Overview of Safety Instrumented Systems

IDC TECHNOLOGIES

Technology Training that Works

Overview of Safety Instrumented Systems

THIS BOOK WAS DEVELOPED BY IDC TECHNOLOGIES

WHO ARE WE?

IDC Technologies is internationally acknowledged as the premier provider of practical, technical training for engineers and technicians.

We specialize in the fields of electrical systems, industrial data communications, telecommunications, automation and control, mechanical engineering, chemical and civil engineering, and are continually adding to our portfolio of over 60 different workshops. Our instructors are highly respected in their fields of expertise and in the last ten years have trained over 200,000 engineers, scientists and technicians.

With offices conveniently located worldwide, IDC Technologies has an enthusiastic team of professional engineers, technicians and support staff who are committed to providing the highest level of training and consultancy.

TECHNICAL WORKSHOPS

TRAINING THAT WORKS

We deliver engineering and technology training that will maximize your business goals. In today's competitive environment, you require training that will help you and your organization to achieve its goals and produce a large return on investment. With our 'training that works' objective you and your organization will:

- Get job-related skills that you need to achieve your business goals
- Improve the operation and design of your equipment and plant
- Improve your troubleshooting abilities
- Sharpen your competitive edge
- Boost morale and retain valuable staff
- Save time and money

EXPERT INSTRUCTORS

We search the world for good quality instructors who have three outstanding attributes:

1. Expert knowledge and experience – of the course topic
2. Superb training abilities – to ensure the know-how is transferred effectively and quickly to you in a practical, hands-on way
3. Listening skills – they listen carefully to the needs of the participants and want to ensure that you benefit from the experience.

Each and every instructor is evaluated by the delegates and we assess the presentation after every class to ensure that the instructor stays on track in presenting outstanding courses.

HANDS-ON APPROACH TO TRAINING

All IDC Technologies workshops include practical, hands-on sessions where the delegates are given the opportunity to apply in practice the theory they have learnt.

REFERENCE MATERIALS

A fully illustrated workshop book with hundreds of pages of tables, charts, figures and handy hints, plus considerable reference material is provided FREE of charge to each delegate.

CERTIFICATE OF ATTENDANCE

Each delegate receives a Certificate of Attendance documenting their experience.

100% MONEY BACK GUARANTEE

IDC Technologies' engineers have put considerable time and experience into ensuring that you gain maximum value from each workshop. If by lunchtime on the first day you decide that the workshop is not appropriate for your requirements, please let us know so that we can arrange a 100% refund of your fee.

ONSITE WORKSHOPS

All IDC Technologies Training Workshops are available on an on-site basis, presented at the venue of your choice, saving delegates travel time and expenses, thus providing your company with even greater savings.

OFFICE LOCATIONS

AUSTRALIA • CANADA • INDIA • IRELAND • MALAYSIA • NEW ZEALAND • SINGAPORE • SOUTH AFRICA • UNITED KINGDOM • UNITED STATES

idc@idc-online.com **www.idc-online.com**

On-Site Training

SAVE MORE THAN 50% OFF the per person cost

CUSTOMISE the training to YOUR WORKPLACE!

Have the training delivered WHEN AND WHERE you need it!

All IDC Technologies Training Workshops are available on an on-site basis, presented at the venue of your choice, saving delegates travel time and expenses, thus providing your company with even greater savings.

For more information or a FREE detailed proposal contact Kevin Baker by e-mailing:
training@idc-online.com

IDC TECHNOLOGIES
Worldwide Offices

AUSTRALIA
Telephone: 1300 138 522 • Facsimile: 1300 138 533

West Coast Office
1031 Wellington Street, West Perth, WA 6005
PO Box 1093, West Perth, WA 6872

CANADA
Toll Free Telephone: 1800 324 4244 • Toll Free Facsimile: 1800 434 4045
Suite 402, 814 Richards Street, Vancouver, NC V6B 3A7

INDIA
Telephone : +91 444 208 9353
35 4th Street, Kumaran Colony, Vadapalani, Chennai 600026

IRELAND
Telephone : +353 1 473 3190 • Facsimile: +353 1 473 3191
Caoran, Baile na hAbhann
Co. Galway

MALAYSIA
Telephone: +60 3 5192 3800 • Facsimile: +60 3 5192 3801
26 Jalan Kota Raja E27/E, Hicom Town Center
Seksyen 27, 40400 Shah Alam, Selangor

NEW ZEALAND
Telephone: +64 9 263 4759 • Facsimile: +64 9 262 2304
Parkview Towers, 28 Davies Avenue, Manukau City
PO Box 76-142, Manukau City

SINGAPORE
Telephone: +65 6224 6298 • Facsimile: + 65 6224 7922
100 Eu Tong Sen Street, #04-11 Pearl’s Centre, Singapore 059812

SOUTH AFRICA
Telephone: +27 11 024 5520 • Facsimile: +27 86 692 4368
68 Pretorius Street, President Park, Midrand
PO Box 389, Halfway House 1685

UNITED KINGDOM
Telephone: +44 20 8335 4014 • Facsimile: +44 20 8335 4120
Suite 18, Fitzroy House, Lynwood Drive, Worcester Park, Surrey KT4 7AT

UNITED STATES
Toll Free Telephone: 1800 324 4244 • Toll Free Facsimile: 1800 434 4045
10685-B Hazelhurst Dr. # 6175, Houston, TX 77043

Website: www.idc-online.com
Email: idc@idc-online.com

IDC
TECHNOLOGIES

Technology Training that Works

Presents

Overview of Safety Instrumented Systems

Revision 1

Website: www.idc-online.com
E-mail: idc@idc-online.com

IDC Technologies Pty Ltd
PO Box 1093, West Perth, Western Australia 6872
Offices in Australia, New Zealand, Singapore, United Kingdom, Ireland, Malaysia, Poland, United States of America, Canada, South Africa and India

Disclaimer

Whilst all reasonable care has been taken to ensure that the descriptions, opinions, programs, listings, software and diagrams are accurate and workable, IDC Technologies do not accept any legal responsibility or liability to any person, organization or other entity for any direct loss, consequential loss or damage, however caused, that may be suffered as a result of the use of this publication or the associated workshop and software.

In case of any uncertainty, we recommend that you contact IDC Technologies for clarification or assistance.

Trademarks

Acknowledgements

IDC Technologies expresses its sincere thanks to all those engineers and technicians on our training workshops who freely made available their expertise in preparing this manual.

Contents

1

Overview of Safety Instrumented Systems

1.1 Summary of contents

The theme of this chapter can be simply stated by two sentences:

- A business that operates any form of hazardous process needs safety systems
- Safety systems do not work without good management

Safety Instrumented Systems are part of the overall risk reduction measures that a company will typically install to deal with a hazardous process. We explain the basic technical features of a safety system and show what tasks must be carried out to ensure that the protection measures are properly defined and implemented. The performance requirements of safety systems are described in non-technical terms and the relevance of safety integrity to the capital cost and operating costs are spelt out.

We look at the developments that have resulted in a comprehensive internationally accepted standard, IEC 61511-2003 being available specifically for use in the process industries. The chapter explains the scope and importance of IEC 61511 as a means to achieve and demonstrate high quality in applied safety systems. The version of IEC 61511 published in the USA as ANSI/ISA S84.00.01:2004 is the standard required by OHSA for SIS to achieve compliance with Process Safety Management and General Duty regulations as applied to process plants.

Past failures of safety systems have very often been attributed to human errors in their design and upkeep. Authorities responsible for enforcement of safety have come to the realization that the management of all safety activities is therefore as important as the technical equipment used to carry out safety functions. This is why IEC 61511 defines the management of safety life cycle activities as one of the critical issues in achieving compliance with the standards. This chapter outlines the requirements for management of safety life cycle activities and introduces issues such as, staff competency requirements and conformity assessment schemes.

1.2 Introduction and objectives

1.2.1 Introduction

This IDC training workshop has been developed to provide a broad introduction to the methods and concepts of applying safety instrumented system to processing plants. The range of process industries that are likely to use this type of safety instrumentation as broad as the range of process control system applications. The only thing they may have in common is that they have potentially hazardous materials or processes or they may have large sources of stored energy that could be harmful if something goes wrong.

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.

IDC’s past experience with training in this field has indicated there is a need for process engineers and technical managers to be conversant with the basics of functional safety systems as they are broadly described in the new standards. The support structures are a crucial part of the assessment scope for compliance with the new IEC 61508 and 61511 standards. This workshop therefore provides a mix of training in the technical issues of safety instrumentation with training in the project engineering and support activities that are essential for success. It is the responsibility of the instrument engineer to involve colleagues from other disciplines in the safety package. It is the responsibility of managements to see that the safety activities are clearly assigned and supported.

The idea of this first training chapter is to provide a substantial overview of the basic issues affecting a safety instrumentation project. It is intended that this chapter can be used as a half day briefing package for any managers and engineers in a company who may wish to learn some more about the subject but do not requires to have deeper knowledge of the technical issues.

1.2.2 Objectives

- To introduce the concepts of functional safety management and the principles of safety systems to both engineering and management personnel
- To provide a foundation for more detailed training of engineers and technicians
- To assist managers in developing safety engineering competencies within their organization

1.2.3 Outcomes

After this training chapter you should:

- Understand the basic concepts of instrumented protection systems
- Recognize the main activities of a safety system project
- Be able to plan a complete lifecycle project using IEC 61511 for guidance
- Be able to identify the main safety system support tasks required in your organization
- Be able to use IEC 61511 to review your existing practices and identify possible shortcomings
- Know the meaning of safety integrity level, and be aware of its relevance to cost of ownership of a safety system

1.2.4 Contents and roadmap

The subjects in the chapter include the follwing:

- Safety system basics
- Risk management principles applied to protection systems
- Process hazard analysis and its link to protection systems
- The legal framework
- The meaning of SILs and their cost implications
- An overview of standards ANSI/ISA S84.01, IEC 61508 and IEC 61511
- An introduction to the safety life cycle as defined in IEC 61511
- The problems and rewards of SIL determination
- Basics of safety instrumentation needed to meet SIL targets
- Why programmable systems need special treatment
- Cost models and the cost ownership
- Management of functional safety
- Competency requirements and conformity assessment programmes

1.2.5 Roadmap

The following diagram provides a graphical indication of the steps we are going to cover in this chapter.

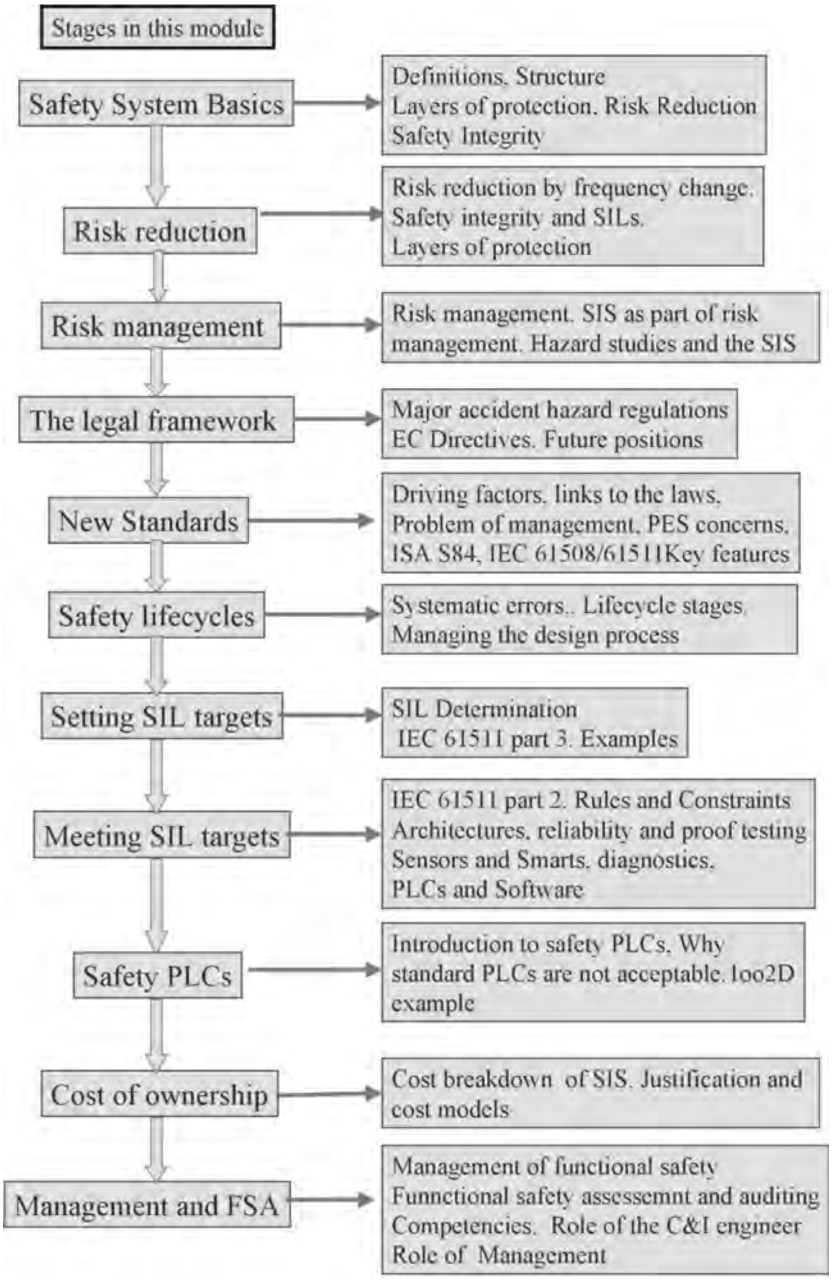

Stages in this module
Safety System Basics
Definitions. Structure
Layers of protection. Risk Reduction
Safety Integrity
Risk reduction
Risk reduction by frequency change.
Safety integrity and SILs.
Layers of protection
Risk management
Risk management. SIS as part of risk
management. Hazard studies and the SIS
The legal framework
Major accident hazard regulations
EC Directives. Future positions
New Standards
Driving factors. links to the laws.
Problem of management. PES concerns.
ISA S84. IEC 61508/61511Key features
Safety lifecycles
Systematic errors.. Lifecycle stages.
Managing the design process
Setting SIL targets
SIL Determination
IEC 61511 part 3. Examples
Meeting SIL targets
IEC 61511 part 2. Rules and Constraints
Architectures, reliability and proof testing
Sensors and Smarts. diagnostics.
PLCs and Software
Safety PLCs
Introduction to safety PLCs. Why
standard PLCs are not acceptable. 1oo2D
example
Cost of ownership
Cost breakdown of SIS. Justification and
cost models
Management and FSA
Management of functional safety
Funnctional safety assessemnt and auditing
Competencies. Role of the C&I engineer
Role of Management

Figure 1.1
A roadmap for the safety systems overview

1.3 Safety system basics

To begin this workshop we first need to answer the question: What is safety instrumentation?

Here is a typical definition as given by the UK Health and Safety Executive in their very useful publication “Out of Control: why safety systems go wrong”.

1.3.1 Definition of Safety Instrumented Systems

Safety Instrumented Systems are control systems that take the process to a safe state on detection of conditions that may be hazardous in themselves or if no action were taken could eventually give rise to a hazard. They perform "safety instrumented functions" by acting to prevent the hazard or mitigate the consequences.

The abbreviation SIS is used for "Safety Instrumented Systems" whilst 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. You may know the subject by other names because of the different ways in which these systems have been applied. Here are some of the other names in use:

Alternative names found in service:

- Trip and Alarm System
- Emergency Shutdown System
- Safety Shutdown System
- Safety Interlock System
- Safety Related Control System (More general term for any system that maintains a safe state for EUC)

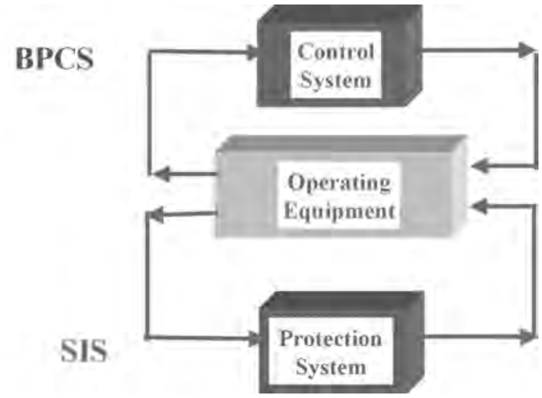


Figure 1.2
SIS operates independently of the Basic Process Control System (BPCS)

We are talking about automatic control systems or devices that will protect personnel, plant equipment or the environment against harm that may arise from specified hazardous conditions.

When applied to a typical process plant situation the SIS is normally seen as a separate control system that acts independently of any other control or persons. The diagram here shows the basic arrangement.

The SIS is an example of a "Functional Safety System." Meaning: 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 of any type whether mechanical, electrical or in any other form that must function properly to provide safety.

1.3.2 The structure of an SIS

Safety Instrumented Systems are normally regarded as being structured into 3 parts within a framework or boundary that defines it. They always require the three parts comprising:

- **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 plant

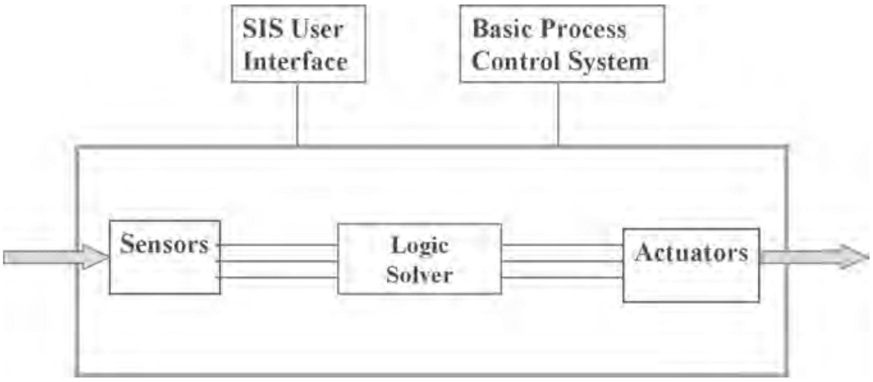


Figure 1.3
Structure of a Safety Instrumented System

Figure 1.3 shows that the subsystems lie within a boundary that defines the essential SIS whilst 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.

1.3.3 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.

These are topics that we must be concerned with if we are to build a credible or “high integrity safety system”.

We shall see in a moment how safety integrity is graded into levels of performance called SILs or safety integrity levels.

It follows from the structure of the SIS that all three subsystems must individually be good enough to ensure that the overall safety integrity of the SIS meets the intended target or SIL target. This is a useful concept because it means we can concentrate on each subsystem separately at the basic engineering stage.

1.3.4 Practical example of an SIS

It may be useful at this stage to translate above concepts into something closer to reality. Let’s consider a simple process plant example as shown in figure 1.4. The hazard in this process is seen as the overfilling of a pressure vessel with a toxic chemical leading to release via the relief valve.

The causes of the overfill could be an operational error or a failure of the basic level control instrumentation. An SIS can be designed to independently shut off the incoming feed if the level or pressure becomes high enough to indicate a dangerous condition.

Figure 1.4 shows the SIS added to the plant as an entirely separate control system capable of acting despite any problems with the rest of the plant equipment.

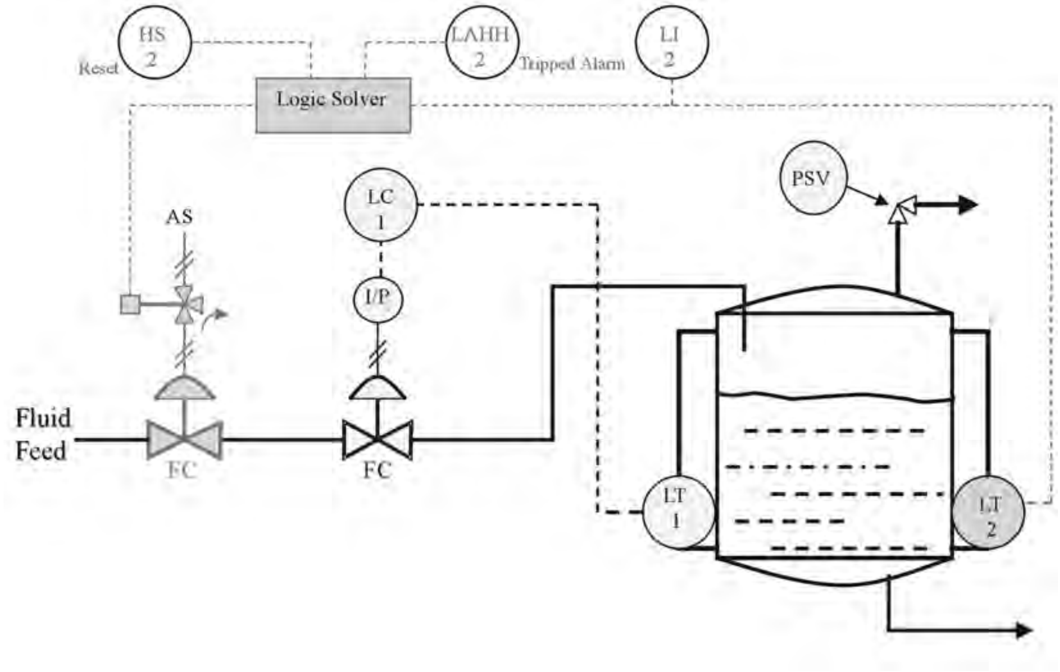


Figure 1. 4
Example of a simple shutdown system

This example is sufficient for our overview work and we can must now attend to the underlying concepts of hazards and risk reduction.

1.4 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. So what we need to measure is: RISK. Here we need to be clear on the terms Hazard and Risk.

1.4.1 What is hazard and what is risk?

A hazard is *"an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment"*.

In chemical processes: "*It is the combination of a hazardous material, an operating environment, and certain unplanned events that could result in an accident*".

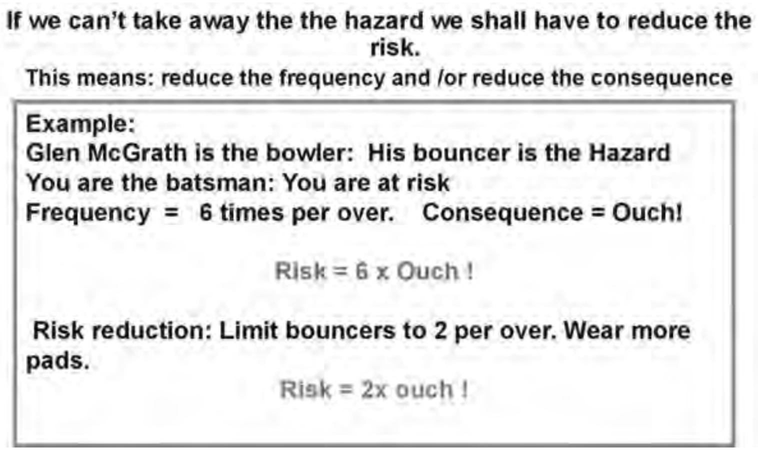
Risk

Risk is usually defined as the combination of the severity and probability of an event. In other words, how often can it happen and how bad is it when it does happen? Risk can be evaluated qualitatively or quantitatively.

Roughly: Risk = Frequency x Consequence of hazard

Risk reduction

Risk reduction can be achieved by reducing either the frequency of a hazardous event or its consequences or by reducing both them. Generally the most desirable approach is to first reduce the frequency since all events are likely to have cost implications even without dire consequences.



If we can't take away the the hazard we shall have to reduce the risk.

This means: reduce the frequency and /or reduce the consequence

Example:
Glen McGrath is the bowler: His bouncer is the Hazard
You are the batsman: You are at risk
Frequency = 6 times per over. Consequence = Ouch!

Risk = 6 x Ouch !

Risk reduction: Limit bouncers to 2 per over. Wear more pads.

Risk = 2x ouch !

Figure 1.5
Example for risk reduction

Safety systems are all about risk reduction. If we can't take away the hazard we shall have to reduce the risk. To know how to do this it helps to look at the theory measuring risk and then reducing it.

1.4.2 Hazards and risks

All types of safety measures are intended to reduce risk of harm to people, the environment and assets. The hazards most commonly found in process industries are those due to:

- Explosions or bursting due to large amounts of stored energy, chemical reactions or release of flammable vapors

- Fires due to combustion of chemical substances internally or externally to the process or through overheating of equipment
- Toxic releases and exposures or entrapment in gas filled spaces
- Mechanical hazards due to large machines, materials handling, steam and gas discharges

We have seen that risk is usually defined as the combination of the severity and probability of an event. In other words, how often can it happen and how bad is it when it does happen?

Roughly: risk = Frequency x Consequence of hazard

1.4.3 Measurement of risk

Risk can be evaluated qualitatively or quantitatively. The qualitative approach requires that we describe risk in descriptive terms such 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 how many people get hurt but it is often hard to extract a firm number from a situation without a lot of statistical evidence. For the moment our studies will assume a quantitative measure of risk is possible.

Figure 1.6 indicates shows that risk levels can be regarded as similar if a severe consequence may occur rarely or if a less severe consequence occurs more often. It follows that risk reduction can be achieved either by reducing the frequency (likelihood) of the hazardous event or by reducing the consequences.

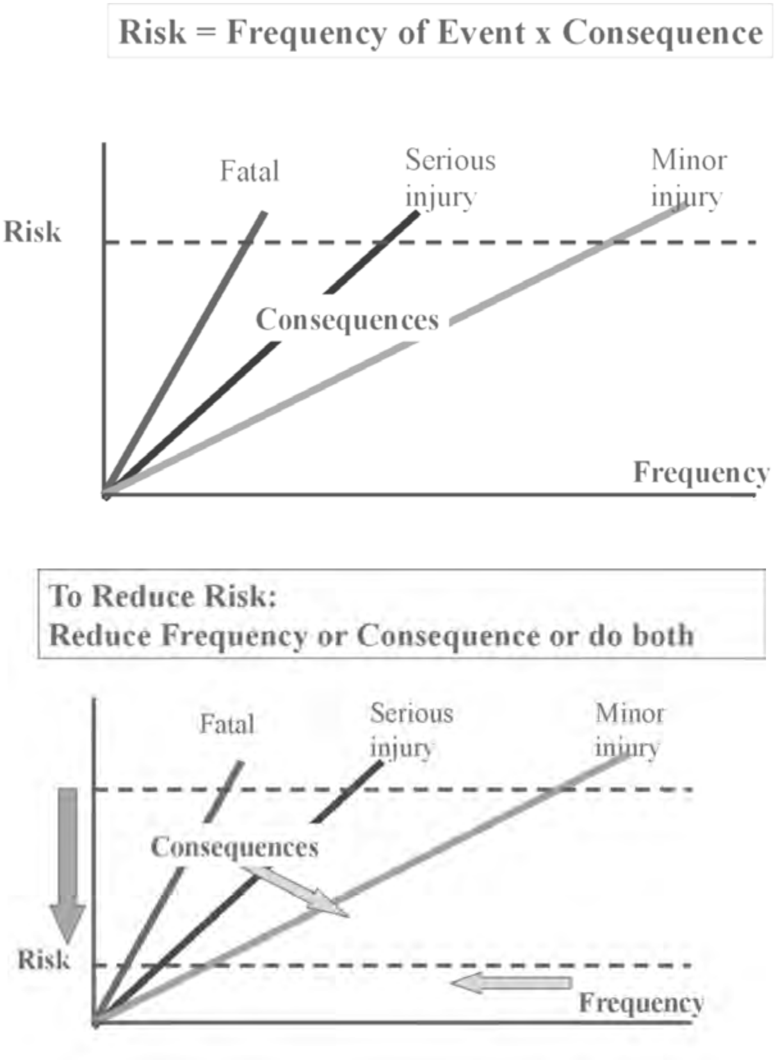


Figure 1.6
Principles of risk reduction by reducing frequency or consequence

Usually a functional safety system acts to reduce the likelihood of the hazardous event whilst other operational measures are used to minimize consequences. For example a blast proof wall may protect people against an explosion but it will not reduce the chances of the explosion.

So the easiest way to visualize an SIS providing safety is to regard it as reducing the event frequency.

As shown in Figure 1.7: A plant without a safety system may have an unprotected risk frequency of Fnp which is reduced to a protected risk frequency, Fp, by adding a safety system. The risk reduction provided by the SIS is called the Risk Reduction factor (RRF) and is simply the ratio of unprotected risk to the protected risk frequency.

RRF = Fnp/Fp

This simple ratio makes RRF a very effective index of safety system performance or integrity. The amount of risk reduction provided by the SIS depends on its "safety integrity ".

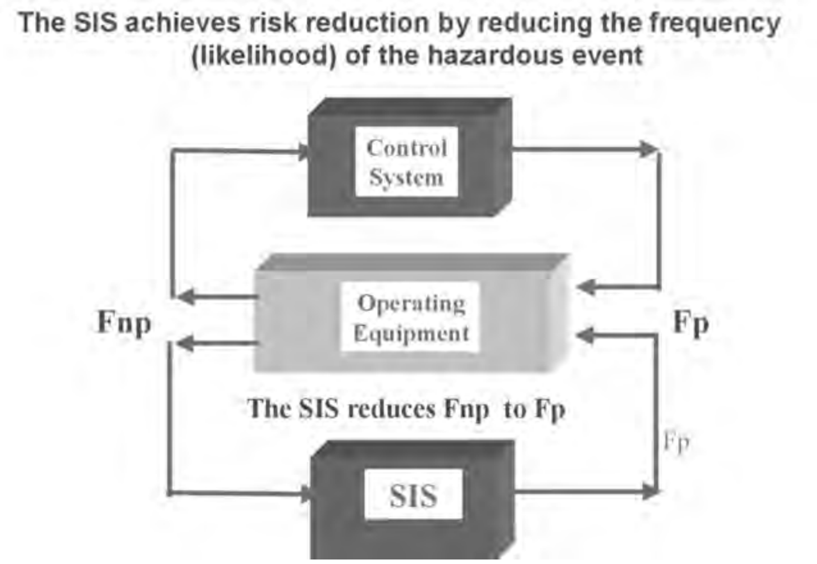

The SIS achieves risk reduction by reducing the frequency (likelihood) of the hazardous event
Control System
Operating Equipment
Fnp
Fp
The SIS reduces Fnp to Fp
Fp
SIS

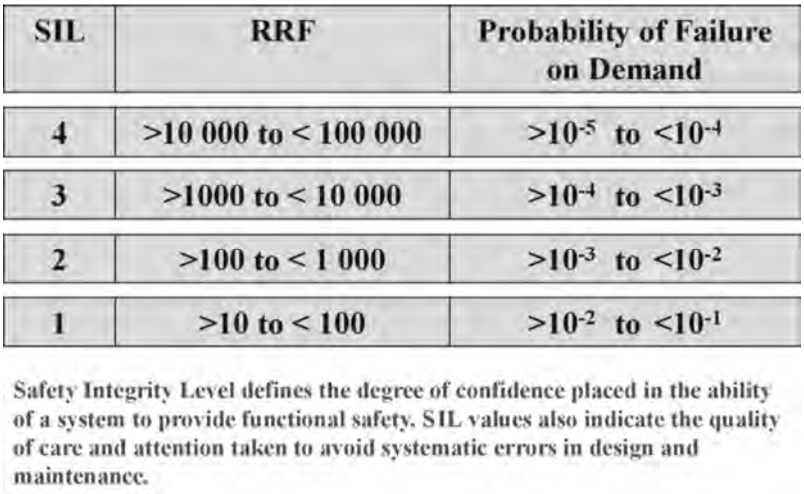
Figure 1.7
SIS reducing the frequency of the hazardous event

1.4.4 Introducing safety integrity levels

We have noted that safety integrity depends on hardware and design. We have seen that the required RRF provides a scale of performance for the ability of a safety system to reduce risk. We can therefore use RRF as a measure of safety integrity. Safety system engineers recognize that it is helpful to grade safety integrity into four distinct bands of risk reduction capability known as the safety integrity levels.

Figure 1.8 shows how 4 safety integrity levels are recognized and how these levels encompass 4 ranges of RRF capability.

In practice a SIL 1 safety system is the most commonly used and provides risk reduction in the range from 10:1 to 100:1. In the process industries the highest SIL rating used is normally SIL 3 whilst SIL 4 is only attempted under very special circumstances. The SIL levels 1 to 3 therefore represent a coarse scale of safety performance for the SIS. The challenge will be to choose the right SIL for any particular problem.



SIL	RRF	Probability of Failure on Demand
4	>10 000 to < 100 000	$>10^{-5}$ to $<10^{-4}$
3	>1000 to < 10 000	$>10^{-4}$ to $<10^{-3}$
2	>100 to < 1 000	$>10^{-3}$ to $<10^{-2}$
1	>10 to < 100	$>10^{-2}$ to $<10^{-1}$

Safety Integrity Level defines the degree of confidence placed in the ability of a system to provide functional safety. SIL values also indicate the quality of care and attention taken to avoid systematic errors in design and maintenance.

Figure 1.8
Table of safety integrity levels

1.4.5 Demand mode and continuous mode

The new standards have clarified the fact that there are two basic types of safety controls. In the process industry, “Demand Mode” is widely used applies when the safety trip is expected less than once per year. These are the familiar safety trip systems that are used to shutdown the process in emergency. The hardware reliability that is expected of a SIL rating is derived from the “Probability of failure on demand”. As can be seen in figure 1.9 this is the PFD avg.

In “Continuous Mode”. The safety trip or control action is expected more than once per year. This would be the case for example where a Start up safety interlock may have to act daily or once per month. This type of control is regarded as a safety control system and the SIL is derived from: Frequency of dangerous failures per hour.

The engineering principles for these two modes are exactly the same but the method of calculating the possible failure and consequent accident rate is different. We shall look at this point in more detail later in the workshop but it is worth noting at this stage that where a plant is encountering trips more often than once per year the validity of its SIS performance claims may have to be revised to lower values.

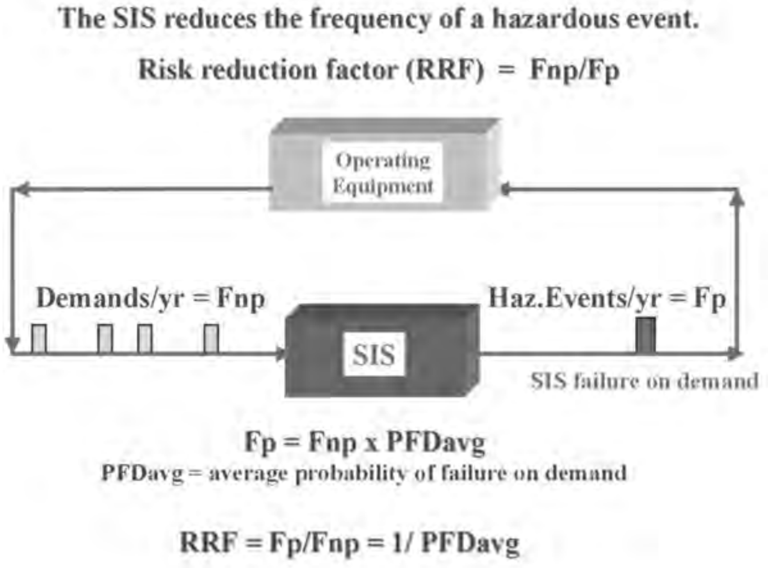

The SIS reduces the frequency of a hazardous event.
Risk reduction factor (RRF) = Fnp/Fp
Operating Equipment
Demands/yr = Fnp
Haz.Events/yr = Fp
SIS
SIS failure on demand
Fp = Fnp x PFDavg
PFDavg = average probability of failure on demand
RRF = Fp/Fnp = 1/ PFDavg

Figure 1.9
SIS operating in demand mode

In conclusion, the Demand Mode features are summarized in figure 1.9 where the SIS can be seen responding to the possible hazard as a demand to take action. Only when the SIS fails will the demand be allowed to become a hazardous event.

1.5 Protection layers

Now that we see the SIS as a risk reduction element it is helpful to see how it fits in 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.

1.5.1 Belt and braces

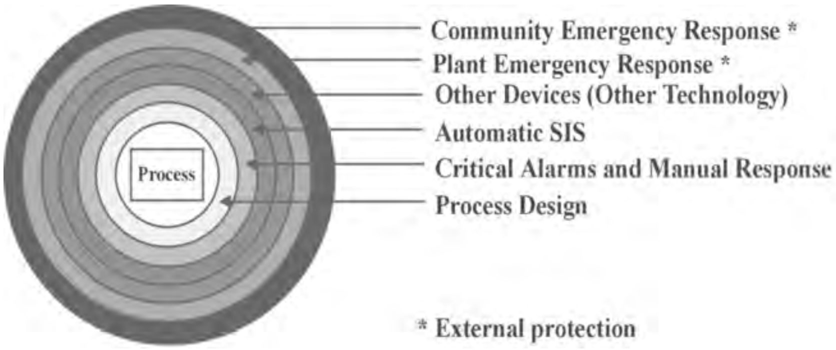

Community Emergency Response *
Plant Emergency Response *
Other Devices (Other Technology)
Automatic SIS
Critical Alarms and Manual Response
Process Design
Process
* External protection

Figure 1.10
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 all “belts and braces” involved in providing protection against a hazardous event or in reducing its consequences. Figure 1.10 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 and Mitigation as seen in figure 1.10:

- **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

1.5.2 Prevention layers

Examples of prevention layers include:

- Plant design

  Plants should be designed as far as possible to be inherently safe. This is the first step in safety and techniques such as the use of low-pressure designs and low inventories are obviously the most desirable route to follow wherever possible
- Process control and work procedures

  The control system and the working procedures for operators play a role in providing a safety layer since they try to keep the machinery or process within safe bounds. However we shall see later that their contribution to plant safety is limited and can sometimes be overrated.
- Alarm systems

  Alarm Systems have a very close relationship to safety shutdown systems but they do not have the same function as a safety instrumented system. Essentially alarms are provided to draw the attention of operators to a condition that is outside the desired range of conditions for normal operation. Such conditions require some decision or intervention by persons. Where this intervention affects safety, the limitations of human operators have to be allowed for.
- Mechanical or Non-SIS protection layers

  A large amount of protection against hazards can be often be performed by mechanical safety devices such as relief valves or overflow devices. These are independent layers of protection and play an important role in many protection schemes.
- Shutdown systems (SIS)

  The safety shutdown system provides a safety layer through taking automatic and independent action to protect the personnel and plant equipment against potentially serious harm. The essence of a shutdown system is that it is able to take direct action and does not require a response from an operator.

1.5.3 Mitigation layers

Mitigation layers are identified as those measures that reduce the consequences of the hazardous event after it has occurred. Examples include: Fire & Gas systems, Containments and Evacuation Procedures.

1.5.4 Diversification

Using more than one method of protection is generally the most successful way of reducing risk. The safety standards rate this approach very highly and it is particularly strong where a SIS is backed up with, say, a mechanical system or another SIS working on a completely different parameter.

1.5.5 Risk reduction models

It is often helpful to visualize risk reduction by using a graphical model as seen in the example shown in figure 1.11.

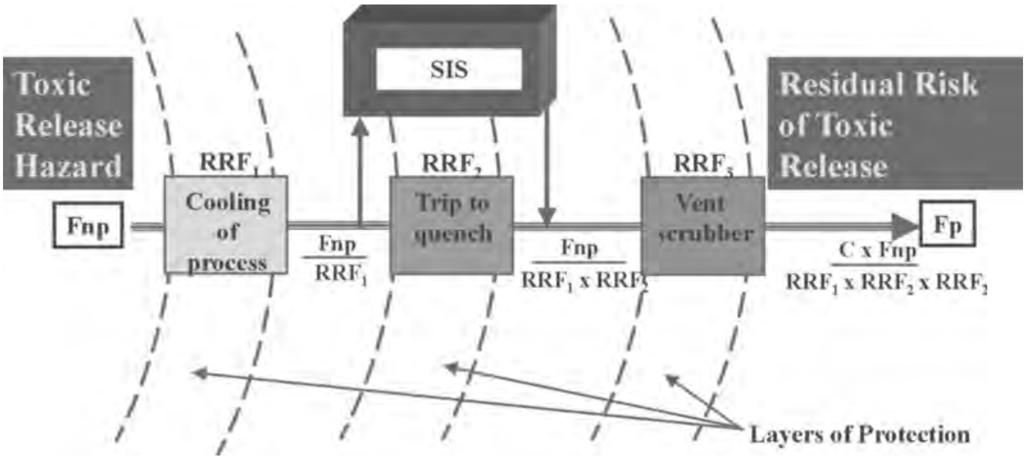


Figure 1.11
SIS seen as a layer of protection

This model indicates the core risk of a toxic release from a hazardous process and shows a potential release frequency of Fnp. The successive and diverse layers of protection reduce the risk frequency at each stage until the residual risk becomes Fp. Note the role of the SIS in this example.

Risk reduction models help us to see how the risk reduction tasks have been “allocated “to various protection layers.

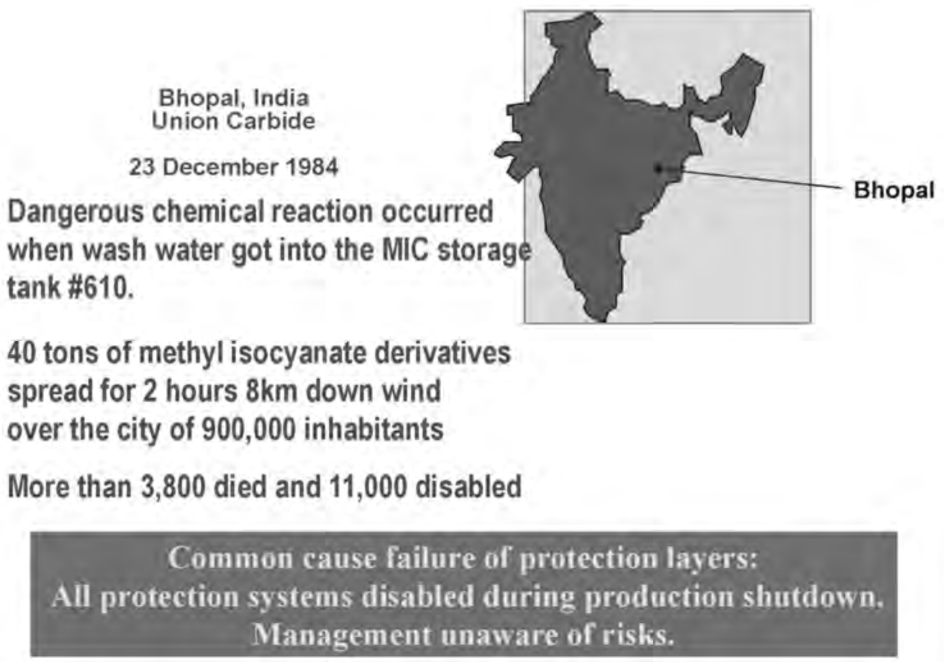
1.5.6 The problem of common cause

The idea of protection layers and successive risk reduction is only valid if the layers are fully independent of each other. It assumes that if one layer fails the other layers will still do the job. If there is a possibility that two or more layers could fail at the same time the assumptions become invalid and the protection systems are said to have a “common cause failure”.

Whilst common cause failures may be attributable some form of engineering factor a more likely cause is the failure to manage overall safety in such a way that it affects two or more safety layers. One tragic example was seen in the events at the Bhopal pesticides plant in India as illustrated by the next figure 1.12.

These notes are based on the account of the accident described in the book “Five Past Midnight in Bophal” by D Lapierre and J Moro (see ref 4 in appendix 1).

The plant had 3 storage tanks for methyl isocyanate (MIC), an unstable liquid that decomposes into a range of toxic components as its temperature rises above 15 C. Most deadly of these is hydrocyanide acid or cyanide gas, which when inhaled, typically leads to death in a very short time.



Bhopal, India
Union Carbide

23 December 1984

Dangerous chemical reaction occurred when wash water got into the MIC storage tank #610.

40 tons of methyl isocyanate derivatives spread for 2 hours 8km down wind over the city of 900,000 inhabitants

More than 3,800 died and 11,000 disabled

Common cause failure of protection layers:
All protection systems disabled during production shutdown.
Management unaware of risks.

Figure 1.12
The Bhopal disaster: all safety layers disabled

The safety systems for the tanks comprised 4 protection layers:

- Each tank was to be operated at no more than 50 % capacity to allow room for a solvent to be added in case a chemical reaction started in the tank
- The tank contents were to be kept below 15C by means of a refrigerant system circulating Freon through cooling pipes at the tanks. A high temperature alarm was provided on each tank to alert operators to an abnormal temperature rise
- Should any gases start to emerge from the tanks they should be absorbed by caustic soda injection as they pass through a decontamination tower
- Finally if any gases escape the absorber tower a flare at the top of a 34-metre flare stack

Due to a lack of demand for the pesticides produced by the plant there had been a long period of time when production had been shutdown or kept to a minimum. The plant equipment and operating standards had been allowed to deteriorate. Finally on the night of 2 December 1984 the tanks appear to have been contaminated with hot water from a pipe-flushing task. This lead to an uncontrollable reaction, which ruptured the tanks, the first of which being 100% full contained 42 tons of MIC. The resulting gas clouds blew across the settlements adjoining the factory fence and onwards into the city. The death toll is disputed but is claimed by Lapierre and Moro to be between 16 000 and 30 000 with around 500 000 people injured.

How could 4 layers of protection be defeated? The simple answer is that there was a common cause failure that was not factored into the safety calculations. Failure to manage the plant according to intended safety and maintenance practices.

The individual failures were:

- Tanks were not kept below 50% full as intended for safe operating practices.
- The refrigeration system had been turned off months earlier including the alarm system because the plant manager did not believe it was necessary to keep the MIC at 5 C. The ambient temperature was 20 C.
- The decontamination tower was offline for maintenance and had been so for a week.
- The flare stack was also out of service for maintenance.

The chemical industry has hopefully learned a lot of hard lessons from the Bhopal disaster but it is informative to read the details and see how familiar the problems are as reported from that experience

1.5.7 Summary of hazards and risk reduction

What we have seen so far indicates that the 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.

- Hazard studies and hazard analysis

  Identify the hazards and estimate the risks.
- Definition of 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 RRFs 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

What does it take to ensure the SIS will deliver the required functional safety?

We are going to investigate the answer to this question in the next sections. To proceed further we should now look for guidance from the standards. The next section introduces the standards, describes how they have come about and shows what they cover.

1.6 Safety management principles

It helps 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.

Why is this important?
Because both managers and engineers can do can do a better job for safety instrumentation by understanding its context and relevance to the overall business and the risk it carries.

1.6.1 The meaning of safety management

What does safety management mean for a manufacturing plant or large item of equipment?

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
- Maintaining a risk register and a safety case report that demonstrates adequate safety measures are in place and are 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. Let’s take a closer look at risk management principles to see what we can learn from them.

1.6.2 Risk management defined

Risk management is a very broadly used term and it is typically applied to business and organizational activities. The broad scope of this term can be seen in the definition of risk management taken from the Australian/New Zealand standard AS/NZ 4360:1999 clause 1.3.24. (Latest version AS/NZS 4360: 2004)

“Risk management-The culture, process and structure, which come together to optimize the management of potential opportunities and adverse effects “

The application of risk management to occupational health and safety is just one of the many areas where the techniques are used. Let’s look at a few basic processes in risk management to show how they match up to established or emerging methods in engineering systems. The following notes are based on guidance provided in the guideline document: “A basic introduction to managing risk” published as an Australian guideline HB 142-1999 by Standards Australia. (Now superseded by HB 436:2004 (Guidelines to AS/NZS 4360:2004): Risk Management Guidelines Companion to AS/NZS 4360:2004.

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.

Hazard studies are part of the disciplined approach to managing risks in plant operations and they must be conducted in accordance with the principles shown here.

1.6.3 The process for managing risk

It turns out that the models suggested for managing risk are the same as those we find in the procedural models described for safety life cycle activities that we shall be looking at later. This is encouraging since it means that one procedural model fits all circumstances and no specialties are involved for safety. If the company recognizes risk management in its business, it should have no problem understanding safety management.

Here is a diagram of a general risk management model based on the version originally published in AS/NZS 4360: 1999. (Latest version AS/NZS 4360: 2004)

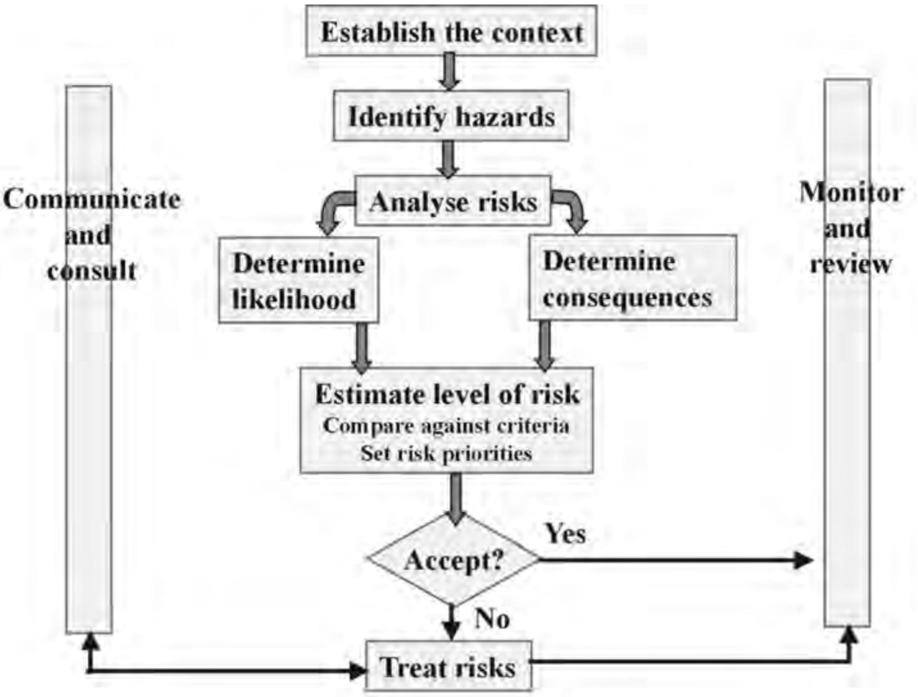


Figure 1.13
The process for managing risk

This model is intended to serve for all risk management activities within a company. These begin with strategic risk management applicable to the corporate planning levels where key business decisions can be subjected to risk evaluation and treatment. There are close parallels with the management of engineering risks and the management of functional safety. Let’s examine the meaning of each step of the process.

1.6.4 Establishing the context

The context includes:

- **Strategic context:** In our field of work this would be typically defined by the organization’s overall Safety Health and Environment (SHE) policy. It would also define the legal framework or regulatory compliance needs for the plant in question.
- **Organizational context:** Requires an understanding of the organization and its capabilities. For example; is the plant in high tech or low-tech area?
- **Risk management context:** Defining which part of the organization or which activities are in the scope. This would be the specific manufacturing plant or process under consideration.
- **Risk evaluation criteria:** Defines the criteria against which any risk is to be evaluated. We shall see that in our field this includes the so-called tolerable risk criteria for risks of harm to persons, environment and asset losses. Risk management and risk reduction cannot be conducted without some reference points for what is acceptable.
- **Structural context:** Deals with how the risk management process is to be handled and documented within the organization. Expect this to lead to a definition of who is responsible for the supply of information, conducting studies and managing the documentary records. In the case of SHE risk

management the documentary records are of critical importance and will require a quality management system.

1.6.5 Identify risks

With the context in place the risk management model says, "identify the risks". The HB 436 guide (see Para.1.6.3) raises the issue of "perceptions of risk" and points out that: *"perceptions of risk can vary significantly between technical experts, project team members, decision makers and stakeholders".*

In this workshop we have to take the "technical experts" route to risks, as we shall see below. It is instructive to note that the layperson sees risk on a more personal and subjective scale.

"…lay persons are less accepting of risk over which they have little or no control (e.g. public transport versus driving one own car), where the consequences are dreaded or the activity is unfamiliar"

This is the stage where hazard studies are performed to answer the questions: "What can happen, how can it happen? The result is a list of risks with the possible causes: This provides the foundation for the "Risk Register"; a convenient way of registering all known risks at the plant and recording what measures have been taken to reduce them to an acceptable level.

1.6.6 Analyze risks

The next step is "Analyze the risk". You can see from the diagram that it is necessary to establish a level of risk based on the criteria we mentioned earlier. The likelihood and the consequences must be found, the resultant risk established and applied to a scale of risk used to set priorities. This is known as risk ranking value and is often performed by using a risk matrix.

1.6.7 Evaluate risks

The next step is to compare the risk level with certain reference points to decide if the risk level is acceptable or not.

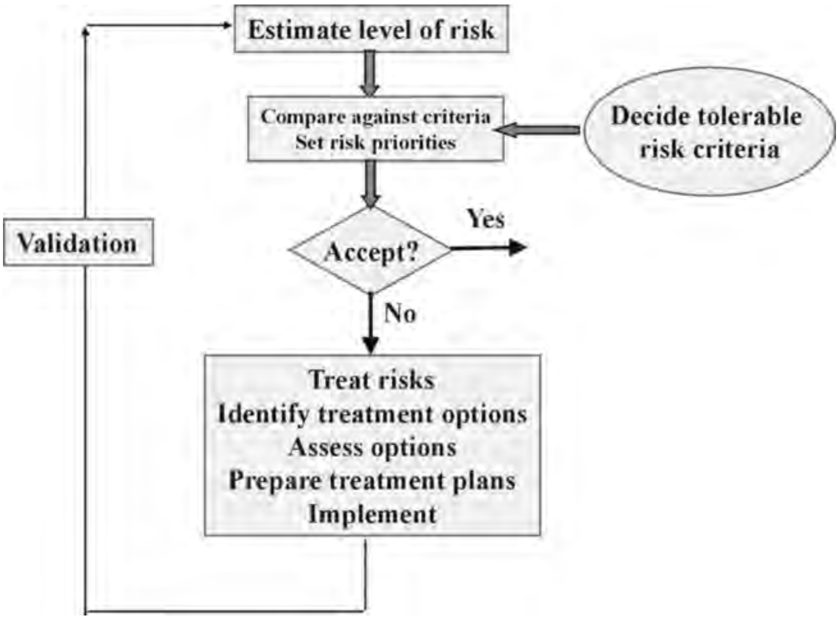


Figure 1.14
Evaluation of risk and the treatment stages

If the risks are unacceptable the choice is to treat the risks or decide to avoid the risks altogether by doing something else.

The diagram introduces the concept of “tolerable risk” or “acceptable risk”. In business practice, the reference point for acceptable risks may depend on the company and its senior management. When it comes to safety and operability there is less room for flexibility. We are concerned with what is acceptable to society and our workers as a “tolerable risk”.

We are going to take a closer look at tolerable risk concepts in a few moments. Before that, let’s look at the general-purpose model for risk treatment.

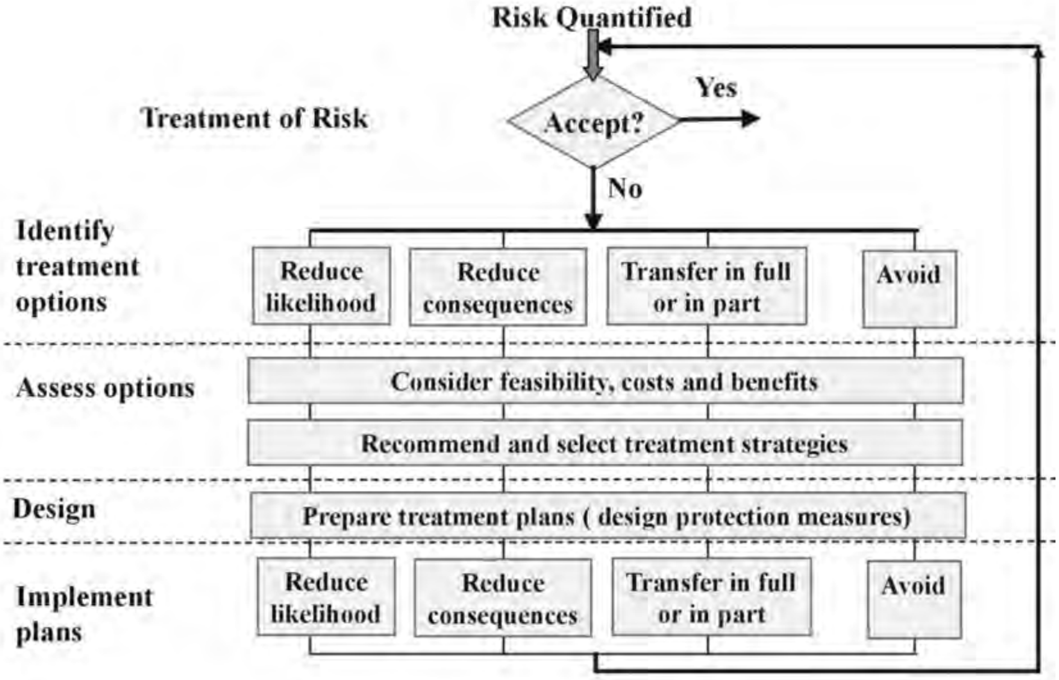

Risk Quantified
Treatment of Risk
Accept?
Yes
No
Identify treatment options
Reduce likelihood
Reduce consequences
Transfer in full or in part
Avoid
Assess options
Consider feasibility, costs and benefits
Recommend and select treatment strategies
Design
Prepare treatment plans (design protection measures)
Implement plans
Reduce likelihood
Reduce consequences
Transfer in full or in part
Avoid

Figure 1.15
Details of treatment of risks (based on AS/NZS 4360: 1999 but modified for safety studies)

This diagram is informative for us in safety management because it demonstrates the options and decision that have to be considered during a hazard analysis and after a Hazop study. In fact this diagram covers all stages in the life cycle of the situation being considered. We shall see this theme recurring throughout the workshop. Let's consider the terms on the left hand side of the diagram:

1.6.8 Identify treatment options

In safety applications we are often able to reduce the risk by treating the likelihood (i.e. reducing the chances of the accident). Sometimes it is necessary to reduce the consequences by what is called "mitigation". (Putting on gas masks after a gas escape is a simple example of mitigation). Protection methods to reduce risk are described as "layers of protection" and we shall be looking at those shortly.

One solution to an unacceptable risk is to avoid it altogether. Unfortunately, this route sometimes implies not building the plant and this has to be considered along with all other options. One of the most important outcomes of a hazard study can be the decision to abort the whole project or adopt an alternative technology on the grounds of unacceptable risk to persons and environment.

1.6.9 Assess treatment options

This is a very interesting stage of risk analysis. We have to consider feasibility, costs and benefits of the possible risk treatment options.

In the case of an engineering project the choices typically come down to:

- Shall we redesign the process to minimize hazard?

- Shall we provide alarms and trips to shutdown the process when the hazardous condition approaches?
- Shall we provide a blast-proof room and evacuation facilities to protect the persons on the plant?
- Shall we do all of these things?

To make a good decision here requires knowledge of the process and the protection methods, some experience and some good cost information. Someone has to do a *quantitative analysis* of the risks. The problem for hazard study teams and project managers is often that the analysis of the risk is approximate and the cost implications of some of the solutions are not readily available. And there may not be much time available for the choices to be made as project deadlines always demand an early decision.

Assume for the moment that the approximate cost of all risk treatment options is known in a particular case. If a choice of options is available, the decision can be made by looking for a trade off between the achievable risk level and cost of achieving it. The relationship model is typically as shown in the next diagram.

Typically, the cost of reducing risk levels will increase with the amount of reduction achieved and it will follow “the law of diminishing returns”. Risk is usually impossible to eliminate so there has to be a cut off point for the risk reduction we are prepared to pay for. We have to decide on a balance between cost and acceptable risk. This is the principle of ALARP that we shall examine in the next section.

The second factor in that will influence the hazard study work is the relationship between design changes and their impact on project costs. There are heavy cost penalties involved in late design changes. Hence it pays to design the hazard study program to identify critical safety and operability problems at an early stage. This is where preliminary hazard study methods are valuable. Preliminary studies can often identify major problems at the early stage of design where risk reduction measures or design changes can be introduced with minimum costs.

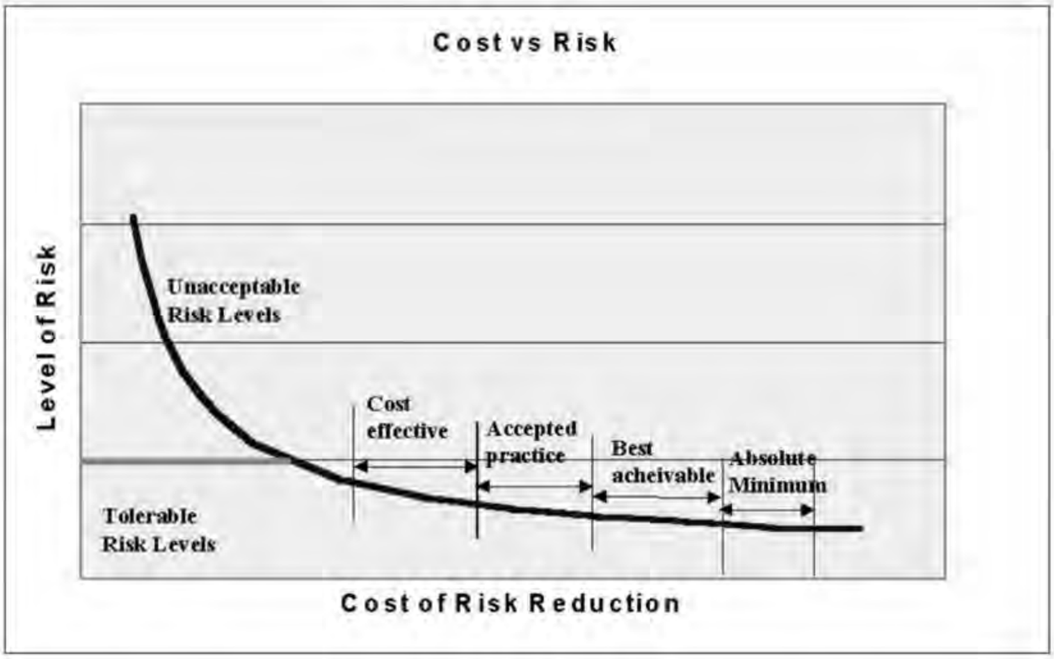


Figure 1.16
Risk reduction versus cost

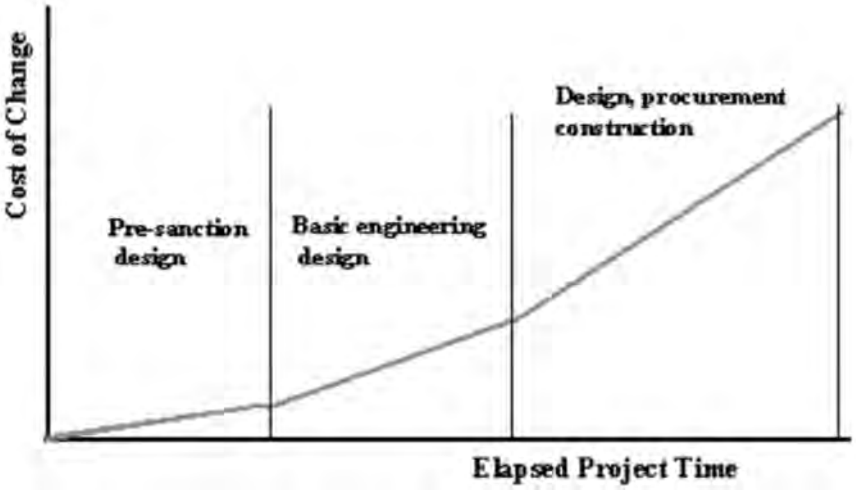


Figure 1.17
Cost of design changes against project time

1.6.10 Prepare treatment plans

The next step in the risk management model is to detail the chosen or proposed solutions to the risk problems. In safety systems, this translates into what is known as the “safety requirements specification”. Later in the workshop we are going to examine this stage in detail to make sure the transition from problem identification to solution works properly. The need for monitoring and review becomes critical from this point on as we seek to make sure the solutions still fit the problem.

This stage is completed when the chosen solutions are ready for use and have been validated to be correct for the original purpose.

1.6.11 Implement treatment plans

Implementation covers the in-service operation of the safety systems and is supported by the monitoring and review process. The model shows that the question of acceptable risk is to be kept open and under review. This philosophy requires, for example, that the hazard study information is kept up to date and that periodic reviews must be held to see that the risks levels are still acceptable.

1.6.12 Practical versions of risk management for plant safety

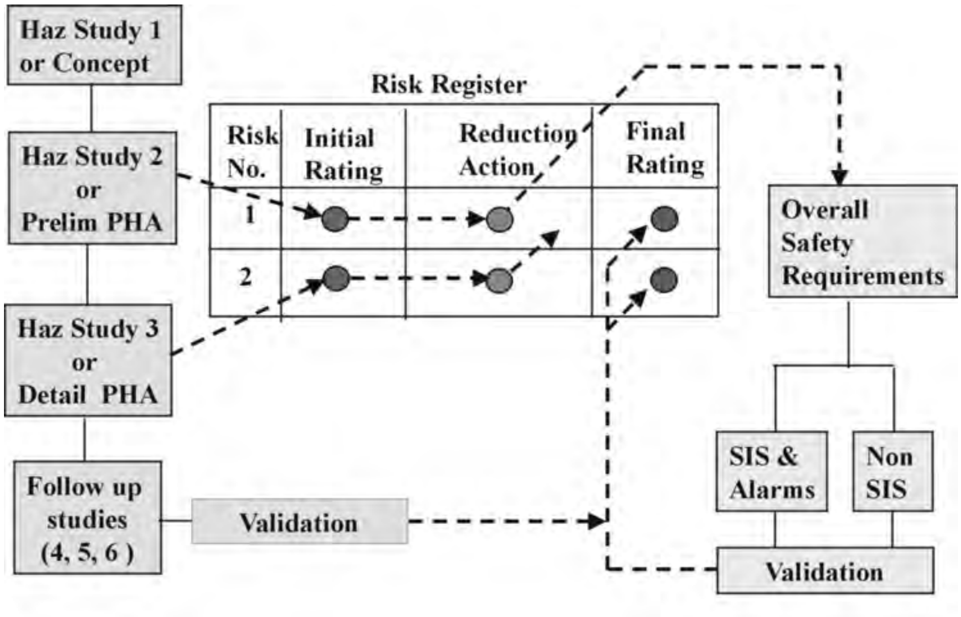


Figure 1.18
Practical implementation of risk management

The SIS project is an integral part of the overall safety management system for a process plant that presents a hazard. All the elements of risk management translate into practical activities for the specification and design of Safety Instrumented Systems. 1.17 shows the key elements of the safety project with the hazard study stages on the left and the SIS implementation on the right.

- The preliminary hazard studies identify the risks and place them into a risk register.
- The risk register records the risk reduction needs for each risk and the treatment options deliver the requirements for safety into the core documents for the plant and for SIS. These are called the safety requirements specifications.
- The requirements are used as the basis for building the safety systems. Non-SIS devices as those such as such as relief valves and protected buildings. The SIS takes it share of the risk reduction, known as its safety allocation.

- Hazop studies examine the detailed P&I diagrams for the plant and should be used confirm that the planned safety measures are still acceptable. Sometimes the Hazops identify new hazards and risks and these are then added to the list.
- As the plant moves into construction and commissioning follow up studies confirm that the measures listed by previous studies have been implemented and these support the validation of the completed SIFs.
- The final risk rating should be low enough to be considered acceptable for all personal, environmental and business risks. Validation of the installed SIS and other measures seeks to confirm the risk reduction objectives have been achieved
- Once fully operational all the operating and maintenance procedures are aimed at keeping up the standard of performance of the various safety systems.
- Periodic reviews of both the hazard studies and the SIS performance are used to ensure risk levels are being kept within the target range.

1.6.13 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. Does it also have legal obligation to use them? Let’s take a look at the legal framework.

1.7 The legal framework for process safety

Where do we stand with regard to the legal requirements for safety? What does the law require us to do? Are there any safety targets that we are legally required to meet?

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.

The general principles that are those that are commonly seen in regulations in the USA and in Europe. 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
- Decide if risk reduction measures are needed

- Implement risk reduction measures
- Confirm that the process is now safe to an acceptable level of risk.
- Carry out periodic audits and reviews of safety studies and achieved performance

In the case of the 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 and this will include 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 treatments methods are up to date with the current version of the plant.

1.7.1 International trends in safety practices

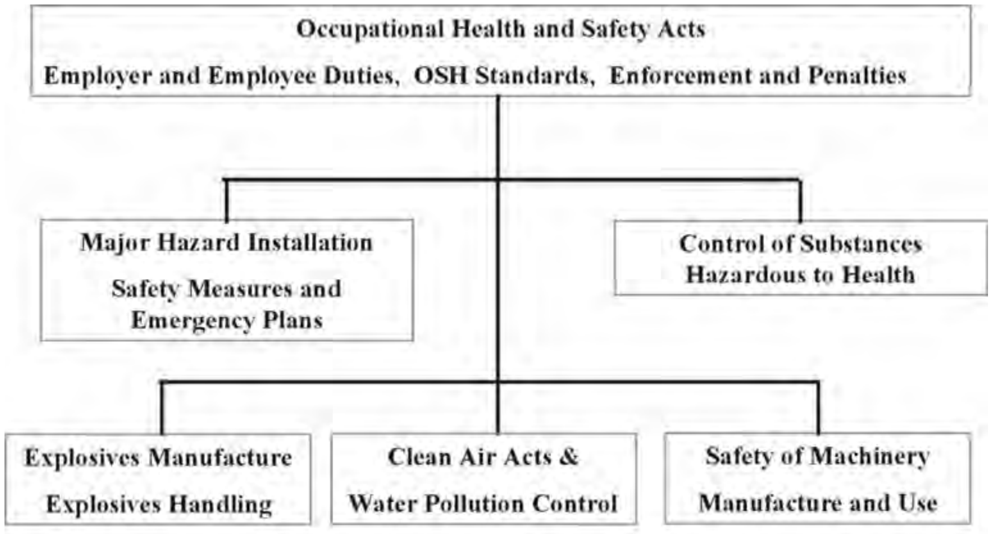

Occupational Health and Safety Acts
Employer and Employee Duties, OSH Standards, Enforcement and Penalties
Major Hazard Installation
Safety Measures and Emergency Plans
Control of Substances Hazardous to Health
Explosives Manufacture
Explosives Handling
Clean Air Acts &
Water Pollution Control
Safety of Machinery
Manufacture and Use

Figure 1.19
Typical structure of health and safety regulations for industry

In most countries Occupational Health and Safety (OHS) regulations lay down basic requirements for employers to safeguard their workers and public from harm. The overall OHS requirements are typically supplemented by additional regulations that target particular sectors of industry where significant problems with hazards are known. The above diagram shows the characteristic structure seen in USA, Europe, South Africa, Australia and other countries.

The OHS types of regulations usually require that a risk assessment be carried out on the occupations and processes at the place of work. They normally require a reporting and review system to assist regulatory oversight.

Specific regulations have been generated for particular types of industry that supplement the basic OHS requirements. For example the principal regulations affecting the chemical industries in the USA are:

- OSHA regulations for “Process Safety Management of Highly Hazardous Chemicals and Blasting Substances (Referred to as the PSM rule) (29 CFR 1910.119)

- USA: Clean Air Act: EPA-40 CFR Part 68: Accidental Release Prevention Requirements. Risk Management Program. Referred to as the "RMP Rule"

The widespread application of the PSM and RMP rules means that process hazard analysis (PHA) is an essential technique for very many companies in the USA. In particular the more critical process plants will be most likely to employ detailed HAZOP procedures as the routine method for assisting them to comply with the regulations.

Periodic reviews of existing hazard studies are part of the mandatory review procedures built into safety management systems. Some countries define mandatory review intervals. The PSM rule in USA requires companies to update or revalidate their process hazard analysis at least every 5 years, in South Africa the Major hazard installations Act set has set the review at every 3 years.

Pasadena incident: Petrochemical plant producing polyethylene at Pasadena, Texas

- October 1989: Release of isobutene , ethylene and catalyst carrier during routine maintenance on a reactor. Vapour cloud ignited after 1 minute with equivalent explosion energy of 10 t of TNT.

Consequence; 23 killed, 130 injured. Damage costs: approx $750 million

The PSM rule was an improvement over earlier safety regulations and was driven by the realization that major hazard potentials at plants were not being managed to adequate standards in some areas. The main driving force was said to be the Pasadena, Texas incident. Subsequently the USA set up the Chemicals Safety Board to track all chemical plant accidents. Their annual reports have shown some startling facts:

On 24 February 1999 the US Chemical Safety and Hazard Investigations Board told Congress that…….
In 1996 chemical incidents claimed the lives of the equivalent of two fully loaded 737 passenger jets
256 people perished, and
an average of 256 people died the year before,
…….. and the year before that.

Source: EPA Guide to Chemical Risk Management - New Ways to Prevent Chemical Incidents

Studies have been carried out in response to these concerns and there have been significant if sometimes conflicting findings.

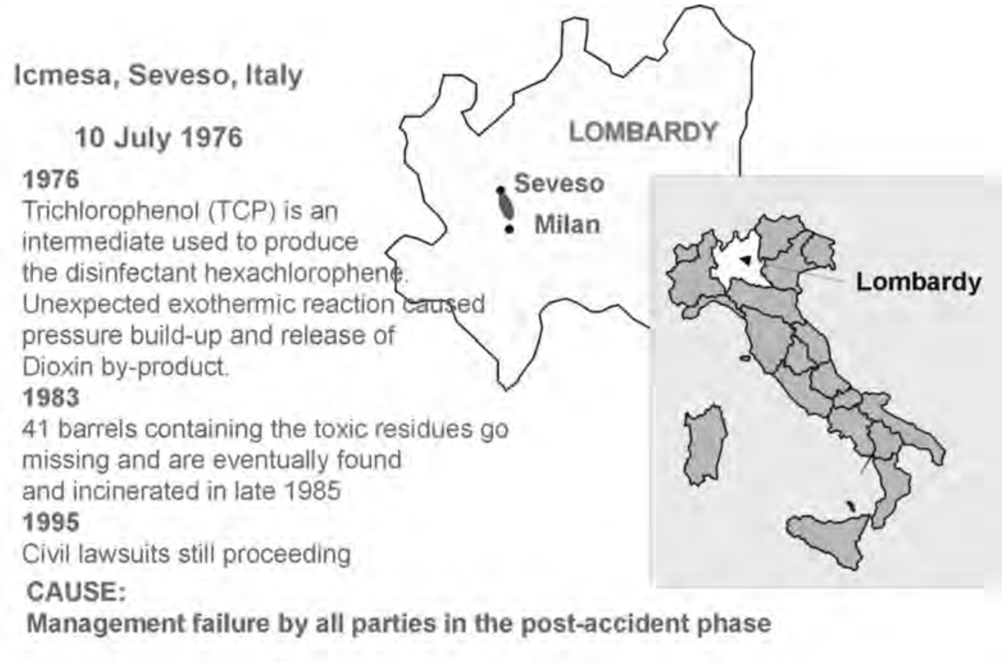
In the period 1978 to 1996 records show that…….an average of 60,000 incidents occurred each year. Of these:
605,000 incidents resulted in **2,565** deaths and 22,949 injuries. Of these:**333** deaths and 9,962 injuries happened on fixed-site facilities
General equipment failure and human error were the key causes of incidents.

Source EPA Guide to Chemical Risk Management - New Ways to Prevent Chemical Incidents

1.7.2 European regulations

In Europe the major hazard regulations are derived from the Seveso II directive (96/82/EEC) and its amendments. The directive originates from the Seveso 1 directive that was introduced following the disastrous events at Seveso in Northern Italy.

The first Seveso directive was later revised and extended, again stimulated by accidents such as Bhopal, India 1984 and Basel, Switzerland, 1986. The current version is known as the Seveso II directive:



Icmesa, Seveso, Italy

10 July 1976

1976
Trichlorophenol (TCP) is an intermediate used to produce the disinfectant hexachlorophene. Unexpected exothermic reaction caused pressure build-up and release of Dioxin by-product.

1983
41 barrels containing the toxic residues go missing and are eventually found and incinerated in late 1985

1995
Civil lawsuits still proceeding

CAUSE:
Management failure by all parties in the post-accident phase

Figure 1.20
Incidents at Seveso, Italy

Outline of Seveso II

The SEVESO II Directive sets out basic principles and requirements for policies and management systems, suitable for the prevention, control and mitigation of major accident hazards.

Establishments that have the potential for major accidents are required to comply with the requirements of the directive in the form of national laws that are passed to enact the EU directives. The establishments are classed into “lower tier” and “upper tier” according to size of inventories and the size of the plant.

- *Lower tier establishments* are to draw up a Major Accident Prevention Policy (MAPP), designed to guarantee a high level of protection for man and the environment by appropriate means including appropriate management systems, taking account of the principles contained in Annex III of the Directive
- *Upper tier establishments* (covered by Article 9 of the Directive and corresponding to a larger inventory of hazardous substances) are required to demonstrate in the ‘safety report’ that a MAPP and a Safety Management System (SMS) for implementing it have been put into effect in accordance with the information set out in Annex III of the Directive

1.7.3 Development of a Major Accident Prevention Policy (MAPP)

The Seveso II directive states:

"The major accident prevention policy should be established in writing and should include the operator's overall aims and principles of action with respect to the control of major accident hazard"

Activities in support of the SMS are defined in the directive. These include:

- **Organization and personnel:** Roles and responsibilities of personnel, identification of training needs and the provision of training. The operator should identify the skills and abilities needed by such personnel, and ensure their provision
- **Hazard identification and evaluation:** includes procedures to systematically identify and evaluate hazards, define measures for the prevention of incidents and mitigation of consequences
- **Operational control:** documented procedures to ensure safe design and operation of the plant. Safe working practices should be defined for all activities relevant for operational safety
- **Management of change:** Operating company should adopt procedures for planning and controlling all changes in people, plant, processes and process variables, materials, equipment, procedures, software, design or external circumstances which are capable of affecting the control of major accident hazards
- **Planning for emergencies:** An emergency plan is required
- **Monitoring performance:** The operator should maintain procedures to ensure that safety performance can be monitored and compared with the safety objectives defined
- **Audit and review:** Independent audit of the organization and its processes. Management to keep its SMS under review for essential correction or changes

The above principles have been transferred into national laws in member states of the EU. So in the UK, for example, the directive is implemented as the Control of Major Accident Hazards (COMAH) regulations and has been in force since Feb 1999. The two tier reporting requirements are defined as per the directive. Additionally, all hazardous chemical and other substances used in industry are subject to the Control of Substances Hazardous to Health (COSHH) regulations, 1994.

1.7.4 Are they any legal requirements for tolerable risk targets

Regulations usually leave open the question of how much is safe? The approach that has been widely adopted in industry is to avoid specifying absolute numbers as a measure of safety but rather to use a comparative scale for similar situations or context to use the term seen earlier.

When considering how much risk reduction is needed for a process risk the general approach by safety authorities is to see if the company has followed the principle of ALARP, meaning As Low AS reasonable Practicable.

The ALARP principle is commonly represented by the following "ALARP Diagram"

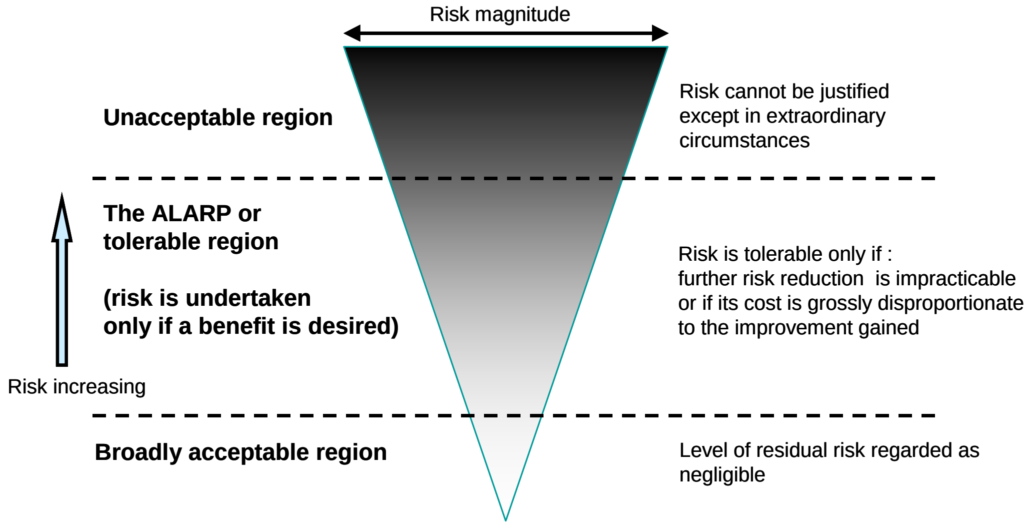

Risk magnitude
Unacceptable region
Risk cannot be justified except in extraordinary circumstances
The ALARP or tolerable region
(risk is undertaken only if a benefit is desired)
Risk increasing
Risk is tolerable only if : further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
Broadly acceptable region
Level of residual risk regarded as negligible

Figure 1.21
ALARP diagram based on the version published in IEC 61511-3 Annex A Figure A-1

The ALARP (as low as reasonably practicable) principle recognizes that there are three broad categories of risks:

- **Negligible risk:** broadly accepted by most people as they go about their everyday lives, these would include the risk of being struck by lightning or of having brake failure in a car
- **Tolerable risk:** We would rather not have the risk but it is tolerable in view of the benefits obtained by accepting it. The cost in inconvenience or in money is balanced against the scale of risk and a compromise is accepted
- **Unacceptable risk:** The risk level is so high that we are not prepared to tolerate it. The losses far outweigh any possible benefits in the situation

The width of the triangle represents risk and hence as it reduces the risk zones change from unacceptable through to negligible. Clearly this is following the same principle that we saw earlier in the risk management section. The hazard study and the design teams for a hazardous process or machine have to find a level of risk that is as low as reasonably practicable in the circumstances or context of the application. The problem here is: How do we find the ALARP level in any application?

The procedure is deceptively simple!

Step 1

The estimated level of risk must first be reduced to below the maximum level of the ALARP region at all costs.

This assumes that the maximum acceptable risk line has been set as the maximum tolerable risk for the society or industry concerned. This line is not always easy to find, as we shall see in a moment

Step 2

Further reduction of risk in the ALARP region requires cost benefit analysis to see if it is justified. This step is a bit easier and many companies define cost benefit formulae to support cost justification decisions on risk reduction projects. The principle is simple:

"If the cost of the hazardous event is likely to exceed the cost of more risk reduction then more risk reduction is justified."

The tolerable risk region remains the problem for us. How do we work out what is tolerable in terms of harm to people, property and environment?

The conclusion to be reached is that there are approximate scales of personal risk that are derived from accident statistics and the knowledge of what is reasonably achievable in different types of industries. Similarly in business the risk frequency for major damage to the plant can be found by considering what scale of loss it will represent. For example a 1 million dollar loss every 10 years may be just acceptable without too much long term harm. But a 50 million dollar loss might be the end of the business and you may want to set that chance at 1 in 10,000 years.

The problem here for the risk assessment team is that someone has to set the targets for tolerable risk so that the risk reduction measures can be adopted to meet or better the target by following the ALARP principle. This comes down to a management or corporate responsibility.

One simple way of presenting the targets is to establish a tolerable risk profile or chart describing what levels of risk are acceptable and what levels are not. Figure 1.22 shows an elementary risk matrix chart with the tolerable and unacceptable areas marked. The overlap region in the middle is the "Grey Area" of uncertainty. This where the where the principle of ALARP must be applied for each individual case.

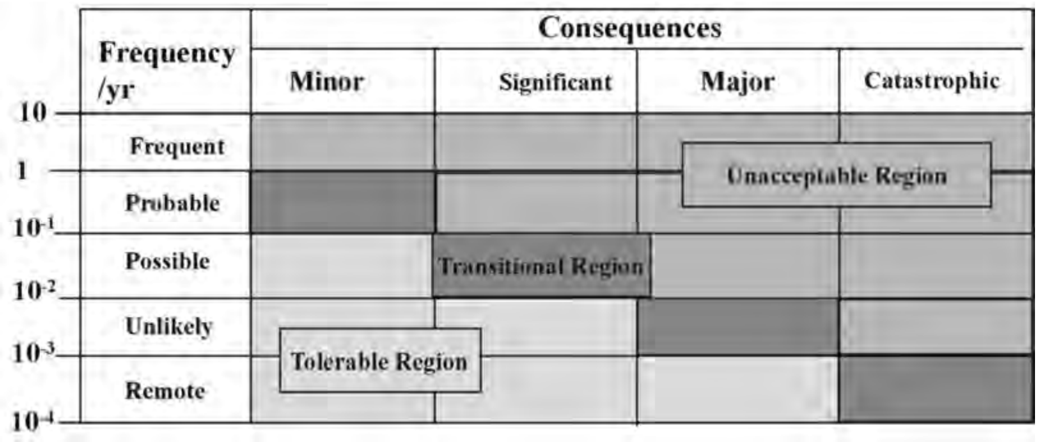


Figure 1.22
Risk matrix with tolerability bands

1.7.5 Legal requirements for safety instrumentation

The provision of a SIS will fall within the overall safety management system wherever it is claimed to be part of the risk reduction measures. Where there are well-established protection methods for known types of hazards in the workplace, (e.g. for many common types of machines), the regulations usually require compliance or will accept conformity to an approved standard.

When it comes to implementing protection measures or trips the solutions are not usually prescribed directly except in the case of boiler and furnace safety interlocks. For process plants there is no specific requirement for safety instrumentation to be applied but it will frequently be claimed as one of the key safety measures applied to make a plant safe.

The questions then arise:

- How can the company substantiate its claim that the plant has been made safe by the fact that it has a safety instrumented trip system?
- How effective is the safety system?
- How does the company ensure that it is kept in working order

This is where the new international standards for functional safety, IEC 61508 and IEC 61511, provide a comprehensive method of assessment for instrumented safety systems. These standards can be used by legislators as references or benchmarks of quality for demonstrating that a suitable regime is being maintained for functional safety.

In summary:

- Operating companies are legally obliged to ensure safety in the workplace and to protect the public and the environment from harm that may arise from their process plants
- Companies must conform to process safety and clean air legislation by having an auditable record of hazard studies and risk assessments. Appropriate risk reduction measures must be implemented and managed through a safety management system. A safety case justifying the risk management position must be written for inspection by regulatory authorities
- Safety Instrumented Systems must be seen to be capable of providing the level of safety improvement (risk reduction) that is claimed in the safety case. This can be done by demonstrating conformity to a national or internationally accepted standard or code of practice
- Conformity to IEC 61508 or IEC 61511 is a very effective way to demonstrate that the safety instrumented protection measures are able to provide the claimed reduction in risk
- Several countries have recognized IEC 61508 as an appropriate reference standard for safety instrument systems but do not require conformity. Some legislation for specific process equipment such as furnaces may insist on conformity to IEC 61508
- In the USA the OHSA has incorporated, by reference, the standard ANSI/ISA S84.01:2004 for instrumented safety systems where these are used for compliance with the process safety regulations. This the same standard as IEC 61511 except for a “grandfather clause” that allows for existing SIS devices

built before issuance of ISA S84.01: 2004 to be exempted provided the owner can show that the equipment is “designed, maintained, inspected and operating in safe manner”.

Conclusions

- The underlying principle for delivering safety in the workplace is to have a good safety management system incorporating best risk management practices
- In all cases where risk to persons are involved the regulations require an identification of hazards and an assessment of risk followed by credible measures to reduce it. Regular hazard studies and analysis must be formally done and recorded
- Safety measures must be implemented to good standards of practice and managed within the safety management system
- Using a recognized engineering standard is the most credible route for demonstrating conformity to best available practices

The trend in international safety practices is to move away from prescribed safety solutions problems in favor of allowing individuals to carry out assessments of risk followed by risk reduction measures appropriate to the problem. Independent but approved assessment bodies are available to carry out conformity assessments. Their reports are then used to show to the authority that a company is competent to apply, operate and maintain a safety instrumented system.

1.8 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. Just to recall where we are headed here is a section of the roadmap.

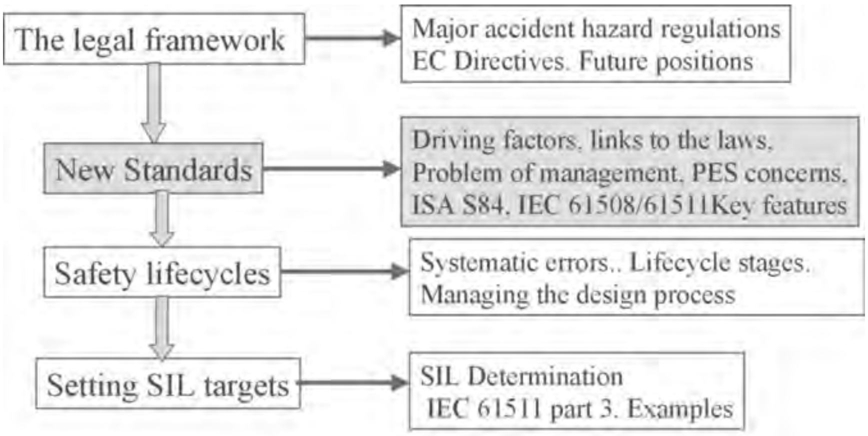

The legal framework
Major accident hazard regulations
EC Directives. Future positions
New Standards
Driving factors, links to the laws,
Problem of management, PES concerns,
ISA S84, IEC 61508/61511Key features
Safety lifecycles
Systematic errors.. Lifecycle stages.
Managing the design process
Setting SIL targets
SIL Determination
IEC 61511 part 3. Examples

Figure 1. 23
Section of roadmap

1.8.1 Driving factors for functional safety standards

Up until the 1980s the codes of practice for design and use of trip and alarm systems were set down by major chemical and petro-chemical companies. Their codes of practice established most of the ground rules that are used today. They provided a solid and well proven technical basis for essentially hardwired, fixed logic safety systems based on analogue sensors or direct acting switches and using relays or hard-wired solid-state modules for logic solving duties.

The codes of practice have served the industry well until a number of changes began to take place along with some external driving factors.

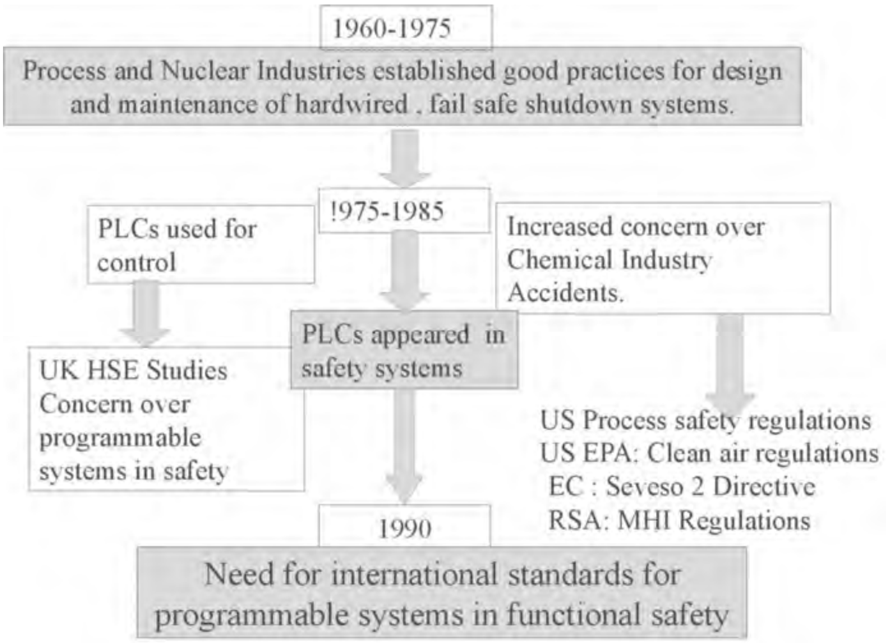

1960-1975
Process and Nuclear Industries established good practices for design and maintenance of hardwired . fail safe shutdown systems.
!975-1985
PLCs used for control
Increased concern over Chemical Industry Accidents.
PLCs appeared in safety systems
UK HSE Studies Concern over programmable systems in safety
US Process safety regulations
US EPA: Clean air regulations
EC : Seveso 2 Directive
RSA: MHI Regulations
1990
Need for international standards for programmable systems in functional safety

Figure 1.24
Driving forces for new standards in functional safety

These included:

- The introduction of PLCs as general purpose logic solvers and the trend to install them for safety system duties. Safety specialists and administrators, particularly the UK Health and Safety Executive became concerned that programmable systems were entering service in safety systems without adequate guidelines on how they should be applied
- General public concern over the increasing scale of chemical industry accidents and the nuclear plant accidents at 3 Mile island and later at Chernobyl. This led to tighter regulations for process industry safety and for environmental protection
- The new industry regulations called for best practices in safety systems but there were no adequate reference standards outside of private company guides
- Programmable systems and network technologies have brought a new set of problems to functional safety systems. Software comes with new possibilities for performance failure due to program errors or untested combinations of coded instructions. Hence conventional precautions against defects in electrical hardware will not be sufficient to ensure reliability of a safety system

Newer standards such as the German VDE 0801 and DIN 19250 emerged in the late 1980s to incorporate quality assurance grading for both hardware and software matched to the class of risk being handled. In the USA the ISA S84.01 standard was issued in 1995 for use in process industry applications including programmable systems. In the UK the HSE promoted the drive for an international standard along with Germany and the ISA in the US. These and many other factors resulted in the issue of an IEC 61508, a generic standard for functional safety using electronic and programmable electronic equipment.

The term generic is used because the standard has been designed to serve many sectors of industry with a generalized approach leaving as much flexibility as possible in its application. It has been issued with the idea of supporting the development of "sector standards"; those that can focus on one area of industry and provide more directly targeted guidelines.

Figure 1.25 shows the progression from figure 1.24

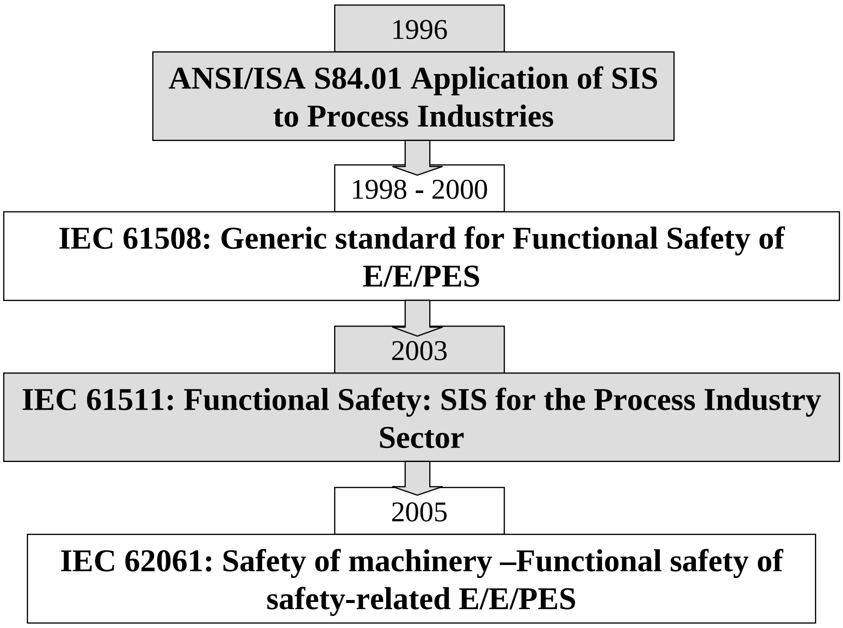

1996
ANSI/ISA S84.01 Application of SIS to Process Industries
1998 - 2000
IEC 61508: Generic standard for Functional Safety of E/E/PES
2003
IEC 61511: Functional Safety: SIS for the Process Industry Sector
2005
IEC 62061: Safety of machinery –Functional safety of safety-related E/E/PES

Figure 1.25
Steps leading to IEC 6151 and beyond

In line with the above plans the process industry sector standard was issued in 2003 as IEC 61511: Functional safety: Safety Instrumented Systems for the process industry and was followed in 2005 by the machinery sector standard IEC 62061.

The style and objectives of the new standards is to set down a framework of good practices leaving the designers room to find appropriate solutions to individual applications. All standards require a quality management system to minimize systematic errors at all project phases and call for extensive verification and validation of each stage of the project or "safety life cycle".

1.8.2 Why are there two standards for SIS?

The position now is that two relevant standards exist for SIS practices and the question arises which one to use?

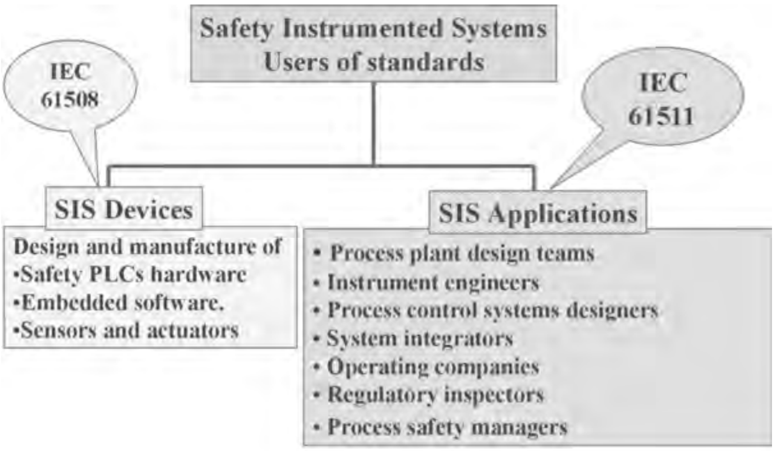


Figure 1.26
Users of the IEC Functional safety standards for SIS

IEC 61511 explains in its introduction that it 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 that we may have to buy from a system supplier or instrument vendor should be engineered in accordance with IEC 61508. We should use IEC 61511 for plant safety projects and use 61508 for design and manufacture of safety system products as indicated in figure 1.26.

1.8.3 Where are the standards recognized?

As shown in figure 1.27 the IEC standards are finding worldwide international approval. In particular IEC 61511 has been developed in co-operation with USA based companies and the ISA. In the US it is published as ANSI/ISA S84.01- 2004 (IEC 61511 Mod).

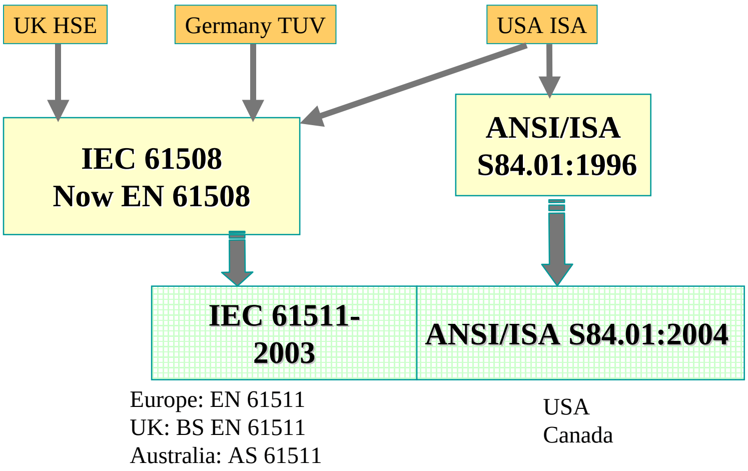


Figure 1.27
Worldwide application of IEC FS standards

1.8.4 Summary of IEC 61508

IEC 61508 part 1was released in 1999 and later parts were released in 2000. The standard was the result of over 10 years of committee activities and represents a comprehensive attempt to cover all aspects of the design and operation of Safety Instrumented Systems using programmable electronics. The principles laid down in this standard are widely applicable to functional safety systems in any form of industry.

International Electrotechnical Commission: IEC 61508

Title:

Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 1:	**General requirements**
Part 2:	**Requirements for electrical / electronic /programmable electronic systems**
Part 3:	**Software requirements**
Part 4:	**Definitions and abbreviations**
Part 5:	**Examples of methods for the determination of safety integrity levels**
Part 6:	**Guidelines on the application of parts 2, 3**
Part 7:	**Overview of techniques and measures**

Figure 1.28
Title and parts of IEC 61508

The standard emphasises the life cycle approach to the overall safety system project and 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 published in 7 parts and the role of each part can be summarized from our perspective as follows:

- **Part 1:** Tells us how to manage the overall safety project by using the safety life cycle approach. It uses the safety lifecycle as framework for a set of requirements to be carried out at each phase of the project
- **Part 2:**Defines SIS design requirements and the detailed procedures to be observed in developing, building and testing the equipment
- **Part 3:** Details the software engineering practices that must be observed for a programmable system to qualify for safety duties. It scales the special engineering requirements against the SILs. This part is largely aimed at developers of operating systems for safety certified controllers
- **Part 4:** Provides definitions of terms
- **Part 5:** Provides advice on methods of determining the SIL requirements from information obtained from hazard studies. Here we find the various methods of quantitative and qualitative analysis including risk graphs

- **Part 6:** Provides guidance on how to carry out the requirements defined in parts 1, 2 and 3. In particular this part contains useful sections on how to do the reliability calculations used to evaluate the SIL of a proposed design
- **Part 7:** Provides references to further reading and techniques used in support of the SIS design work

1.8.5 Key elements of IEC 61508

The standard is large and requires a lot of study before it can be used effectively in a company. However it is of great value to both manufacturers and end users of safety systems 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.

Some key points for the project team are noted here:

- Management of functional safety is just as important as the way we design the SIS

  You cannot claim compliance with the standard unless you can demonstrate that the project has been run under a formalized set of management procedures ensuring everyone knows what they are required to do to support the safety systems at the plant
- Technical requirements cover hardware, software, testing

  SIS designs must satisfy constraints on architectures and safe failure fractions. Equipment must have essential proven characteristics. This leads to the certification of devices by third parties. E.g. TUV SIL 3 certification. Self-certification is also permitted
- Documentation is mandatory and must be kept current

  Companies must keep a complete set of records of the safety life cycle activities and show that the SIS as installed is valid for the current plant design and its hazard analysis. The testing regimes must match the SIL performance requirements. . The testing records must line up with the reliability analysis
- Competence of persons

  Individual assigned by companies to work on safety systems are must be competent to perform the tasks. The standard does not detail the experience of skills needed but other bodies have developed guidelines

The principles laid down in IEC 61508 are intended to be adopted by other standards committees wishing to create “sector standards” that are more closely written for a particular sector of industry. As we have seen this has lead to the production of IEC 61511, based on all the requirements of IEC 61508 but directed at the process industries.

1.8.6 Summary of IEC 61511

The title and contents information are as follows:

IEC 61511

Functional safety- safety instrumented systems for the process industry sector

- Part 1: Framework, definitions, system hardware and software requirements
- Part 2: Guidelines in the application of part 1
- Part 3: Guidance for the determination of safety integrity levels

Published by

IEC: International Electrotechnical Commission,
PO Box 131, CH –1211, Geneva, Switzerland

The normal route for obtaining copies of the standard is from the IEC Web store at http://www.iec.ch. Participants are advised that the costs for this standard are high with an average cost per part of 187 Swiss Francs.

Summary of parts

Part 1: Defines all technical terms and abbreviations and then defines requirements for:

- Management of functional safety
- Safety life cycle activities from initial hazard analysis through to operation and maintenance
- Verification activities
- Risk assessment and safety requirements specification
- Design and engineering of hardware and application software
- Factory acceptance testing
- Installation and commissioning
- Safety validation

Part 2: Extensive guidance on methods and design features to achieve required levels of safety integrity:

- The guidance includes wide use of practical advice taken from ISA S84.01
- This part carries substantial practical advice on good practices for selection and installation of instrumentation for safety systems based on previous experience of participants in the standards committees

Part 3: Provides guidance on several different methods of determining the required Safety Integrity Level (SIL) for any Safety Instrumented Function (SIF):

- SIL determination methods apply to protection of either personnel, general public or the environment. May also be applied to non-safety applications such as for protection against asset losses through plant damage
- Quantitative and qualitative methods (e.g. risk graph method) are described

The conclusion from this scope is that the new standard provides a valuable reference for companies wishing to embark on a safety system application project or upgrade their present codes of practice.

Commentary

It is worth noting that the IEC 61511 standard is described by its writers as a “process sector implementation of IEC 61508”. Readers of IEC 61508 will find the same scope and very similar coverage of requirements in IEC 61508 and in some cases companies may elect to continue using sections of IEC 61508.

This approach is probably equally valid because of the way the two standards are linked. However there has been criticism of IEC 61508 for its complexity and readers complain that it takes too much study to understand the meaning of some sections. It is hoped that the new standard will be easier to translate into practical applications.

Throughout in this workshop we shall be referring to some aspects of the standards in more detail. At this stage we are going to concentrate on the aspects that affect the overall projects and involve company management as well as engineers from mechanical, chemical and electrical disciplines.

1.9 The safety lifecycle

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

1.9.1 The problem of systematic errors

During the evolution of the new standards it was realised that whilst the hardware can achieve a high degree of safety integrity through good engineering practices this would not be much help if the project engineering work was vulnerable to making errors in the basic specification or testing of the overall application.

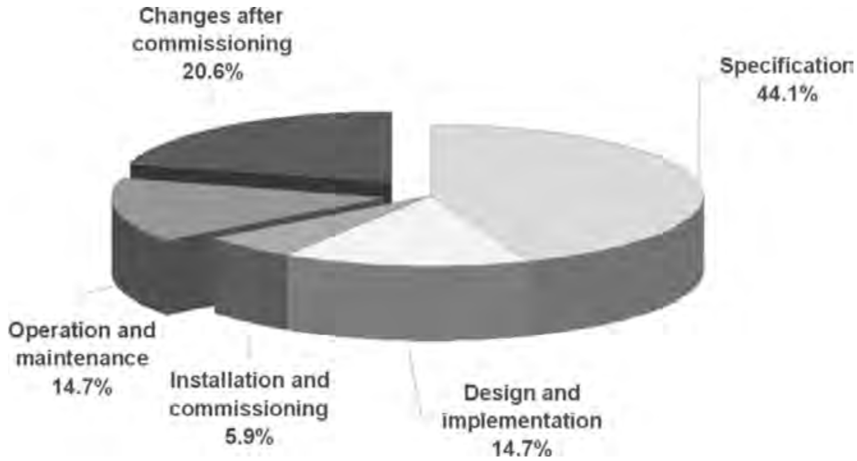


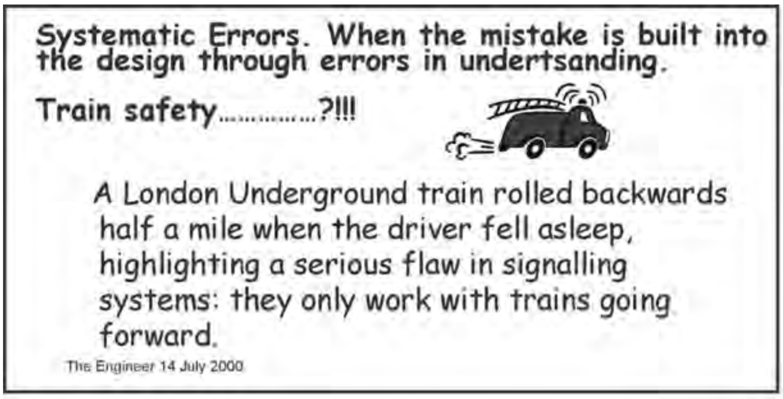
Figure 1.29
Results of HSE’s study of 34 incidents attributed to control system faults

Supporting evidence for this problem was found through a study conducted by UK HSE in 1994 by rounding up details of accident records involving failures of safety instrumentation. The results shown in figure 1.29 indicated that specification errors and errors during design changes accounted for approximately 65% of all failures.

These type of errors are called systematic errors and arise through weaknesses in the way the various parties involved in project arrive at an understanding of what is required. A common example is in the interface between say a process engineer and a computer programmer. Both parties may believe they are working to the same functional requirements in a program but somehow the program does not do what the process engineer really intended.

An example of a systematic error in design: There is the recorded case of a London Underground train that ran backwards down a tunnel when the driver fell asleep. See figure 1.30.

Since you cannot buy hardware or software to overcome systematic errors it is clear something else has to be attended to. The answer is believed to lie in Quality Assurance methods; making sure that the product is fit for purpose and definitely meets its original intentions. This is realised in safety systems by working to a systematic method called the safety lifecycle.



Systematic Errors. When the mistake is built into the design through errors in undertsanding.

Train safety…………?!!!

A London Underground train rolled backwards half a mile when the driver fell asleep, highlighting a serious flaw in signalling systems: they only work with trains going forward.

The Engineer 14 July 2000

Figure1.30
Example of systematic error

1.9.2 The safety life cycle

The safety life cycle is an orderly sequence of design and build stages with each activity being mapped out with essential requirements that must be satisfied at each phase. It is visualized by a flow chart diagram showing the procedures suggested for the management of the safety functions at each stage of the life cycle. Figure 1.31: shows a simplified version that identifies the main stages.

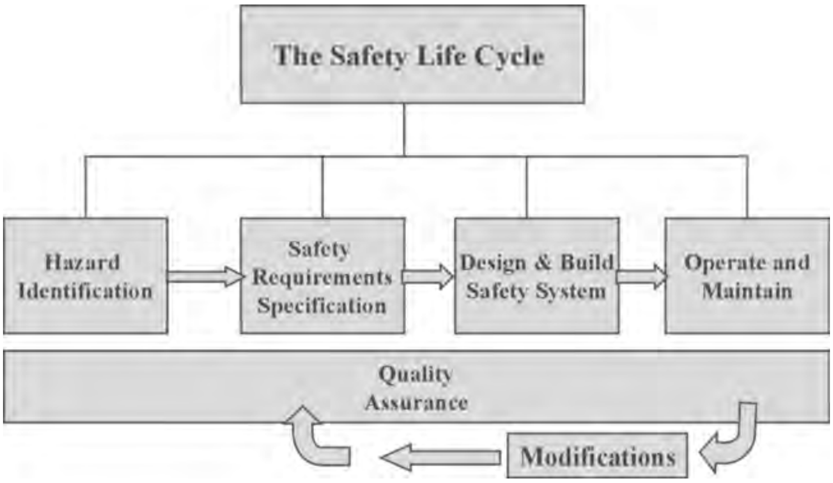


Figure 1.31
A simplified version of the SLC that identifies the main stages

- 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 build 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. Since it is not unusual to see design changes in the process equipment as the plant is being detailed it is essential that verification keeps track of the latest versions of all documents
- 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. This is supported by periodic reviews of performance to see that the SIS is still meeting its safety targets
- Change management procedures remain in force throughout the safety lifecycle and any recorded changes are recycled back through the relevant design and testing stages to see that all documents and decisions remain current for the present state of the plant

1.9.3 The safety lifecycle phases in IEC 61511

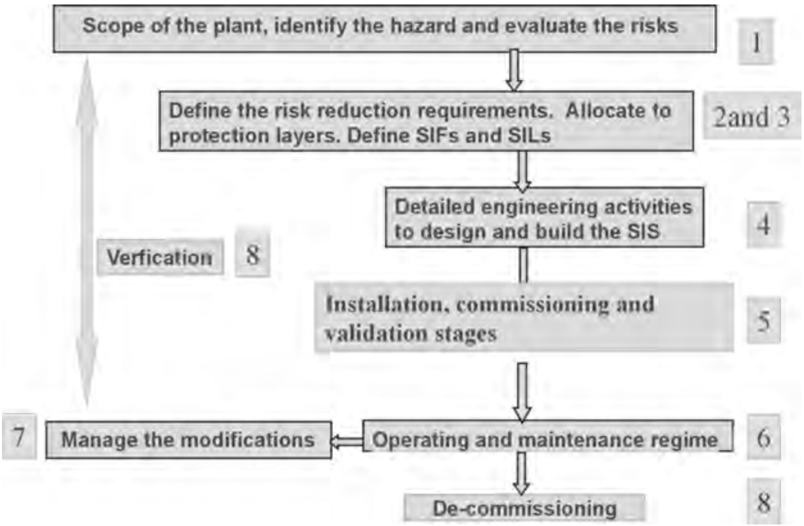

Scope of the plant, identify the hazard and evaluate the risks
1
Define the risk reduction requirements. Allocate to protection layers. Define SIFs and SILs
2and 3
Detailed engineering activities to design and build the SIS
4
Verfication
8
Installation, commissioning and validation stages
5
7
Manage the modifications
Operating and maintenance regime
6
De-commissioning
8

Figure 1.32
IEC 61511 safety lifecycle phases

At this stage is sufficient to note that the standard lays down the essential requirements for working through each stage. Figure 1.32 shows the activities of the SLC as a flowchart and the boxed numbers indicate the numbered boxes that are described in IEC 61511. The activities to be carried out for each box are defined in normative clauses of the standard.

What is meant by "normative clauses". This means that these are essential tasks for a project wishing to conform to the standard.

1.9.4 The SLC as a project management tool

From a project management viewpoint the SLC approach is attractive because the engineer can layout a complete set of inputs and deliverables that will be needed to execute the projects. An outline project plan is available from the beginning and the dependencies on other activities can clearly be seen.

IEC 61511-2 says

"The key consideration is to define in advance the safety lifecycle that is going to be used.

Experience has shown that problems are likely to occur, unless this activity is planned well in advance and agreements are reached with all persons, departments and organizations taking responsibility."

Conclusion

- Safety system projects must be treated as an integrated and formalised activity subject to typical Quality Management
- The SLC provides the tool for the job

The project planning and control task is a key part of the "Management of Functional Safety". We shall look at this subject again towards the end of this chapter when we have seen more of the scope of SIS engineering.

1.10 Setting SIL targets

Let's now take a look at the two practical aspects of SIS design that usually attract the most attention. Firstly we look at how to set the SIL target for a Safety Instrumented Function, then we shall look at some key issues involved in building the SIS to meet the target SIL.

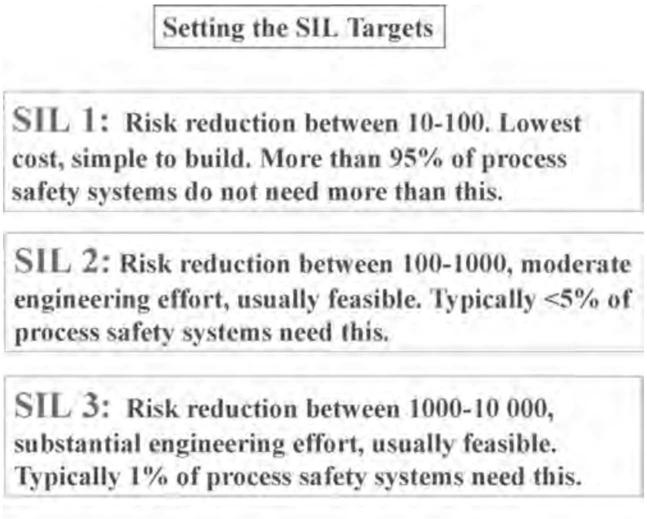
The target Safety Integrity Level (SIL) represents the broad scale of risk reduction to be expected from a SIS. We know that the higher the SIL, the more difficult it will be to achieve and hence the costs will escalate. So we will want to avoid over specifying the SIL to save cost and complexity. But if we under specify the SIL it may be that the protection reliability of the SIS will not be good enough.

It is natural in any safety system to try to err on the side of greater safety but the cost can be high. In addition there is the possibility that the design is not as safe as may be claimed because the reliability analysis is not accurate. Perhaps one will compensate for the other!

In summary:

- Problem: How to determine the amount of risk reduction we want from each safety function?
- It's too easy to just say" We want the best" It pays to look at the choices and the implications.
- SIL 1, 2 or 3 are available, SIL 4 is not normally considered practicable for a process application

The next figure summarizes the choice.



Setting the SIL Targets

SIL 1: Risk reduction between 10-100. Lowest cost, simple to build. More than 95% of process safety systems do not need more than this.

SIL 2: Risk reduction between 100-1000, moderate engineering effort, usually feasible. Typically <5% of process safety systems need this.

SIL 3: Risk reduction between 1000-10 000, substantial engineering effort, usually feasible. Typically 1% of process safety systems need this.

Figure 1.33
Guide to SIL targets

SIL 4 systems provide risk reduction between 10 000-100 000. These are very difficult to engineer and are not justified for the majority of process applications, alternatives are usually found by using multiple independent layers of protection.

However SIL 4 is used in high value machinery related processes such as gas pipeline compressor stations. SIL-4 hardware solutions must backed by SIL 4 quality assurance and management systems.

Clearly there is going to be a cost penalty to implement high SIL solutions and as we have seen this must be considered against the desired risk reduction and by using the ALARP principle as we have seen in section 1.1.

Figure 1.34. Provides a rough estimate of the relative costs for achieving different SILs in a typical process SIS application. This chart allows for the possibility that the usually expensive logic solver section performs several functions and hence its cost can be shared between the functions.

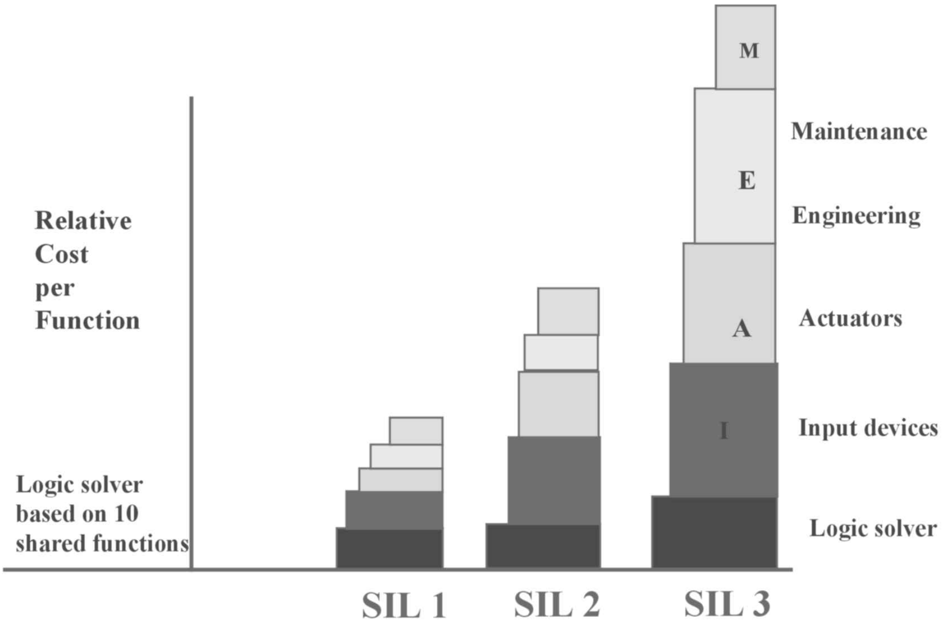


Figure 1.34
Installed cost versus SIL per function

This chart is drawn on the basis that as the SIL increases so does the need for redundancy in the field devices. The engineering effort also rises steeply due to greater care and attention to detail needed to satisfy SIL 2 or SIL 3 applications.

1.10.1 IEC 61511 part 3 guidance on SIL determination

Part 3 of IEC 61511 describes the issues involved in deciding on risk reduction targets. We have already been through this when we looked at risk management. If you feel the need to establish company policies on risk targets it’s a good idea to read the general guidance in clause 3 of part 3.

Figure 1.35, which is based on Figure 3 in part 3, captures the essential points;

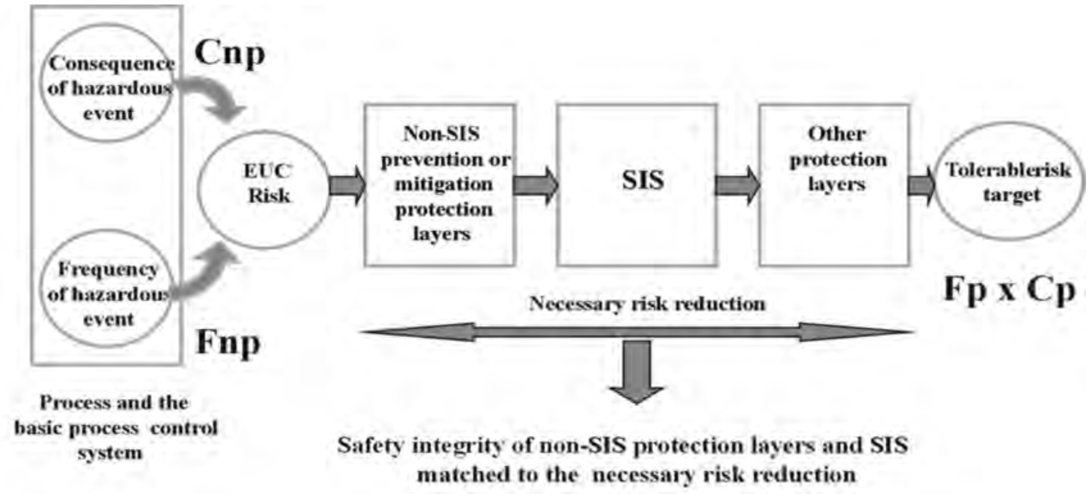

Consequence of hazardous event
Cnp
Frequency of hazardous event
Fnp
EUC Risk
Non-SIS prevention or mitigation protection layers
SIS
Other protection layers
Tolerablerisk target
Fp x Cp
Necessary risk reduction
Process and the basic process control system
Safety integrity of non-SIS protection layers and SIS matched to the necessary risk reduction

Figure 1.35
Risk reduction and safety integrity concepts from IEC 61511

The figure shows how successive layers of protection reduce the unprotected risk. The portion of risk reduction we allocate to the SIS depends on how much we are prepared to allocate to the other risk reduction layers if any are available to us.

So typically for an overpressure protection we may have a relief valve and an SIS tripping a feed valve to give us the protection we need. What is interesting here is that gives us a chance to balance the cost of mechanical protection schemes against the cost of instrumented functional safety schemes. Figure 1.36 illustrates the point.

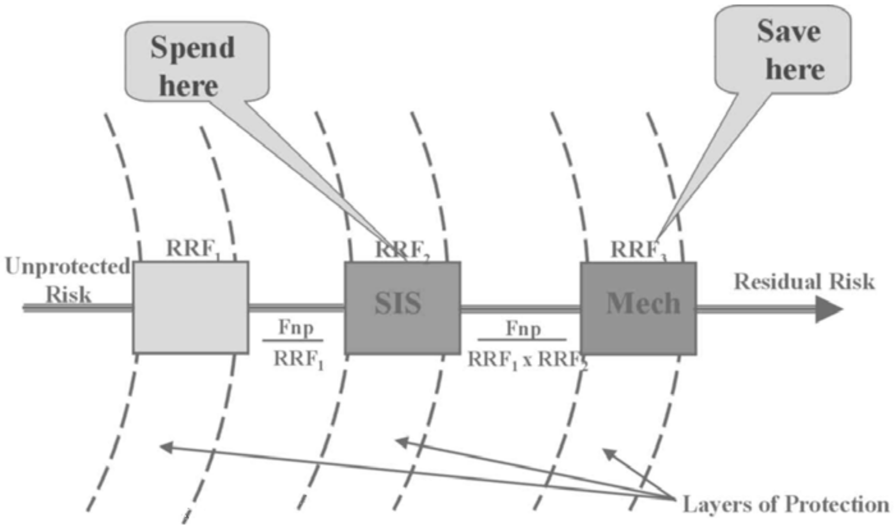


Figure 1.36
Optimising risk reduction costs

With the overall risk reduction in mind and knowledge of the possible contribution of other risk reduction layers we can proceed with SIL determination for the SIS.

1.10.2 Choices for SIL determination methods offered in IEC 61511

IEC 61511 offers us a choice of 5 methods of SIL determination, but the essentials can be seen as two main choices:

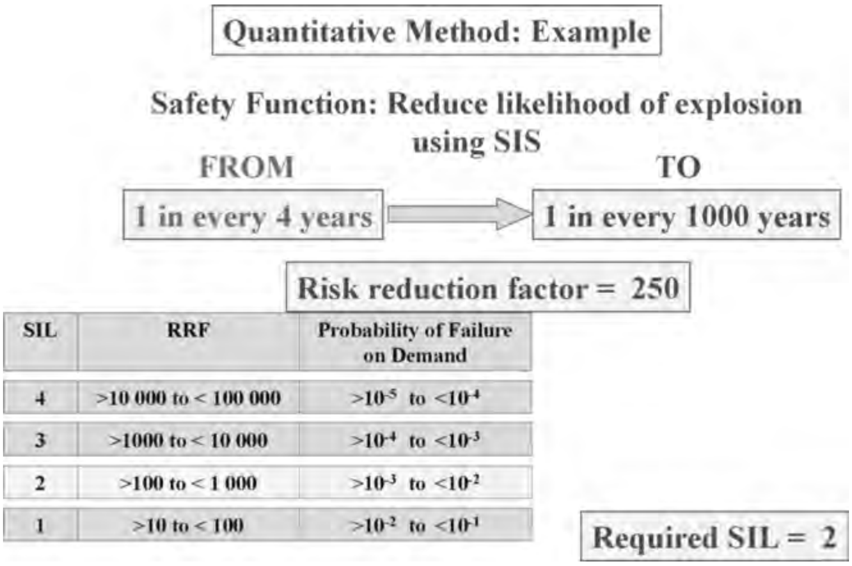
Quantitative methods: use estimated frequencies of the hazard rate. This will work if you have some confidence in the estimates of event frequencies and are prepared to declare a tolerable event frequency that you can accept.

Qualitative methods: use descriptive terms for a range of conditions. This method avoids the problem of using actual numbers to describe the event likelihood and the tolerable frequency of the accident. It disguises the tolerable risk frequency in the choice of words or in the range of values. This works well if the company can standardise on the parameter descriptions.

It is important to be clear that IEC 61511 does not define any risk values or targets; this is the responsibility of the operating company.

1.10.3 Summary example of the quantitative method

In this example the model assumes no other risk reduction device is present.



Quantitative Method: Example

Safety Function: Reduce likelihood of explosion using SIS

FROM

1 in every 4 years

TO

1 in every 1000 years

Risk reduction factor = 250

SIL	RRF	Probability of Failure on Demand
4	>10 000 to < 100 000	$>10^{-5}$ to $<10^{-4}$
3	>1000 to < 10 000	$>10^{-4}$ to $<10^{-3}$
2	>100 to < 1 000	$>10^{-3}$ to $<10^{-2}$
1	>10 to < 100	$>10^{-2}$ to $<10^{-1}$

Required SIL = 2

Figure 1.37
Outline example of quantitative method of SIL determination

If there is another risk reduction layer the method remains the same but the frequencies are changed to allow the effect of the other protection.

The quantitative method is attractive for its direct translation into SIL from estimated risk frequencies. Wherever it is possible to carry out a risk analysis that describes the risk in terms of projected frequency of an event it is fairly simple to apply the method shown above.

Note that this approach can also be aligned with Risk Matrix charts used by some companies as a reference for all risk assessment studies. The risk matrix chart is simply a graphical representation of the quantitative method.

1.10.4 Qualitative method using risk graphs

This is essentially a decision tree method aided by a by chart with the various risk parameters established as reference values.

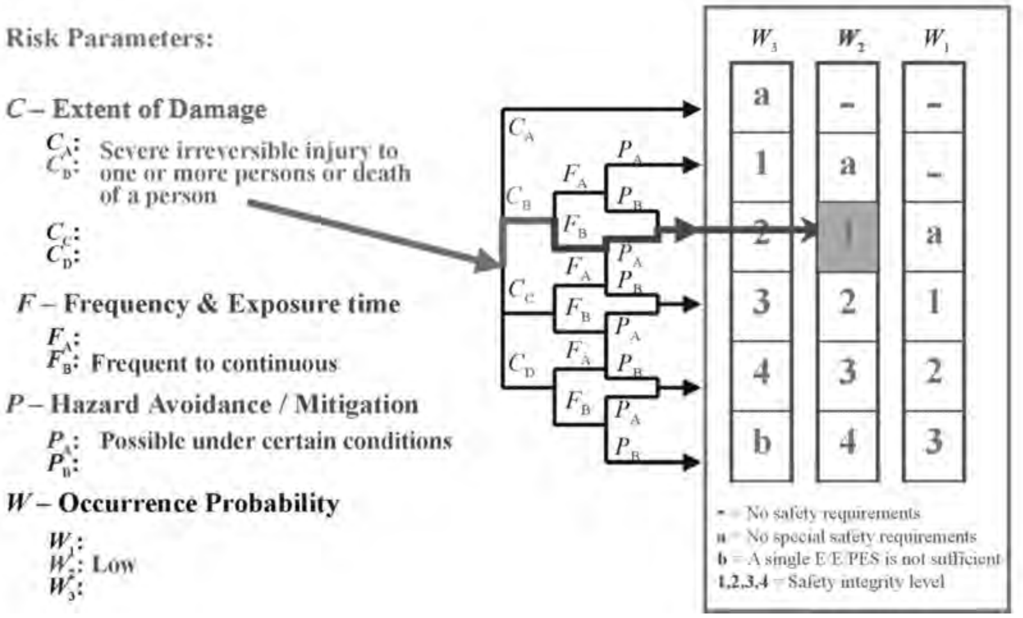
The values are described in qualitative terms to cover the essential elements of risk. I.e.:

- Consequence scale
- Exposure scale
- Possibilities of avoidance (modifying factor on likelihood)
- Likelihood (frequency)

The key points to note about this method are that the parameters must be established by agreement within a company and they must be defined consistently to all users. This is fundamentally a corporate responsibility related to the ALARP policy diagram we saw earlier and to the corporate targets for acceptable risk levels. Here we see the critical linkage back to overall risk management policies of the company.

IEC 61511 offers a particularly useful version of the risk graph called the "semi-qualitative, calibrated risk chart". This allows the user to define a range of values for event frequencies, exposure levels and scales of consequence. This approach has been widely adopted for use where large numbers of relatively simple safety functions are being evaluated.

Example:


Risk Parameters:
C – Extent of Damage
C_A:
C_B: Severe irreversible injury to one or more persons or death of a person
C_C:
C_D:
F – Frequency & Exposure time
F_A:
F_B: Frequent to continuous
P – Hazard Avoidance / Mitigation
P_A: Possible under certain conditions
P_B:
W – Occurrence Probability
W_1:
W_2: Low
W_3:
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B

W_3	W_2	W_1
a	-	-
1	a	-
2	1	a
3	2	1
4	3	2
b	4	3

- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level

Figure 1.38
Outline example of a qualitative method of SIL determination(Risk graph)

1.10.5 Which to Use?

Generally companies will review the available techniques for SIL determination and then take a policy decision on which approach to adopt. By standardising on one method the company can develop expertise, establish consistent results and build up an experience track record. Sometimes it pays to test the answers on more than one method to verify the results. It is not unusual to find a discrepancy but this can usually be used to refine the quality of the final answer.

The choice will depend on the nature of the business and its processes. This is an issue suitable for debate in the workshop sessions. Who uses what method?

1.10.6 Conclusion on SIL determination overview

The discipline needed for SIL targeting improves management of safety in the process industries because it defines the risk and the tolerable risk policy. The records of how the SIL was decided is documented and there can be no disagreement about what was decided at the time of the study.
The IEC 61511 guidelines are easy to follow and apply and there is no reason why one of the choice of 5 methods for SIL determination should not be adopted by a company. It also ago idea to try more than one method for the same problem. Sometimes a discrepancy between results will occur but this serves to identify situations where interpretation or data is critical.

The benefits of formalised SIL determination include:

- Participation by all parties improves awareness of the issues
- High potential for savings in safety costs
- Avoids over specifying SIS performance
- UK audits show many SILs previously estimated are higher than necessary
- Software packages available for SIL selection and recording. These lead to a consistent and systematic way of recording all safety functions

1.11 Meeting SIL targets

This section considers the response to having a SIL target. What do we have to do the build the SIS to meet the targets we have set? This where the basic design rules for SIS are to be applied and where the detailed requirements of IEC 61511 are applied to make sure that the design can actually meet the SIL targets.

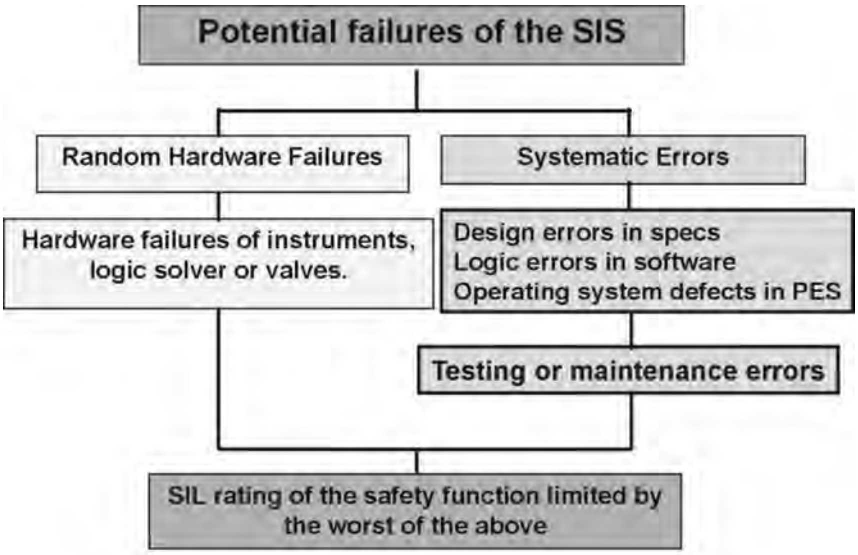
The advantage of knowing the ground rules up front in a project comes into play here because the trained instrument engineer will be able to decide what is feasible within the limits set by the standard.

The next figure considers ways in which the SIS could fail, the figure after that describes what is basically done to overcome these failures.

The figure shows how failures of the SIS are divided between random hardware failures and systematic errors. All errors that may be built into the design by mistake during the life of the SIS are regarded as systematic errors. Even testing errors are regarded as systematic when they are due to errors in procedures. All software engineering errors are also regarded as systematic since they are built in during the design stages and have no potential for random failure even though it may feel like this some times!

The safety integrity level of the SIS describes the degree of confidence in the ability of the SIS to perform its intended safety function. Hence if the design project has been badly planned and poorly managed the degree of confidence that there are no systematic errors will be very low. Equally if the instruments are of poor quality and if they are not tested regularly the potential for random failures is high and the reliability calculation will predict. A high failure rate.

The essential methods of reducing the chances of failures and thereby reaching the desired SIL are shown in the next figure.



Potential failures of the SIS

Random Hardware Failures

Systematic Errors

Hardware failures of instruments, logic solver or valves.

Design errors in specs
Logic errors in software
Operating system defects in PES

Testing or maintenance errors

SIL rating of the safety function limited by the worst of the above

Figure 1.39
Reasons why the SIS might fail

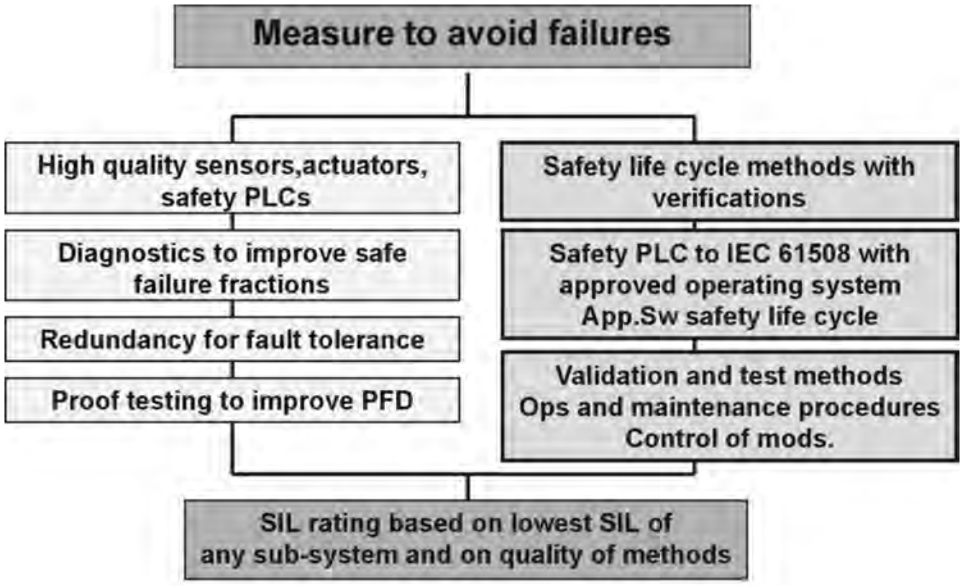

Measure to avoid failures
High quality sensors,actuators, safety PLCs
Diagnostics to improve safe failure fractions
Redundancy for fault tolerance
Proof testing to improve PFD
Safety life cycle methods with verifications
Safety PLC to IEC 61508 with approved operating system App.Sw safety life cycle
Validation and test methods Ops and maintenance procedures Control of mods.
SIL rating based on lowest SIL of any sub-system and on quality of methods

Figure 1.40
Measure in the design and selection of equipment to achieve SIL target

Dealing with random hardware failures:

- As seen in the diagram random failures are first minimized by selection of instruments and installation practices that are well proven and have characteristics that generally favour failure into a safe and detected condition.
- Diagnostics are techniques of automatic testing that help to detect faults that are not otherwise revealed. Diagnostic tests can be arranged to force the instrument into a safe state thereby reducing the chances of hidden fault.
- Redundancy is used to provide the ability to perform the safety function even in the presence of an existing dangerous fault. Basically if one channel fails the other will do the job.
- Proof testing exercises the complete safety function or its sub-systems to prove that it is capable of doing its job. This reduces the average probability that the system will be in a failed condition when the demand to operate comes along.

Figure 1.41 show the combined effect of periodic proof testing and the application of diagnostics to an instrument subsystem. The problem with increasing the frequency of proof testing is that it can be expensive on plant production losses and maintenance labour; It also carries the risk of errors or unwanted spurious trips of the plant. There is therefore an incentive to replace manual proof testing with automatic diagnostics wherever possible. Notice how this example based on a typical instrument failure rate is able to qualify for SIL 2 rating with proof test interval greater than 2 years thanks to the diagnostics.

IEC 61511 supports the use of diagnostics and these can often provide an alternative to redundancy in the structures of the SIS. The intelligence available in microprocessor based instruments and logic solvers is being exploited by manufacturers to provide high levels of diagnostics. The result is that in some critical applications the use of redundant devices can be avoided and testing intervals can be extended. These offer potentially large savings for the end user.

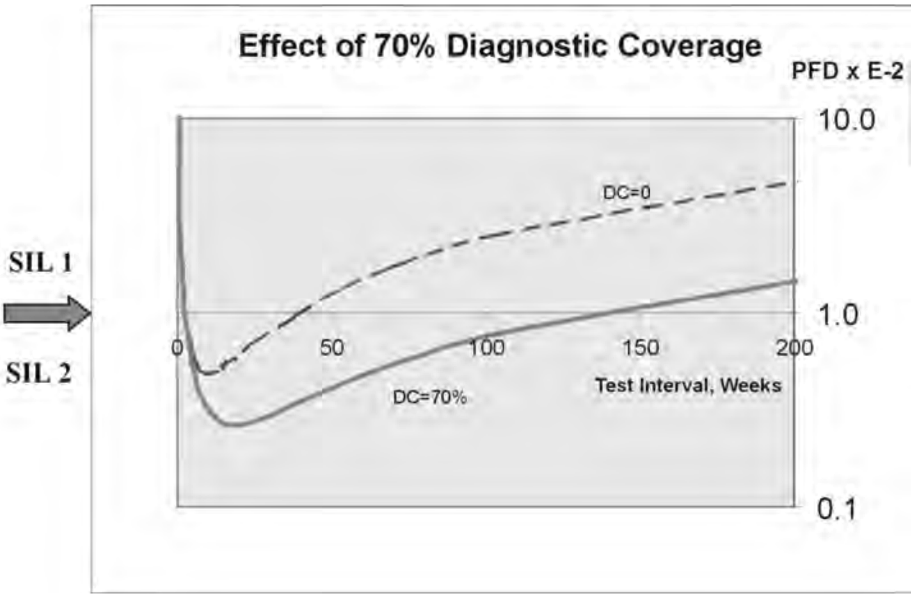


Figure 1.41
Proof testing and diagnostic coverage used to reduce average PFD

Dealing with systematic errors

We have already noted that the safety life cycle and its formal procedures provides one means of reducing the chances of systematic errors. Software errors are minimized by the application of quality assurance methods in software engineering. These are applied to the operating systems through the methods described in IEC 61508 part 3. Certified safety PLC systems are supplied with operating systems and programming packages that have been audited by independent test houses to have been built to methods in accordance with IEC 61508.

Application software is in the hands of the project team and the end user. This where IEC 61511 comes in because it provides detailed software life cycle procedures for application software.

Validation, also known as pre-start up acceptance testing is done at the point where the plant is ready to start using the SIS. This is the final p[roving test that should reduce the chances of systematic errors.

Finally the continuing operating and maintenance practices must be correctly defined and executed for the quality of the SIS to be maintained. The procedures for control of modifications must be secure and effectively deployed.

All of these measures contribute to reducing the chances of errors but none of them can be fully effective unless the overall "Management of Functional Safety" is carried out consistently and effectively.

1.11.1 IEC 61511 rules and guidance: Hardware

Here is very cryptic summary of the main requirements for SIS design set out in the standard. This is just a summary of the high impact items:

- Ensure functional independence from basic controls.
- Any safety functions performed in the BPCS cannot be claimed to have a RRF greater 10. This is logical since if more than 10 is claimed the BPCS would qualify as an SIS and would be subject to IEC 61508 requirements.
- SIL 2 systems may require redundant instrument structures for fault tolerance. SIL 3 systems usually require redundant structures.
- Instruments must be qualified for use in SIS duties. They must either conform to IEC 61508 or if you prove that they have a good history of reliability on plants they may be qualified through “prior use”.
- Instruments that are programmable such as a smart transmitter can be used in the SIS provided they have limitations placed on their scope of configuration and are password protected. They must still be qualified by the methods above.
- Standard industrial PLCs are not acceptable unless they are “safety configured” through the use of extra diagnostic devices to detect dangerous hidden failures. Even then there are severe conditions for the software to be acceptable. This normally means that for most projects only specially built safety certified logic solvers can be used in practice. Some provision has been made for concessions for SIL 1 applications.
- All interfaces to SIS subsystems must have secure features to prevent corruption of the SIS.
- Reliability calculations must provide to justify the SIL and define the maximum proof test intervals.
- Proof testing is to be carried to check for dangerous undetected faults.

1.11.2 IEC 61511 rules and guidance: Software

The software design and implementation section provides guidance on the complete life cycle of activities that should be performed to ensure quality control in preparation and testing of the application software that is to be used in the logic solver. This forms the foundation for a complete software project.

It essential for the purposes of satisfying the SIL target that the software engineering project is conducted in accordance with the rules given in this section. The objective of the software safety life cycle is to minimize the possibilities of systematic errors in the design, programming and testing of the application program.

All of the programming must be done with the aid of certified software tools. The logic solver operating system must be according the requirements of IEC 61508. In summary:

- Use a safety approved operating system (to IEC 61508 part 3).
- Use safety approved application package matched to PLC.
- Follow QA procedures for application software.
- Perform testing of all stages of the software development from function block modules up to full software integration.

- Complete the application project by software/hardware integration and a factory acceptance test.

1.12 Safety reliability versus availability for production

So far we have been looking at what it takes to satisfy the SIL targets. However the fact of having instruments that always fail-safe when they detect something wrong may not suit the production objectives of the business.

What we are looking for 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. For example:

- A short cycle time batch process will not be drastically affected by say 2 spurious or nuisance trips per year
- A glass furnace with a refractory lining may need substantial re-lining after a shutdown and this will only be contemplated once every year or less
- A boiler trip may bring down a large integrated petrochemical process

In the latter two cases, the last thing we want is for the safety system to be blamed for an unnecessary trip! So the design objectives will be to have the flexibility to build in protection against spurious trips when they are needed but to always be able to meet SIL targets for safety reliability.

The ability to adjust the level of safety reliability (i.e. the SIL) in combination with the degree of protection against spurious trips is provided by the application of redundant structures. Figure 1.42 illustrates the typical 2oo3 arrangement for achieving good safety performance whilst having a low risk of spurious trips. In the diagram the plant will trip if 2 out of 3 sensors detect a trip condition. If one of the sensors fails to tripped state whilst the other two remain normal the plant will not trip but the discrepancy will alert the operators to the need for repairs. Provided these are done in reasonable time the plant will have adequate protection through the remaining 2 sensors.

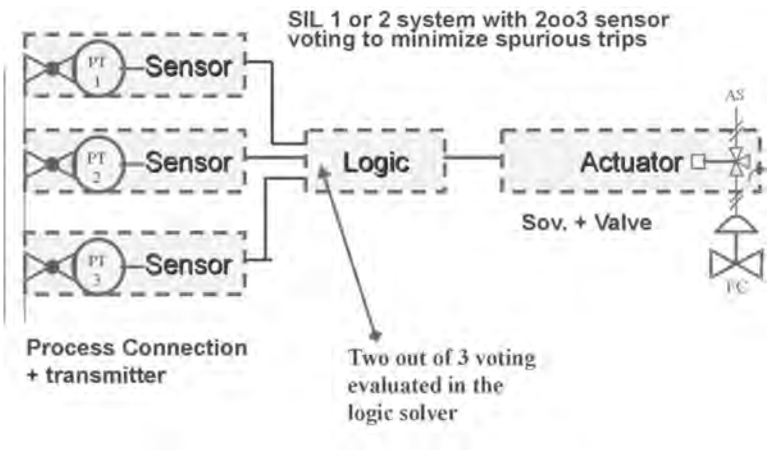


Figure 1.42
Example of 2oo3 voting in an SIS function

Alternative configurations of redundant instruments can be selected to obtain the desired characteristics. The performance is evaluated through reliability modeling. To summarize the relative merits of different configurations we have generated the chart seen in figure 1.43.

PFD avg.= avg. probability of failure on demand based on
$\lambda d = 0.1/yr$, T = 0.5 yr, ß =10%, MTTR = 24 hrs
ST = Spurious trip rate based on 0.3/yr

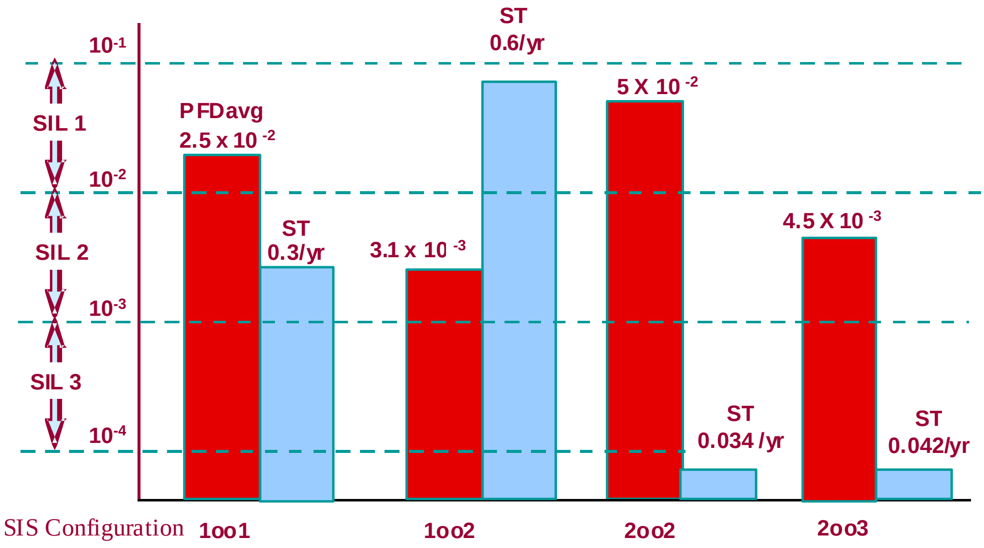


Figure 1.43
Comparative SILS and spurious trip rates for commonly used architectures

Using figure 1.43 it's easy to see that some arrangements such as 1oo2 architecture will deliver good safety availability as measured by the low probability of failure on demand (PFD_{avg}) whilst suffering relatively poor availability in terms of spurious trips. A 2oo3 architecture will deliver much improved performance for spurious trips but a slightly reduced performance for safety. It's essential therefore to have a good understanding of the concepts of redundancy and what is known as fault tolerant architectures.

Conclusions on SIL targets

We have taken a brief look at some key issues that are raised by the need to engineer an SIS to a given SIL. It should be clear there exists a defined set of requirements and provided we are familiar with them it is possible to proceed with confidence in designing, installing and using an SIS that can qualify to the desired SIL rating.

It should also be clear that it pays to get the initial SIL target right as the engineering constraints and costs increase with the SIL. The advantage using of IEC 61511 is that it provides flexibility in the way the SIS can be configured to meet its target and it encourages the use of technologies such as diagnostics to provide the most cost efficient solutions.

For those SIS installations that have not previously been engineered to a recognized SIS standard it is possible that some aspects of the systems may not comply with the present standard sets by IEC 61511. In most areas except the use of programmable systems the new standard does not impose any requirements that are radically different from practices that have been used for many years.

When it comes to programmable systems, and in particular the use of PLCs there is a definite risk that some existing installations will not match up to the IEC standards. We look briefly at this in the next section.

1.13 Introduction to safety PLCs

Safety PLCs have become the dominant form of logic solver stage 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 cycle of the application logic. Effectively the PLC detects its own faults and switches itself into a safe condition before the process has time to get 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 and smaller cheaper units are now available. IEC 61511 also makes provision for “safety configured industrial PLCs” but it is not clear yet how much this will help. In some plants it has been common practice to make use of a standard industrial grade PLC for some trip system tasks. This is unlikely to be compliant with IEC 61511 due to the typical problems shown next.

1.13.1 Why is a standard PLC not acceptable for an SIS?

Standard PLCs initially appear to be attractive for safety system duties for many reasons such as those listed here:

- Low cost
- Scalable product ranges
- Familiarity with products
- Ease of use
- Flexibility through programmable logic
- Good programming tools available
- Good communications

The PLC fits in easily to the SIS model as shown in the next figure.

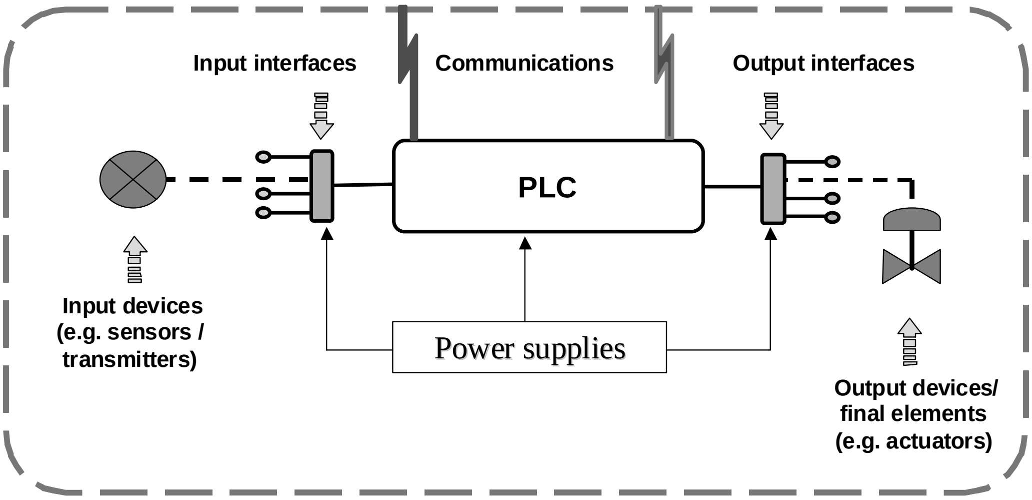

Input interfaces
Communications
Output interfaces
PLC
Input devices (e.g. sensors / transmitters)
Power supplies
Output devices/ final elements (e.g. actuators)

Figure 1.44
General arrangement of a programmable system in a safety instrumented system

But there are significant problems:

- Standard PLCs were not designed for safety applications
- Limited fail safe characteristics
- High risk of covert failures (undetected dangerous failure modes) through lack of diagnostics
- Reliability of software (also stability of versions)
- Flexibility without security
- Unprotected Communications
- Limited redundancy

The IEC standards require that programmable system have information on measures and techniques used in the design to prevent systematic faults being introduced in hardware and software (including the PLC system software). The requirements are likely to be in excess of those available in standard industrial PLCs.

Industrial PLCs are not generally required to have high levels of protection against random hardware faults because they depend on basic reliability to be sufficient for the industrial control user. The problem with a PLC in safety is that the hardware is not exercised frequently and hence failed output states or stuck program loops will not be revealed as easily as they are when a machine stops or a continuous control loop goes wrong.

If the designer chooses to add extra diagnostics to the PLC to detect dangerous failures this will certainly help. Here is a simple example in figure 1.45

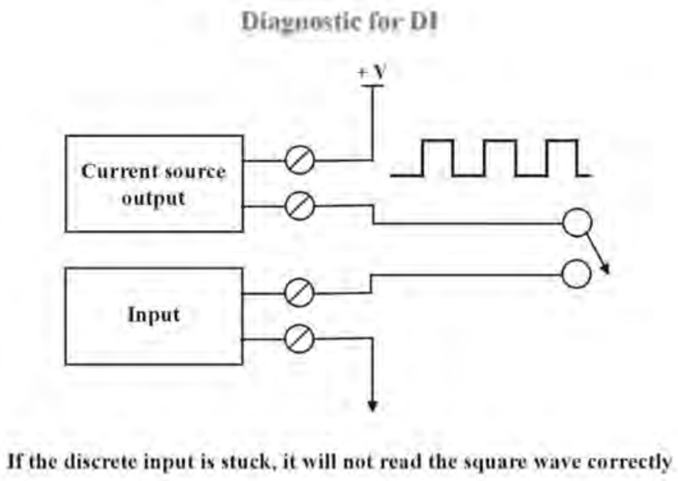

Diagnostic for DI
+ V
Current source output
Input
If the discrete input is stuck, it will not read the square wave correctly

Figure 1.45
Example of external diagnostics to test the input to a PLC

However the designer will have to provide adequate coverage for many types of possible dangerous failures and this effectively what a manufacturer does when he builds a safety PLC. In fact IEC 61511 makes provision for us to use a “safety configured PLC” in SIL 1 and SIL 2 applications. There are stringent requirements however and in addition the standard requires that we meet the conditions for “prior use” just as we have to with an instrument.

Generally these requirements are beyond the scope of the average PLC user but it may be that conversion of some PLCs can be achieved at an economic cost where a large population exists.

One of the most widely used configurations is shown in the next figure.

1.13.2 1002D safety PLC

In this safety PLC the entire logic solver stage from input to output is duplicated and if one unit fails its diagnostic contact will open the output channel and remove that unit from service. The SIS function then continues to be performed by the remaining channel whilst the faulty unit is being repaired.

The notation 1oo2D applies because the system will still perform in the presence of 1 fault amongst 2 units. The parallel connection of the two units substantially improves the availability. Note that diagnostic performance is further improved by cross-linking between the CPU of one channel and the diagnostics of the second channel.

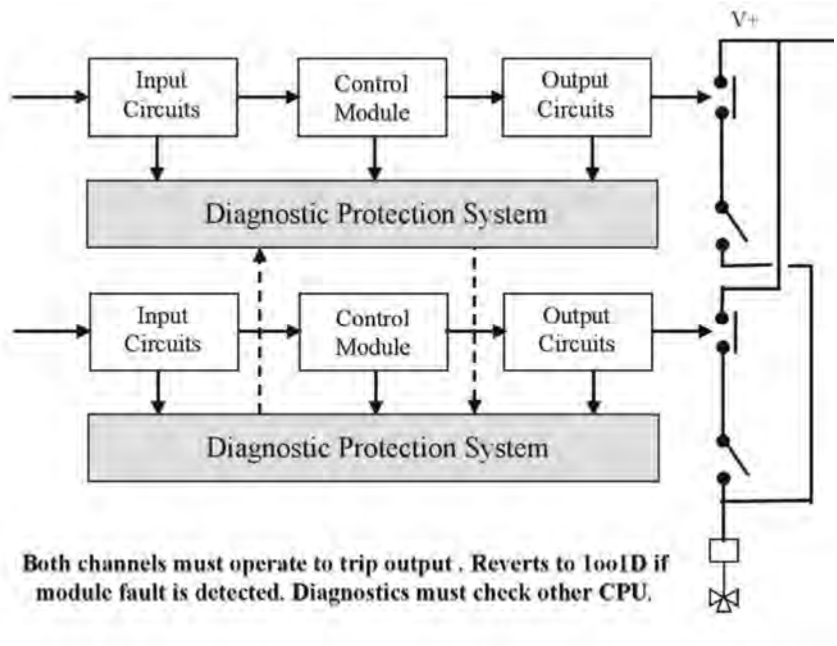

V+
Input Circuits
Control Module
Output Circuits
Diagnostic Protection System
Input Circuits
Control Module
Output Circuits
Diagnostic Protection System
Both channels must operate to trip output . Reverts to 1oo1D if module fault is detected. Diagnostics must check other CPU.

Figure 1.46
Dual redundant channel safety PLC architecture with diagnostics

1.13.3 Conclusions on PLCs

A PLC logic solver forms the heart of an SIS installation. It will provide the central point for the engineering of all functions required from SIS and all critical trip functions will be kept secure through the program protection features. It will require some investment in time and training for the plant technicians.

It is important to proceed carefully with the selection of the logic solver product for a new project because this is going to be a long life item. It may require a considerable amount of expense over the years to ensure the product support and its software are available to the plant. However most users for safety PLCs seem to find that the integrity the whole trip system is improved when compared with relay based trip systems by virtue of having all the logic functions in controlled software format.

When selecting a logic solver always look for the complete hardware and software package to be from the same manufacturer and always ensure that is available with certification for at least the highest SIL that you intend to use in your applications. The certification should always be to IEC 61508 and it should cover the hardware, the operating system, the programming tools and the safety manual that must be supplied with the product.

1.14 The cost of ownership

Now that we have seen something of the project activities and the 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:

- Essential for safety and no alternative methods exist:
- Lowest cost option for safety
- Prevention of environmental harm or violation of emission limits
- Protection 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. To help with this we need to have an approximate cost model that can be used as a basis for establishing to total costs involved in SIS. With this in mind we are also able to show how the case for performance improvement may be justified by further reducing operating costs.

1.14.1 Life cycle cost models

Life cycle costing presents the total cost of an installation in terms that a business man will understand and appreciate. The true cost of ownership of any plant item is measured by this method as an equivalent lump sum price in the present day money.

The next figure is tree structure diagram showing typical components of life cycle cost for a safety instrumented system. A more comprehensive list would have to show details of all project related costs. For annual costs the model has to include items such as the service agreement and software licensing costs for the logic solver. A model with suitable headings soon prompts the user to fill in details of related cost items. This is not difficult to set up if you know your particular operation quite well. Our example here is very minimal.

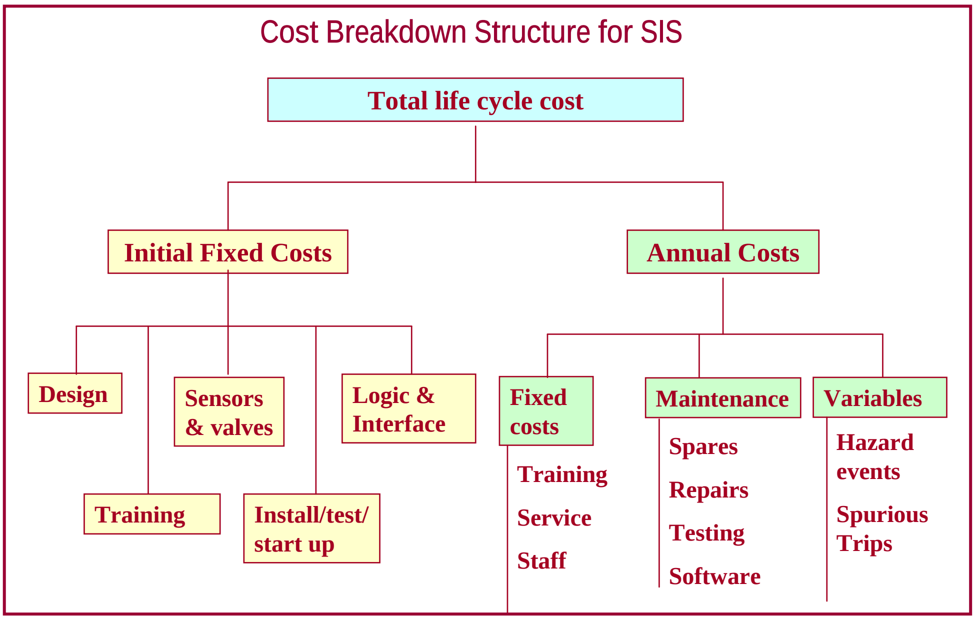


Figure 1.47
Cost breakdown structure for SIS

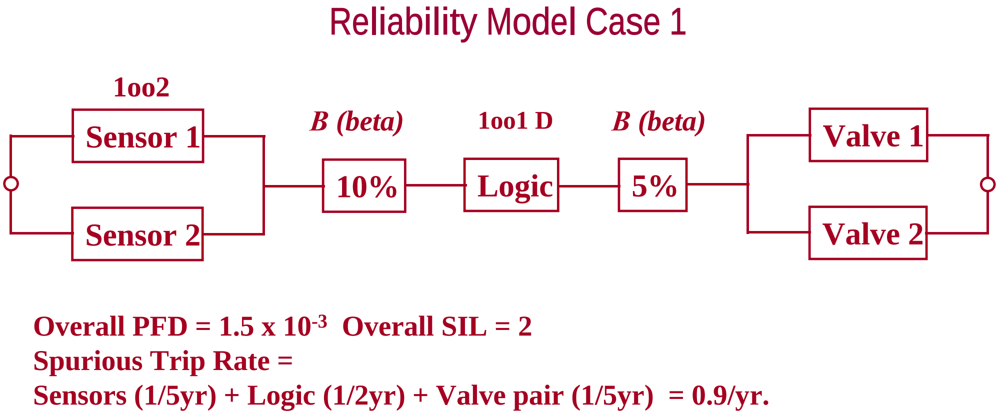
Use the structure diagram to develop and expand the headings for costs. The difficult part is to put real numbers in the boxes! In particular it may be contentious to try and include an annualized figure for the cost of hazardous events. This is not so difficult to justify in the case of asset loss applications. For example the cost of failure of a turbo-compressor protection system can be measured as the price of a new rotor plus the cost of lost production.

The next step will be to set up a costing spreadsheet for the agreed version of life cycle costs so that various scenarios can be tested for cost. Examples are shown in figures 1.48 and 1.49. The method of representing the accumulated value of annual maintenance costs is based on a simple addition over 10 years. An assumed life for the SIS has to be used but more sophisticated cash flow models would probably be available in most companies.

1.14.2 Costing example

Here is an example of a simple exercise in evaluating the cost of alternative design options for a safety instrumented function. We have to imagine there is a process plant with say 8 separate safety functions all served by a common PES logic solver with an interface to the plant BPCS (Basic Process Control System).

The next figure shows a reliability block diagram for a single loop function in the plant that shuts down the operation if the conditions become hazardous. The reliability data used is arbitrary but may be realistic for installed performance as opposed to manufacturer's product data.


Reliability Model Case 1

Overall PFD = 1.5 x 10^{-3} Overall SIL = 2
Spurious Trip Rate =
Sensors (1/5yr) + Logic (1/2yr) + Valve pair (1/5yr) = 0.9/yr.

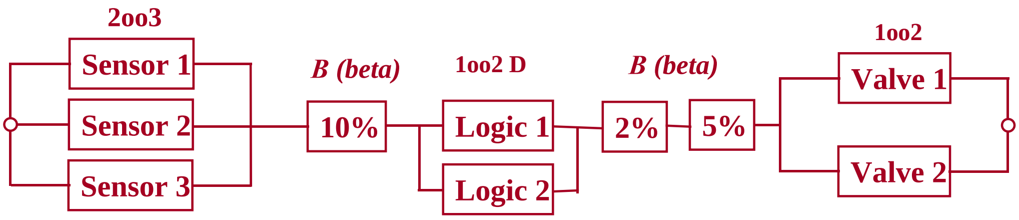
Figure 1.48
Reliability model: case 1

Case 1 employs a dual 1oo2 sensor pair as inputs to a single channel logic solver with diagnostics, 1oo1 D. A dual redundant pair of valves are used to shutoff feed to the process.

The Safety Requirements Specification for this function calls for SIL 2 integrity to protect against the hazardous condition that could arise as much as once per year. (i.e. Demand rate D = 1/yr).

Reliability analysis results as shown in figure 1.48 indicate that the SIL 2 target can be met with the assistance of proof testing at 2 times per year. The nuisance trip rate is predicted at 0.9 times per year based on the sum of the spurious trip rates found for the 3 elements of the loop. Note that a single channel logic solver with diagnostics can often satisfy SIL 2 is but may experience a relatively high tripping rate due to the absence of a back up unit.

Reliability Model Case 2



Overall PFD = 1.5 x 10^{-3} Overall SIL = 2
Spurious Trip Rate =
Sensors (1/100 yr) + Logic (1/100 yr) + Valve pair (1/5 yr) = 0.22/yr.

Figure 1.49
Reliability model: case 2

The issue here is: Can we find a viable way to reduce the production losses due to spurious tripping without compromising safety? We need to perform a benefits analysis on any proposed upgrade to get a feel for the options and ultimately to be able to justify the upgrade.

We show here one possible upgrade scenario and call it case 2. The sensor pair have been upgraded to 2oo3 voting to reduce their spurious trip rate. The logic solver is to be upgraded to 1oo2D for the same reason, but keep in mind this will benefit the spurious trip rate for all 8 safety functions. In this example the plant costing models share the basic PES logic solver costs equally across each function but the cost of upgrading to 1oo2D will be attributed to the single function. In practice the full cost benefit analysis would have to generate a cost sheet for each function.

1.14.3 PFD comparisons

- Case 1 meets SIL 2 with proof testing 2 times per year. PFDavg is .0015 and hazard rate is (D x PFDavg) = 1x.0015/yr = 0 .0015/yr
- Case 2 still meets SIL 2 with proof testing 2 times per year. PFDavg is .0018 and the hazard rate remains approximately the same.

Note that we can’t save costs on testing because the sensor group PFD is not changed very much by going to 2oo3 voting.

1.14.4 Nuisance trip comparisons

Case 1 nuisance trip rate = 0.9 per year. Production loss = £ 30 000 per trip event x 0.9 = £27 000 per yearCase 2 nuisance trip rate = 0.22 per year. Production loss = £ 30 000 per trip event x 0.22 = £6 600 per year

- Additional costs for sensors and PES upgrade costs have been attributed to this function only. Benefits to other functions excluded

Case 2 delivers a substantially improved nuisance trip rate mainly through benefits gained by reducing the spurious trip figures for sensors and PES. The redundant valve pair are now the main contributors to spurious trips but moving these to a 2oo3 design presents an increase in complexity that may outweigh the benefits. Further savings may be possible by reducing the frequency of proof testing on the sensors and logic solvers.

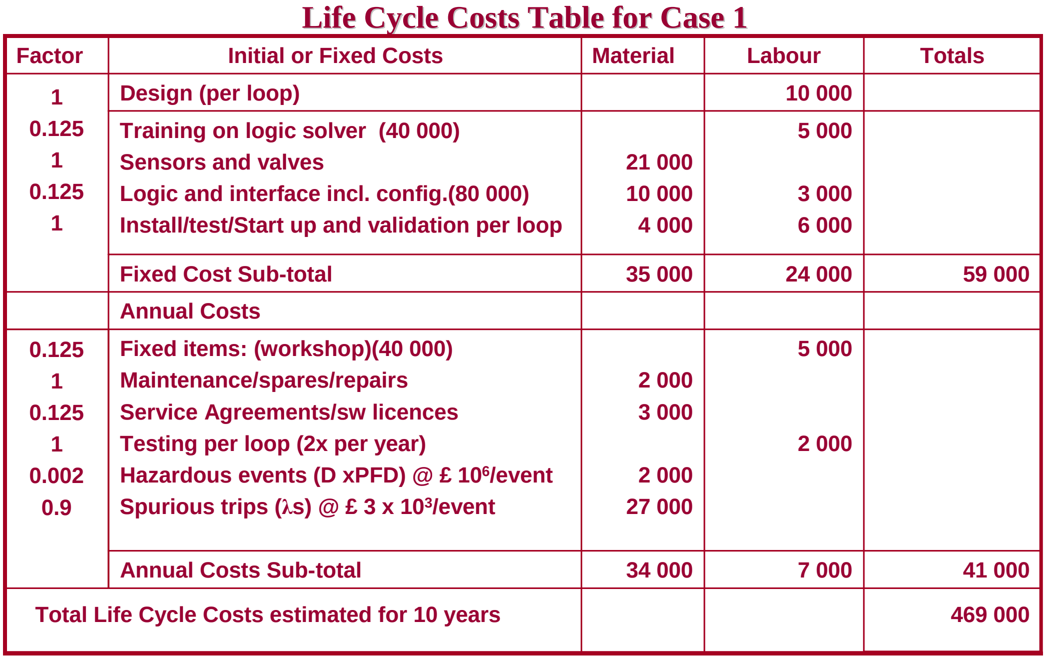
1.14.5 Cost comparisons

Now we fill in some cost data on the tables to see how the two cases compare. Again the data is arbitrary and does not imply any standard value of costs. Costs are in UK pounds.

Case 1, as shown in figure 1.50, indicates an initial investment of £ 59 000 and a yearly operating cost of £ 41 000 including for the possible cost of spurious trips at rate of .9/yr.

Case 2, as shown in figure 1.51, indicates an initial investment of £ 86 000 and a yearly operating cost of 23 600 including for the possible cost of spurious trips at a rate of .22/yr. The saving in annual cost of spurious trips offsets the increased capital cost (£ 27 000) of the upgraded design by saving £15 400 per year in production losses.

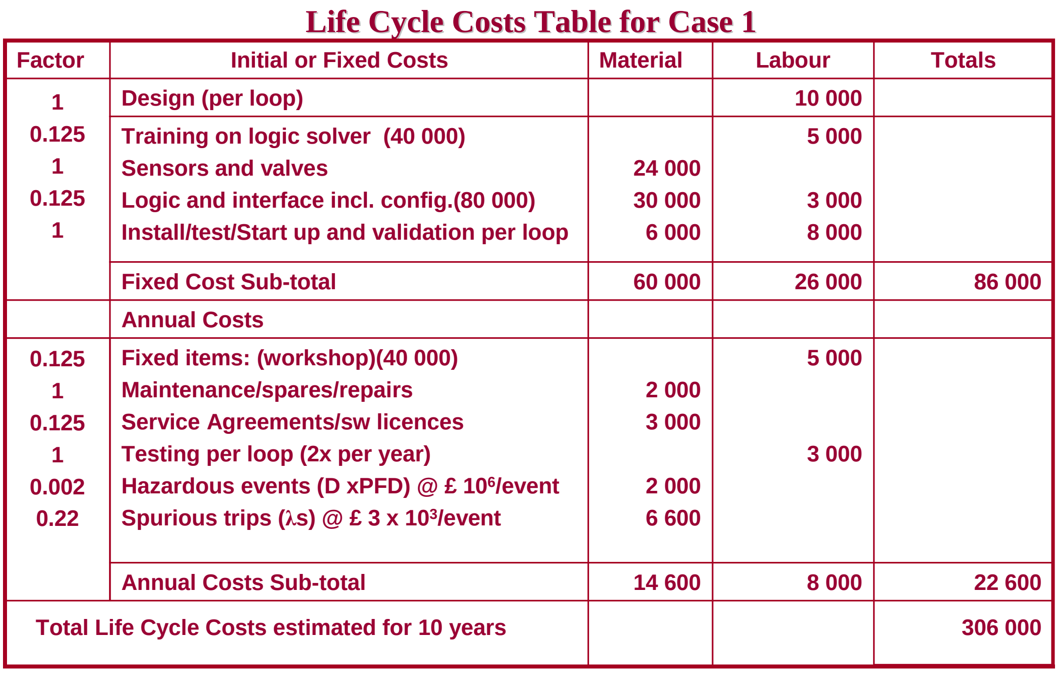
This suggests a payback period of less than 2 years for the additional investment in improved SIS equipment. Savings on life cycle costs aggregated over 10 or 20 years will be substantial but would be evaluated using cost models taking into account the present day value of the initial investment for the improved SIS.



Life Cycle Costs Table for Case 1

Factor	Initial or Fixed Costs	Material	Labour	Totals
1	Design (per loop)		10 000	
0.125	Training on logic solver (40 000)		5 000	
1	Sensors and valves	21 000		
0.125	Logic and interface incl. config.(80 000)	10 000	3 000	
1	Install/test/Start up and validation per loop	4 000	6 000	
	Fixed Cost Sub-total	35 000	24 000	59 000
	Annual Costs			
0.125	Fixed items: (workshop)(40 000)		5 000	
1	Maintenance/spares/repairs	2 000		
0.125	Service Agreements/sw licences	3 000		
1	Testing per loop (2x per year)		2 000	
0.002	Hazardous events (D xPFD) @ £ 10^6/event	2 000		
0.9	Spurious trips (λs) @ £ 3 x 10^3/event	27 000		
	Annual Costs Sub-total	34 000	7 000	41 000
Total Life Cycle Costs estimated for 10 years				469 000

Figure 1.50
Investment and operating costs table for case 1



Life Cycle Costs Table for Case 1

Factor	Initial or Fixed Costs	Material	Labour	Totals
1	Design (per loop)		10 000	
0.125	Training on logic solver (40 000)		5 000	
1	Sensors and valves	24 000		
0.125	Logic and interface incl. config.(80 000)	30 000	3 000	
1	Install/test/Start up and validation per loop	6 000	8 000	
	Fixed Cost Sub-total	60 000	26 000	86 000
	Annual Costs			
0.125	Fixed items: (workshop)(40 000)		5 000	
1	Maintenance/spares/repairs	2 000		
0.125	Service Agreements/sw licences	3 000		
1	Testing per loop (2x per year)		3 000	
0.002	Hazardous events (D xPFD) @ £ 10^6/event	2 000		
0.22	Spurious trips (λs) @ £ 3 x 10^3/event	6 600		
	Annual Costs Sub-total	14 600	8 000	22 600
Total Life Cycle Costs estimated for 10 years				306 000

Figure 1.51
Investment and operating costs table for case 2

In practice we would have to extend this study to all safety functions sharing the logic solver. It may be that several of the other functions do not have much impact on spurious trips and in this case the loading factors shown in the table would have to be weighted for the critical items.

Clearly this is a simplified case but it indicates the approach to justification. A well verified spreadsheet model will of course enable many alternative designs to be evaluated. If the reliability analysis models can be supported by software based calculation sheet or a package the procedure can be made reasonably efficient.

The benefits of life cycle cost models can be seen in the improved perceptions of what each safety function is really doing for the business. The problem of credibility remains in the area of predicting losses from a probability based model. After all, “it may never happen”.

1.14.6 Conclusion on costing

The combination of reliability modelling and life cycle cost analysis can produce very useful data for use in the decision and justification tasks. The issue of credibility has to be taken into account, particularly when the savings are claimed for items dependant on probability analysis. What is clear that many issues of design selection and operating philosophy are well supported by maintaining good cost models for the SIS.

1.15 Management of functional safety

Finally in this chapter we conclude with some notes on the issues of supporting all the work that has to be done to build a safety instrument system in conformance with IEC 61511.

1.15.1 Requirements for functional safety management

IEC 61511 has mandatory requirements for the management of functional safety. In summary the key requirements are:

- *A safety management system* must be in place at the company that ensures that where safety systems are used they are able to place or maintain the process plant in safe state. This statement seems suggests that you should not allow the safety system to be bypassed or switched off. This has often happened, particularly if the SIS is prone to spurious trips.
- *Persons responsible* for carrying out life cycle phases are to be identified and informed of responsibilities assigned to them.
- *Competency of persons:* Those involved in safety life cycle activities shall be competent to carry out the activities for which they are accountable. This clause adds details of the type of knowledge that should be considered. This may be a useful item when planning competencies for an SIS project.
- *Follow up procedures* are required ensure prompt follow up of problems or actions identified by safety life cycle activities such as hazard studies or testing.
- *Planning of safety life cycle activities* is to be carried out either in a project quality plan or in a company procedures manual.
- *Suppliers to have quality management systems;* Any supplier of products or services to the company having responsibility for one or phases of the safety life cycle is to have a quality management system.
- *SIS performance evaluation procedures* are required to evaluate the performance of the safety system against its safety requirements specification and to check the failure rates of the SIS. Evaluate actual demand rates and failure rates. This is particularly important where the tolerable risk and SIL decisions have been based on an assumed demand rate. If the actual rate is much higher the likely accident rate will be higher than intended.

More information on these requirements can be found in part 2 of IEC 61511 and substantial guidance is offered. Companies wishing to work toward conformity to IEC 61511 will need to study the notes in part 2.

Is this standard of management achievable?

All of the above requirement seem to be achievable for a project engineering organization but perhaps one of the difficulties here is that the organization being asked to perform the task may be a production company. This level of planning and competency in the subject may be higher than necessary for the rest of its work. If the end user is going to contract out the engineering phases it will still need to have a reasonably good management system in place for the operation and maintenance tasks.

Additionally there may the problem that the contracting organization may not have a good management system in place. As noted above the contractor as supplier the end user should have a quality management system in place.

1.15.2 Functional safety assessment

Functional safety assessment is to be carried out during the safety life cycle at least once and preferably at key stages of the project. The assessment work is to be done by a team of persons with at least one senior person who is not involved in the project design team.

Details of the scope of assessment are given in the standard but the key issue here is that the assessment is part of the conformity process. The problem at present is that there is a shortage of skills to carryout functional safety assessment and the conformity assessment in general. The UK has in place a training facility for assessors and some companies are able to offer assessment services. A number of UK companies have achieved conformity to IEC 61508 after a period of transition form their previously existing codes of practice.

1.15.3 Competency issues

IEC 61511 describes basic requirements for competencies of those persons involved in safety lifecycle activities. There is strong drive, particularly, in the UK to see that this is developed so that persons have the required level of skills and experience for the responsibilities they have been given. Technicians and engineers are expected the have the right amount of engineering knowledge for the tasks in hand. Part 2 of IEC 61511 provides greater detail on this subject and suggests that companies should identify the skills needed and assess the resources available. Where skills shortages are identified a programme of training and improvement is to be established.

For individual instrument engineers or process engineers, training course such as this one combined with the information in IEC 61508 and IEC 61511 will enable you to build up your knowledge of the subject and support the drive for improved skills in safety systems. Internationally there is the widely recognised qualification offered by TUV in Germany and in USA for the “Certified Functional Safety Expert”. This requires considerable study and represents a specialist level qualification. In the UK conformity assessment training course and qualification s are available through the SIRA organization.

1.15.4 Configuration management

This term refers to the need to impose formal configuration control on the SIS and its software. Again management procedures are to be defined for this. Procedures are needed to ensure that all parts of the SIS are uniquely identified. This then supports the procedure for preventing any unauthorised items from entering service. This is particularly thorny problem for maintenance departments where the replacement part may not be acceptable for the SIS even though it appears to have similar characteristics. For example: When an old analogue pressure transmitter of a defined range is replaced by a new smart transmitter the new part is probably not qualified for use in the SIS under the rules of IEC 61511.

1.15.5 Conclusions on safety management

The requirements for safety management are not exceptional but it will need a considerable effort in most companies to ensure that they are implemented. Some large UK companies have been carrying out a gradual transition to IEC 61508 over a period of years. The requirements are similar in nature to ISO 9001 quality management systems. For a plant with a few simple trip systems this seems to be overkill but each procedure in that case should be simple.

However, based on the experience of previous IDC workshops there is a considerable shortfall in this area regarding even basic compliance with the safety life cycle procedures. There are a lot of essential things that could be checked at a practical level. For example the following questions do not always get a Yes!

- Are the hazard study files easy to find and are the studies up to date with the present state of the plant?
- Is there a risk register that defines each risk and the intended measures to keep it in safe limits?
- Has each Safety Instrumented Function been explicitly identified?
- Is there any recorded linkage between each Safety Instrumented Function and the original hazard studies?
- Has the required SIL for each SIF been formally determined and recorded?
- Has each safety instrumented function and its SIL target been defined and issued as a Safety Requirements Specification (SRS) ?
- Has the SIS design been formally verified against the SRS?
- Has the expected PFDavg of the SIS been calculated to verify that the SIL target can be met?
- Do the planned proof testing intervals match the intervals used in the reliability calculations?
- Are the instruments selected for the SIS known to be suitable for safety duties in terms of IEC 61511 requirements either by design or by proven in use records?
- Does the company have a defined and working policy for management of change in the SIS designs?

1.16 Conclusion

This chapter has introduced the main concepts, procedures and standards relevant to safety instrumentation in the process industries. The principles we have seen are not new, but their application using programmable devices has potential for both higher performance and for possibilities of errors.

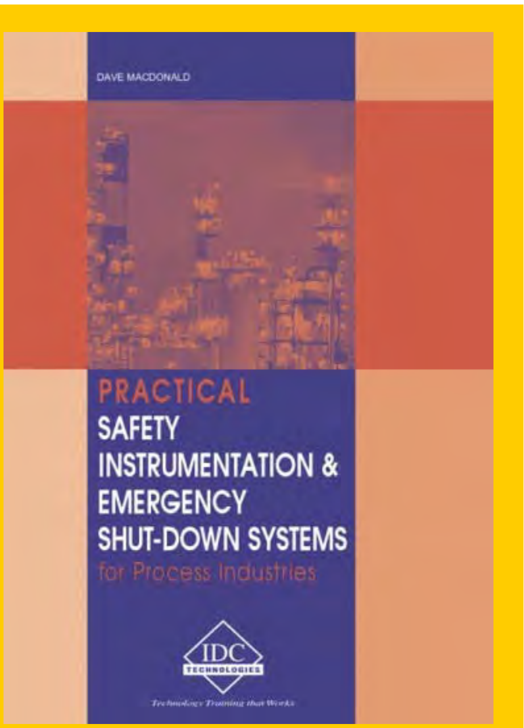
The new standards emphasise a systematic approach to all stages of the project through the use of the safety life cycle. In particular, they provide a complete plan for dealing with programmable devices and allow us to take advantage of their features wherever possible.

Underlying all safety activities is the clear need for companies to have in place a well defined and properly supported set of work procedures based on the guidelines found in IEC 61511.

IDC TECHNOLOGIES

YOU MAY ALSO BE INTERESTED IN THE FOLLOWING TITLE:

Practical Safety Instrumentation & Emergency Shutdown Systems for Process Industries



This book is available for purchase in printed form or as an eBook

For more details about this title please visit the link below:
http://idc-online.com/products/?country=%23

If you would like a quote or any further information please do not hesitate to contact us:

books@idc-online.com