Chapter 6. HAZOPs Hazard Operations

6.1. Introduction

HAZOP stands for Hazard and Operability. It is a method of study for identifying hazards and operability problems in many operational situations ranging from chemicals and fuels processing through to electrical and machinery systems. It is also finding applications in the planning of operational activities such as emergency response and disaster management.

The HAZOP technique is applied to piping and instrumentation drawings (P&IDs) of a process.

For a new facility, ideally a HAZOP workshop would be carried out at the end of the detailed design stage when all P&IDs have been finalized and issued for detailed design and construction.

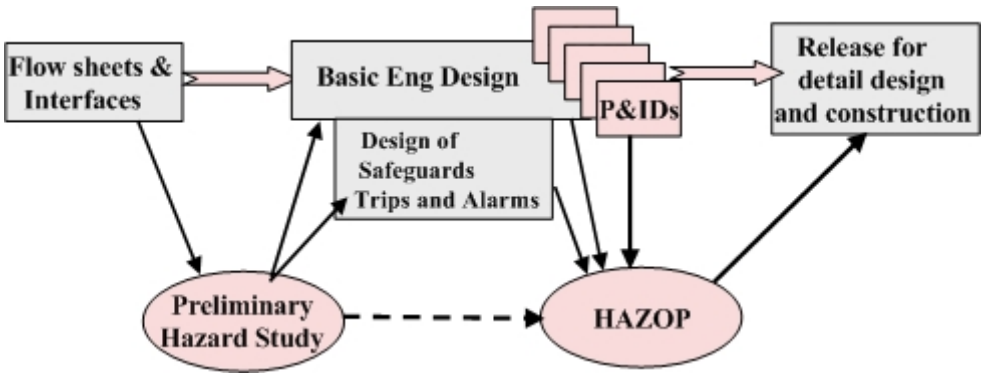

Figure 6.1
HAZOPS should be done when the design is ready for detail engineering

Therefore, in practical terms, the HAZOP workshop is carried out as late as possible in the detailed design stage when P&IDs are as complete as possible while still allowing sufficient time for HAZOP recommendations to be considered and incorporated into the design.

6.2. HAZOP Workshop

In preparation for the HAZOP workshop, the facilitator will have agreed with the client/project on:

- Terms of reference
- Documents required
- Team membership and availability
  - Team Structure
  - Team attitudes
- Estimated duration of workshop
- Venue for workshop meetings
- Reporting method
- Scope of work
- Timing of HAZOP Studies

6.2.1. Team Leader and Team

The first requirement of the team leader is to see that the Hazop methodology is used effectively and productively. The IEC 61882 standard describes the study leader's skills and duties as follows. He should:

- Not be closely associated with the design team and the project
- Be trained and experienced in leading HAZOP studies
- Be responsible for communications between project management and the HAZOP team
- Plan the study
- Agree to the study team composition
- Ensure that the study team is supplied with a design representation package
- Suggest guidewords and guideword-element/characteristic interpretations to be used in the study.
- Conduct the study
- Ensure the results are documented

Who is in the team?

In addition to the team leader the essential players are:

- Recorder or "scribe".
- Designer (process engineer, control engineer, mechanical engineer etc according to project).
- Project engineer (may also be designer).
- User (commissioning manager or production manager).
- Instrument/control engineer.
- SHE expert (mandatory in some countries).
- Contractor and Client representatives.

6.2.2. Good HAZOP Workshop Records

- Record during the HAZOP Workshop
- Record comprehensively
- Record format and content.

6.2.3. Quality HAZOP Reports

Reporting: Depending upon the client/project, the required format of the report may vary.

Contents of the Report: The contents list is based on descriptions in IEC 61882 and EPSC guide.

6.2.4. Hazard Identification and Risk Management

Hazard analysis is used to help quantify the risks associated with a hazard. The task of Hazard analysis includes.

- Estimating how often an incident (Hazardous event) will occur.
- Estimating the consequences to persons, environment and plant.
- Deciding on the required amount of risk reduction (if any).

Two methods of hazard analysis are widely used.

Failure mode and effects analysis (FMEA): looks at possible component faults and tabulates their impact on risks.

Fault tree analysis: looks at a hazard event and resolves the causes into basic events.

6.2.5. Cost Consideration

Market Structure: Hazard analysis & cost consideration rules mandated across an industry will have different impacts on the industry, depending on the market structure of the industry.

Policy Issues: Additional issues that must be considered for a complete evaluation of the benefits and costs of food safety risk reductions relate to information, public versus private intervention, accurateness of illness estimates, marginal benefit-cost analysis and efficiency in production.

Chapter 7. Safety Instrumentation and Machinery

7.1. Introduction

Safety instrumentation is not exclusively an instrument and control engineering subject. The successful implementation of a safety system project depends on the support and knowledge of other disciplines as well as being dependent on a full commitment from company management structures. It requires the environment of a well defined safety management system within the company. Without proper support structures and a good understanding by all involved in defining safety requirements the safety instrumentation on its own will be unlikely to deliver the levels of safety that are expected of it.

The support structures are a crucial part of the assessment scope for compliance with the new IEC 61508 and 61511 standards. It is the responsibility of the instrument engineer to involve colleagues from other disciplines in the safety package. It is the responsibility of the management to see that the safety activities are clearly assigned and supported.

7.1.1. Safety system basics

7.1.1.1. Definition of Safety Instrumented Systems

Safety Instrument Systems are control systems that take the process to a safe state in terms of conditions that may be hazardous or could eventually give rise to a hazard if no action were taken. They perform “safety instrumented functions” by acting to prevent the hazard or mitigating the consequences.

The abbreviation SIS is used for “Safety Instrumented Systems” while the abbreviation SIF means “Safety Instrumented Function” which is the task or function performed by the SIS. These are terms generally used in engineering standards. Other names may be used, however, because of the different ways in which these systems have been applied.

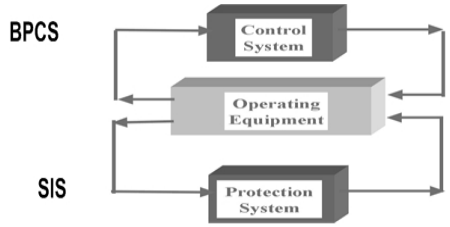

Figure 7.1
SIS operates independently of the Basic Process Control System (BPCS)

The SIS is an example of a "Functional Safety System." In other words safety depends on the correct functions being performed. This distinguishes functional safety from "passive safety "devices such as handrails, or blast proof walls. It is a useful term because it distinguishes the active safety system, in its range of uses, as a system that must function properly to provide safety.

7.1.1.2. The structure of an SIS

Safety Instrumented Systems are normally structured into three parts within a framework or boundary that defines it:

- Sensor sub-system: To capture the data on line from the process
- Logic solver sub-system: To evaluate the data and make decisions on when and how to act
- Actuator sub-system: To execute the required actions on a plant

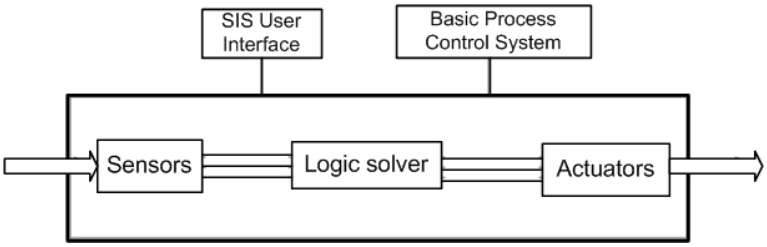

Figure 7.2
Structure of a Safety Instrumented System

Figure 7. shows that the subsystems lie within a boundary that defines the essential SIS while it also needs to have interfaces to its users and those who maintain it as well as to the basic plant controls. Items within the boundary must be engineered to the standards required for functional safety systems.

All three sub-systems must perform correctly to ensure that the SIS can provide the required protection, which brings us to one of the key design principles.

7.1.2. Risk reduction and safety integrity

There is a common saying in the control systems world: "if you want to control something, first make sure you can measure it." We need to control the risks of harm or losses in the workplace due to hazards of all forms. Therefore, Risk is to be measured before controlling it.

7.1.2.1. Measurement of risk

Risk can be evaluated qualitatively or quantitatively. The qualitative approach requires that risk is described in such terms as “high” or “low’ or “moderate”. These terms are only effective if everyone has a good understanding of what they mean in the context of use. Hence a “high risk neighborhood” is not popular with insurance companies. If the terms are well defined or “calibrated” against a scale of values that is generally accepted the qualitative risk measurement can be very effective.

The quantitative approach is easier to define in terms of frequency of events and then the number of people getting hurt, but it is often hard to extract a firm number from a situation without a lot of statistical evidence.

7.1.2.2. Safety integrity

The degree of confidence that can be placed in the reliability of the SIS to perform its intended safety function is known as its “Safety Integrity”. The concept of safety integrity includes all aspects of a safety system that are needed to ensure it does the job it is intended to perform. One of these aspects will be the hardware reliability of the equipment and the way it responds under all conditions. Other aspects include the accuracy with which it has been designed and the level of understanding of the hazards that went into its original design

7.1.3. Protection layers

Now that we see the SIS as a risk reduction element, it is helpful to see how it fits into the context of overall plant safety. This will enable us to see how the SIL target can be adjusted to provide best overall value from the plant safety systems.

Belt and braces

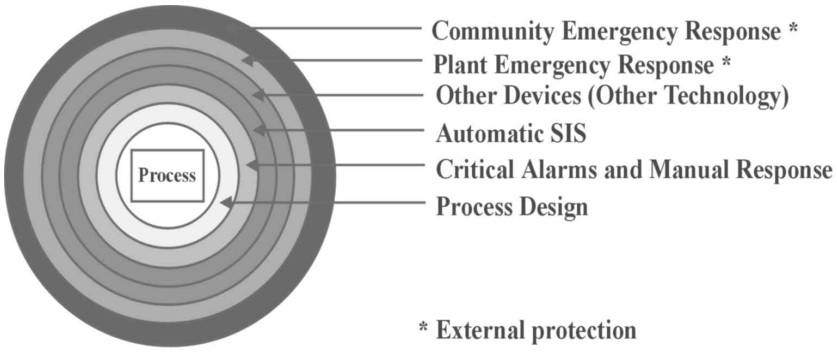

Figure 7. 3
Layers of protection model

The concept of protection layers applies to the use of a number of safety measures all designed to prevent the accidents that are seen to be possible. Essentially, this concept identifies “belts and braces” involved in providing protection against a hazardous event or in reducing its consequences. Figure 7. shows the concept where the core risk, due to a hazard, is seen to be contained by successive layers of protection leaving a minimal or acceptable risk level at the outside boundary.

Protection layers can be divided into two main types:

- **Prevention layers**: These try to stop the hazardous event from occurring
- **Mitigation layers**: Mitigation layers reduce the consequences after the hazardous event has taken place

To summarize, SIS is just one component of an overall risk management strategy for a hazardous activity in a manufacturing plant. For a SIS to be effectively designed and implemented, the following key aspects of a SIS project will have to be assured.

- Identify the hazards and estimate the risks: Hazard studies and hazard analysis
- Define the overall safety targets for each type of risk: The overall amount of risk reduction needed for the hazard needs to be defined by someone who knows what is acceptable: This is a management or corporate responsibility
- Allocate risk reduction functions and RRF's to layers of protection: This defines the risk reduction contribution of the SIS and hence defines its target SIL
- Ensure that each safety layer is managed to deliver the required risk reduction: This requires correct design procedures in each discipline and requires work procedures and responsibilities to be defined and supported by management
- Ensure that the SIS delivers the required functional safety

7.1.4. Safety management principles

Safety management principles help to look at the principles of risk management because they can be applied directly to safety management. Understanding risk management will show us how the application of Safety Instrumented Systems is an integral part of the overall task of managing risk in a company.

The meaning of safety management: Safety management involves the provision of a safe working environment for all persons involved in the manufacturing process. It extends to cover the safety of the environment and the security of the business from losses.

The fundamental components of safety management will include:

- Having a systematic method of identifying and recording all hazards and risks presented by the subject plant or equipment
- Ensuring that all unacceptable risks are reduced to an acceptably low level by recognized and controllable methods that can be sustained throughout the life cycle of the plant
- Having a monitoring and review system in place that monitors implementation and performance of all safety measures
- Ensuring all departments and personnel involved in safety administration are aware of their individual responsibilities

- Responding to regulatory requirements from national and local authorities for the provision of adequate safeguards against harm to persons and the environment.

Maintain a risk register and a safety case report that demonstrates adequate safety measures are in place and being maintained at all times. Safety management is effectively the same as the more general term, risk management, but applied specifically to risks associated with harm to persons, property or environment.

Risk management: Risk management is a very broadly used term and is typically applied to business and organizational activities.

Managing risk

- Requires rigorous thinking. It is a logical process, which can be used when making decisions to improve the effectiveness and efficiency of performance.
- Encourages an organization to manage pro-actively rather than reactively.
- Requires responsible thinking and improves the accountability in decision making.
- Requires balanced thinking "Recognizing that a risk-free environment is uneconomic (if not impossible) to achieve, a decision is needed to decide what level of risk is acceptable".

Requires understanding of business operations carried on, where conformity with process will alleviate or reduce risk.

Conclusions from risk management: We have seen how the generalized models for risk management are directly applicable in safety management. Risk management involves the systematic analysis of risk levels, knowledge of acceptable risk levels and the selection of measures to reduce risk to the acceptable level. The selection of measures involves balancing the level of safety achieved against the cost of achieving it.

When we look at the new application standards for Safety Instrumented Systems it is easy to recognize the same principles being applied. Industry therefore has available a set of recognized standards and practices for designing and operating safety systems that aligns with well established principles of risk management.

7.1.5. The legal framework for process safety

Most industrialized countries have legal frameworks in place that are similar in nature and have been substantially improved in recent years. Safety regulation now emphasizes the need for a complete safety management system. This aims to deal with the fact that many accidents can be traced back to failures to manage the various aspects of safety from identification of hazards through to training and continued monitoring of safety performance.

These provide a good indication of what one should expect to be doing to satisfy good practices anywhere. The most commonly seen principle is that all potentially hazardous activities must be subject to a risk assessment process. This comprises:

- Hazard studies to identify hazards and risks
- Risk analysis to decide the level of risk
- Risk reduction measures to decide if they are needed
- Risk reduction measures to be implemented
- Confirmation that the process is now safe to an acceptable level of risk
- Periodic audits and reviews of safety studies to be carried out

In the case of process industries, plants having a known hazardous process or having major accident potential are required to develop a comprehensive safety case for inspection by authorities. This includes proving that they have a good safety management system in place. They are required to carry out process hazard analysis studies at frequent intervals to ensure the plant risk assessments and treatment methods are up to date with the current version of the plant.

7.1.6. New standards

In this section, we look at the background to the new standards and examine some of the key features that make the standards of great value to system users and designers.

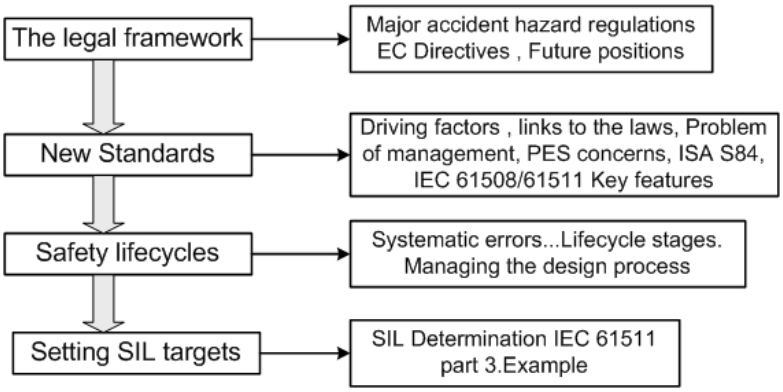

Figure 7.4
Section of roadmap

Two relevant standards exist for SIS practices. Which one is to be used?

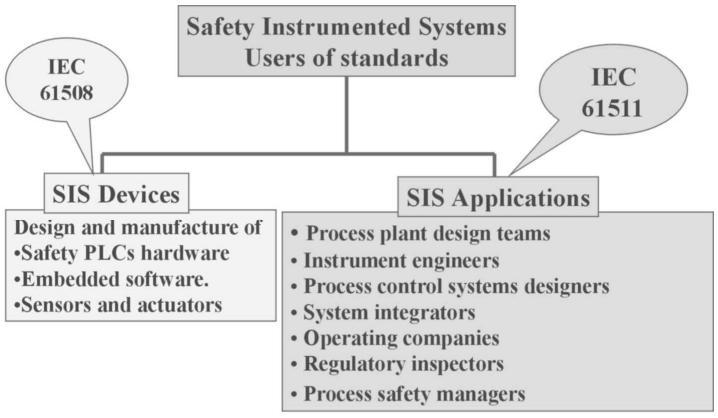

Figure 7.5
Users of the IEC Functional safety standards for SIS

IEC 61511 is to be used by those who are managing, designing, implementing or operating a safety instrumented system application in a process or similar plant. The safety equipment products bought from a system supplier or instrument vendor should be engineered in accordance with IEC 61508. IEC 61511 should be used for plant safety projects and IEC 61508 for design and manufacture of safety system products.

IEC 61508: The standard emphasises the life cycle approach to the overall safety system project. Perhaps the most significant feature to note is that conformity to this standard requires both technical items and the overall management of the safety project to be in compliance with the mandatory parts of the standard.

The scope includes all project stages from initial concepts and hazard studies through to operation, maintenance and modification. The standard covers electrical, electronic and programmmable electronic systems and lays down standards of engineering and quality assurance for both hardware and software.

The standard is large and requires a lot of study for effective use in a company. However it is of great value to both manufacturers and end users and despite some criticisms of its complexity, it has been adopted by many large processing companies as their standard reference for design and operation of Safety Instrumented Systems.

7.1.7. The safety lifecycle

It is important to examine why the standards advocate a safety life cycle approach to an SIS project and see how this approach shows the way to plan and manage a safety project.

The safety life cycle is an orderly sequence of design and builds stages with each activity being mapped out with essential requirements that must be satisfied at each phase. It is visualized by a flow chart showing the procedures suggested for the management of the safety functions at each stage of the life cycle. Figure 7. shows a simplified version that identifies the main stages.

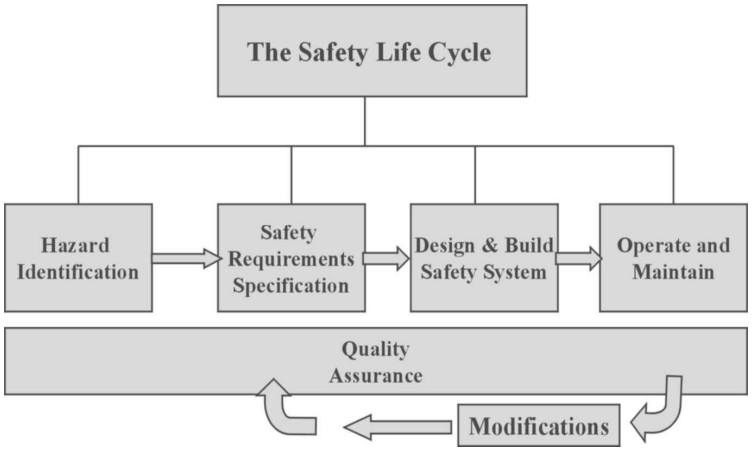

Figure 7.6
A simplified version of the SLC that identifies the main stages

Safety projects begin with a phase where the scope of the plant is defined and the hazards are identified. The hazard study identifies hazards and a hazard analysis leads to the estimation or ranking of risks.

The next stage involves determining the risk reduction needed to meet a safety target and this leads to the production of the Safety Requirements Specification (SRS); a key document that will be a design reference throughout the life of the safety system.

The design and building stages of the SIS project can now follow from the approved baseline of the SRS. As this stage progresses, the project team will continue to carry out verification exercises to ensure that the design remains true to the SRS and that the SRS remains true to the hazard studies.

Before the SIS enters service, it will be subjected to a rigorous validation exercise that involves testing of the functions against the details defined in the SRS. It then moves into the operations and maintenance phase where a strict set of procedural rules will be implemented.

Change management procedures remain in force throughout the safety lifecycle and any recorded changes are recycled back through the relevant design and testing stages. This ensures that all documents and decisions remain current for the present state of the plant.

7.1.8. Introduction to safety PLCs

Safety PLCs have become the dominant form of logic solver in the past 10 years through their ability to provide shared logic solver duties for many safety functions within one SIS. They offer the facilities needed by most safety functions to perform fairly simple logic combined with efficient operator interfacing and secure management of the program logic.

Safety PLCs are specially developed for their tasks through the provision of extensive diagnostic coverage using internal testing signals operating between scanning cycles of the application logic. Effectively, the PLC detects its own faults and switches itself into a safe condition before the process gets into a dangerous condition.

The software of a safety PLC is specially developed to have a range of error detecting and monitoring measures to provide assurance at all times that the program modules are operating correctly. The application programs are developed with aid of function block or ladder logic languages where each function has been extensively tested for robustness and only limited configuration options are available.

One major objection to safety PLCs has been their cost and this is particularly a problem for small plant applications. This is gradually being addressed as smaller and cheaper units are now available.

7.1.9. The cost of ownership

Having discussed something of the project activities and some technical aspects of safety system, it may be helpful to consider the issues of cost and justification for installing an SIS.

The justification for installing an SIS may be for one or more of the following reasons:

- It is essential for safety where no alternative methods exist
- It is the lowest cost option for safety
- It helps prevent environmental harm and/or guards against emission limit violation
- It helps protect against asset losses through plant damage and lost production capacity.

From the management perspective, it will be essential to have a measure of the costs involved in buying, maintaining and operating a safety system. If the true operating costs of the SIS can be evaluated, these will help to identify potential for cost savings and performance improvements. It will help to have an approximate cost model that can be used as a basis for establishing the total costs involved in SIS. With this in mind, it is possible to show how the case for performance improvement may be justified by further reducing operating costs.

7.2. Introduction to IEC 61511 and the safety lifecycle

The idea of a safety lifecycle model is to plan and control the various activities of a project so that each step follows logically and accurately from the previous step. The main steps are:

- Identification of plant scope and its hazards
- Evaluation of any risks to determine risk reduction needs
- Allocation of risk reduction duties to SIS and non-SIS layers of protection
- Development of the safety requirements specification
- The building and testing of the SIS to specification (known as the realization phase)
- Installation and testing of the SIS
- Operation and maintenance of the SIS
- The managing of changes to the SIS design or equipment

Each phase of the lifecycle requires input information and delivers output information. The relevant clauses of the standards define the inputs, activities and outputs for each phase.

IEC 61508 offers a safety lifecycle model that will serve any project and many companies may elect to use this version for their applications. IEC 61511 offers a similar project model but it has been designed specifically for process applications.

7.2.1. IEC 61508 SLC version

IEC 61508 version of the SLC is the most general version and forms the basis of all the IEC standards. Box numbers are used to reference a detailed set of clauses defining the requirements of the standard for that activity.

The clauses are easy to follow because they are defined in terms of:

- Scope
- Objectives

- Requirements
- Inputs from previous boxes
- Outputs to next boxes

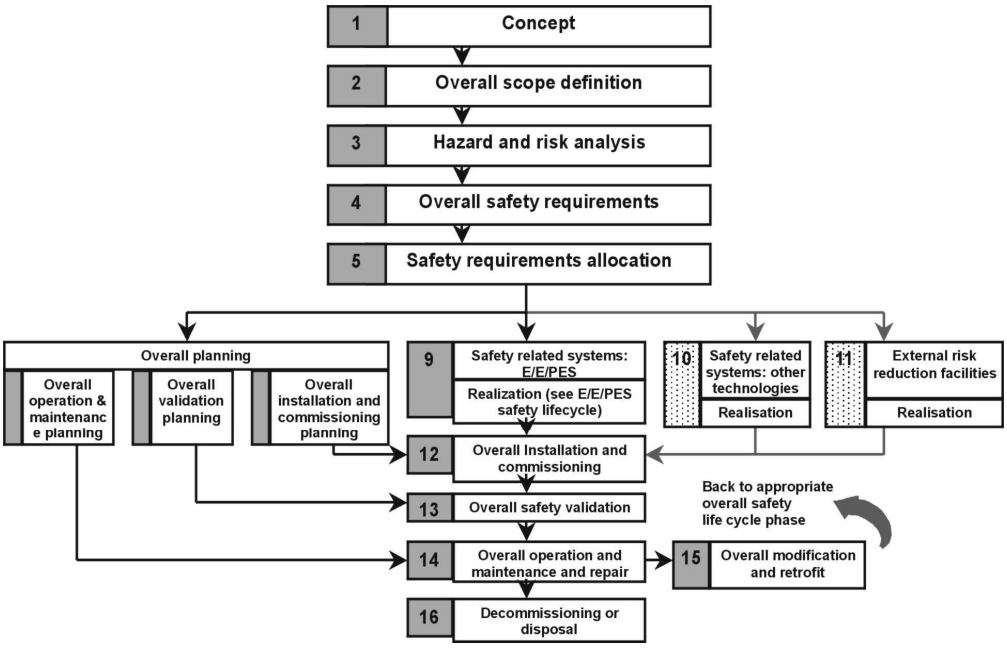

Figure 7.7
IEC 61508 SLC version

Developing the overall safety requirements: The first 4 phases deal with the tasks of defining the scope of the plant, identifying hazards and risks and deciding the overall safety requirements. This work has been defined as an integral part of the standard as it must be done according to the correct procedures to achieve compliance.

Safety allocations: Once the overall safety targets have been established, the SLC moves on to the "Safety Allocations" phase where the various layers of protection are defined and allocated a certain portion of the risk reduction task. This results in the SIS risk reduction task being clearly identified and hence the SIL targets can be defined for each individual safety function.

Realization phase: These stages are followed by the "realization" phase. This term describes the job of actually building the safety system and implementing any software that it contains. Large sections of IEC 61508 are concerned with the details of the realization phase and there are whole lifecycle models for the activities contained within this stage.

Validation and operations: Once the SIS has been built, the lifecycle activities move on to the "installation, commissioning and validation". All the standards place great emphasis on validation. This activity is seen particularly in the form of the final site acceptance testing using methods that test the SIS response under plant operating conditions in the most realistic way possible.

Finally we get to use the safety system for real duties and arrive at the operating and maintenance phase.

7.2.2. IEC 61511 SLC Version

Shown in Figure 7. is a version of the SLC model. Comparing this version with the 61508 model, we can see that the tasks have been grouped into more familiar sets of activities that will match up easily to the natural progression of a process safety project.

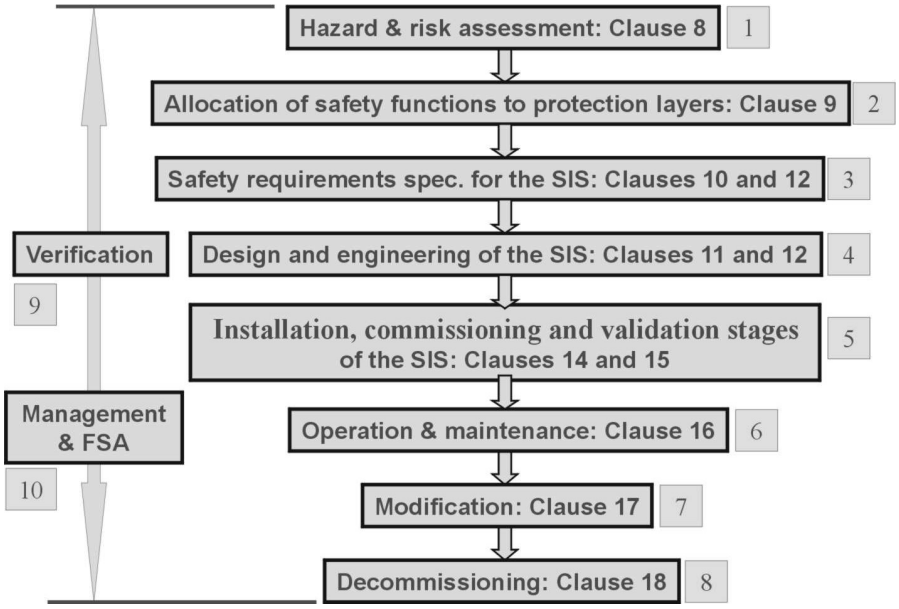

Figure 7. 8
IEC 61511-safety lifecycle model

Phase 1: Hazard and risk assessment

The model refers us to Clause 8. This describes objectives and requirements.

The first phase of the SLC delivers a sound basis of information about the hazards and records assumptions made about the risks. It is the essential foundation for the safety functions that will be needed.

IEC 61511 does not set out to provide detailed requirements for the hazard and risk assessment phase. It restricts itself to those aspects relevant to specifying the SIS requirements.

Phase 2: Allocation of safety functions to protection layers: clause 9

The idea of this phase is to decide on how much risk reduction is to be allocated to the identified or planned layers of protection.

The objectives of this phase are to:

- Allocate safety functions to protection layers
- Determine required safety instrumented functions (SIF)
- Determine the associated SIL for each SIF

The requirements clause requires us to identify all risk reduction measures and define each Safety Function (SIF) with its own SIL.

SIS safety requirements specification: clause 10

The Safety Requirements Specification (SRS) is a formalized and detailed document describing all essential functions of the SIS needed for the plant. This phase with the preceding two included is known in IEC 61511 as “Stage 1”.

SIS design and engineering: clauses 11 and 12

The requirements of this section comprise all the essential design constraints that the standard mandates. This is therefore the place to look for any design rules that are to be imposed on the SIS.

Clause 12 describes the requirements for the application software engineering and includes selection criteria for the utility software. This is the programming tools, compilers and display software that enables an engineer to configure the application logic using a high level language such function block or ladder logic. The specially restricted versions used in safety PLCs are described here as “Limited Variability Languages “or LVLs.

The end of this phase is achieved when all the design has been done, all the components and instruments have been decided and the software has been written, tested, integrated into the hardware platform and tested as a complete logic solver. Completion of the design and engineering activities is also known in the standard as “Stage 2”. Optionally this stage can include the Factory Acceptance Test (FAT).

SIS Installation, commissioning and validation: clauses 12.3,14, 15

This phase begins with the equipment at site and the logic solver FAT completed. Clause 12.3 is included here as this concerns safety validation planning.

After installation, Clause 14.2.3 outlines the commissioning requirements in terms of essential features that must be checked. The list includes things such as power supplies, removal of packaging, instruments calibration, instruments and logic solver operations and loops to be checked.

Clause 15 then describes the essential requirements for safety validation. In process control terminology this is the start up acceptance testing. Validation is of critical importance to safety system installations because it is the only way of knowing that the final result of the design and building effort can provide the required safety.

Completion of these activities is also known in the standard as “Stage 3”.

SIS operation and maintenance: clause 16

This phase covers the operating life of the SIS on the plant. Clause 16 of the standard defines the essential subjects for routine and abnormal operation of the SIS. The objectives are to ensure that the required SIL is maintained during Operation and Maintenance (O&M) and conversely to see that maintenance is adequate to keep the SIL at its intended level.

This stage is also known in the standard as “Stage 4”.

SIS modifications: clause 17

The objectives of this phase, defined in clause 17, are: "those modifications to any safety instrumented system are properly planned, reviewed and approved prior to making the change; and to ensure that the required safety integrity of the SIS is maintained despite any changes made to the SIS."

The completion of a modification activity is also known as "Stage 5"

SIS decommissioning: clause 18

This phase is similar to the modification phase because it requires an impact analysis on the effects on safety of de-commissioning.

Verification activities: clause 7 and 12.7

Clause 7 of IEC 61511 details the requirements for verification, which is essentially aimed at establishing that each phase has been completed properly and that the results are verified to be in accordance with the objectives of that phase and is traceable to the input information.

Assessment, auditing and revision: clause 5

Functional safety assessment and auditing are part of the overall requirements of IEC 61511 for management of functional safety. Clause 5 of IEC 61511 discusses these requirements. We have considered the organizational issues but when it comes to any of the project life cycle, the standard also requires that we carry out an assessment of how well the safety objectives have been met for that project.

7.3. SIS configurations for safety and availability targets

Once the requirement specification is established, the final design of the SIS can be carried out. The design process is concerned with finding suitable instruments in an independent SIS loop that has a structure or architecture appropriate to the SIL reliability targets. This also takes into account, the expected reliability and failure modes of the instruments. If the instrument is good, there is less need of redundancy for safety but this choice has to be made within a framework of rules.

7.3.1. The design process

To establish the design process, it helps to first look at what IEC 61511 requires to be done to build the SIS to meet the targets. Figure 7. spells out the evaluation process that should be followed once a design concept has been proposed. The preliminary evaluation of these points can be done at the concept stage and these points should be confirmed before the final design.

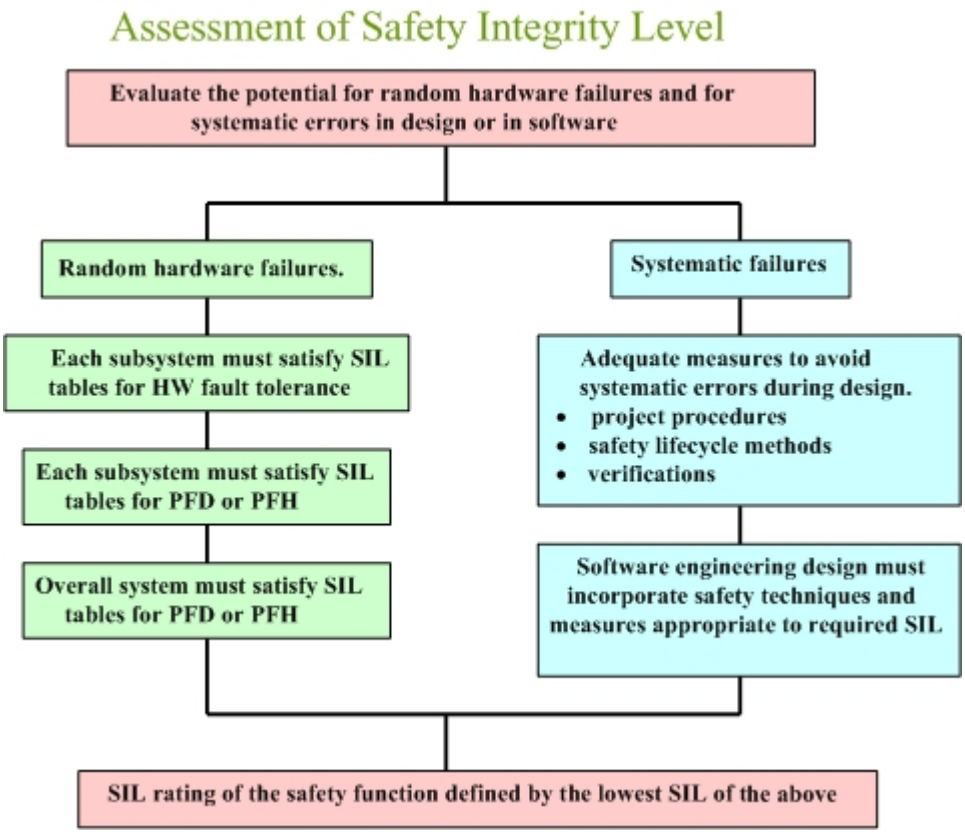

Figure 7.9
Overall design requirements for meeting the SIL target

Figure 7. shows that the assessment of the safety integrity level for an SIS design is divided into two measures a) that avoid systematic failures and b) that avoid random hardware failures. We will consider one of the ways in which hardware design can be developed to minimize the hardware failures. This introduces the subject of hardware fault tolerance.

7.3.2. Safety reliability versus availability for production

Functional safety is achieved by the SIS doing the safety job and when failures occur, the system must act in a manner that still ensures safety. i.e. the system will fail safely or will indicate a fault for suitable action. For a single channel SIS, this usually means shutting down the process even if it is only for the reason that the safety system has found a fault. This behavior meets the needs of the SIL target but it may not satisfy the business objectives of the process.

What is desired is a plant where safety is achieved at a reasonably economic cost. The components of cost here are:

- The capital cost and maintenance cost of the SIS
- The cost of accidents should they occur, including the production losses
- The lost production costs associated with achieving safety

The third item depends on whether or not the process operating costs are sensitive to downtime.

7.3.3. Architectures and fault tolerance concepts

Fault tolerance is one of the most important underlying principles of all safety systems whether used in chemical plants, machinery, automobiles or in business planning. If a safety system can still provide protection in the presence of dangerous faults, it reduces the chances that an accident can occur.

7.3.3.1. Terminologies

Dangerous failure: IEC 61511-1 defines dangerous failure as: “failure which has the potential to put the safety instrumented system into a hazardous or fail-to-danger state”.

Dangerous detected failure: If the dangerous fault can be detected by some method of diagnostic testing or by the way the circuits are arranged, it will be known as a “revealed” or “overt” fault. When found by a diagnostic test procedure, these are usually known as “dangerous detected failures”.

Safe failure: Conversely this is a failure that “does not have the potential to put the safety instrumented system into a hazardous or fail-to-danger state.” It is also called “nuisance trip”.

Safe detected failure: Some safe failures may not be revealed by causing a trip but they may be detected by other means such as a diagnostic test.

Common mode failure: Applies to any of the above failure modes where they are likely to affect two or more devices or instruments at the same time for the same reasons. Where redundant instruments of the same design or the same principles are used, the likelihood of common mode failures can be in the range 5% to 20 % of all failures. Without diverse instruments, common mode failures will limit the availability benefits achieved through redundancy.

Fault tolerance: Hardware fault tolerance is the ability of a system to continue to undertake the required safety function in the presence of one or more dangerous faults in hardware. Hence a fault tolerance level of 1 means that a single dangerous fault in the equipment will not prevent the system from performing its safety functions. A fault tolerance level of zero implies that the system cannot protect the process if a single dangerous fault occurs in the equipment.

Safe failure fraction: This parameter is vitally important for the safety integrity or confidence level and it will determine if greater levels of fault tolerance has to be built into a given application.

7.3.4. Identification of subsystems

The first step in evaluating the structures of an SIS is to recall that the SIS is conveniently divided into subsystems of Input, Logic and Actuator. See Figure 7.. These subsystems must be decided at the beginning of the design procedure. It is not always as simple as identifying the instruments and the valves or motors because the signal transmission and conversion devices will also fall into the sensor and actuator subsystem. What about the input and output circuits of the

PLC logic solver? Sometimes these can be lumped in with the sensors, but usually they are part of the logic solver.

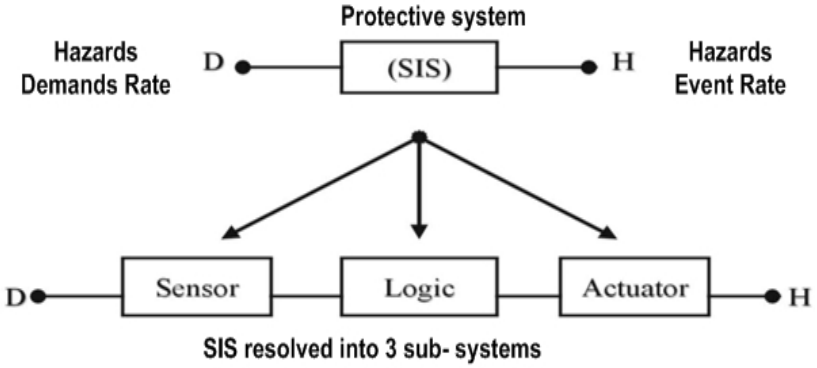

Figure 7.10
The SIS must first be resolved into 3 subsystems

Once defined, each subsystem must be evaluated individually for its ability to meet the SIL target. Because they are working in series, any failure of a sub-system will contribute to the failure of the overall SIS. Each subsystem must be qualified to meet the SIL and when joined together, the overall SIS must still satisfy the SIL target for PFD.

7.4. Selection of sensors and actuators for safety duties

7.4.1. Field devices for safety

Field devices basically comprise the sensors to provide the input information to the logic solver and the actuation devices required to carry out the trip function when the demand comes along. They are supported by the wiring and process connection arrangements. Taken together, they comprise the area with the greatest potential for problems. They are also the area where most engineers have a chance to exercise their skills and judgment in design, selection and maintenance.

7.4.2. Sensor types

Sensors are devices that can represent the value or status of a chosen parameter in a form suitable for decision-making in the SIS logic solver. Some illustrations are shown in Figure 7.11.

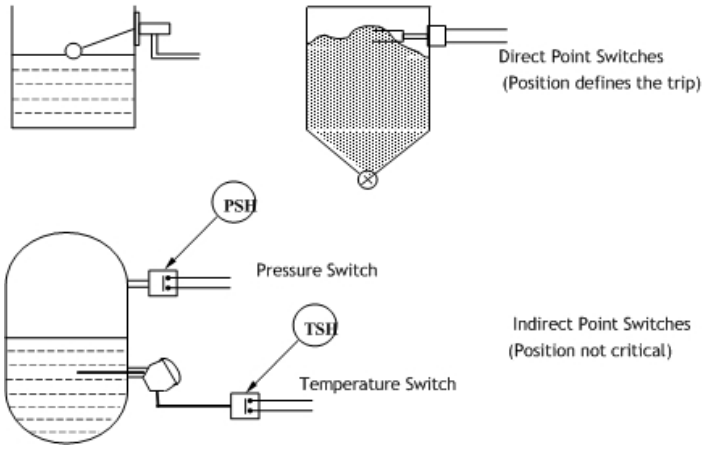

Figure 7.11
Categories of sensors

There are two basic categories of sensors: switches and transmitters that are discussed below.

A list of potential causes of failures in sensors: It is helpful to have a list of potential failures in sensor systems for reference in each application. Such a list also helps to identify ways in which the EUC control system can fail and create a hazardous event.

- Components of the instrument
- Accidental isolation
- Hostile process conditions
- Wiring errors
- Environmental electrical
- Calibration errors
- Response time
- Power supplies
- Lightning damage

7.4.3. Actuator types

The term actuator can be misleading. The devices used by the SIS to actuate the protective function should more correctly be called final elements.

Final elements are most commonly seen as process valves with air or hydraulic power to actuators that are spring loaded to close on release of the actuator fluid (typically described as “air to open, spring to close”). Or they are simply motor starter contactors that must be de-energized to break the power supply to the drives that must be tripped.

In large power control applications or in large valve applications, the final elements may have to use active power to carry out its trip task. These applications require backed up (i.e. redundant) power supplies to operate heavy-duty power isolating contactors or to drive motorized valves. In such cases the power system becomes an integral part of the final element and would require diagnostic monitoring.

In all cases there must obviously be a high degree of assurance that the final element will do the job when called upon to act. Hence there will be an emphasis on diagnostics and regular proof testing.

7.4.4. Guidelines for application of field devices

The application of any measurement and control device for duties in a safety instrumented system must take into account two primary considerations:

- The device must be applied using the best design techniques to minimize failures
- The device should meet the design requirements of IEC 61508 or IEC 61511

Given the diversity of failure modes, the design techniques required to minimize the fail-to-danger rate will be application dependent. The ground rules for design to minimize dangerous failure rates include the following techniques:

Fail-safe design: Design sensors and actuators to result in fail safe responses to their most likely failure modes. Then review spurious trip rates to see if they are acceptable.

Separation: Ensure separation between BPCS and SIS sensor/actuator systems as far as practicable.

Diagnostics: Search for ways of introducing diagnostics to frequently confirm the healthy operation of the device.

Redundancy: Use redundancy where a reduction in fail to danger rate is needed or where a low spurious trip rate is essential.

Diversity: Search for diversity of sensors where the risk of common cause failures is significant.

Armed with the knowledge of failure possibilities and knowing the redundancy rules we should now be ready to specify and select particular types of instruments for any given application. But, firstly we must remember that whatever instrument we use it must be qualified for use in our SIS.

7.4.5. Instrument selection

The IEC standards do not attempt to dictate what instruments to use. The ISA standard does offer some basic guidelines. The selection is almost entirely dependent on the application; hence it is not practicable to list any hard and fast rules about what instruments to use. The following points have been gleaned from the ISA standard and from personal experience.

Flow meters

- Vortex Shedding and Magnetic Flow meters are preferred due to proven performance
- Head-type flow measurements are to be avoided, if possible, due to impulse line problems – leakage, condensation, freezing and drift

Temperature sensors

- RTD and Thermocouple types: require burnout detection and alarm

- Be careful to locate sensors properly
- Ensure probes are seated in thermo wells
- Avoid thermistor types
- Infra red types with diagnostics

Pressure

- Gauge, differential pressure and absolute pressure types are very reliable
- Ensure range and trip setting are compatible
- Ensure impulse lines do not risk condensate build up or blocking
- Use remote diaphragm seals instead of long leg links, but: beware of drift; beware of vacuum effects on diaphragms

Level

- Wide range of devices – good possibilities for diversity
- Check process for effects of aeration, entrained solids, density shift
- Differential pressure types are reliable but prone to process effects
- Ultrasonic and radar types have smart electronics, hence:
- Check compliance with IEC rules for PES
- Exploit diagnostics
- Check process for foaming, vapor, boiling
- Nucleonic types – reliable, often with diagnostics

Analyzers: reliability and proven performance

- Gas detectors often used in redundant modes
- Lower for diagnostic facilities
- Use comparative process signals where possible to support diagnostics

Limit switches

- Use best quality industrial grade
- Sealed contacts where possible
- Proximity switches available with diagnostics
- Check leakage currents in OFF state to avoid false ON condition at SIS

Selection factors

- Material compatibility
- Shut off duty, shock loadings, leakage, fire resistance
- Speed of response
- Element types most used are: Ball, Gate, and Globe
- Butterfly valves used on air systems, large sizes
- Spring/actuator performance margins. Fail close/open
- Requirements for diagnostics
- Requirements for limit switch and/or position transmitter
- Sharing of valve duties with BPCS
- Cost

Solenoids: Critical components

- High-grade versions only, Stainless steel bodies

- Rated for outdoor service – sunshine to snow or enclosed
- Venting capacity to meet speed of response
- Use direct acting types – avoid pilot operated
- Use direct mounting, avoids risk of pinched vent lines

Installation design features

- Direct connections to process for field sensors, separate taps and impulse lines
- Dedicated cables, junction boxes, airlines and termination panels
- Dedicated power supplies
- Identification such as painting and labels
- Devices to have local indication to assist proof testing.

It is important for keeping the safety integrity of field devices in order that details of the installation do not lead to accidental malfunctions. It is useless if a perfectly good pressure transmitter can be accidentally shorted out or cross connected to another circuit. Hence segregation of shutdown system wiring and special identification are features that will repay the extra effort involved.

7.4.6. Technology issues

This section considers the impact of new technologies on SIS field device practices. The two items that have a major impact on field devices are instruments with self-testing diagnostics and bus communications. We need to consider how these technologies fit in with SIS concepts.

Intelligent field devices: Advantages and disadvantages

Intelligent instruments offer safety systems the advantages of being able to perform better quality measurements supported by internal diagnostics. Self-testing and safe responses to faults will help increase the safe failure fraction of a field device.

There are disadvantages for safety systems. Firstly, there are the general reservations about the risks of programmable systems in safety applications. These include:

- The potential for systematic errors in the software
- User configurations that may create new untested versions of the instrument
- The unauthorized in-service changes to settings, zero, range, mode etc.

One of the main purposes of IEC 61508 and IEC 61511 was to address these types of issues and find ways of dealing with them. Hence with the aid of safeguards based on IEC 61508 through design or IEC 61511 through prior use it becomes possible to use intelligent instruments in a safety system provided we stick to the rules. In brief, the answers to the above possible problems are:

- Instruments using PES should be manufactured using hardware and software engineering procedures in accordance with IEC 61508
- Limited ranges of software instructions should be made available to the end user to program the instrument within a tested range of configurations

- The program of the instruments should be password protected

Unless the above requirements are met, the fault tolerant rating of the instrument is loaded down by comparison with a non-PES version (see Redundancy section).

7.5. Selection of safety controllers

The logic solver stage of an SIS is where all the decisions are made to execute the safety function. Some SIS designs can actually operate without a logic solver if the sensors have the ability to directly operate the final elements. For example, a high-pressure trip switch connected directly to a solenoid valve releasing a shut off valve. However, in most applications the need for additional logic or signaling dictates that some form of logic function must be performed.

Traditionally, relay systems have been used for the logic function and these remain an attractive option for simple applications. In practice, most process plants, with hazardous materials, find the need for several safety functions and with this comes the need to manage the safety trips in an efficient manner. The need for interfacing to the operator increases and often there is a linkage between one trip function and another. As complexity grows, so does the need to have efficient supervision and control of the trip functions and their equipment. There is a need to be sure that all logic functions perform in such a way that start up and other plant operations interact smoothly with trip systems - the sophistication of the safety function begins to increase. These pressures, as well as the concern that relay systems are difficult to make secure and reliable as they grow in siz,e have caused many users to move first to solid-state hardwired logic and then to PLC based logic solvers.

The need for PLCs to have special protection against unpredictable failure modes and untested software logic combinations was realized many years ago and this has lead to a range of possible solutions being developed. The new standards addressed many of the potential problems of using basic PLCs for safety and have delivered a range of requirements that are usually satisfied by the specially designed safety PLCs. IEC 61511 has also addressed the issue of process plant equipment where a standard PLC has been provided with certain safeguards and has proved itself to be effective and reliable for safety. Rather than declare these PLC’s unacceptable, it has made provision for these to be used with the safeguards being well defined.

With these choices available, the end user shall have a reasonable knowledge of the characteristics of the principal types of logic solver systems on the market in addition to the ability to relate these features to the needs of the project. This chapter outlines the operating principles of various types of logic solver, which should assist, with the initial steps of selecting the type and scope of logic solver to be used for the project.

7.6. System integration and application software

The objective of this module is to provide some guidance on how to deal with the application software stages of a SIS project. From the point of view of the end user of a safety PLC system, the software can appear to be deceptively simple. As soon as PLCs began to appear in safety systems, the specialists realized that there was a great danger that systematic design errors could be introduced into the logic

solver through problems with operating systems and through errors in the application logic.

The problem with software in safety systems is that it can be very difficult to control exactly what has gone into the system. Unacceptable in a safety system is an unpredictable response to a hazard demand.

IEC 61508 was the first major standard to lay down basic concepts and requirements for the control of systematic errors in software for safety applications. Part 3 provided comprehensive details of quality assurance procedures designed for the development of embedded operating system software as well as for the application layer. The impact of this approach is found in the availability, for end users, of certified operating systems supported by certified programming packages.

IEC 61508 part 3 is suitable for use by a manufacturer specializing in safety system products but is far too complex for the average instrument project team seeking to configure the logic for its safety functions. IEC 61511 has provided a more practical set of requirements and guidance notes designed for the application stage of a safety project while still following all the essential requirements of IEC 61508.

7.7. Programming tools

For most process plant applications, the engineer will require access to a configuration package supplied as part of the PES solution package. It may be helpful here to know the basic features to look for in a programming package.

It is a fundamental requirement of a safety certified PLC that the integrity of the whole software package is assured. Thus the embedded software and the application tools should be developed by the same vendor and should be proven to meet all the constraints of the IEC standard when operated as a complete facility.

IEC 61511 part 2 describes the programming and support tools as “the developers’ workbench”.

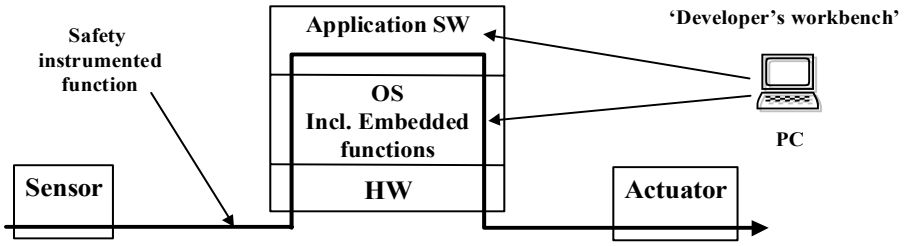

Figure 7.12
Programming tools

Tasks

- Configures logic solver I/O and communication subsystems
- Programs the logic and arithmetic functions of the application
- Facilitates testing of applications

7.8. Machinery safety

The safety of machinery affects all of us in everyday life, at home or at work or at leisure. Machines are part of our lives and our safety is dependent on the machines being safe for us to use at all times.

The following are the aspects that show how a machine should be made safe.

- **Physically Safe:** No sharp edges, spikes or projections that can be bumped into. No chance of it falling on someone. No ways in which it can throw objects around or let out jets of steam or noxious gases. No chance of explosions or radiation.
- **Mechanically safe:** The moving parts must not be able to hurt someone. If there's a risk that this can happen, then protection measures are required; fixed guards, movable guards, area sensing devices that stop the machine quickly if someone is in the danger zone.
- **Electrically safe**: There must be no chance of an electrical shock or a dangerous electrical circuit arrangement.
- **Functionally safe:** All the stops switches, guards and safety sensing devices are there to protect us must function properly. All safety controls that prevent movement at the wrong time must be reliable.

Safety measures based on sensors and control systems that are designed to ensure safe working of the machines are also known as Safety-Related Electrical Control Systems (SRECS).

7.8.1. Machinery and controls

Any assembly of devices designed to protect people from hazards or injuries that could arise from the use of the machine can be considered to be a **machinery safety system**. The machinery safety system may also provide protection for the machine itself or other machines against damage due to malfunctioning of the machine.

Fixed guards are usually the first line of defence. These prevent a person from being hurt by the machine, but in many cases the situation will require a logical action from the control system to prevent movement or other physical events from happening until safe conditions are proved to exist. These protective measures are the "safety functions" to be provided by the control system. Those parts of the basic control system, as well as any specially provided safety parts, are known as the **"safety related parts of the control system".**

Safety related controls include all parts involved in the safety function. In other words; the sensors, logic or evaluation units and the final drive interlocks and contactors or valves all belong to the safety control system.

While some safety devices can simply be passive guards such as shields or covers, it is most likely that many of the safety functions will be provided by a combination of mechanical devices and a safety related electrical control system. (SRECS).

7.8.2. Distinction between Machinery and Process Safety Control Systems

For process technology, the identification of unacceptable risks leads to a set of risk reduction measures that often include what is known as a safety-instrumented system. (SIS) or emergency shutdown system.

- Process plant shutdown systems define the grade or performance of their applications in terms of safety integrity levels or SILs.
- Machinery safety systems have been traditionally defined for performance by "safety categories" but will in future be moving to the same basis of SILs for complex and/or programmable safety systems.
- Process plant safety is subject to different regulations and design standards from those applicable to machinery safety, but the basic principles are essentially the same.

Some interesting questions arise when a section of process plant has a large and dangerous machine in the plant.

- Is the hazard coming from the process or from the machine?
- Which regulations are applicable?
- What design standard shall we apply?

If the hazard is due to the process, the plant safety systems can deal with it. If the machine presents hazards of its own the safety requirements will fall under machinery safety regulations.

7.9. Guide to Regulations and Standards

This topic provides outline information on the typical safety-relevant regulations and legal requirements applicable to both the supplier and the end users of machinery.

The legal aspects of moving machinery safety are generally arranged to cover two primary stages in the life of a machine.

- **Safe Manufacture –** this includes design and installation of plant and equipment.
- **Safe Operation –** this includes maintenance and modification of plant and equipment.

Generally, Laws and Regulations deal with these two aspects separately although regulators are increasingly aware of the need to improve the links from the supplier to the user.

Essentially, the safety of machinery must be tackled from two sides:

- The manufacturers and suppliers must build machines that are safe to use
- The users of machines (i.e. employers and workers) must ensure the machines are used in a safe manner and the workplace environment is safe for the workers.

Principles of EU Directives :

The sources of EU law through which the EU regulations are implemented can be divided into three categories,

- **Primary sources** - comprising the founding treaties, Community Acts (such as SEA) and further treaties (such as Maastricht or accession treaties).
- **Secondary sources** - comprising of regulations, directives and decisions. Through this EU implements the policy in more detail.
- **Non-legally-binding** - sources-opinions and other non-treaty acts (such as guidelines, resolutions, communications etc.)

Supply side laws: the EU "New Approach" Directives :

The term "New Approach Directives" applies to a range of EU directives that have certain basic principles in common. These include:

- Mandatory essential provisions, which apply to the product.
- Requirements for member states to ensure that products not in conformity with essential provisions are not allowed to circulate within the member states.
- The manufacturer is provided with the opportunity to certify conformity with the relevant directives. This leads to the manufacturer placing the CE mark on his product if it is claimed to conform.
- Legislation no longer specifies that specific standards have to be met. However, It can be "reasonably assumed" that when Harmonized standards are met, the associated goals of the EU directives are fulfilled.
- The manufacturer achieves conformity by compliance with a national law or regulation. This implies compliance with the equivalent laws in any other member state.

The CE mark is the characteristic symbol shown in the Figure 7.. This is applied to a product when the manufacturer or an appointed body certifies that the product conforms to the requirements of all applicable EU Directives.

Figure 7.13
The standard CE mark signifying a claim to conform to relevant directives

The products, which come under European Directives, and are to be placed on the market in the EU, must bear CE marking as it is a legal requirement. The affixing of CE marking to machinery by the manufacturer is to show its conformance to

that essential requirement as per 'New Approach' European Directives. The CE mark shall be distinct, visible, legible and indelible.

7.9.1. Some Machinery Safety Standards

7.9.1.1. Type A Standards – Basic Standards

These provide essential information for all machine builders. Generally there are three standards, which relate to machine safety:

- EN 414 - Safety of machinery: Rules for the drafting and presentation of safety standards. This defines the way standards are to be written.
- EN 292 Parts 1 & 2 - Safety of Machinery: Basic concepts, general principles for design. This defines the concepts of machine safety and specifies the general principles and techniques to help machine designers achieve safety. It incorporates in Annex 1 the EHSRs defined by the Machinery Directive
- EN 1050 - Safety of Machinery**:** Principles for risk assessment. This defines how to assess the risk of injury or damage to health, so that appropriate safety measures can be selected.

7.9.1.2. Type B Standards – Group standards

B standards are subdivided into two groups,

- Group B1: These cover higher-level safety aspects for design and are always applicable. E.g; ergonomic design principles, safety distances from potential sources of danger, minimum clearances to prevent crushing of body parts. Examples of these are EN 294 on safety distances and EN 563 on temperatures of touchable surfaces;
- Group B2: These cover safety components and devices for various machine types. These are applied when required. E.g; emergency stop equipment, two-hand controls, interlocking/ latching, non-contact protective devices, safety-related parts of controls. EN 281, on the design of pedals, is an example.

Standard EN 954 – 1 is of particular interest here, to control and electrical engineers, because it provides a method of defining the safety related parts of control systems used in machinery applications. This is the standard that defines our control system functions into safety categories such as 1,2, 3 or 4. It has close similarities to the safety categories used in safety instrument systems used for process control where they are known as Safety Integrity levels or SILs.

7.9.1.3. Type C Standards - Product Standards

These identify specific types or group of machines and involve the machinery-specific Standards. These inform machine manufacturers and users about the specific safety precautions they should take and safety devices they should use. e.g. for machine tools, woodworking machines, elevators, packaging machines, printing machines etc.

Chapter 8. Hazardous Areas and Intrinsic Safety

8.1. Introduction

A HAZARDOUS area / environment may be potentially prone to:

- An accident
- The creation of a dangerous situation
- Being beset with dangerous situations
- Flash points
- Being explosive
- Being inflammable or flammable
- Being radioactive etc

Hazards can be defined as the following:

Urban Structure Fires: Perhaps the most common human-caused hazard (often a disaster) is fire in large occupied buildings. Causes can be accidental or deliberate, but unless structures have been built to safe fire standards, and sound emergency procedures are used, heavy loss of life can result.

BLEVE: An entire community was involved at Mississauga, Ontario, Canada when 250,000 had to be evacuated to avert disaster following a train accident which triggered a series of BLEVE (Boiling Liquid Expanding Vapour Explosions).

Other Explosions: Great loss of life occurred in Halifax, Nova Scotia, Canada in 1917 when a ship carrying explosives collided with another. Australia's most disastrous explosion was in the Mt Kembla mine, Wollongong, in 1902, when 95 miners died. One of the worst non-mining explosions occurred in 1974 at the Mt St Candice Convent in Hobart, when seven died in a boiler explosion.

Toxic Emission: During 1984 cyanide gas escaped from a fertilizer factory in Bhopal, India. The resulting deadly cloud caused the deaths of approximately 2,000 people living close-by. In Australia in August 1991, the Coode Island fire burnt 8.6 million litres of chemicals in the heart of Melbourne and loomed as a potential disaster.

An area may also be considered "hazardous" for various other reasons. These may also include the use of electrical equipment in the vicinity of water, the risk of personal injury from moving or falling parts, or even the presence of biological hazards.

8.1.1. Basis of area classification

The first step in Area Classification is to list and identify the areas in the plant where there is the possibility of a conducive atmosphere for explosion or fire to occur. Based on the knowledge so acquired, the design, selection and operation of the equipment has to be influenced in such a way that the risk of fire or explosion taking place is minimized.

It is useful to understand what a Non-hazardous (safe) Area is.

“An area classified as non-hazardous has a small probability of a flammable mixture being present. It is also called a "safe area" and includes most control rooms.”

Area classification cannot be set rigidly into any standard. Each installation will be different in some respect and therefore each site must be examined on its individual merits.

There are three situations that can occur in an operating plant with reference to hazardous areas:

- A situation where an explosive atmosphere is present always or for long periods because of operational requirement, i.e. continuous.
- A situation where explosive atmosphere occurs frequently, or if infrequently may persist for a considerable time, i.e. primary.
- A situation in which explosive atmosphere occurs rarely and normally results from failure of equipment or procedures, i.e. secondary.

The above criteria are used in classifying the areas under ‘Source of Release’ methodology of classification.

Some typical examples of sources of release are:

- Open surface of liquid
- Virtually instantaneous evaporation of a liquid (for example from a jet or spray)
- Leakage of a gas mixture
- principles governing the sources of release
    - Sources giving a continuous grade of release
    - Sources giving a primary grade of release
    - Sources giving a secondary grade of release

8.2. Zonal Classification

8.2.1. Gases, vapor and mists

Areas where there is the likelihood of the presence of explosive gas-air mixtures are referred to as zones. Zones are classified as shown in the table below. The higher the number in this 'Zonal classification' the smaller is the risk of an explosion. This is as per IEC 79:

Zone 0	An area in which an explosive gas/air mixture is continually present or present for long periods
Zone 1	An area in which a gas/air mixture is likely to occur in normal operation
Zone 2	An area in which a gas/air mixture is not likely to occur in normal operation, and if it occurs, it will exist only for a short time.

8.2.2. Dusts

In respect of dust, the situation had been much more fluid. In recent times effort has been made to address this by classifying the Zones in a way which is similar to that adopted for gas and vapour.

Zone 20	An area in which combustible dust, as a cloud, is present continuously or frequently, during normal operation, in sufficient quantity to be capable of producing an explosive concentration of combustible dust in mixture with air, and / or where layers of dust of uncontrollable and excessive thickness can be formed.
Zone 21	Zone 21 is a Zone not classified as Zone 20 in which combustible dust, as a cloud, is present continuously or frequently, during normal operation, in sufficient quantity to be capable of producing an explosive concentration of combustible dust in mixture with air.
Zone 22	Zone 22 is a Zone not classified as Zone 21 in which combustible dust, as a cloud, is present continuously or frequently, during normal operation, in sufficient quantity to be capable of producing an explosive concentration of combustible dust in mixture with air.

Generally it is considered that 1 mm or less thickness of dust is not likely to result in the formation of an explosive atmosphere.

In carrying out an area classification, it is necessary to:

- Identify those parts of the plant where flammable dust can exist including, where appropriate, the interior of process equipment
- Assess the likelihood of occurrence of a flammable atmosphere thereby establishing the appropriate zonal classification
- Delineate the boundaries of the zones taking into account the effect of likely air movement
- Take into account, when assessing the area classification of a plant, the influence of the classification of adjacent plants

8.3. Area classification

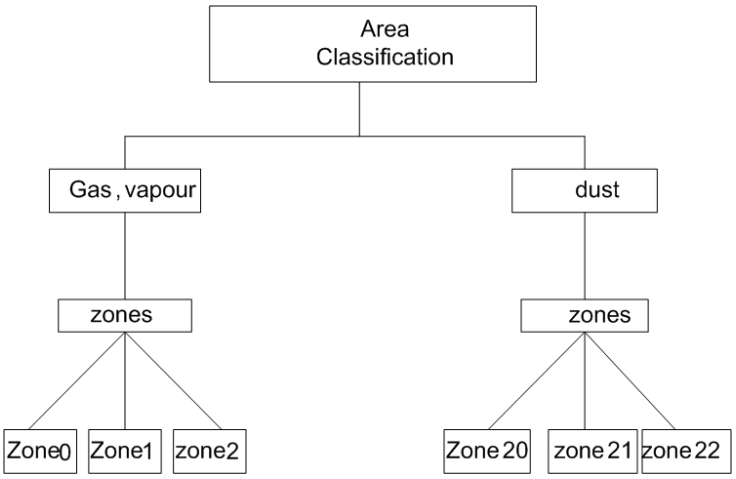

Figure 8.1
Area classification

8.3.1. Area classification – Gas and vapors

Area classification is a method of analysing and classifying the environment where explosive gas atmospheres may occur so as to facilitate the proper selection and installation of apparatus to be used safely in that environment, taking into account gas groups and temperature classes.

8.3.2. Sources of release

The basic elements for establishing the hazardous zone types are the identification of the source of release and the determination of the grade of release.

Since an explosive gas atmosphere can exist only if a flammable gas or vapour is present with air, it is necessary to decide if any of these flammable materials can exist in the area concerned.

If it is established that the item may release flammable material into the atmosphere, it is necessary, first of all, to determine the grade of release in accordance with the definitions, by establishing the likely frequency and duration of the release.

Having established the grade of the release, it is necessary to determine the release rate and other factors, which may influence the *type and extent* of the zone.

8.3.3. Type of zone

The likelihood of the presence of an explosive gas atmosphere and hence the type of zone depends mainly on the grade of release and the ventilation. A continuous grade of release normally leads to a zone 0, a primary grade to zone 1 and a secondary grade to zone 2.

8.3.4. Extent of zone

Consideration should always be given to the possibility that a gas which is heavier than air may flow into areas below ground level for example pits or depressions and that a gas which is lighter than air may be retained at high level, for example in a roof space.

The penetration of a significant quantity of flammable gas or vapour into the area can be prevented by suitable means such as:

- Physical barriers
- Maintaining a static overpressure in the area relative to the adjacent hazardous areas
- Purging the area with a significant flow of air.

Release rate of gas or vapor: The greater the release rates the larger the extent of the zone. The release rate itself depends on other parameters, namely:

- Geometry of the source of release
- Release velocity
- Concentration
- Volatility of a flammable liquid
- Flashpoints of flammable liquids
- Liquid temperature.

Lower explosive limit (LEL): For a given release volume, the lower the LEL, the greater will be the extent of the zone.

Ventilation: With increased ventilation, the extent of the zone will be reduced. Obstacles, which impede the ventilation, may increase the extent of the zone.

Relative density of the gas or vapor when it is released

- The horizontal extent of the zone at ground level will increase with increasing relative density and the vertical extent above the source will increase with decreasing relative density.

8.3.5. Openings

Openings between areas should be considered as possible sources of release. The grade of release will depend upon:

- The zone type of the adjoining area
- The frequency and duration of opening periods
- The effectiveness of seals or joints;

Openings are classified as A, B, C, and D with the following characteristics:

- Type A: Openings not conforming to the characteristics specified for types B, C or D
- Type B: Openings that are normally closed (for example automatic closing) and infrequently opened and which are close fitting
- Type C: Openings normally closed and infrequently opened, conforming to type B, which are also fitted with sealing devices
- Type D: Type D openings are effectively sealed, such as in utility passages (for example ducts, pipes) or can be a combination of one

opening type C adjacent to a hazardous area and one opening type B in series.

8.3.6. Ventilation

Ventilation, i.e. air movement leading to replacement of the atmosphere in a (hypothetical) volume around the source of release by fresh air will promote dispersion. Two main types of ventilation are thus recognized**:**

- Natural ventilation
- Artificial ventilation, general or local.

8.4. Methods of explosion protection

When electrical equipment is to be located in a hazardous area it must be designed manufactured and certified for that purpose. There are several methods of protection available and these are based upon the various protection techniques.

The zonal classification of the hazardous area that the equipment is to be located in will, or partially, determine the equipment's method of protection. This electrical equipment is known as 'explosion protected' equipment, the symbol being Ex, or as per CENELEC standards EEx, followed by the letter designating the mode of protection. Care must be taken not to confuse the term 'explosion protected' with the North American term of 'explosion proof' used to describe their hazardous area equipment. Each technique of protection is assigned a code letter depicting the type of protection.

Each technique of protection is assigned a code letter depicting the type of protection.

8.4.1. Exclusion of the explosive atmosphere (criterion a)

This is when the gas / air or vapour / air mixture is prevented into coming into contact with components or equipment that could cause ignition.

Pressurized (Ex 'p') - if clean dry air or an inert gas is pumped into an enclosure housing electrical equipment and a positive pressure is maintained at 50Pa with respect to the surrounding atmosphere then flammable gas or vapour will be excluded.

Purged (Ex 'pl') - similar to Ex 'p' except that an air flow or inert gas flow is maintained in an enclosure to ensure that there is no build up or presence of a flammable gas or vapour.

Ventilated (Ex 'v') - used in large areas to dilute flammable gas or vapour to well below L.E.L. and to reduce the temperature of electrical equipment by airflow passing over the equipment.

Encapsulation (Ex 'm') - the main requirement for encapsulation is that the apparatus to be protected is encapsulated in resin with at least 3 mm of resin between it and the surface.

8.4.2. Prevention of sparking (criterion b)

This involves selecting components or equipment that will not provide a source of ignition when in normal use.

Increased safety (Ex 'e') - perhaps the most widely used method of protection.The design and manufacture of this equipment assures safety against ignition through ensuring that the temperature of the equipment will not become excessive and that the incidence of arcs and sparks in normal service is prevented.

Non-sparking (Ex 'n') - apparatus which does not produce arcs, sparks or hot surfaces in normal operation are considered within this scope and this system of protection is common amongst three-phase induction motors used in hazardous areas.

8.4.3. Explosion containment (criterion c)

If a gas / air or vapour / air mixture manages to enter an enclosure that contains electrical equipment and that mixture is ignited then this enclosure must be robust enough to contain the explosion and ensure that the escaping products of the explosion do not cause ignition outside of the enclosure.

Examples:-Flameproof (Ex 'd') , Sand filled (Ex 'q') .

8.4.4. Energy limitation (criterion d)

This involves the limitation of energy into a hazardous area so that there is insufficient energy allowed into the circuit to cause ignition.

Intrinsically safe (Ex 'ia' and Ex 'ib') - this is a common type of protection where the required limitations of voltage and current allow its use. With intrinsic safety, there is always the need for a certified interface unit such as a Zener barrier or galvanic coupler to couple the supply from the safe area to the intrinsically safe equipment in the hazardous area.

8.5. Flameproof concept Ex d

This method is also widely used along with the equally popular Ex 'e' concept.

The basis of Ex 'd' equipment is that ordinary non-certified electrical apparatus such as relays, switches, terminal blocks etc are located in an enclosure. If a gas / air or vapor / air mixture enters the enclosure in sufficient quantities and ignites, the enclosure will contain the effects of the ignition.

This method is generally suitable for Zone 1 and 2.

8.5.1. Flameproof enclosure

The term FLP (mnemonic for flameproof) originates from the mining industry where it was first used.

A flameproof enclosure is defined in the standards as: ‘An enclosure for electrical apparatus that will withstand an internal explosion of the flammable gas or vapor which may enter it without suffering damage and without communicating the

internal flammation to the external flammable gas or vapor for which it is designed, through any joints or structural openings in the enclosure'.

A flameproof enclosure is designed to withstand the pressure of an internal explosion; it is not necessary therefore to provide openings for pressure-relief. Where there is a joint, however, or where a spindle or shaft passes through the enclosure, the products of the explosion can escape. It should be understood that the aim of a flameproof enclosure is not necessarily the total avoidance of any gaps in an enclosure. The misconception that it should be 'gas-tight' is misplaced. The principle recognizes that some openings are unavoidable in practice and so restricts itself to requiring that the size of such openings should not exceed the safe limit above which the nature of the escaping flame is such as to ignite a specified flammable atmosphere. On the other hand, it is not the aim to require joints to be deliberately spaced to give an opening.

Flameproof Joint: The place where the corresponding surfaces of the different parts of a flameproof enclosure come together; where the flame or products of combustion may be transmitted from the inside to the outside of the enclosure.

Length of Flame Path: The shortest path traversed by a flame through a joint from the inside to the outside of an enclosure.

Gap: The distance between the corresponding surfaces of a flameproof joint after the electrical equipment has been assembled.

Pressure Piling: A condition of rise in pressure resulting from ignition of pre-compressed gases in compartments or subdivisions other than those in which ignition was initiated and which may lead to a higher maximum pressure than would otherwise be expected.

Maximum experimental safe gap (MESG): Any path, which the flame or hot gases may take, needs to be of sufficient length and constriction to cool the products of the explosion so as to prevent ignition of a flammable atmosphere external to the enclosure.

8.6. Intrinsic safety

The Fire Triangle (Figure 8.2) analogy can be used to explain the objective of Intrinsic Safety. In the presence of the "most easily ignitable mixture" of a given flammable vapour with air, ignition cannot occur if the levels of heat or sparks are insufficient.

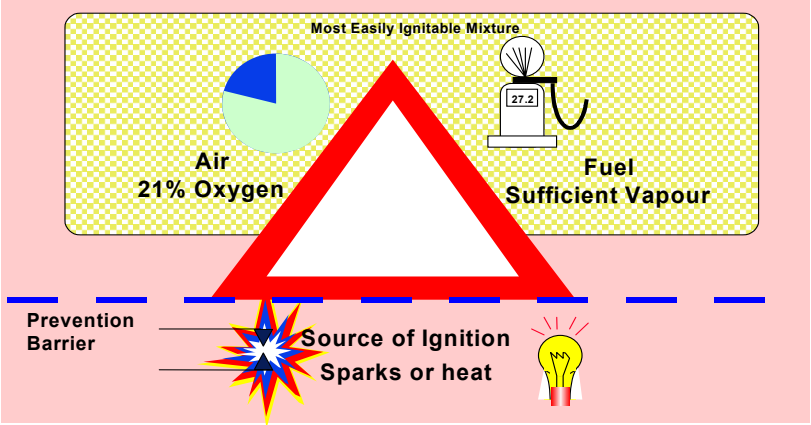

Figure 8.2
The fire triangle

The principle of IS to ensure that levels of heat or size of sparks that occur in an electrical circuit which comes into contact with a flammable gas, are limited to below those which will cause ignition.

An IS circuit is defined in Standard IEC 60079-11 as:

"A circuit in which any spark or thermal effect produced in the condition specified in this international standard, which include normal operation and specified fault conditions is not capable of causing ignition in a given explosive gas atmosphere."

The standard repeats and qualifies this where it declares that three basic criteria must be satisfied;

- Separation from other circuits
- Temperature classification; and
- The inability to cause ignition by sparking.

The definition suggests that sparks and heat are permitted in a circuit under specified fault conditions, but these must never exceed levels that could be incentive. These criteria and the requirement for separation from other circuits provide the high integrity necessary.

The use of the term 'circuit' has important implications. Electrical energy can only produce heat or sparks when electricity is flowing. Since it can only flow in a complete circuit, it is the safety of the circuit that is of concern. The components of the circuit do not pose a threat unless electricity is passing through them, in which case they must be part of a 'circuit'. Heat and sparks occurring in this circuit can be assessed for compliance with the standards for IS.

A 'circuit' can mean any of the following arrangements, increasing in complexity:

- A single cable looped through a hazardous area
- An assembly of electrical components working together as an electronic device (such as an instrument)
- A number of assemblies can be interconnected in the same circuit.

The circuit may operate with energy levels that are quite safe under normal conditions. Under probable fault conditions acting within or onto the circuit, the

circuit must still not be able to emit heat or sparks in sufficient quantities to cause ignition where it encounters a hazardous area. Internal faults and certain external faults must be adequately protected against.

The possible 'faults' are predicted by careful examination of what failure mechanisms could occur. Components are built into the design of the complete circuit in order to maintain energy to known safe levels under these fault conditions. These components are termed, 'safety components' and are in-built into the operation of the circuit. To further enhance the integrity, the failures of the 'in-built' components are separately assessed to ensure that if they fail in a specified manner, safety is still maintained.

8.7. Increased safety

The protection concept of increased safety is one intended for use in Zone I and less hazardous areas. It is generally denoted by adding suffix 'e', i.e., Ex 'e'.

Increased safety is a type of protection applied to electrical equipment that does not produce arcs or sparks in normal service and under specified abnormal conditions, in which additional measures are applied so as to give increased security against the possibility of excessive temperature and of the occurrence of arcs and sparks.

Electrical apparatus with type of protection increased safety 'e' is distinguished by the fact that it does not generate any ignitable sparks during normal operation. The aim of this type of protection is to avoid the occurrence of ignitable sparks and thus have a distinctly higher degree of safety compared with conventional electrical apparatus.

The Ex 'e' standard specifically does not permit the inclusion of any discontinuous contact. No switches or switching mechanisms are allowed in this concept of protection. Sparks therefore cannot occur and spark energy does not need to be considered.

This protection aims are mainly reached by applying the following principles:

- The enclosures are designed in such a way that the entry of moisture and dirt in hazardous quantities is prevented. The IP protection class IP 54 is laid down as the minimum requirement and the enclosures have a mechanical strength that can withstand the typical harsh operating conditions in an industrial plant. Enclosures must guarantee the minimum Protection standard IP 54 even under severe external mechanical forces
- Internally, the clearance and creepage distances must also be so dimensioned that even under harsh ambient conditions, no short circuits via creepage paths or flashovers can occur
- The electrical connection terminals are designed in such a way that it is not possible for the cable connected to them to come loose
- The dimensioning of the apparatus in electrical terms ensures that no inadmissible temperatures can occur inside or on outer parts of the apparatus.

8.8. Certification (components)

Component parts to be included in larger arrangements may be 'component certified' for some flexibility. In an Ex 'e' junction box for example, the enclosure will be impact tested. The terminals to be used within will be component approved.

The main uses of this technique are found in higher power circuits such as induction motors, fluorescent lighting fittings, junction boxes, and terminal housings. The German standards from which this came promote the use of toughened plastic cable sheaths on permanent installations as opposed to the more expensive steel wire armoured cable used elsewhere.

When applied to junction boxes, an Ex 'e' enclosure is given an 'enclosure factor' when certified. This represents the highest number of 'terminal-amps' permitted in the box. Terminals mounted in the box must be component approved. The total of terminal-amps must be calculated and must be equal to or less than the enclosure factor.

Construction requirements: The standards permit the construction of apparatus in such a way that during normal operation of the equipment, it is unlikely to become a source of ignition. The rules therefore seek to develop an acceptable level of integrity by considering standard industrial grade equipment and enhancing some aspects of its construction. This is as opposed to the inclusion of specific electrical or mechanical techniques to prevent ignition, which are applied in some of the other methods.

8.9. Principles of testing

As we have seen that increased safety apparatus calls for a high degree of integrity of material and manufacturing and hence its assessment involves checking that the manufacturer has complied with the design parameters of the standard.

Thus it follows that a testing program for any type of device should include the following as a minimum:

Test of creepage distances: This will involve determining the comparative tracking index of the insulating material. This is required to be done to establish the minimum distance, also known as creepage distance, required between the live parts or live parts and ground.

Special apparatus consisting of application of test voltages and ammonium chloride are applied to the material. Two electrodes spaced 4 mm apart are used to apply the test voltage. This determines the grade of insulating material and hence the resultant properties.

Ceramic material is exempted from this test.

Temperature-rise test: This test is carried out so as to determine the temperature class of the apparatus. Unlike flameproof apparatus, all surfaces, including internal surfaces of the apparatus, are considered. Exceptions would be internal components using exclusion or containment techniques, e.g. encapsulation or flame proofing.

For the apparatus to pass the tests not only for itself, but also for the components that are housed in it, they should also be within the limiting temperature range as per limits of the insulating material used. These limits are to be in line with industry Standards, e.g. cable insulation, or are given in AS 2380.6, e.g. insulation of motor windings.

Degree of protection tests: As this is an important aspect of protection and the apparatus has to meet various levels of protection against the ingress of solid objects or water are specified which must be tested in accordance with codes and standards as specified for degrees of protection provided by enclosures for electrical apparatus (IP Code).

8.10. Non Sparking concept

The most widely used forms of explosion protection, which utilize the technique of energy limitation, are non-sparking and intrinsic safety. While both share a common foundation, they do differ greatly in many aspects. These differences deal mainly with the application of safety factors. It is for this reason that non-sparking is limited to Zone 2 hazardous locations while intrinsic safety is acceptable for Zone 0, 1 & 2 locations. Each does have its merits, which is why it is not uncommon to see the two techniques used together.

The perspective of the user is that Ex ‘n’ is a less costly approach than IS because no interface (e.g. barrier or isolator) is required. It could be argued that the overall installation is less safe with Ex ‘n’ than with Ex ‘i’ with only a marginal cost saving. The use of Ex ‘n’ remains restricted to Zone 2 only. This raises the concern that area classification may be influenced in order to accommodate Ex ‘n’ apparatus.

8.10.1. Definitions

Type of protection ‘n’ is defined in the standard as:

“A type of protection applied to electrical apparatus’ such that, in normal operation, it is not capable of igniting a surrounding explosive atmosphere and a fault capable of causing ignition is not likely to occur.”

The general requirements of such apparatus are that it shall not, in normal operation:

- Produce an arc or spark unless
- The operational arc or spark occurs in an enclosed break device
- The operational arc or spark has insufficient energy to cause ignition of a flammable atmosphere
- The operational arc or spark occurs in a hermetically sealed device.

(It is to be noted that sliding contacts are considered to be sparking in normal operation.)

- Develop a surface temperature or hot spot capable of causing ignition of an external flammable atmosphere.

(It is to be noted that this requirement applies to the temperature of internal and external surfaces to which a surrounding atmosphere has access except internal

surfaces within enclosed-break devices, hermetically sealed devices or restricted-breathing enclosure.)

8.10.2. Principles of design

The ‘non-sparking’ concept of protection was originally accepted as safe on the basis that manufacturers used good quality and well designed industrial equipment with little or no additional requirements. This is if it is operated well within its rating and installed in areas where the risk of contact with a potentially flammable atmosphere was adequately low (Zone 2 only).

The Standard BS 4683: Part 3: 1983 in UK, AS 2380.9 in Australia and IEC 60079-15 internationally, eventually emerged to formalize the concept of good design using industrially graded apparatus and this was termed Type ‘n’ equipment. The standard clarified the method in that it permitted equipment to produce sparks or for the surface temperature of electrical assemblies to rise in temperature, but not to levels that could cause ignition.

More recently, the method was re-designated Type ‘n’ under BS 6941:1988. It has been updated and made more flexible to include the specific needs of instrumentation where circuits with less than 75V DC were recognized. Discontinuous contacts were permitted provided the resultant spark could be shown non-sparking. The same curves are now required to assess the safety of type ‘n’ circuits. The system is deemed safe in normal operation only and faults in the equipment or components and their effect on the explosion protection integrity are not considered. There are some parallels with Ex 'i' in that this technique is ‘safe with no faults’ and therefore could be likened to an unofficial grade of safety Ex ‘ic’ if the same logic applied to the IS technique is followed.

8.11. Concept Ex p

This is one of most popular and widely used protection concepts using ‘the principle of separation’ of three elements of the fire triangle in order to prevent ignition (see Figure 8.3).

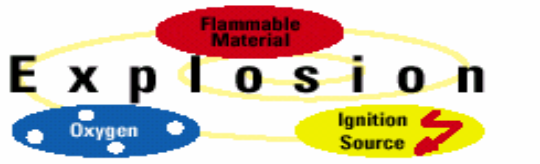

Figure 8.3
Explosion / Fire triangle

This is a useful technique because an artificial ‘safe area’ having sufficient integrity can surround virtually any electrical equipment. The technique is flexible in that it can be adopted for many situations. The system is not used often due to:

- High cost, and
- Inconvenience of equipment accessibility of this solution

The system is expensive to operate and maintain because the clean air must be pumped and controlled by other equipment exposed to the hazardous area. The major benefit is that it can be used on very small enclosures up to complete control

rooms. The problems associated with this tend to complicate area classification. A guaranteed gas free air supply must be maintained so it must be piped in from a safe area. Disposal of used air, if it is likely to contain gas during the initial purge, must be handled such that it does not convert a safe area to a hazardous area.

Of the four techniques using the principle of separation, the Ex p technique is very versatile. Any uncertified equipment may be placed in an enclosure where an inert gas or air is supplied and maintained at a slightly higher than atmospheric pressure level. Ordinary air is most commonly used although there may be cases where nitrogen is preferred.

8.11.1. Definitions

Control of the atmosphere within a room or apparatus enclosure permits the safe use of electrical apparatus, which in the absence of the control would be unsuitable. The pressurizing or purging of the room or enclosure can achieve this. In some cases the two methods cannot be regarded as independent but for the purpose of this discourse the following definitions apply:

Pressurizing: It is a method of safeguarding, whereby air or inert gas in a room or enclosure, is maintained at a pressure sufficient to prevent the ingress of the surrounding atmosphere, which might be flammable. Where appropriate, the pressure may be provided by a mechanical ventilation system.

A variant of this is also known as static pressurization. With static pressurization, the overpressure is created before the system is commissioned by charging the enclosure with protective gas and maintained solely by the sealing of the enclosure without any protective gas being supplied in the hazardous area. The protective gas must be inert. A maximum oxygen concentration of 1 per cent by volume is permitted. Measuring equipment should be used to check this on every charging process.

Purging: This is a method of safeguarding whereby a flow of air or inert gas is maintained through a room or enclosure in sufficient quantity to reduce or prevent any hazard, which could arise in the absence of the purge. (To ‘reduce’ in this context means to reduce the risk of a flammable atmosphere occurring, thus permitting the use of electrical apparatus with a lower standard of safeguarding. Where the object is to ‘prevent’ a hazard, ‘sufficient’ shall take account of the highest likely rate of release of flammable material within or into the room or enclosure).

Where appropriate the purging may be provided by mechanical ventilation of the forced or induced type.

Pressurizing/ Purging: This is a method of safeguarding employing both pressurizing and purging.

Pressurization with leakage compensation is characterized by the fact that the required overpressure is established in the interior of the enclosure after purging. With closed outlet, a supply of protective gas (instrument air or inert gas) is sufficient to compensate for the leakage flow from the pressurized enclosure and pipelines.

In the case of pressurization with continuous flow of protective gas, the overpressure is achieved by the continuous flow of protective gas within the pressurized enclosure. Pressurization with leakage compensation and pressurization with continuous flow are based on a similar technical principle. However, the required protective gas flow rates differ greatly, leading to different designs. Due to its drawbacks in operation, static pressurization is not widely used. Continuous flow only offers advantages in the relatively rare case of internal release (analyzers).

8.11.2. Principles of application

The type of protection, pressurized apparatus “p” encloses electrical equipment or systems representing potential ignition sources in a tight enclosure. Instrument air or inert gas is introduced into this enclosure until a defined overpressure in relation to the external atmosphere is achieved, which is then maintained during the operation of the system. This overpressure prevents penetration of flammable gas or combustible dust from outside into the enclosure and hence the coincidence of an explosive atmosphere and an ignition source. In principle, pressurization technology is also used for online analyzers, which in turn may be used to analyze flammable gases (or liquids). In such cases, flammable gases are fed via a pipeline to the analyzer in a pressurized enclosure. Any leakage in these pipelines or even in the analyzer may constitute an internal source of flammable gases inside the pressurized enclosure.

The area containing the flammable gas (i.e. the pipelines and analyzer) is described as a containment system. Depending on the technical design of this containment system and gas feed system; it is described as an infallible containment system (no release), a limited release system with a predictable maximum release rate or an unlimited release system. With unlimited release, overpressure must be created by an inert protective gas, which prevents oxygen from penetrating the enclosure. With limited release, a sufficiently large volume of air is used to dilute the combustible gas outside a small “dilution area” so that an explosive atmosphere is unable to form.

Relative to the explosion triangle mentioned at the start, this means that, there is no explosive mixture inside the enclosure (there is no flammable gas, or it is only present in amounts below the lower explosive limit (LEL), or there is no oxygen). In principle, any non-explosion protected apparatus and systems may be installed in the enclosure.

8.12. Other protection concepts

There are additional concepts that are not so widely used, but have been developed and find their use in specific applications. These, when used in conjunction with one or more of the popular methods of protection, can really lead to economically safe solutions.

8.12.1. Ex ‘o’: oil filling

This is one of the separation methods where the oil is used as a separation medium. The Ex ‘o’ method shown in Figure 8.4 was originally conceived for

high power equipment. It provides explosion protection on a similar basis to Ex 'p'.

The definition of Ex 'o' protection concept in standards is,

'A type of protection in which the electrical apparatus or parts of the electrical apparatus are immersed in a protective liquid in such a way that an explosive atmosphere which maybe above the liquid or outside the enclosure cannot be ignited.'

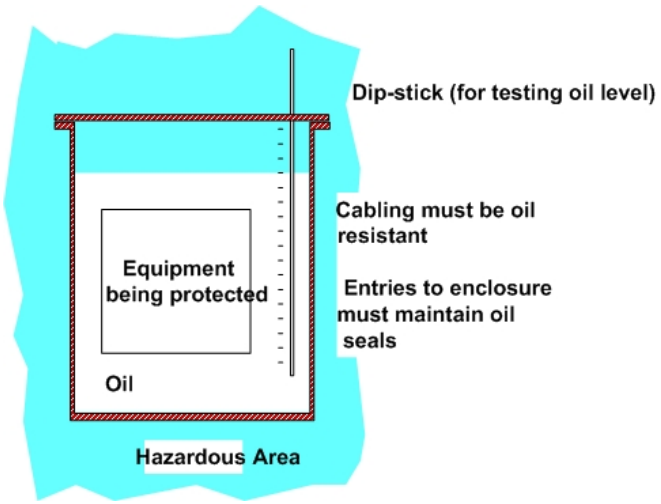

Figure 8.4
Ex o oil immersion

8.12.2. Ex 'q': Quartz/sand filling

This is another of the methods of protection under concept of separation.

'A type of protection in which the parts capable of igniting an explosive atmosphere are fixed in position and completely surrounded by filling material to prevent the ignition of an external explosive atmosphere.'

It is rarely used on its own and is mainly found in combination with the other construction techniques described here. It cannot be used in situations where movement is required, i.e., for the protection of relay contacts.

8.12.3. Ex 'm': Encapsulation

Encapsulation is used to prevent flammable gases from reaching a potential source of ignition in its own right. It may be thought of as the method of electrical protection using solids whereas Ex 'o' uses liquid and Ex 'p' uses gas.

The standards define it as follows:

'Protection of electrical components by enclosure in a resin in such a way that an explosive atmosphere cannot be ignited during operation by either sparking or overheating which may occur within the encapsulation.'

In other words encapsulation is used to prevent flammable gases from reaching a potential source of ignition within the encapsulated apparatus.

8.13. Earthing and Bonding

Correct "Earthing" is primarily required for the assurance of general electrical safety, reducing the risks to both human life and installations.

Electrical "earthing" is required for five main purposes:

- To reduce the risk of personnel shock
- To operate electrical protective devices
- To guard against lightning surges
- To control electrostatic discharge
- To minimize electrical interference.

8.13.1. Personnel safety

The effects of electricity on humans depend on the level of current and where it enters and leaves the body. Research shows that the limbs have a resistance of about 500 Ohms. The central torso has a very low resistance value owing to the high water content. The effect of electricity penetrating the skin can be liked to the characteristics of a zener diode with a reverse breakdown voltage of 5 to 10 V. This depends on the individual's skin characteristics and the tendency to dry or greasy skin.

8.13.2. Hazardous area considerations

Structural or fault currents arising from electrical equipment operating in hazardous areas must not become a source of heat or sparks. Equipment must be adequately earthed to ensure that connections are of high integrity and low impedance.

8.13.3. Definitions

There is a subtle but essential difference between earthing and bonding, which must be understood.

"Earthing" is where a low impedance path is provided in order for return currents to operate electrical protection devices such as fuses and over-current trips in an appropriately short time.

"Bonding" is where voltage differences between electrical conducting parts are eliminated.

International electrical supply regulations (ESRs) that cover fixed electrical equipment and installations require that there be an earth return that is backed up by a physical connection to "terrestrial" earth. In this way there are two return paths acting in parallel, which enhances the integrity of an earthing system. One path is an earth path because its primary function is to conduct fault currents. The other connection is to ensure that significant voltage differences do not appear between devices. Refer to Figure 8.5.

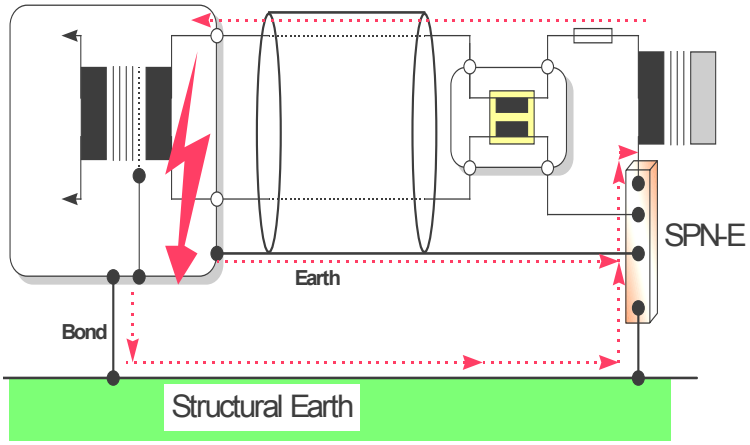

Figure 8.5
Earthing and bonding in parallel

The "Earth" and "Bond" conductors act in parallel. This is an advantage in that the two paths reduce the impedance. One path may be viewed as backing up the other lest it should fail.

8.13.4. Clean and dirty earthing

In any electrical system using ac supplies, current will flow in earthing and bonding paths. These are unavoidable and have to be coped with in the course of devising strategies. There are two reasons for this.

- Parasitic capacitance
- Fault currents

8.14. Standards and codes of practice

The Standards and Codes of Practice that apply in various countries are not always specific in their requirements for earthing as applied to IS and related topics.

In the UK, BS5345 states specific reference to the Star-point Neutral Earthing system of the incoming supply. In Germany, VDE 0165 requires the creation of a reference potential to which plant and supply are connected. A Canadian standard allow the designation of an Earth reference but does not state to what else it is to be connected to other than the Barrier earth.

8.15. Fault finding and repairs

There is no right or wrong way to fault find on instrument loops and systems. There are however, safe and potentially unsafe ways that are of the greatest importance to consider.

8.15.1. Fault finding routine

It is usual for a fault to be investigated by following a logical routine, an example of which is shown in Figure 8.6.

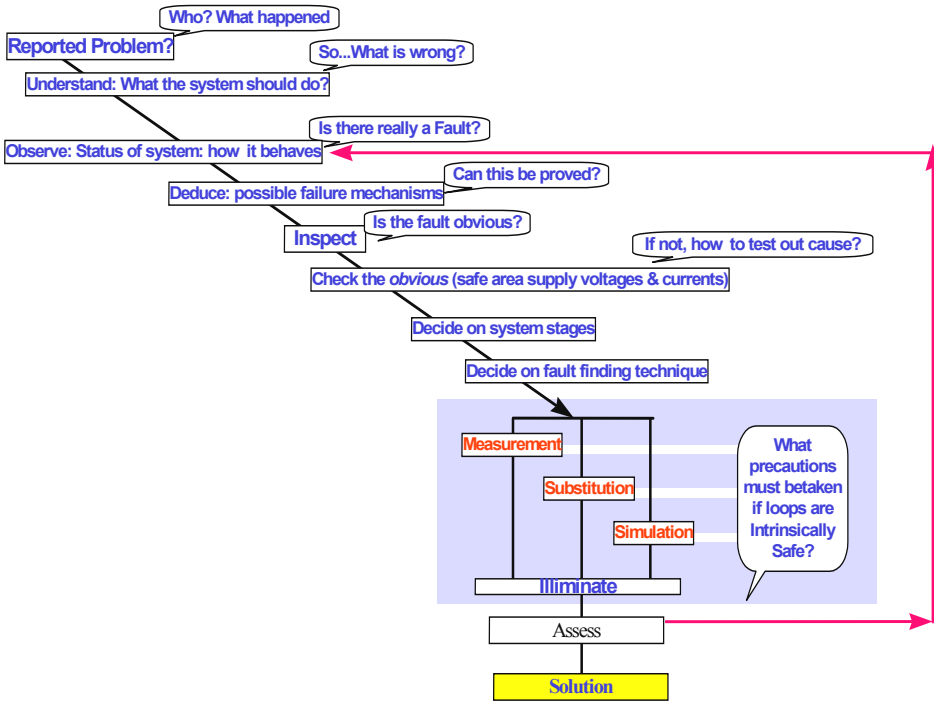

Figure 8.6
Possible fault finding routine

8.15.2. Safety assessment of testing

There is a legal 'duty of care' on all industrial personnel that adequate precautions are taken so as not to endanger life or investment during the course of work. Some assessment of work on electrical apparatus is required in order to ensure that the integrity of protection is not compromised.

8.15.3. Test equipment

There is a great variety of test equipment available on the market. It may seem obvious to point out that test equipment for hazardous area use will be either certified or uncertified.

The following are the types of tests conducted.

Insulation testing: Insulation testing is a requirement of all Standards. The test used is for the circuit to withstand 500Vac rms for one minute

Low voltage insulation test: The principle of this test is applying a low voltage source and monitoring the current taken with an adequately sensitive measuring instrument

The 500Vac test: The high voltage test to instrumentation should be performed as shown in Figure 8.7. This is preferably carried out in the safe area or if necessary in the hazardous area.

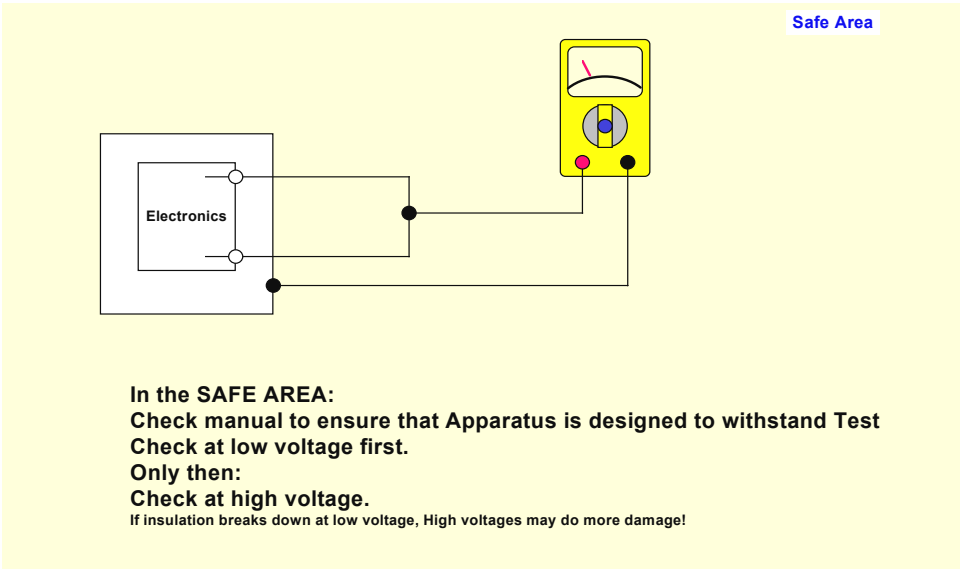

Figure 8.7
High voltage testing of instruments