DESIGN FOR SAFETY APPLYING IEC 6-1508
"from the manufacturer's point of view"

S. De Vries, M. Van den Schoor, R. Bours
Fike Europe, Explosion protection systems manufacturer, Herentals, Belgium

Explosion protection systems are as a well-known technique widely used to prevent process plants from hazardous events and personal injuries. The design of such systems requires knowledge of system design, the user requirements, legislation and hazards. The process of translating between these parameters is often a point of discussion. The IEC 6-1508 document provides a framework for all involved partners in order to communicate and work in a structured and quantifiable way. This paper introduces IEC 6-1508 and handles some of the latest evolutions in explosion protection design techniques and regulations.

Keywords: ATEX 100a, Safety Integrity, Life cycle, E/E/PES, Software design

SAFETY: A QUALITY CHARACTERISTIC

People tend to use the word quality in reference to products, often without even knowing how to define and measure quality. The reason for this is that many different definitions for quality are being used. The definition used for quality and stated in the ISO 8402 dictionary is as follows;

> *" Quality is the totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs".*

Examples of other quality definitions:

Quality is the absence of unpleasant surprises

Quality is hard to define, impossible to measure, but easy to recognize

Quality is when the customer comes back and the product doesn't

Safety can be categorized into quality, as a quality attribute such as cost effective, maintainable, reliable, The safety definition can also be found in ISO 8402.

Safety is a state in which the risk of harm or damage is limited to an acceptable level.

EXPLOSION PROTECTION: ATEX 100a DIRECTIVE

General

On 23/03/1994 Directive 94/9/EC, also known as ATEX 100a, has been approved by the European Parliament. This Directive will become mandatory from 1 July 2003; all previous Directives in contradiction with this Directive will be overruled. ATEX100a is mandatory on all (electrical and non-electrical) equipment for use in explosion hazardous areas. The Directive will define the essential safety aspects necessary for each equipment like for the Machinery-Directive (89/336/EC) and the EMC-Directive (89/336/EC). The individual technical requirements, which are applicable for each device, are to be defined by normative organizations such as CEN and CENELEC. The Directive also describes conformity procedures to be followed by the manufacturer in order to achieve the CE-label. The CE-label is necessary in order to allow for trade of products between the European community states. The CE-label guarantees no quality but states that the product has been made in accordance with all applicable CE-Directives. Electrical equipment for use in an explosive hazardous environment will have to comply with the ATEX 100a Directive as well as with the Machinery-Directive and the EMC-Directive.

Apparatus division

The ATEX 100a-Directive applies to apparatus and systems, which can be used in explosion hazardous environments: mining, gas- and dust-explosion hazardous zones. It applies to all kinds of apparatus and protection systems, electrical and non-electrical. The base for the identification of environments where explosion hazards can be present, is the so-called hazardous zone-classification.

The zone-classification will be mandatory for dust as well as for gas. The Directives are based on a classification of apparatus in groups and categories. The protection level for each apparatus needs to be aligned with the zone-classification of the environment in which the apparatus is being placed and used. For dust explosion hazards there are new obligations for hazardous zone-classification (ref. ATEX 118a, IEC 61241-3 and EN1127-1).

New Zone-classes	**Old Zone-classes**
gas/dust	gas/dust
zone 0 / 20	zone 0 /Z or 10
zone 1 / 21	zone 1 /Y or 11
zone 2 / 22	zone 2

New apparatus classes

group I: underground

category M1: must remain functional in case of an exceptional fault

category M2: must interrupt energy supply in case of danger

group II: above surface

category 1: must maintain safety level, even in case of exceptional fault (zone 0,20)

category 2: must maintain safety level, even in case of frequent faults (zone 1,21)

category 3: maintain safety level in normal operation (zone 2,22)

Zone 0/20: area in which an explosive atmosphere is continuously present, for a long period of time (more than 1000 hours per year).
Applies to apparatus in group II (above surface) category 1 (very high protection level)
Zone 1/21: area in which an explosive atmosphere can occur occasionally in normal operation (100 to 1000 hours a year).
Applies to apparatus in group II (above surface) category 2 (high protection level)

Zone 2/22: area in which an explosive atmosphere is not likely to occur during normal operation, or for very short periods of time (less than 10 hours per year).
Applies to apparatus in group II (above surface) category 3 (normal protection level)

Examples of zones *20* and *21* are areas where in normal operation an explosive dust/air mixture is continuously present. These areas may include elevators, pneumatic transportation installations, silos, bunkers, mixture systems, sieves, cyclones, dryers, dust-chambers, filters, etc.

PROTECTION AGAINST GAS AND DUST EXPLOSIONS

General

In the design of apparatus and protection systems for use in explosion hazardous environments the explosion protection must be integrated. Therefore measures must be taken in order to:

1. Prevent these apparatus and protections systems from creating an explosive environment.

2. Prevent the ignition of an explosive atmosphere, considering the nature of each potential electrical and non-electrical ignition source.

3. In case an explosion occurs, immediately stop this event and/or reduce the zone, which is affected by the flames and pressure rise due to the explosion, in order to come to a normal safety level.

Corrective protection systems

Explosions can be stopped, and the zone, which is affected by the flames and the pressure, can be reduced, by re-directing the explosion in a safe and known direction, by compartment, extinguishing, pressure relief or a combination of these measures. Therefore different possibilities are available.

Explosion pressure relief

This is a corrective protection method designed to re-direct an explosion into a more safe area. Inside the wall of an apparatus a weak construction is placed deliberately. Explosion vents or explosion rupture disks are specially designed and accepted passive protection systems.

Compartment or isolation

These methods prevent the explosion from propagating to other apparatus, installations or workplaces. Compartment or isolation is obtained by using mechanically or chemical explosion-isolation systems with autonomic functions.

Explosion suppression or extinguishing

By applying these methods the explosion will be extinguished by the quickly injection of a suitable extinguishing agent. The explosion will be detected in the incipient stage and suppressed in order to maintain the explosion pressure under a given acceptable limit.

IEC 6-1508 A SAFETY DESIGN GUIDELINE

General

"Design for safety"; one of the most used slogans in sales meetings concerning protection systems and devices. In the designing of these devices the most difficult questions to answer will be: which level of safety is necessary for implementation, how do we define this safety level in order to have both users and designers understand it's meaning, and how do we validate or measure the safety level in the acceptance of a developed device or system? Different techniques have been used in order to have a clear communication between designer-groups and sales/user-groups. The most common way is to have a project analyst who translates between both groups and who has both technical and commercial expertise and experiences. Without guidelines however the analyst can never succeed in this job. When using tools such as the IEC 6-1508 guideline his goal can be reached more effectively and successfully.
The document IEC 6-1508 defines safety as: *"the freedom from unacceptable risk of harm"*.

Scope

IEC 6-1508:

1. Applies to safety related systems when one or more of such systems incorporate electrical, electronic or programmable electronic systems (E/E/PES).
2. Is mainly concerned with safety to persons.
3. Does not specify those who shall be responsible.
4. Uses Safety Integrity Levels (SIL) for specifying the target level of safety integrity to E/E/PES.

Conformance

Conformance to IEC 6-1508 can be reached as follows:

1. Use as a minimum a quality system, such as ISO 9000 series or similar.
2. If a measure or technique is ranked as Highly Recommended (HR) the reason for not using that measure or technique should be recorded with details

in the safety plan.

3. Compliance shall be assessed by the review of documents required for this guideline and by witnessing tests

4. In general the IEC 6-1508 document provides a framework for a safety life-cycle model, which can be incorporated by its users as an expansion of their quality and safety assessment procedures.

IEC 6-1508 Safety Framework

The framework as shown can be divided into different steps for the design and assessment of a safety device or system. (Fig. 1)

Step 1: Define the system

The first step is to carry out a systematic analysis of the system starting from its functional and qualitative design requirements.

Different techniques can be used depending on the nature of the device or system by using the ISO 9000 quality structure and company internal procedures as a guideline.

Step 2: Analysis of the hazards

Identify the hazards and the events, which could give, rise to them, identifying in particular the way in which an E/E/PES malfunction could contribute to a hazard. There are several formal hazard analysis (HAZAN) techniques, each with particular strengths and weaknesses and fields of application. The most widely used techniques are hazard and operability (HAZOP) studies; failure mode and effect \analysis; event tree analysis; and fault-tree analysis.

Step 3: The risks and risk reduction

After defining any identifiable hazard, a risk analysis must be performed for each individual hazard in order to calculate the risk of hazardous events to occur for the particular device or system in its application. The risk analysis will incorporate frequency of failures from hardware and software devices, frequency at which a person or people are exposed to a risk, the duration of the exposure and the severity of injury after exposure. This analysis will lead to a necessary risk reduction calculation for each type of hazard. The application of the above stated hazard analysis techniques will incorporate risk calculation as well as different standards techniques using checklists and/or mathematical approaches.

Step 4: Safety Functions

In order to have the necessary risk reduction the design has to be equipped with safety functions, each of them preventing hazard events to occur during the operation of the device or system. Each safety function has a measure of safety called the Safety Integrity Level (SIL).

SAFETY INTEGRITY LEVEL (SIL)	Probability of failure on demand or probability of one dangerous failure in one year
4	>= 10E-5 to < 10E-4
3	>= 10E-4 to < 10E-3
2	>= 10E-3 to < 10E-2
1	>= 10E-2 to < 10E-1

Step 5: Safety Allocation
Each safety function requires the implementation of safety function technology.

1. E/E/PE, requiring electrical hardware and/or software techniques.
2. Other technology, such as pneumatically or hydraulic techniques.
3. External safety product implementation, by using standard devices or systems in order to achieve the required level of safety integrity for a specific safety function.

The IEC 6-1508 only takes the E/E/PE techniques into further consideration.

Step 6: E/E/PES Allocation
The considered safety functions will be divided into Safety Related Systems (SRS) with hardware and/or software requirements. These requirements will be formalized in a way to allow designers of hardware and software to clearly understand the specific demands and to measure the required safety integrity level for each safety related specification. The independent test group or person will base the validation of their specific design efforts on the same SRS hardware and software requirements.

Safety Life-cycle

By implementing the Safety Framework into the overall System Life cycle, (as used by ISO 9001) a Safety Life-cycle can be created as the complete Life-cycle model for the design and development of Safety Related Systems. (Fig.2)
This Safety Life cycle can be divided into:

1. Safety Life-cycle for specific E/E/PES allocation (Fig. 3)
2. Safety Life cycle for Software allocation. (Fig . 4)

E/E/PES Safety Life-cycle

General .
The safety requirement specification can be divided into: a) The safety functions requirement specification (which identifies and specifies the required safety functions in order to achieve functional safety), the hardware system, operator interfaces and all relevant modes of operation of the equipment under control. b) The safety integrity requirement specification shall contain requirements necessary in the design phase to achieve functional safety of the system, including requirements for the SIL level for each function, techniques for avoiding systematic and random hardware faults during

design and development. The next step is the safety validation planning to enable the validation of the safety requirement specifications to take place. To ensure that, in all respects the requirements in the SRS have been included in the design. The design will meet all safety functions and safety integrity as specified. All necessary procedures must be developed to ensure that the functional safety of the safety related E/E/PES is maintained during operation and maintenance. These procedures must allow corrections, enhancements or adaptations to the E/E/PES, ensuring that the required Safety Integrity Level is achieved. Procedures must be developed to test and evaluate the products of a given phase ensuring the correctness and consistency with respect to the product and provided standards.

E/E/PES design considerations

1.At switch-on, or when power is restored following a failure, hardware should ensure to reset the system only from a point that it is safe to do so.
2.Power-supply interruption should not lead to unidentified or unsafe conditions
3.Where all safety related systems are PES based, particular attention is required to minimize the risk of common cause failures (CCF's) such as electrical interference.
4.For systems performing actions on demand, such as emergency shutdown systems or protection systems, some form of on-line proof testing for unrevealed faults may be required.
5.Wherever possible ROM's should be used in preference to RAM's since they are less susceptible to electrical interference.
6.In many industrial applications a specially controlled environment must be provided to promote reliable operation; dust, humidity, temperature and pollution must be taken into account. Corrosive atmospheres for example, often affect printed circuit boards.
7.The level of electrical interference in the environment of the PES must be taken into account, to minimize the effects on the performance of the system, therefore attention should be paid in the design of the equipment and the installation.

Implementation of Safety in E/E/PES

Many different techniques and criteria must be taken into account in order to have safe E/E/PES hardware. Some of the most fundamental criteria and techniques will be given in the following. Depending on the required Safety Integrity Level and the required Functional Safety as specified in the E/E/PES Requirement Specification, one or more of these techniques/ criteria must be applied and will be categorized as being Highly Recommended (HR).

Redundancy
Systematic Failure testing
PE logic configuration
Electronic considerations
Memories
Data paths
Watchdog
Communication, mass-storage
Actuators
Environmental failures

Ventilation-, Heating-System
Random Failure testing
Electrical considerations
Processing units
I/O units and interfaces
Power supplies
Clocks
Sensors
Systematic failures
Operational failures

E/E/PES directives

All hardware related safety products do however have to comply with all applicable mandatory requirements. The most common known Directives in hardware are:

1. Machinery Directive (89/392/EC) which applies to products with at least one element, able to move without applying physical human power.

2. Directive on EMC (89/336/EC)
EN 50081-2 Generic Emission Standard (1993)
EN 50082-2 Generic Immunity Standard (1994)
Applies to all electrical products. Specific care must be taken that the Equipment Under Test (EUT) does not generate a level of Electro-Magnetic Energy (EME) which is at higher level than specified in the Immunity Standard, in order not to influence other devices in a way that they will go into a faulty operation mode. Also care must be taken that the EUT will not be affected, and therefore will not perform its normal operation by EME influences generated from external devices. Both EMC-standards provide a safety margin between both immunity and emission levels. Compliance against EMC can be obtained by testing for the following:

Immunity
1.conducted via cabling
2.effects of lightning
3.electrostatic effects
4.electromagnetic fields of surrounding devices

Emission
1.ground plane
2.enclosure design

3. The Low Voltage Directive (72/23/EC)
Applies to product safety related to personal for all products with working voltages between 50 V to 1000 V (AC), and 75 V to 1500 V (DC).

4. Explosion protection Directive ATEX 100a (94/9/EC)
Applies to all products for use in explosive atmospheres (ATEX 118a and EN 1127-1). This Directive will be mandatory from July 2003.

Software Safety Life-cycle

Basic Steps

1. Develop the software safety requirement specification in terms of the software safety function requirements and software safety integrity requirements.
2. Develop the software safety function requirement specification for each E/E/PES safety-related system necessary to implement the required safety-functions.
3. Develop the software safety integrity requirement specification for each E/E/PES safety related system necessary to achieve the safety integrity level specified for each safety function allocated to that safety related system.
4. Develop a software safety validation plan to enable the validation of the software

5. Select a software architecture that fulfills the requirements of the software safety requirements, to select a suitable set of tools, including languages and compilers. Design and implement software which achieves the required safety integrity level, and which is analyzable, verifiable and maintainable.
6. Integrate the software onto the target programmable electronics.
7. Provide information and procedures concerning software necessary to ensure that the functional safety of the E/E/PES is maintained during operation and maintenance.
8.Test the integrated system to ensure compliance with the Software Safety requirements specification, at the intended safety integrity level.
Make corrections, enhancements or adaptations to the software, ensuring that the required Safety Integrity Level is achieved.
To the extent required by the safety integrity level, test and evaluate the deliverables of a given phase to ensure correctness and consistency with respect to the deliverables and standards provided as input to that phase.

Implementation of Software Safety

Many different techniques and criteria must be taken into account in order to have Safe Software. Some of the most fundamental criteria and techniques will be given in the following. Depending on the required Safety Integrity Level and the required Functional Safety, as specified in the Software Requirement Specification, one or more of these techniques/ criteria must be applied and will be categorized as being Highly Recommended (HR).

Structured Methodology for example YOURDON, MASCOT
Re-try fault recovery mechanisms
Development tools and programming languages
Formal Methods
Modular approach
Software module testing
Functional, performance testing
Data recording and analysis
Simulation
Static analysis
Dynamic analysis
Checklists

Software standards and guidelines

1. ISO 9000-3
These are a set of guidelines for the application of ISO 9001, to the development, supply, installation and maintenance of (computer) software. We define 'Firmware' as software written for the application into embedded hardware that can not be changed by the user operations, and stored into non-volatile memory. Extensive Firmware is written for protection systems and control applications. The most basic form of Firmware is machine code for micro-controllers and microprocessors, many times written in Assembler-language.

2. ISO/IEC 9126
This provides for the information technology (IT) product evaluation quality characteristics and guidelines for their use. Differentiated into 6 main characteristics and 21 sub-characteristics, each of them requires consideration in the requirement specification phase of the software product. The main software quality characteristics are:

- Functionality
- Usability
- Maintainability
- Reliability
- Efficiency
- Portability

TECHNOLOGY UPGRADE FOR SAFETY PRODUCTS

General

Nowadays technology creates perspectives for miniaturizing and IT-implementation into unlimited ranges of products and devices. Here are some technology upgrades for consideration into safety related systems with protection functionality.

Bus systems

Standard protection systems use 'sensor-PES-actuator' configurations.
In safety applications redundancy of electronics can increase the efficiency and reliability of these systems. But still each type of hardware solution uses single-bit information. By using bus-systems all field devices, which are anyway susceptible to false triggering and data disturbances, can be provided with multiple-bit communication to have: a) complete reliability in their functional safety b) reach a higher level of safety integrity. Due to the bus-protocol (fault and retry-mechanisms), all data will be validated correctly by both communicating devices. Current technology allows implementation for bus-structures even for high-speed protection systems such as active explosion suppression or isolation.
Each device will be addressable having a unique bus-address and can be remotely monitored while it is performing its protection function, without having any delay on its safety function when required to take place. By using special cable types and/or fiber optics the susceptibility for introducing retries into the data transfer will be reduced enormously.

Intelligent active validation

Using software validation techniques on analog signal coming from primary sensor elements prevents false readings. For example, an analog 4-20 mA signal, converted by an 8-bit analog to digital converter, can be sampled and stored multiple times before a validated value is used for further comparison against preset levels. The stored pre-validated values can be software integrated to eliminate spikes and noise of the signal.

For example a sample rate of 200 μSec results in a validation value each 1 mSec after integration of the 5 stored samples.

Measurement is knowledge (monitoring/events)

In most active safety protection systems actuator devices use critical components. All failure modes and frequencies are well known and therefore redundant hardware has been installed for these critical components. However, automatic self-checking to inform the user of any malfunction not always provided, many times sensors are applied which should be inspected by the user at frequent intervals. Redundancy can be lost, or the whole risk and failure analysis can become invalid without the customer knowing. The incorporation of monitoring electronics may solve a lot of these problems because they can immediately affect the working mode of the protection devices and/or process plant. Enhanced techniques shall keep a record of all unsafe conditions and all process characteristics before and after a protection event on demand has occurred. For example an explosion detector will measure and store the pressure after triggering the explosion protection system, providing information on the maximum achieved explosion pressure and response time of the suppression system.

WHY DO WE KEEP MAKING THE SAME MISTAKES?

General

Practical experiences in how to avoid unsafe conditions regarding dust and gas explosions, from an electrical point of view.

Design Considerations

Specifications
In the specification phase the analyst tends to make mistakes by not having all related groups involved in the requirements specifications. (from managers to operators, from designers to testers, from technicians to sales person)

Design Techniques
Many errors are made in the design by implementing unfamiliar techniques. Many designers think they know it all and do not use the skills of specific specialists for certain tasks or problems. Two persons will know more than one and each will have their own area of specialization and limits of knowledge.

Testing
Having a test plan is great, but the implementation of the tests will sometimes be placed in the background due to time limits and project costs. Many project leaders tend to use the testing plan if their still is enough time and money to do the job. A lot of in the field-faults and extra costs are the unfortionally result of such an approach.

Installation Considerations

Documents

Users tend to apply all manuals and prescriptions when things go badly. However by reading these documents in advance many mistakes could be avoided in operating devices for safety applications.

Pre-Commissioning

Cabling, earthing, positioning and handling protection devices require information in advance. Having a knowledgeable person on-site before installing a protection system will avoid maintenance and commissioning problems.

Commissioning

The commissioning part of a protection system is a very critical phase to have a good practical solution for a specific hazardous problem. It is at that very moment that all-normal and abnormal modes of operation of the protection system and process should be tested on-site. The execution of process-shutdown and process-startup will tackle a lot of potential problems (electrical interference). In most cases the normal plant operation will not be the cause of problems.

Maintenance

Frequent maintenance tends to create a lack of specific perception for potential problems. This should be avoided by procedures and job-diversity for the maintenance group or by extended use of self-checking E/E/PES hardware.

RESULTS AND CONCLUSIONS

General

1. By using the IEC 6-1508 Safety Life-cycle in the overall System Life-cycle more specific safety based approach was obtained in our products.
2. We learned not to underestimate the power of metrics and quantitative data.
3. IEC 6-1508 was found to be applicable to large-scale projects in order to absorb the overhead introduced from the initial phases of the project.
4. Applying a Safety Life-cycle model ensures confidence and awareness into Safety Related Systems from the users, the sales group and management.

Conclusion

It is our believe that the use of IEC 6-1508 or a similar approach towards complete 'Design for Safety' will be even more stimulated in the future. As manufacturers we therefore must comply to all related documents, and with all mandatory Directives, in order to take the necessary measures in the design of our future products. It will demand a "Safety Culture" in all phases of the product life by all related person. It is therefore necessary and extremely useful to have different information channels in order to educate all the related persons in the "Safety Culture". The ICHEME symposium helps in the creation of such a "Safety Culture".

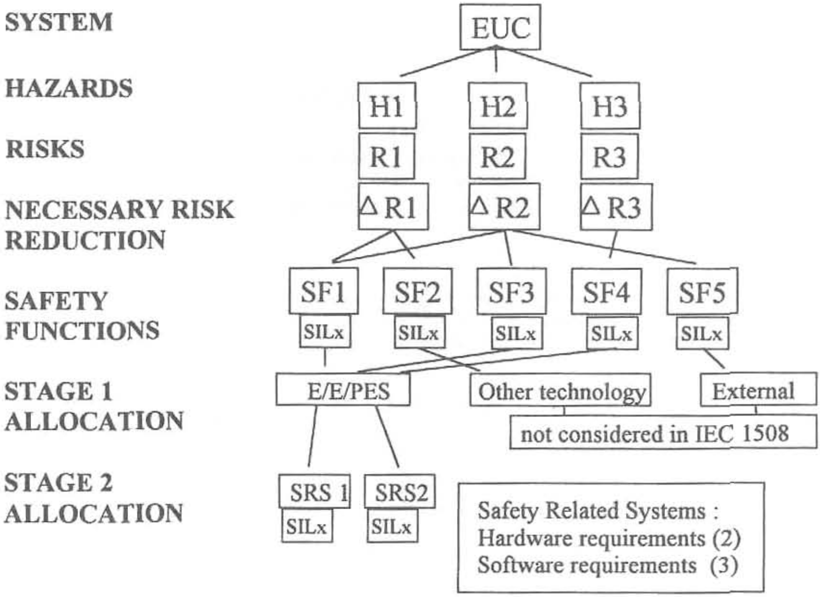
SYSTEM
HAZARDS
RISKS
NECESSARY RISK REDUCTION
SAFETY FUNCTIONS
STAGE 1 ALLOCATION
STAGE 2 ALLOCATION
EUC
H1
H2
H3
R1
R2
R3
Δ R1
Δ R2
Δ R3
SF1
SF2
SF3
SF4
SF5
SILx
SILx
SILx
SILx
SILx
E/E/PES
Other technology
External
not considered in IEC 1508
SRS 1
SRS2
SILx
SILx
Safety Related Systems :
Hardware requirements (2)
Software requirements (3)

Fig. 1

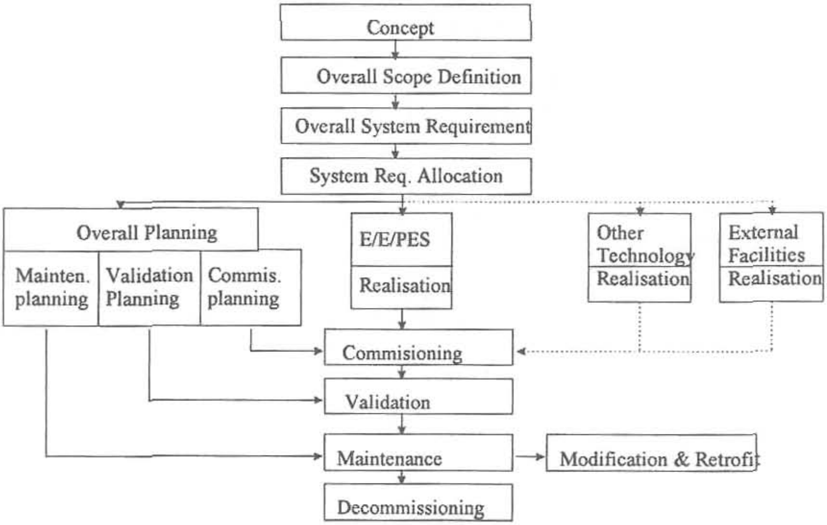
Concept
Overall Scope Definition
Overall System Requirement
System Req. Allocation
Overall Planning
Mainten. planning
Validation Planning
Commis. planning
E/E/PES
Realisation
Other Technology
Realisation
External Facilities
Realisation
Commisioning
Validation
Maintenance
Modification & Retrofit
Decommissioning

Fig. 2

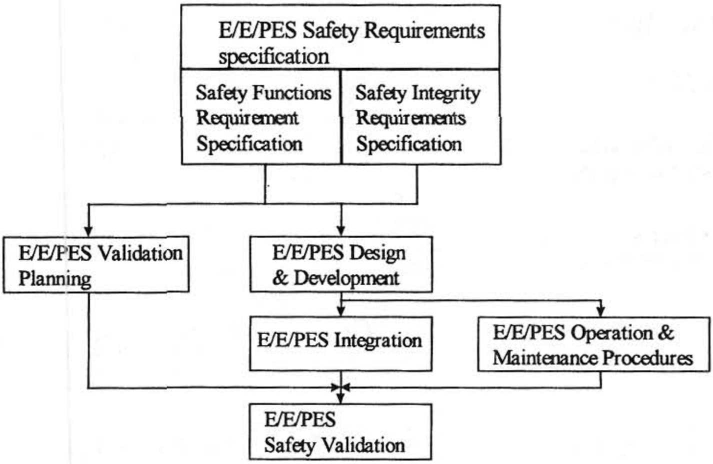
E/E/PES Safety Requirements specification
Safety Functions Requirement Specification
Safety Integrity Requirements Specification
E/E/PES Validation Planning
E/E/PES Design & Development
E/E/PES Integration
E/E/PES Operation & Maintenance Procedures
E/E/PES Safety Validation

Fig. 3

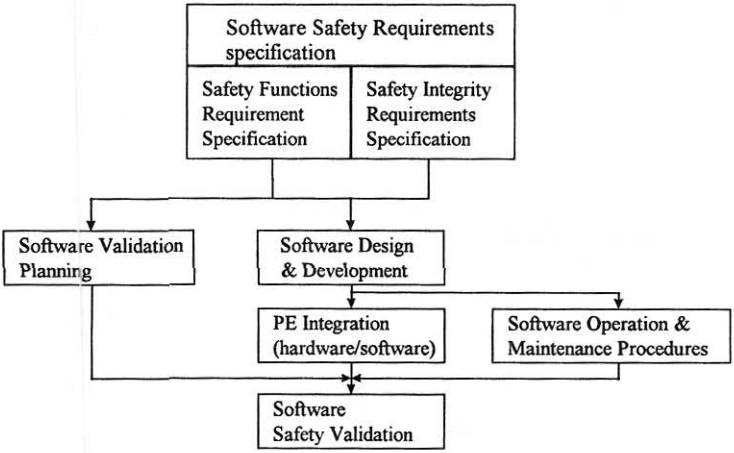
Software Safety Requirements specification
Safety Functions Requirement Specification
Safety Integrity Requirements Specification
Software Validation Planning
Software Design & Development
PE Integration (hardware/software)
Software Operation & Maintenance Procedures
Software Safety Validation

Fig. 4