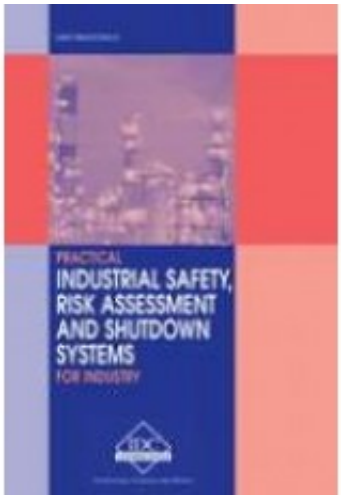
IDC Technologies - Books - 1031 Wellington Street
West Perth
WA 6005

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

SI-E - Practical Industrial Safety, Risk Assessment and Shutdown Systems for Industry



Price: $65.95

Ex Tax: $59.95

Short Description

This manual will provide you with a broad understanding of the latest safety instrumentation practices and their applications to functional safety in manufacturing and process industries. This manual is an investment - it could save your business a fortune in possible downtime and financial loss.

Description

This manual will provide you with a broad understanding of the latest safety instrumentation practices and their applications to functional safety in manufacturing and process industries. This manual is an investment - it could save your business a fortune in possible downtime and financial loss.

This manual offers you the most vital, up-to-date information and practical know-how to enable you to participate in hazard studies and specify, design, install and operate the safety and emergency shut-down systems in your plant using international safety practices.

Table of Contents

Download Chapter List

Table of Contents

First Chapter

Activity	**FAR per 10^{-8}**	**Individual risk of death per person per year × 10^{-4}**
Travel		
Air		0.02
Train	3–5	0.03
Bus	4	2
Car	50–60	2
Occupation		
Chemical industry	4	0.5
Manufacturing	8	
Shipping	8	9
Coal mining	10	2
Agriculture	10	
Boxing	20 000	
Rock climbing	4 000	1.4
Staying at home	1–4	
Living at 75 (based on simple calculation of hr/lifetime)	152	133

Table 1.1

Individual risk and fatal accident rates based on UK data

FAR can be used as basis for setting the tolerable rate of occurrence for a hazardous event. For example:

Suppose a plant has an average of 5 persons on site at all times and suppose that 1 explosion event is likely to cause 1 person to be killed. The site FAR has been set at 2.0×10^{-8}/hr. We can calculate the minimum average period between explosions that could be regarded as tolerable, as follows:

Fatality rate per year = (FAR/hr) x (hours exposed/yr)

$= (2 \times 10^{-8}) \times (5 \times 8760)$

$= 8.76 \times 10^{-4}$

Avg. years per explosion $= 1/8.76 \times 10^{-4} = 1140$ year

Note: If there are N separate sources of explosion of the same type the period for each source will be: N × 1140 years. These figures will define the target risk frequencies for determining the scale of risk reduction needed from a safety system.

1.7 Overview of safety systems engineering (SSE)

The term safety systems engineering is used to describe the systematic approach to the design and management of safety-instrumented systems.

1.7.1 Introduction

Safety systems engineering (SSE) comprises all the activities associated with the specification and design of systems to perform safety functions. SSE has become a discipline within the general field of engineering. Whenever there is a clear and obvious need for safety to be engineered into any activity it should be done properly and in a systematic manner

1.7.2 What do we mean by safety functions?

We mean any function that specifically provides safety in any situation. E.g. a seat belt in a car, an air bag, a pressure relief valve on a boiler or an instrumented shutdown system. Thus an air bag has a safety function to prevent injury in the event of collision. The safety system of an air bag comprises the sensor, the release mechanism, the inflator and the bag itself.

1.7.3 Functional safety

The term ‘functional safety’ is a concept directed at the functioning of the safety device or safety system itself. It describes the aspect of safety that is associated with the functioning of any device or system that is intended to provide safety. The best description might be this one from the following journal article:
‘*Functional Safety in the field of industrial automation*’ by Hartmut von Krosigk. Computing and Control Engineering Journal (UK IEE) Feb 2000.
‘*In order to achieve functional safety of a machine or a plant the safety related protective or control system must function correctly and, when a failure occurs, must behave in a defined manner so that the plant or machine remains in safe state or is brought into a safe state.*’

Short form: '*Functional safety is that part of the overall safety of a plant that depends on the correct functioning of its safety related systems.*' (modified from IEC 61508 part 4)
The next diagram shows how functional safety makes a contribution to overall safety.

Figure 1.5

Overall safety

The well-known standards certification authority in Germany is TUV. Their web-site answers the question '*What is functional safety?*'
Random hardware faults or systematic design errors – e.g. in software – or human mistakes shall not result in a malfunction of a safety-related unit/ system with the potential consequence of:

- Injury or death of humans or
- Hazards to the environment or
- Loss of equipment or production

Then follows an explanation of the term '*unit/system*'*;* for example:

- A simple device as a gas burner control unit
- A large distributed computer system like emergency shutdown and fire & gas systems
- A field instrument
- The complete instrumented protective equipment of a plant

So we can conclude that *functional safety* is about the correct functioning of a unit or system designed to protect people and equipment from hazards

1.8 Why be systematic?

Why be so formal? Why be systematic?
Critics might say...

- We don't need all these rules!
- Why not just use common sense?
- Whose job is it anyway?
- Make the contractor do it!

But now let’s take a look at the problem.

Figure 1.6

Causes of control system failures

Specification errors dominate the causes of accidents analyzed in the above survey.

1.8.1 UKHSE Publication

One of best advocates for a systematic approach to safety engineering is the UK Health and Safety Executive (HSE): Their publication: ‘*Out of Control*’ is a very useful little book about ‘*Why control systems go wrong and how to prevent failure*’ and it is the origin of the analysis we have just seen.

This book not only provides extracts from the analyses of accidents but also explains with great clarity the need for a systematic approach to the engineering of functional safety. It also provides a valuable outline of the safety life cycle.

1.8.2 HSE Summary

Some of the key points from the study are listed below:

Analysis of Incidents

- Majority of incidents could have been anticipated if a systematic risk-based approach had been used throughout the life of the system
- Safety principles are independent of the technology
- Situations often missed through lack of systematic approach

Design problems

- Need to verify that the specification has been met
- Over dependence on single channel of safety
- Failure to verify software
- Poor consideration of human factors

Operational problems

- Training of staff
- Safety analysis
- Management control of procedures

(An extract from the Summary is given below).

'*The analysis of the incidents shows that the majority were not caused by some subtle failure mode of the control system, but by defects which could have been anticipated if a systematic risk-based approach had been used throughout the life of the system. It is also clear that despite differences in the underlying technology of control systems, the safety principles needed to prevent failure remain the same.*'

Specification

'*The analysis shows that a significant percentage of the incidents can be attributed to inadequacies in the specification of the control system. This may have been due either to poor hazard analysis of the equipment under control, or to inadequate assessment of the impact of failure modes of the control system on the specification. Whatever the cause, situations which should have been identified are often missed because a systematic approach had not been used. It is difficult to incorporate the changes required to deal with the late identification of hazards after the design process has begun, and more difficult, (and expensive), to make such changes later in the life of the control system. It is preferable to expend resources eliminating a problem, than to expend resources in dealing with its effects.*'

Design

'*Close attention to detail is essential in the design of all safety-related control systems, whether they are simple hard-wired systems, or complex systems implemented by software. It is important that safety analysis techniques are used to ensure that the requirements in the specification are met, and that the foreseeable failure modes of the control system do not compromise that specification. Issues of concern, which have been identified, include an over-optimistic dependence on the safety integrity of single channel systems, failure to adequately verify software, and poor consideration of human factors. Good design can also eliminate, or at least reduce, the chance of error on the part of the operator or maintenance technician.*'

Maintenance and modification

'*The safety integrity of a well designed system can be severely impaired by inadequate operational procedures for carrying out the maintenance and modification of safety-related systems. Training of staff, inadequate safety analysis, inadequate testing, and inadequate management control of procedures were recurring themes of operational failures.*'

1.8.3 Conclusion: It pays to be systematic

Being systematic allows us to:

- Benefit from previously acquired knowledge and experience
- Minimize the chances of errors
- Demonstrates to others that we have done the job properly... they recognize our way of doing things as legitimate
- Makes it easier to compare one solution or problem with another and hence leads to generally accepted standards of protection
- Allows continuity between individuals and between different participants in any common venture – makes the safety system less dependent on any one individual
- Encourages the development of safety products that can be used by many
- Support regulatory supervision and compliance

1.8.4 Scope 1 of safety systems engineering

The next diagram shows how safety system engineering covers the whole life of an application. Quality assurance practices support the application at every stage.

Figure 1.7

Scope of safety systems engineering

1.9 Introduction to standards: IEC 61508 and ISA S84

Up until the 1980s the management of safety in hazardous processes was left to the individual companies within the process industries. Responsible companies evolved sensible guidelines out of the knowledge that if they didn't take care of

the problem they would be the nearest people to the explosion when it happened. The chemical industry for example was always aware that self-regulation would be better than rules imposed by a worried public through government action.
More recently, industry guidelines have matured into international standards and government regulators are seeing the potential benefits of asking companies and products to conform to what are becoming generally agreed standards. It's ironic that the better the standard the easier it becomes to enforce laws requiring conformance to that standard.
Here we take a look at how we have arrived at the point where new international standards are available. Then we look at the main standards to be used in this book.

1.9.1 Driving forces for management of safety

There are many reasons for wanting to improve the management of safety.

- We (the public) want to know that safety is properly organized
- Cost of accidents, catastrophes
- Rewards are high if the risk is low (Nuclear power)
- SHE Responsibilities of companies, designers and operators
- Legal requirements
- Complexities of processes and plants
- Hazards of multiple ownership
- Falling through the cracks. (Railways)
- Liabilities of owners, operators and designers.
- Insurance risks and certification
- Programmable Electronic Systems (PES)

1.9.2 Evolution of functional safety standards

Figure 1.8

Evolution of functional safety standards

· **TUV (1984)**

· **DIN V 19250 / VDE V 0801 (Germany)**

– Risk classification 1989

– Safety system requirements

· **Various national standards**

· **ANSI / ISA S84.01 (USA) 1996**

– Safety procedures

– Safety life cycle

· **NFPA / UL1998**

· **OSHA (29 CFR 1910.119)**

· **UK HSE**

Courtesy: Honeywell SMS

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.

Earlier design standards did not provide for such possibilities and hence they became obsolete.

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. These and many other factors have resulted in the issue of a new general standard for functional safety using electronic and programmable electronic equipment. The new standard issued by the IEC is IEC-61508 and it covers a wide range of activities and equipment associated with functional safety.

The newer standards bring a new approach to the management and design of functional safety systems. They try to avoid being prescriptive and specific because experience has shown that: '*A cookbook of preplanned solutions does not work.*'

The new approach is to set down a framework of good practices and limitations leaving the designers room to find appropriate solutions to individual applications.

1.9.3 Introducing standard IEC 61508

Figure 1.9

Standard IEC 61508

This diagram shows the title of the standard and its 7 parts issued to date. An additional part 8 is in preparation, which will provide a further set of guidelines for the application of the standard.

1.9.4 Key elements of IEC 61508

- Management of functional safety
- Technical safety requirements
- Documentation
- Competence of persons

1.9.5 Features of IEC 61508

- Applies to safety systems using Electrical/ Electronic/ Programmable Electronic Systems (abbreviation: E/E/PES) e.g. Relays, PLCs, Instruments, Networks
- Considers all phases of the safety lifecycle including software lifecycle
- Designed to cater for rapidly developing technology
- Sets out a 'generic approach' for safety lifecycle activities for E/E/PES
- Objective to 'facilitate the development of application sector standards'
- IEC 61511: process industry sector standard on the way

The standard is ‘generic’, i.e. it provides a generalized approach to the management and design of functional safety systems that can be applicable to any type of industry. It is intended for direct use in any project but it is also intended to be the basis for ‘industry sector’ standards. Hence, more specific industry sector standards will be expected to follow with alignment of their principles to the ‘master standard’.

The IEC standard sets out procedures for managing and implementing a safety life cycle (abbr: SLC) of activities in support of a functional safety system. Hence, we can map the various parts of the standard on to our previous diagram of the safety life cycle as show in the next diagram.

Figure 1.10

Framework of IEC 61508 relevant to SLC

1.9.6 Introducing Standard ANSI/S 84.01

Instrument Society of America

Title:

Application of Safety instrumented Systems for the Process Industries

Sections of ISA S84.01

Clauses 1-11: Mandatory requirements

Clause 12: Key differences from IEC 61508

Annexes A-E: Non mandatory (informative) technical information

Associated Document:

Draft Technical Report: 84.02 (ISA-dTR84.02)

Provides non mandatory technical guidance in Safety Integrity Levels
Figure 1.11

Standard ANSI/ISA S84.01 (USA) 1996

Features of ISA S84.01

- Applies to safety instrumented systems for the process industries
- Applies to safety systems using electrical/electronic/programmable electronic systems (abbr: E/E/PES)
- Defines safety lifecycle activities for E/E/PES but excludes hazard definition steps associated with process engineering
- Objective: 'Intended for those who are involved with SIS in the areas of: design and manufacture of SIS products, selection and application installation, commissioning and Pre-start-up Acceptance Test operation, maintenance, documentation and testing'

The ISA standard is a much less ambitious standard than IEC 61508 and it confines itself to the core instrument engineering activities relevant to process industries. It does not attempt to deal with the hazard study and risk definition phases of the safety life cycle.

1.9.7 Introducing Draft Standard IEC 61511

IEC 61511 is a process sector implementation of IEC 61508 and part 1 has been released in 2003. The standard comprises three parts and includes extensive guidance on the determination of target safety integrity levels that are to be set by the process design team at the start of the design phase of a protection system.

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

IEC 61511 is directed at the end user who has the task of designing and operating an SIS in a hazardous plant. It follows the requirements of IEC 61508 but modifies

them to suit the practical situation in a process plant. It does not cover design and manufacture of products for use in safety, as these remain covered by IEC 61508.

Once IEC 61511 is released the process industries will be able to use it for end user applications whilst devices such as safety certified PLCs will be built in compliance with IEC 61508. IEC 61511 is expected to adopted in the USA and in the EU as the standard for acceptable safety practices in the process industries. ISA S84 will then be superseded.

Figure 1.12:

Relationship of present and future standards

This diagram shows how S84.01 is the precursor of a process industry sector version of IEC 61508. It came out before the IEC standard but was designed to be compatible with it. Eventually a new standard, IEC 61511, will fulfill the role and S84.01 will possibly be superseded, for the present S84.01 is a very useful and practical standard with a lot of engineering details clearly spelt out. Draft copies of parts of IEC 61511 are incorporating many of the good features set out in ISA S84.01 whilst at the same time aligning its requirements with IEC 61508.

1.10 Equipment under control

The term EUC or equipment under control is widely used in the IEC standard and has become accepted as the basis for describing the process or machinery for which a protection system may be required. The following diagram, Figure 1.13, based on a diagram published in the HSE book ‘Out of Control’ illustrates what is meant by the term ‘equipment under control’, abbreviated: EUC.

Figure 1.13

EUC

The definition of equipment under control given in the IEC standards is:

‘*Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.*’ This includes the EUC Control system and the human activities associated with operating the EUC.

This terminology is significant because it makes it clear that the risks we have to consider include those arising from a failure of the control system and any human operating errors.

1.11 The safety lifecycle model and its phases (SLC Phases)

Introducing the safety lifecycle

The foundation for all procedural guidelines in *Safety Instrumented Systems is the Safety Life Cycle (SLC).*

The safety life cycle model is a useful tool in the development of safety related control systems. In concept it represents the interconnected stages from conception through specification, manufacture, installation, commissioning, operation, maintenance, modification and eventual de-commissioning of the plant.

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.

1.11.1 Basic SLC

There are a number of versions of the SLC and there is no reason why a particular design team should not draw its own variations. However the standards we have been looking at have drawn up their versions and have laid out their detailed requirements around the framework provided by the SLC.

1.11.2 ISA SLC

Notice how the activities outside of the ISA scope are shown in fainter outlines. See also references to applicable clauses in the text of the standard.

Figure 1.14

ISA SLC

1.11.3 IEC SLC versions

Finally we need to look at the IEC version as this is the most general version and forms the essential core of the IEC standard.

Figure 1.15

IEC SLC version

The IEC SLC indicates the same basic model that we have been considering but adds very specific detail phases as numbered boxes. Each box is a reference to a detailed set of clauses defining the requirements of the standard for that activity. The boxes are easy to follow because they are defined in terms of:

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

Using the SLC assists participants in a safety project to navigate through the procedures needed for the systematic approach we saw earlier

Note the stages of the IEC model. The first 4 phases are concerned with design, then the ‘realization’ phase is reached. This term describes in very general terms the job of actually building the safety system and implementing any software that it contains.

Once the SIS has been built, the lifecycle activities move on to ‘installation, commissioning, and validation’. Finally we get to use the safety system for real duties and arrive at the operating and maintenance phase.

In the ‘Out of Control’ book the HSE provides a commentary on the method of working with the safety lifecycle. Like any project model the stages are basically in sequence ‘the deliverables of one stage provide the inputs to the next’. However, unlike a project plan the safety lifecycle must be regarded as a set of interconnected activities rather than a simple top down design method. It is intended that iteration loops may be carried out at any stage of work; it does not require the completion of one activity before starting another: i.e., ‘a concurrent design approach can be used’.

Figure 1.16

Safety lifecycle progression

This shows the idea of a continual iteration between life cycle activities and the verification/assessment task. This is to maintain vigilance that a new activity is always compatible with what has gone before. We might add that this presents a potential nightmare for a project manager!

Large sections of IEC 61508 are concerned with the details of the realization phase and there are whole lifecycle models for the activities contained within this stage. Some sections of the IEC standard are dedicated to these specialized tasks. Bear in mind that some of the deeper parts of this standard will be applicable to manufacturers of certified safety PLCs and their associated software packages. A process engineering project would not be expected to dive into such depths.

1.12 Implications of IEC 61508 for control systems

1.12.1 Some Implications of IEC 61508 for Control Systems

1. This standard is the first international standard that sets out a complete management procedure and design requirements for overall safety control systems. Hence it opens up the way for conformance to be enforced by legislation.
2. Control systems and PLCs serving in safety related applications may be required in the future to be in conformance with the requirements laid down in IEC 61508. Conformance may be required by regulatory authorities before licenses are issued.
3. All forms of control systems with any potential safety implications could be subject to evaluation or audit in terms of IEC 61508.
4. Design and hardware/software engineering of any safety related control system is to be evaluated and matched to required SILs.
5. Integrates responsibility for delivering safety across engineering disciplines, e.g. process engineer, instrument engineer, software engineer, maintenance manager and maintenance technician are all required to work to the same standard procedures and share all documentation.
6. Software engineering procedures and software quality assurance are mandatory requirements for a PES in safety applications. The standard provides the basis for certification of software packages by authorities such as TUV.
7. Industry specific standards will be derived from guidelines set down in IEC

61508. (Hence all control system safety related applications in any industry may in future be subjected to similar safety lifecycle design requirements).

8. Responsibilities of users and vendors are clearly defined:

- The user must define his requirements in terms of functional safety (via the SRS);
- The vendor must show how his solution meets the requirements in terms of the user's specific requirements (compliance with SRS and SIL). It is not sufficient to supply a general purpose ESD logic solver for any application;
- The user's responsibilities for operation, maintenance and change control are defined as part of the conformance.

1.12.2 Potential problems using IEC 61508

W S Black, an IEC working group member, has commented in the IEE journal, Feb 2000 on the potential problems some users may face in using the new standard. Some of his points are listed here:

- Deviates from some industry practices
- Sector standards needed to align existing practices e.g. API 41C
- Unfamiliar terminology for USA etc
- Does not match with existing procedures at the start and end of a project
- Project and technical management procedures may need to be redefined to cover key tasks.

1.13 Summary

- The overall design of a safety-instrumented system requires that the project participants have a broad knowledge of the hazards and risks as well as the intended protection measures.
- Great care is required in the initial specification stages.
- Successful implementation of a safety system depends on quality assurance in the design process and on good management of all aspects of the project throughout its lifecycle
- The safety lifecycle provides the framework for the design and management process.
- New standards describe the procedural and design requirements at each stage of the project lifecycle.

1.14 Safety lifecycle descriptions

Summary description of safety lifecycle phases from HSE's 'Out of Control'

Table 1.2

Safety lifecycle phases

Figure 1.17

IEC overall safety lifecycle diagram

1.14.1 Overview of the safety lifecycle based on Table 1 of IEC 61508 part 1

Notes:

This table is based on the IEC Table but some phrases have been changed for emphasis; please refer to the IEC standard for exact wording.

Table 13

IEC 61508: Safety Lifecycle

SLC phase no. and name	Objectives	Scope	Inputs	Outputs
1 Concept	To develop a level of understanding of the EUC and its environment (physical, legislative etc) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out	EUC and its environment (physical, legislative etc)	All relevant information	Information acquired agains a checklist give in the std
2 Overall scope definitions	Define the boundaries of the EUC and the	EUC and its environment	Information acquired in step	Information acquired agains

	EUC control system. To specify the scope of the hazard and risk analysis (e.g. process hazards, environmental hazards, etc)		1	the phase 2 checklist
3 Hazard and risk analysis	To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse. To determine the event sequences leading to the hazardous events determined.	For the preliminary hazard and risk analysis, the scope will comprise the EUC, the EUC control system and human factors. Further h & r analysis may be needed later as the design develops.	Information acquired in step 2	Description of and information relating to the hazard and risk analysis.
4 Overall safety requirements	To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements.	EUC, the EUC control system and human factors.	Description of, and information relating to, the hazard and risk analysis	Specification fo the overall safety requirements in terms of the functions and safety integrity. Includes SIS, non-SIS and external risk reduction measures.
5 Safety requirements' allocation	To allocate a safety function to SIS, non-SIS and external risk reduction measures. To allocate safety integrity, level to each safety function.	EUC, the EUC control system and human factors.	Specification from stage 4.	Allocation decisions for SIS, Non SIS and external measures. Expansion of the SRS for the SIS.

6 Overall operation and maintenance planning	To develop a plan for operating and maintaining the E/E/PE safety-related systems	EUC, the EUC control system and human factors; E/E/PES safety-related systems	As above i.e. Safety requirements Spec.	A plan for operating and maintaining the E/E/PE safety-related systems (SIS)
7 Overall safety validation planning	To develop a safety validation plan for the SIS	As for stage 6	Safety requirements Spec	A plan to facilitate the validation of the SIS

Table 1.3 (contd.)
IEC 61508: Safety Lifecycle

SLC phase no. and name	Objectives	Scope	Inputs	Outputs
8 Overall installation and commissioning	To develop an installation and commissioning plan to ensure the required	As for stage 6	Safety requirements Spec	A plan for the installation and commissioning of the SIS.
9 E/E/PE safety related systems realization	To create non-SIS safety systems conforming to the relevant SRS (outside of scope of IEC 61508)	Other technology related systems	Other technology safety requirements spec	Confirmation that each other technology safety related systems meet the safety requirements for that system.
10 Other technology related systems realization	To create non-SIS safety systems conforming to the relevant SRS (outside of scope of IEC 61508)	Other technology related systems	Other technology safety requirements spec	Confirmation that each other technology safety related systems meet the safety requirements for that system.
11 External risk reduction factors	To create external risk reduction facilities to meet the relevant SRS (outside of scope of IEC 61508)		External risk, reduction facilities safety requirements specification (outside the scope and not considered	Confirmation that each external risk reduction facility meets the safety requirements for that facility

			further in this standard)	
12 Overall installation and commissioning	To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems	E/E/PES safety-related systems	Plans from stage 10	Fully installed SIS Fully commissioned SIS
13 Overall safety validation	To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements	E/E/PES safety-related systems	Plan from stage 9	Confirmation that the SIS meet the safety requirements spec
14 Overall operation, maintenance and repair	To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained	EUC and the EUC control system; E/E/PE safety-related systems.	Requirement for the modification or retrofit under the procedures for the management of functional safety	Continuing achievement of th required functiona safety for the SIS; Chronological records of operation repair and maintenance
15 Overall modifications and retrofit	To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place	EUC and the EUC control system; E/E/PE safety-related systems	Request for modification or retrofit under the procedures for management of functional safety	Achievement of th required functiona safety for the SIS, both during and after the modification and retrofit phase has taken place; chronological records.

Table 13 (cont.)

IEC 61508: Safety Lifecycle

SLC phase no. and name	Objectives	Scope	Inputs	Outputs
16 Decommissioning or disposal	To ensure that the functional safety for the E/E/PE safety-	EUC and the EUC control system;	Request for dec ommissioning or disposal	Achievement of th required functiona safety for the SIS

	related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.	E/E/PE safety-related systems	under the procedures for management of functional safety	both during and after the decommissioning or disposal activities; Chronological records of activitie

1.15 Some websites for safety systems information

1.16 Bibliography and sources of information

This bibliography contains a list of sources of information relating to safety-instrumented systems or associated activities such as hazard studies. References used in preparing this book.

Ref No	**Title/subject**	**Origin**
1	Safety Shutdown Systems: Design, Analysis and Justification, ISBN 1-55617-665-1	Paul Gruhn P.E. and Harry Cheddie P.E., 1998 ISA, PO Box 12277, Research Triangle Park NC 27709, USA www.isa.org
2	Out of Control: Why control systems go wrong and how to prevent failure. . ISBN 0 7176 0847 6	UK Health and Safety Executive. HSE Books. www.hse.gov.uk
3	Tolerable Risk Guidelines	Edward M Marzal: Principal Engineer, Exida .com
4	Five Past Midnight in Bhopal. ISBN 0-7432-2034-X	D Lapierre and J Moro. Scribner UK. 2002 (Simon and Schuster UK).
5	HAZOP and HAZAN by Trevor Kletz 4th edition. 1999	I Chem. Eng Rugby, UK
6	The design of new chemical plants using hazard analysis. By S B Gibson, 1975	I Chem.E Symposium series no 47. I Chem. Eng Rugby, UK

7	Guidelines on a Major Accident Prevention Policy and Safety Management System, as Required by Council Directive 96/82/EC (Seveso II) ISBN 92-828-4664-4, *N. Mitchison, S. Porter (Eds)*	European Commission – Major Accident Hazards Bureau *It is available as a Free download from* Luxembourg: Office for Official Publications of the European Communities, 1998.
8	IEC 61882: Hazard and Operability Studies (HAZOP studies)- Application Guide. 1st edition 2001-05	International Electro-Technical Commission, Geneva, Switzerland. Download/purchase from: www.iec.ch
9	Hazard and Operability Study Manual. AECI Engineering Process Safety	D Rademeyer Ishecon SHE Consulatnts Ltd, PO Box 320 Modderfontein, 1645, South Africa.
10	HAZOP Guide to Best Practice: by Frank Crawley, Malcom Preston and Brian Tyler. (ISBN0-85295-427-1) Published in 2000 and reprinted 2002.	Published by: European Process Safety Centre, Inst of Chemical Engineers, 165-189 Railway Terrace , Rugby, CV21 3HQ, UK www.icheme.org
Ref No	**Title/subject**	**Origin**
11	Alarm systems: A guide to design, management and procurement. EEMUA Publication No 191. 1999	Engineering Equipment and Materials Users Association. UK.
12	IEC 61508 Functional safety of E/E/PES systems. Parts 1 to 7	International Electro-Technical Commission, Geneva, Switzerland. www.iec.ch
13	IEC 61511 Safety instrumented systems for the process industry sector. Parts 1 and 3. 2002.	IEC
14	ANSI/ISA –S84.01 Application of safety instrumented systems for the process industries	ISA.Org
15	DEF 00-55 Hazop studies on systems containing programmable electronics	UK Defence dept. www.dstan.mod

1.16.1 Suggested books

Dr David J Smith: *Reliability Maintainability and Risk,* 6th edition 2001, Butterworth Heinemann

Trevor Kletz: *HAZOP and HAZAN – Identifying and Assessing Process Hazards*, IChemE, 1999

Felix Redmill, Morris Chudleigh and James Catmur: *System Safety – HAZOP and Software HAZOP*, John Wiley and Sons, 1999

William M Goble: *Control Systems Safety Evaluation and Reliability*, 2nd edition 1998, ISA

Trevor Kletz, Paul Chung, Eamon Broomfield and Chaim Shen-Orr: *Computer Control and Human Error,* I.ChemE, 1995

E.Knowlton: *An introduction to Hazard and Operability Studies – the Guide Word Approach*. Chemetics International, Vancouver, BC, Canada, 1992

1.16.2 Publications

Center for Chemical Process Safety of the American Institute of Chemical Engineers:

Guidelines for Safe Automation of Chemical Processes, AIChE New York 1999, ISBN 0-8169-0554-1

Guidelines for hazard evaluation procedures*. ISBN 0-8169-0491-X*

Institution of Electrical Engineers

Safety, Competence and Commitment - Competency Guidelines for Safety-related System Practitioners*,* 1999

Engineering Equipment and Materials Users' Association

Alarm Systems – A guide to design, management and *procurement.*
EEMUA Publication No. 191, 1999

CASS Limited

The CASS Assessor Guide – The CASS Assessor Competency Scheme,
CASS Ltd 1999

The CASS Guide - Guide to Functional Safety Capability Assessment (FSCA), CASS Ltd 1999

Simmons Associates

Technical briefs on safety systems. Short descriptions of key issues in safety systems. Available as free downloads from: Simmons Associates: www.tony-s.co.uk

1.16.3 Reports

Health and Safety Commission

The use of computers in safety-critical applications – final report of the study group on the safety of operational computer systems, HSC, 1998

Health and Safety Executive

The explosion and fire at the Texaco Refinery, Milford Haven 24, July 1994, 1997

Health and Safety Executive

The use of commercial off-the-shelf (COTS) software in safety-related applications, HSE Contract Research Report No. 80/1995

1.17 Guidelines on sector standards

Process industry

Reference: IEC 61511

Date: 11th June 1999

Title: Functional Safety Instrumented systems for the process industry sector

Description: This standard is an adaptation of IEC 61508 for the process industry and provides details on a general framework, definitions and system software and hardware requirements.

Part 1: Framework, definitions, system, hardware and software requirements

Part 2: Guidelines in the application of IEC 61511-1

Part 3: Guidelines in the application of Hazard & Risk Analysis

Draft copies of this standard have been in circulation amongst contributing parties but publication of the approved version is not expected to be complete until later in 2003. Parts 1 and 2 have been available for purchase from IEC from February 2003. This standard will be of great value for practical application in the process industries. It incorporates substantial sections of guide material previously published in ISA S84.01 and is expected to replace ISA S84.01.

Oil and gas industries

Reference: UK Offshore Operators Association

Date: December 1995

Title: Guidelines for Instrument-based Protective Systems

Description: The guidelines have been prepared to provide guidance on good practice for the design, operation, maintenance and modification of instrument-based protective systems on oil and gas installations. The guidelines advocate and translate a risk-based approach to the specification and design of protective instrumentation

Reference: American Petroleum Institute, API 41C 4th edition

Date: (sixth edition)

Title: Recommended Practice for Analysis, Design, Installation and Testing of Basic Surface Safety Systems

Reference: ISO Standard 10418

Date: 1993

Title: Offshore Production Platform – Analysis, Design, Installation and Testing of Basic Surface Safety Systems

Identical content with API 41C 4th edition. Revised version being developed incorporating instrument protection systems to be implemented according to IEC 61508.

Machinery sector

Reference: EN 954 Parts 1 and 2 Draft

Date: March 1997

Title: Safety of Machinery – Safety Related Parts of Control Systems

Description: Parts of machinery control systems are frequently assigned to perform safety functions. Part 1 of this standard provides safety requirements and guidance on the general principles of safety related parts of control systems. Part 2 specifies the validation process including both analysis and testing for the safety functions and categories for the safety-related control systems.

Reference: EN 1050

Date: November 1996

Title: Safety of Machinery – Principles of Risk Assessment

Description: The standard establishes general principles for risk assessment, and gives guidance on the information required to allow risk assessment to be carried out. The purpose of the standard is to provide advice for decisions to be made on the safety of machinery.

Reference: EN 61496 parts 1, 2 and 3.

Dates: 1997-2001

Titles: Safety of machinery – Electro sensitive protective equipment

Part 1: General requirements and tests.

Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)

Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)

Railway industry

Reference: Cenelec prEN 50126

Date: 27/11/95

&