in other standards for explosion protection, this common database must be established before certification can bases on IEC 61508 alone.

The authors do certification for some pressurized system controller according EN 954-1. The systems were suitable for application in category 3. Category 3 was recommend in an earlier draft for pressurised systems.

The controllers were also validated applying IEC 61508 - 2. Special attention was given to the dangerous undetected faults. The probability for dangerous undetected faults was calculated to give special information in the instruction if necessary. Two databases had been used ([22], [23]). The probability for failure in low demand mode of operation was low enough to fulfill safety integrity level 3. Because of a lack for proof testing the controllers are only suitable for a SIL 2 application (because of architectural constraints 61508 – 2, 7.4.5). This is the recommended SIL for pressurised system controller in Task 2. The result from EN 954-1 and IEC 61508 fits in this special application.

4.6 Independence for validation / conformity assessment procedures

IEC 61508 gives recommendation for level of independence for validation. This is shown in the following passage taken from the IEC 61508.

> *8.2.12 Unless otherwise stated in application sector international standards, the minimum level of independence of those carrying out the functional safety assessment shall be as specified in tables 4 and 5. The recommendations in the tables are as follows.*
>
> - *HR: the level of independence specified is highly recommended as a minimum for the specified consequence (table 4) or safety integrity level (table 5). If a lower level of independence is adopted then the rationale for not using the HR level should be detailed.*
> - *NR: the level of independence specified is considered insufficient and is positively not recommended for the specified consequence (table 4) or safety integrity level (table 5). If this level of independence is adapted then the rationale for using it should be detailed.*
>
> *-: the level of independence specified has no recommendation for or against being used.*
> *NOTE 1 Prior to the application of table 4, it will be necessary to define the resulting categories taking into account current good practices in the application sector. The consequences are those that would arise in the event of failure, when required to operate, of the E/E/PE safety-related systems.*
> *NOTE 2 Depending upon the company organisation and expertise within the company, the requirement for independent persons and departments may have to be met by using an external organisation. Conversely, companies which have internal organisations skilled in risk assessment and the application of safety-related systems, which are independent of*

and separate (by ways of management and other resources) from those responsible for the main development, may be able to use their own resources to meet the requirements for an independent organization.
NOTE 3 See 3.8.10, 3.8.11 and 3.8.12 of part 4 for definitions of independent person, independent department and independent organisation respectively.

8.2.13 In the context of tables 4 and 5, either HR[1] or HR[2] is applicable (not both), depending on a number of factors specific to the application. If HR[1] is applicable then HR[2] should be read as no requirement; if HR[2] is applicable then HR[1] should be read as NR (not recommended). If no application sector standard exists, the rationale for choosing HR[1] or HR[2] should be detailed. Factors that will tend to make HR[2] more appropriate than HR[1] are:

- *lack of previous experience with a similar design;*
- *greater degree of complexity;*
- *greater degree of novelty of design;*
- *greater degree of novelty of technology;*
- *lack of degree of standardisation of design features.*

8.2.14 In the context of table 4, the minimum levels of independence shall be based on the safety function, carried out by the E/E/PE safety-related system, that has the highest safety integrity level.

Minimum level of Independence	Safety integrity level			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	-	-	HR[2]	HR
NOTE See 8.2.12 (including notes), 8.2.13 and 8.2.14 for details on interpreting this table.				

Table 4 - Minimum levels of independence of those carrying out functional safety assessment (overall safety lifecycle phase 9 - includes all phases of E/E/PES and software safety lifecycles (see Figure 3, Figure 5 and Figure 6))

IEC 61508 is not written to a special scope of application. The tables given by IEC 61508 part 1 have to change in respect to the regulations of 94/9/EC CHAPTER II Conformity assessment procedures, Article 8. Under the scope of the directive 94/9/EC, the table have to be divided into two parts, because the certification of electrical and non-electrical equipment is different ([1], Chapter II, Article 8)

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

Table 5 - Target SIL determination for protection systems used in Hazardous Zones (Task 2 [11], Table 14)

In reference to the results of Task 2 the levels of independence are changed by the 94/9/EC to the two groups "notified bodies" and "manufactures". Therefore, the Table 4 changed to Table 6 and Table 7.

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

Table 6 - Responsibility for conformity assessment procedure of safety devices in use with electrical equipment or internal combustion engines

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

Table 7 - Responsibility for conformity assessment procedure of safety devices in use with non-electrical equipment

5 Summary

For the conformity assessment procedure, several standards are available. The most general standard is the IEC 61508. Because there is a large number of very different safety devices identified in Task 3 [13] it is important to take a general standard. This should be the IEC 61508, because this standards covers although the production and the use of electrical / electronic / programmable electronic systems. This is an important fact because for safety devices the two areas defined by the directives 94/9/EC [1] and 1999/92/EC [3] cannot be separated.

The IEC 61508 is open for the use of other standards for the validation of safety devices. This is even an important fact. For example, the EN 50 016 [16] recommends the use of the EN 954-1 for the validation of the used safety devices. This is done even in other standards or drafts [24].

The IEC 61508 can be regarded as a standard for the basic procedure and as "generic standard" for safety devices. In some cases "products standards" can be used if they are recommended from the specific standardisation committee. This is nearly the same principle like in the directive 89/336/EC for electromagnetic compatibility (“generic standards” 50082-xx together with test standards IEC 61000-4-xx and “product standards” with test standards IEC 61000-4-xx).

Common database is urgently needed (reliability of used components) for application of IEC 61508-2 in certification of safety devices. Without such a data base a certification in the scope of 94/9/EG in an equal safety level in different European countries cannot be achieved.

Furthermore today certification of safety devices is only possible according to harmonized standards like EN 954-1 or according to the directive 94/9/EC itself.

6 References

[1] Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, 394L0009

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

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

[4] IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems - Part 1: General requirements, 1998-12

[5] Draft IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[6] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 1998-12

[7] EN 954-1: 1997, Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design

[8] prEN 954-2:1998, Safety of machinery - Safety-related parts of control systems - Part 2: Validation

[9] EN 1441:1997 Medical devices - Risk analysis

[10] Draft EN xxxxx Explosives for civil uses - Detonators and relays , Part 27 Definitions, methods and requirements for electronic initiation systems

[11] Determination of safety categories of electrical devices used in potentially explosive atmospheres: Report on Task 1: Derivation of Target Failure Measures

[12] Determination of safety categories of electrical devices used in potentially explosive atmospheres: Report on Task 2: Assessment of Current Control System Standards, SAFEC project, Contract SMT4-CT98-2255, A. M. Wray, Engineering Control Group, Health & Safety Executive, 01/2000

[13] Determination of safety categories of Electrical devices used in Potentially Explosive Atmospheres: Report on Task 3:, Identification of “Used Safety Devices”, SAFEC project, Contract SMT4-CT98-2255, E. Conde, LABORATORIO OFICIAL MADARIAGA (LOM), November 1999

[14] Determination of safety categories of Electrical devices used in Potentially Explosive Atmospheres: Report on Task 4:, Study of “Used Safety Devices”, SAFEC project, Contract SMT4-CT98-2255, E. Faé, S. Halama, Institut National De L'Environnement Industriel Et Des Risques (INERIS), November 1999

[15] EN 50014:1999 Electrical apparatus for potentially explosive atmospheres - General requirements

[16] EN 50016:1995 Electrical apparatus for potentially explosive atmospheres - Pressurised apparatus "p"

[17] EN 50281-1-2:1999 Electrical apparatus for use in the presence of combustible dust - Part 1-2: Electrical apparatus protected by enclosure - Selection, installation and maintenance

[18] EN 60079-10:1996 Electrical apparatus for explosive atmospheres - Part 10: Classification of hazardous areas

[19] EN 60079-14:1997 Electrical apparatus for potentially explosive atmospheres - Electrical installations in hazardous areas (other than mines)

[20] EN 60079-17:1997 Electrical apparatus for potentially explosive atmospheres - Inspection and maintenance of electrical installations in hazardous areas (other than mines)

[21] prEN60079-19:1992 Installation of electrical apparatus in hazardous areas; Repair and overhaul for apparatus used in explosive atmospheres (other than mines)

[22] SN 29000 Teil 1 - 14, Ausfallraten Bauelemente, Erwartungswerte, Allgemeines, Siemens AG, 11.1991

[23] Reliability, Maintainability and Risk, Practical methods for engineers, David J. Smith, Butterworth Heinemann, Fifth Edition

[24] Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen; Requirements on the functional safety of fixed gas detection systems, First draft**,** 15.12.1999

[25] TC31-WG9, CENELEC, Electrical equipment for potentially explosive atmospheres, Reliability of safety-related devices, 1. Draft proposal 1999-xx-yy, 12/02/1999.