

Risk management —

Part 3: Guide to risk analysis of technological systems

ICS 03.120.10; 29.020

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee DS/1, Reliability and maintainability upon which the following bodies were represented:

Association of Consulting Engineers
 Association of Project Managers
 British Gas plc
 British Railways Board
 British Telecommunications plc
 Chartered Institution of Building Services Engineers
 City University
 Civil Aviation Authority
 Consumer Policy Committee of BSI
 Consumers' Association
 Cornfield University
 Defence Manufacturers Association
 Electricity Association
 Federation of the Electronics Industry
 GAMBICA (BEAMA Ltd.)
 Institute of Logistics
 Institute of Quality Assurance
 Institute of Risk management
 Institute of Value Management
 Institution of Electrical Engineers
 Institution of Mechanical Engineers
 Institution of Plant Engineers
 London underground Ltd.
 Loughborough University of Technology
 Mercury Communication Limited
 Ministry of Defence
 National Computing Centre Ltd.
 Railtrack
 Railway Industry Association
 Royal Institution of Chartered Surveyors
 Royal Statistical Society
 Safety and Reliability Society
 Society of Environmental Engineers
 Society of Motor Manufacturers and Traders Limited
 University of Bradford
 West Midlands Enterprise Board

This British Standard, having been prepared under the direction of the Management Systems Sector Board, was published under the authority of the Standards Board and comes into effect on 15 August 1996

© BSI 12-1998

The following BSI references relate to the work on this standard:
 Committee reference DS/1
 Draft for comment 93/408655 DC

ISBN 0 580 26110 7

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Introduction	1
1 Scope	1
2 Normative references	1
3 Definitions	2
4 Risk analysis concepts	2
5 Risk analysis process	4
6 Audits	7
7 Risk analysis methods	7
Annex A (informative) Methods of analysis	15
Figure 1 — A simplified relationship between risk analysis and other risk management activities	11
Figure 2 — The risk analysis process	12
Figure 3 — Typical considerations in selecting type of analysis and depth of study	13
Figure 4 — A risk matrix	14
Figure A.1 — Fault tree example	17
Figure A.2 — Fault tree symbols	18
Figure A.3 — Example of an event tree for a dust explosion	19
Table 1 — Methods used in risk analysis	10
Table A.1 — HAZOP II guide words	15
Table A.2 — Sample HAZOP II worksheet for guideword “not, no”	16
List of references	Inside back cover

National foreword

This Part of BS 8444 has been prepared by Technical Committee DS/1. It is identical with IEC 300-3-9:1995 *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems* published by the International Electrotechnical Commission (IEC).

This Part provides guidelines for selecting and implementing risk analysis techniques presented as risk analysis concepts, risk analysis process and risk analysis methods. It provides an input to risk management activities.

Cross-references

Publication referred to	Corresponding British Standard
IEC 50(191):1990	BS 4778 <i>Quality vocabulary</i> Part 3 <i>Availability, reliability and maintainability terms</i> Section 3.2:1991 <i>Glossary of international terms</i> (Identical) BS 5760 <i>Reliability of systems, equipment and components</i>
IEC 300-2:1996	Part 1:1996 <i>Dependability programme elements and tasks</i> (Identical)
IEC 1025:1990	Part 7:1991 <i>Guide to fault tree analysis</i> (Identical)
IEC 1078:1991	BS EN 61078:1994 <i>Reliability of systems, equipment and components. Guide to the block diagram technique</i> (Identical)

A related British Standard to IEC 812:1985 is BS 5760 *Reliability of systems, equipment and components* Part 5:1991 *Guide to failure modes, effects and criticality analysis (FMEA and FMECA)*.

Additional information

This standard is a guide and the use of the verbal forms “must” and “shall” in the text does not indicate mandatory requirements.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summery of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 20, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

Introduction

The process of risk management incorporates many different elements from the initial identification and analysis of risk, to the evaluation of its tolerability and identification of potential risk reduction options, through to the selection, implementation and monitoring of appropriate control and reduction measures. This is illustrated in Figure 1.

Risk analysis, which is the subject of this section of IEC 300-3, is a structured process that identifies both the likelihood and extent of adverse consequences arising from a given activity, facility or system. Within the context of this standard, the adverse consequences of concern are physical harm to people, property or the environment.

Risk analysis attempts to answer three fundamental questions:

- What can go wrong (by hazard identification)?
- How likely is this to happen (by frequency analysis)?
- What are the consequences (by consequence analysis)?

This standard is intended to reflect current good practices in selection and utilisation of the risk analysis techniques and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of systems. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of analysis for particular applications. If these standards are in harmony with this publication, the specific standards will generally be sufficient.

This standard only covers the risk analysis portion of the broader risk assessment and risk management activities. The latter may become the subject of future standards. To the extent possible, this standard has built on the concepts and terminology given in the documents listed in clause 2 and other standards. There are numerous instances where these documents are not entirely consistent or where they principally apply to one industry alone. In these cases, this standard may use one of the approaches/definitions available or may present a more general one.

1 Scope

This section of IEC 300-3 provides guidelines for selecting and implementing risk analysis techniques, primarily for risk assessment of technological systems. The objective of this standard is to ensure quality and consistency in the planning and execution of risk analyses and the presentation of results and conclusions.

This standard contains guidelines for risk analysis, presented as follows: risk analysis concepts, risk analysis process, risk analysis methods.

This section of IEC 300-3 is applicable as:

- a guideline for planning, executing and documenting risk analyses;
- a basis for specifying quality requirements for risk analysis (this can be particularly important when dealing with external consultants);
- a basis for evaluating risk analyses after completion.

Risk analysis carried out to this standard provides an input to risk management activities (see Figure 1).

NOTE This standard does not provide specific criteria for identifying the need for risk analysis, or specify the type of risk analysis method that is required for a given situation. Nor does it offer detailed guidelines for specific hazards or include insurance, actuarial, legal, or financial interests.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 300-3. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this section of IEC 300-3 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below.

Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191):1990, *International Electrotechnical Vocabulary (IEV) — Chapter 191: Dependability and quality of service*.

IEC 300-2, *Dependability management — Part 2: Dependability programme elements and tasks*.

IEC 812:1985, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*.

IEC 1025:1990, *Fault tree analysis (FTA)*.

IEC 1078:1991, *Analysis techniques for dependability — Reliability block diagram method*.

3 Definitions

For the purposes of this section of IEC 300-3, the terms and definitions of IEC 50(191) apply. In addition, the following terms and definitions apply:

3.1 harm¹⁾

physical injury or damage to health, property or the environment

3.2 hazard¹⁾

source of potential harm or a situation with a potential for harm

3.3 hazardous event

event which can cause harm

3.4 hazard identification

process of recognizing that a hazard exists and defining its characteristics

3.5 risk¹⁾

combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event

NOTE The concept of risk always has two elements: the frequency or probability with which a hazardous event occurs and the consequences of the hazardous event.

3.6 risk analysis

systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment (See Figure 1.)

NOTE Risk analysis is also sometimes referred to as probabilistic safety analysis, probabilistic risk analysis, quantitative safety analysis and quantitative risk analysis.

3.7 risk assessment

overall process of risk analysis and risk evaluation. (See Figure 1.)

3.8 risk control

process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using the results of risk assessment as one input

3.9 risk estimation

process used to produce a measure of the level of risks being analysed. Risk estimation consists of the following steps: frequency analysis, consequence analysis and their integration

3.10 risk evaluation

process in which judgements are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects

3.11 risk management

systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. (See Figure 1.)

3.12 system

composite entity, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific objective

4 Risk analysis concepts

4.1 Objective and basic concepts of risk analysis

Risk is present in all human activity; it can be health and safety related (involving, for example, both immediate and long-term health effects of exposure to toxic chemicals), economic (resulting in, for example, destruction of equipment and lost production due to fires, explosions or other accidents) or affect the environment. The objective of risk management is to control, prevent or reduce loss of life, illness, or injury, damage to property and consequential loss, and environmental impact.

Before risk can be effectively managed, it should be analysed. The analysis of risk is a useful tool for:

- a) identifying risks and approaches to their solution;
- b) providing objective information for decision making;
- c) meeting regulatory requirements.

¹⁾ These definitions deviate from those given in ISO/IEC Guide 51:1990, which is currently under revision.

The results of a risk analysis can be used by a decision-maker to help judge the tolerability of risk and aid in choosing between potential risk-reduction or risk avoidance measures. From the decision-maker's perspective some of the principal benefits of risk analysis include:

- a) systematic identification of potential hazards;
- b) systematic identification of potential failure modes;
- c) quantitative risk statements or ranking;
- d) evaluation of possible modifications to reduce risk or achieve better dependability levels;
- e) identification of the important contributors to risk and weak links in a system;
- f) better understanding of the system and its installation;
- g) comparison of risks to those of alternative systems or technologies;
- h) identification and communication of risks and uncertainties;
- i) help in establishing priorities for improving health and safety;
- j) a basis for preventive maintenance and inspection to be rationalised;
- k) post-accident investigation and prevention;
- l) selection between alternatives such as different risk-reduction measures and technologies.

All these play an important role in effective risk management, whether the objective is improving conditions related to health and safety, prevention of economic loss, or compliance with government regulations.

Risk analysis often requires a multidisciplinary approach, since it may cover such areas of expertise as:

- a) systems analysis;
- b) probability and statistics;
- c) chemical, mechanical, electrical, structural or nuclear engineering;
- d) physical, chemical, or biological sciences;
- e) health sciences, including toxicology and epidemiology;
- f) social sciences, including economics, psychology, and sociology;
- g) human factors, ergonomics and management science.

4.2 Risk management and risk categorization

Risk analysis is a part of the risk assessment and management process as illustrated in Figure 1 and consists of scope definition, hazard identification, and risk estimation.

Hazards may be grouped into four general categories, namely:

- a) natural hazards (floods, earthquakes, tornadoes, lightning, etc.);
- b) technological hazards (industrial facilities, structures, transportation systems, consumer products, pesticides, herbicides, pharmaceuticals, etc.);
- c) social hazards (assault, war, sabotage, communicable disease, etc.);
- d) lifestyle hazards (drug abuse, alcohol, smoking, etc.).

These groups are clearly not mutually exclusive, and in analysing technological hazards it is often necessary to consider the influence of factors from other categories (particularly natural hazards) and other systems, as part of the risk analysis.

Risk can also be categorized by the nature of the consequences that are being investigated, for example:

- a) individual (impact on individual members of the general public);
- b) occupational (impact on workers);
- c) societal (overall impact on the general public);
- d) property damage and economic losses (business interruptions, penalties, etc.);
- e) environmental (impact on land, air, water, flora, fauna and cultural heritage).

The overall objective of risk analysis is to provide a rational foundation for decisions concerning risk. Such decisions can be made as part of the larger risk management process, through the comparison of results of risk analysis with tolerable risk criteria. In many situations there will be a need to assess benefits on a case-by-case basis, in order to make a balanced decision. The overall subject of tolerable risk criteria is very complex, involving social, economic and political considerations and as such is outside the scope of this standard.

4.3 Application of risk analysis during life cycle phases

Some specific objectives of risk analysis pertinent to various life cycle phases (see IEC 300-2) of hazardous systems, facilities, or products are listed below.

- a) Concept and definition/design and development phases:
 - 1) to identify major contributors to risk and significant factors involved;
 - 2) to provide input to the design process and to assess the adequacy of the overall design;
 - 3) to identify and evaluate possible safety measures in design;

- 4) to provide input to the assessment of the acceptability of proposed potentially hazardous facilities, activities or systems;
 - 5) to provide information to assist in developing procedures for normal and emergency conditions;
 - 6) to evaluate risk with respect to regulatory and other requirements;
 - 7) to evaluate alternative design concepts.
- b) Manufacturing, installation, operation and maintenance phases:
- 1) to monitor and evaluate experience for the purpose of comparing actual performance with relevant requirements;
 - 2) to provide input into the optimization of normal operating, maintenance/inspection and emergency procedures;
 - 3) to update information on major contributors to risk and influencing factors;
 - 4) to provide information on the significance of the risk for operational decision-making;
 - 5) to evaluate the effects of changes in organizational structure, operational practices and procedures, and system components.
 - 6) to focus training efforts;
- c) Disposal phase; decommissioning:
- 1) to evaluate the risk related to system disposal activities and to ensure that relevant requirements can be met;
 - 2) to provide input into disposal procedures.

5 Risk analysis process

5.1 Overview

General rules should be followed in order to both enhance the effectiveness and objectivity of a risk analysis, and to facilitate comparison with other risk analyses. The risk analysis process should be performed according to a defined sequence of steps:

- a) scope definition;
- b) hazard identification and initial consequence evaluation;
- c) risk estimation;
- d) verification;
- e) documentation;
- f) analysis update.

This process is shown in Figure 2. Risk estimation incorporates frequency and consequence analysis. While documentation is shown as a separate item it is developed at each stage of the process. Depending on the area of application, only certain elements of the process shown may need to be considered. For example, in some instances it may not be necessary to go beyond an initial hazard and consequence analysis.

A thorough knowledge of the system and of the analysis methods used is required. If a risk analysis is available for a similar system, it may be used as a reference. However, it should be demonstrated that the processes are similar or that the changes that have been made will not introduce significant differences in results. This should be based on a systematic evaluation of the changes and the ways they can influence the various hazards present.

5.1.1 Risk analysis personnel

Risk analysts should be competent to undertake the task. Many systems are too complex to be fully understood by one person and a group of analysts will be required to carry out the work. The individual or working group should be familiar with the methods used for risk analysis and have a thorough knowledge of the subject under consideration. Other necessary specialised knowledge should be provided and integrated into the analysis as required. The expertise of the working group should be specified and recorded.

5.2 Scope definition

The scope of the risk analysis should be defined and documented to create a risk analysis plan at the start of the project (see IEC 300-2). Defining the scope of a risk analysis should involve the following steps:

- a) describe the reasons for and/or the problems that originated the risk analysis. This will involve:
 - 1) formulating the objectives of the risk analysis based on the main concerns identified;
 - 2) defining the criteria for success/failure of the system. The main concern may be some undesirable outcome (e.g. system failure, release of poisonous material) or it may be a condition which is potentially harmful.
- b) define the system being analysed. The definition should include:
 - 1) a general description of the system;
 - 2) a definition of boundaries and interfaces with related systems both physical and functional;
 - 3) a definition of the environment;