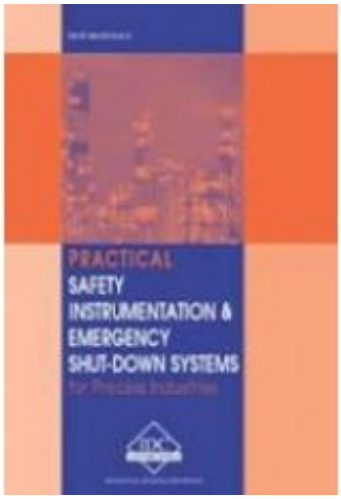
IDC Technologies - Books - 1031 Wellington Street
West Perth
WA 6005

Phone: +61 8 9321 1702 - Email: books@idc-online.com

SS-E - Practical Safety Instrumentation & Emergency Shutdown Systems for Process Industries



Price: $139.94

Ex Tax: $127.22

Short Description

For project managers and engineers involved with hazardous processes, this manual focuses on the management, planning and execution of automatic safety systems in accordance with IEC 61511, the newly released international standard for process industry safety controls.

Description

For project managers and engineers involved with hazardous processes, this manual focuses on the management, planning and execution of automatic safety systems in accordance with IEC 61511, the newly released international standard for process industry safety controls.

Table of Contents

Download Chapter List

Table of Contents

First Chapter

In the

an ave

these:

605,00
9,962 i

Genera

Source
Incider

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:

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. We are going to study this issue in chapter 4 but here is brief summary of the subject.

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”

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?

In chapter 4 you will find some notes on this subject. 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 safe