TECHNICAL REPORT

ISO/TR 12489

First edition
2013-11-01

Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems

Pétrole, pétrochimie et gaz naturel — Modélisation et calcul fiabilistes des systèmes de sécurité

Reference number
ISO/TR 12489:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 67, *Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries*.

This first edition of ISO/TR 12489 belongs of the family of reliability related standards developed by ISO/TC 67:

— ISO 14224, *Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment*

— ISO 20815, *Petroleum, petrochemical and natural gas industries — Production assurance and reliability management*

Introduction

Safety systems have a vital function in petroleum, petrochemical and natural gas industries where safety systems range from simple mechanical safety devices to safety instrumented systems.

They share three important characteristics which make them difficult to handle:

1) They should be designed to achieve good balance between safety and production. This implies a high probability of performing the safety action as well as a low frequency of spurious actions.

2) Some of their failures are not revealed until relevant periodic tests are performed to detect and repair them.

3) A given safety system rarely works alone. It generally belongs to a set of several safety systems (so-called multiple safety systems) working together to prevent accidents.

Therefore improving safety may be detrimental to dependability and vice versa. These two aspects should therefore, ideally, be handled at the same time by the same reliability engineers. However, in reality they are generally considered separately and handled by different persons belonging to different departments. Moreover this is encouraged by the international safety standards, which exclude dependability from their scopes, and the international dependability (see 3.1.1) standard, which excludes safety from theirs. This may lead to dangerous situations (e.g. safety system disconnected because of too many spurious trips) as well as high production losses.

The proof of the conservativeness of probabilistic calculations of safety systems is generally required by safety authorities. Unfortunately, managing the systemic dependencies introduced by the periodic tests to obtain conservative results implies mathematical difficulties which are frequently ignored. The impact is particularly noticeable for redundant safety systems and multiple safety systems. Awareness of these challenges is important for reliability engineers as well as safety managers and decision makers, utilizing reliability analytical support.

Most of the methods and tools presently applied in reliability engineering have been developed since the 1950s before the emergence of personal computers when only pencil and paper were available. At that time the reliability pioneers could only manage simplified models and calculations but this has completely changed because of the tremendous improvement in the computation means achieved over the past 30 years. Nowadays, models and calculations which were once impossible are carried out with a simple laptop computer. Flexible (graphical) models and powerful algorithms based on sound mathematics are now available to handle “industrial size” systems (i.e. many components with complex interactions). This allows the users to focus on the analysis of the systems and assessment of results, rather than on the calculations themselves. All the approaches described in this Technical Report have been introduced in the petroleum, petrochemical and natural gas industries as early as the 1970s where they have proven to be very effective. They constitute the present time state-of-the-art in reliability calculations. Nevertheless some of them have not been widely disseminated in this sector although they can be of great help for reliability engineers to overcome the problems mentioned above. This is particularly true when quantitative reliability or availability requirements need confirmation and/or when the objective of the reliability study lay beyond the scope of the elementary approaches.

The present document is a “technical” report and its content is obviously “technical”. Nevertheless, it only requires a basic knowledge in probabilistic calculation and mathematics and any skilled reliability engineer should have no difficulties in using it.

Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems

1 Scope

This Technical Report aims to close the gap between the state-of-the-art and the application of probabilistic calculations for the safety systems of the petroleum, petrochemical and natural gas industries. It provides guidelines for reliability and safety system analysts and the oil and gas industries to:

- understand the correct meaning of the definitions used in the reliability field;
- identify
  - the safety systems which may be concerned,
  - the difficulties encountered when dealing with reliability modelling and calculation of safety systems,
  - the relevant probabilistic parameters to be considered;
- be informed of effective solutions overcoming the encountered difficulties and allowing to undertake the calculations of relevant probabilistic parameters;
- obtain sufficient knowledge of the principles and framework (e.g. the modelling power and limitations) of the well-established approaches currently used in the reliability field:
  - analytical formulae;[1][2][13]
  - Boolean:
    - reliability block diagrams;[4]
    - fault trees;[5]
  - sequential: event trees,[8] cause consequence diagrams[10] and LOPA;[9]
  - Markovian;[6]
  - Petri nets;[7]
- obtain sufficient knowledge of the principles of probabilistic evaluations:
  - analytical calculations (e.g. performed on Boolean or Markovian models);[1][2][3]
  - and Monte Carlo simulation (e.g. performed on Petri nets[7]);
- select an approach suitable with the complexity of the related safety system and the reliability study which is undertaken;
- handle safety and dependability (e.g. for production assurance purpose, see 3.1.1) within the same reliability framework.

The elementary approaches (e.g. PHA, HAZID, HAZOP, FMECA) are out of the scope of this Technical Report. Yet they are of utmost importance and ought to be applied first as their results provide the input information essential to properly undertake the implementation of the approaches described in this Technical Report: analytical formulae, Boolean approaches (reliability block diagrams, fault trees, event trees, etc.), Markov graphs and Petri nets.

This Technical Report is focused on probabilistic calculations of random failures and, therefore, the non-random (i.e. systematic failures as per the international reliability vocabulary IEV 191[14]) failures are out of the scope even if, to some extent, they are partly included into the reliability data collected from the field.

2 Analysis framework

2.1 Users of this Technical Report

This Technical Report is intended for the following users, in a role defining the scope of work of reliability models (customer or decision-maker), executing reliability analysis or as a risk analyst using these calculations:

- **Installation/Plant/Facility:** operating facility staff, e.g. safety, maintenance and engineering personnel.
- **Owner/Operator/Company:** reliability staff or others analysing or responsible for reliability studies for safety related equipment located in company facilities.
- **Industry:** groups of companies collaborating to enhance reliability of safety systems and safety functions. The use of this Technical Report supports "reliability analytical best practices" for the benefit of societal risk management in accordance with ISO 26000[54].
- **Manufacturers/Designers:** users having to document the reliability of their safety equipment.
- **Authorities/Regulatory bodies:** enforcers of regulatory requirements which can quote these guidelines to enhance quality and resource utilization.
- **Consultant/Contractor:** experts and contractors/consultants undertaking reliability modelling and probabilistic calculation studies.
- **University bodies:** those having educational roles in society and experts that might improve methods on these matters.
- **Research institutions:** experts that might improve reliability modelling and probabilistic calculation methods.

2.2 ISO/TR 12489 with regard to risk and reliability analysis processes

When a safety system has been designed using good engineering practice (i.e. applying the relevant regulations, standards, rules and technical and safety requirements) it is expected to work properly. After that a reliability analysis is usually undertaken in order to evaluate its probability of failure and, if needed, identify how it can be improved to reach some safety targets.

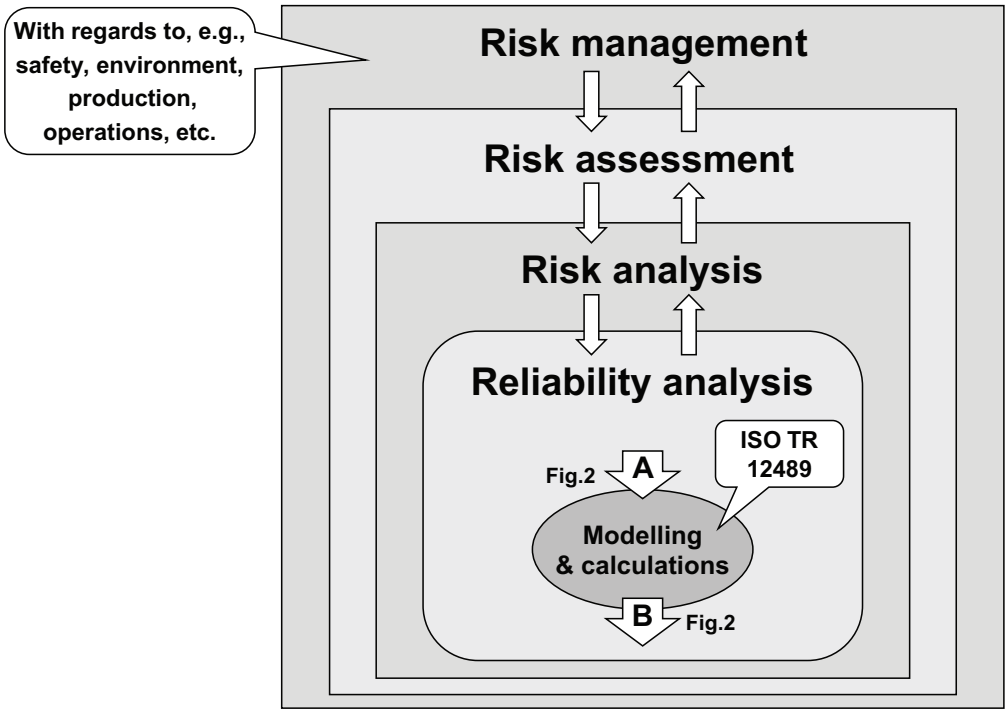


Figure 1 — ISO/TR 12489 within the framework of risk management

Relevant interdisciplinary communication and a good understanding of the safety system life cycle are required to have qualified inputs and correct result interpretations. Applying this Technical Report also requires interaction and compliance with other standards such as ISO 20815[16] (production assurance), ISO 14224[15] (reliability data collection) or ISO 17776[29] and ISO 31000[28] (risk management). As shown in Figure 1, this Technical Report contributes to the risk management process which encompasses both safety and production (dependability, cf. 3.1.1) aspects and involves different stages such as risk assessment and risk analysis. More precisely, this Technical Report contributes to the probabilistic part (reliability analysis) of the risk analysis stage.

NOTE ISO 20815[16] gives further information on reliability/availability in a production assurance perspective, while ISO 14224[15] which is devoted to reliability data collection is another fundamental reference for both safety and production within our industries (within ISO/TC67 business arena). ISO 17776[29] and ISO 31000[28] are devoted to risk management.

When such a process is undertaken, the usual steps are the following:

a) Defining the objective of the study and system boundaries in order to identify the limits of the process and the safety system(s) to be analysed.

b) Functioning analysis to understand how the safety system works.

c) Dysfunctioning analysis to understand how the safety system may fail:

   1) risk identification and establishment of the safety targets;

   2) elementary analyses (e.g. HAZOP, FMEA, etc.);

   3) common cause failures identification.

d) **Modelling and calculations:**

   1) **Modelling:**

      i) **functioning and dysfunctioning modelling**

ii) **common cause/ Common mode failures modelling**

2) **Qualitative analysis;**

3) **Quantitative analysis** (if qualitative analysis is not sufficient).

e) Discussion with field specialists and redesign if improvements are needed.

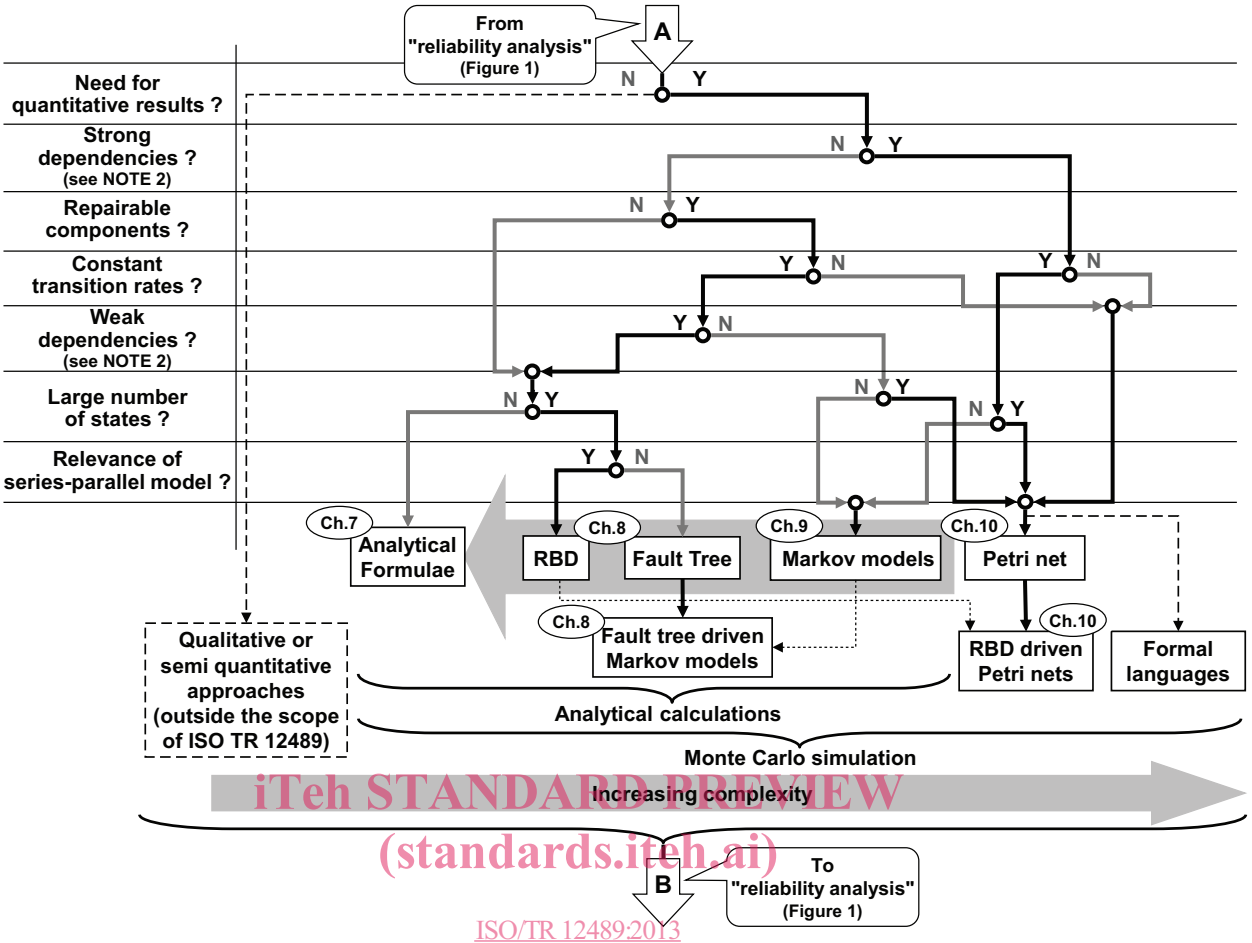
f) **Final results** (weak points, failure contributors, failure probabilities, interpretation, specifications, etc.).

The present Technical Report is focused on the steps written in bold and underlined characters: modelling and calculations [step d)] and final results of interest [step f)]. Nevertheless, step d) and consequently f) can be achieved only if the steps a), b) and c) and consequently e) have been properly undertaken first. Therefore in this Technical Report it is supposed that the limits of the safety system and the objective of the study have been properly identified [step a)], that the analyst has acquired a sound understanding about the functioning [step b)] and dysfunctioning of the safety system under study, that the relevant risk identification and the safety targets have been properly established [and c)] and that field specialists have been invited to give their advice in due time [step e)] to ensure that the final results are close to real life feedback.

This Technical Report also suggests the safety systems and safety functions typically requiring such reliability analysis support in order to utilize resources effectively. See Annex A.

2.3 Overview of the reliability modelling and calculation approaches considered in this Technical Report

Figure 2 gives an overview of the approaches selected for the purpose of this Technical Report and provides some guidelines to select them when the level in difficulty and complexity increases.



NOTE 1 The questions on the left hand side can be used as guidelines to choose an adequate approach to study a given safety system.

NOTE 2 Systems without dependencies do not really exist in the real world but the dependencies may have a negligible impact (weak dependencies) or a strong impact (strong dependencies) on the probability of failure. An example of weak dependency is the use of a single repair team for a topside periodically tested component (because the repair time is negligible compared to the MFDT (Mean Fault Detection Time, see 3.1.35). An example of strong dependency is when a stand-by component starts when another fails.

NOTE 3 "Series-parallel model" refers to a popular model found in numerous text books which uses only series and parallel structures to model the logic of the systems, for example, reliability block diagrams[4].

NOTE 4 The arrow from "Markov" to "Analytical Formulae" through "fault tree" and "RBD" highlights the fact that the analytical formulae are obtained through models mixing Boolean[4][5] and Markov[6] models.

Figure 2 — Overview of reliability modelling and calculation approaches currently used

Other criteria can be used to classify the reliability modelling and calculation approaches:

- the accuracy of results (approximated or exact);
- conservativeness of the results (pessimistic or optimistic);
- the nature of the calculations (analytical or Monte Carlo simulation);
- the nature of the modelling (static or dynamic);
- the user friendliness (graphical or non graphical);
- the input data which can be made available;

- the possibility to update the model after several years by someone else.

The various approaches currently used in reliability engineering have different characteristics (strengths and limitations). It is important for the selection and use of these approaches to be aware of their limitations and conservativeness:

a) **Analytical formulae**:[1][2][13] analytical methods which provide approximated suitable results when used skilfully. They are useful for quick calculations but the underlying limits and approximations often limit their application to systems of limited complexity. This also limits their application to systems where sequence-dependent failures or other time-dependent failures, such as desynchronized testing (see 3.4.10), are not important contributors to the overall performance. Analytical formulae are generally obtained from underlying Boolean and/or Markovian models.

b) **Boolean models:** static and graphical models supporting analytical calculations. "Reliability block diagrams" (RBD)[4] and fault trees (FT)[5] belong to Boolean models. To some extent, the sequential approaches event trees (ET)[8], LOPA[9] or cause consequence diagrams[10] can also be associated with Boolean models. These approaches provide clear and understandable models for large or complex systems. Boolean models are limited to "two-state" systems (working, failed) and handling of time evolution requires a high level of understanding in probabilistic calculations.

c) **Markovian models**[6]**:** dynamic and graphical models supporting analytical calculations and modelling of sequence-dependent or time-dependent failures. A Markovian model is a "state-transition" model limited to exponentially distributed events. The combinatory explosion of the number of system states limits this approach to small (simple or complex) systems with few states. The impact of approximations performed to deal with larger systems is often difficult to evaluate. Boolean and Markovian approaches can be mixed to model large systems when weak dependencies between the components are involved. This can be achieved by implementing the fault tree driven Markov models (see Figure 2).

d) **Petri nets**[7]**:** dynamic and graphical models supporting Monte Carlo simulation to provide statistical results associated with their confidence intervals. A Petri net is a "state-transition" model handling any kind of probabilistic distributions. Time-, state-, or sequence-dependent failures can be modelled explicitly. The size of the model is linear with regard to the number of components. This makes possible the modelling of very large complex systems. The Monte Carlo simulation computation time increases when low probability events are calculated but probabilities of failure as low as 10^{-5} over one year can be handled with modern personal computers. For large safety systems, the Petri net may become difficult to handle. The use of the RBD driven PN overcomes this difficulty (see Figure 2).

e) **Formal languages**[11][12]: dynamic models used to generate analytical models (e.g. Markovian models or fault trees, when possible) or used directly for Monte Carlo simulation. The other characteristics are same as Petri nets except that computations may be slower. They are just mentioned but they are outside the scope of this Technical Report.

Except for bullet e), more details can be found in Clauses 7 to 10. All these models can be mathematically described in terms of "finite states automata" (i.e. a mathematical *state machine* with a finite number of discrete states). The system behaviour can be modelled more and more rigorously when going from a) to e) but, of course, every approach can be used to model simple safety systems.

Figure 2 gives advice to the analyst to select the relevant approach in order to optimize the design of a safety system and meet some reliability targets. This choice depends on the safety function, purpose and complexity the analyst has to face. When several approaches are relevant, the analyst may choose his favourite.

A warning may be raised here: using a software package as a black box or a formula as a magic recipe is likely to lead to inaccurate, often non-conservative, results. In all cases the reliability engineers should be aware of the limitations of the tools that they are using and they should have a minimum understanding of the mathematics behind the calculations and a good knowledge of the nature of the results that they obtain (unreliability, point unavailability, average unavailability, frequency, etc.), of the

conservativeness and of the associated uncertainties. Without adequate understanding of the software tool, erroneous results can be obtained through its misuse.

Table 1 — Road map of ISO/TR 12489

Topic	Reference to main report (sub)clause	Reference to annexes
I- General issues		
a) Terms and definitions	3, 4	-
b) General analytical overview	5, 6	B, C, D, E, F
c) Human factors	5.5	H
d) Common cause	5.4.2	G
e) Monte Carlo simulation	11	N
f) Uncertainty	12	O
g) Reliability data	13	-
h) Systems with safety functions	2.4	A
II- Approaches		
a) Analytical formulae	7	I
b) Boolean	8	K
- Reliability Block Diagram	8.2	
- Fault Tree	8.3	
- Sequence modelling	8.4	J
c) Markovian	9	L
d) Petri net	10	M
III- Examples	14	-
IV- Bibliography	End of ISO/TR 12489	-

It is important that the reliability methods and application of those, including the available input data are adapted to the life cycle phase. Uncertainty handling is further addressed in Clause 12.

The human factor is addressed in 5.5 and Annex H in terms of the quantification of the reliability of human performed tasks. This inclusion is intended to support assessment of the pros and cons of including human tasks with the potential for failure in safety systems.

Table 1 gives a road map for these issues and the supporting annexes and supplement Figure 2.

2.4 Safety systems and safety functions

Numerous safety systems are implemented in the petroleum, petrochemical and natural gas industries. They range from very simple to very complex systems, used on-demand or in continuous mode of operation.

Table A.1 gives a non-exhaustive list of safety systems and safety functions which may require reliability modelling in the petroleum, petrochemical and natural gas industries. It has been built in relationship with the taxonomy developed in the ISO 14224[15] standard and covers either safety systems (taxonomy level 5) or other systems with safety function(s). A summary is given below:

A. Emergency/process shutdown (split in A.1 and A.2)

B. Fire and gas detection

C. Fire water

D. Fire-fighting

E. Process control

F. Public alarm

G. Emergency preparedness systems

H. Marine equipment

I. Electrical and Telecommunication

J. Other utilities

K. Drilling and Wells

L. Subsea

NOTE A to G are covered as safety and control systems in Table A.3 of ISO 14224[15]. The list has been extended from H to L to give a broader coverage.

This Technical Report provides a number of reliability modelling and calculation approaches large enough to cope with any kind of safety system like those identified in Table A.1. They can be used when the objectives of the reliability studies lay beyond the scope of the elementary approaches (e.g. PHA, HAZID, HAZOP, FMECA ...) and selected according to Figure 2.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE 1 Since their introduction more than 50 years ago, the core concepts of the reliability engineering field have been used and adapted for various purposes. Over time this has caused "semantic" drifts and most of the terms have various meanings. They have become so polysemic now that it is necessary to define them accurately to avoid confusion, even when they seem well known.

NOTE 2 The terms are divided into:

— 3.1 Basic reliability concepts

— 3.2 Failure classification

— 3.3 Safety systems typology

— 3.4 Maintenance issues

— 3.5 Other terms

— 3.6 Equipment related terms

Textual definitions are provided as well as, when this is possible, the corresponding mathematical formulae which leave less place to interpretation. Notes are added when clarifications are useful.

3.1 Basic reliability concepts

3.1.1
dependability
ability to perform as and when required

Note 1 to entry: Dependability is mainly business oriented.

Note 2 to entry: IEC/TC 56 which is the international "dependability" technical committee deals with reliability, availability, maintainability and maintenance support. More than 80 dependability standards have been published by the IEC/TC56. In particular, it is in charge of the international vocabulary related to those topics (IEV 191[14]) and also of the methods used in the reliability field (e.g. FMEA, HAZOP, reliability block diagrams, fault trees, Markovian approach, event tree, Petri nets).

Note 3 to entry: The *production availability* is an extension, for production systems, of the classical dependability measures. This term is defined in the ISO 20815[16] standard which deals with *production assurance* and relates to systems and operations associated with drilling, processing and transport of petroleum, petrochemical and natural gas. The relationship between production-assurance terms can be found in Figure G.1 of ISO 20815[16].

[SOURCE: IEC 60050 –191]

3.1.2
safety integrity
ability of a safety instrumented system to perform the required safety instrumented functions as and when required

Note 1 to entry: This definition is equivalent to the dependability of the SIS (Safety Instrumented System) with regard to the required safety instrumented function. Dependability, being often understood as an economical rather a safety concept, has not been used to avoid confusion.

Note 2 to entry: The term "integrity" is used to point out that a SIS aims to protect the integrity of the operators as well as of the process and its related equipment from hazardous events.

3.1.3
SIL
Safety Integrity Level
discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems

Note 1 to entry: Safety integrity level 4 is related to the highest level of safety integrity; safety integrity level 1 has the lowest.

Note 2 to entry: The safety integrity level is a requirement about a safety instrumented function. The higher the safety integrity level, the higher the probability that the required safety instrumented function (SIF) will be carried out upon a real demand.

Note 3 to entry: This term differs from the definition in IEC 61508–4[2] to reflect differences in process sector terminology.

3.1.4
safe state
state of the process when safety is achieved

Note 1 to entry: Some states are safer than others (see Figures B.1, B.2 and B.3) and in going from a potentially hazardous condition to the final safe state, or in going from the nominal safe condition to a potentially hazardous condition, the process may have to go through a number of intermediate safe-states.

Note 2 to entry: For some situations, a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

Note 3 to entry: A state which is safe with regard to a given safety function may increase the probability of hazardous event with regard to another given safety function. In this case, the maximum allowable spurious trip rate (see 10.3) for the first function should consider the potential increased risk associated with the other function.

3.1.5
dangerous state
state of the process when safety is not achieved

Note 1 to entry: A dangerous state is the result of the occurrence of a critical dangerous failure (3.2.4, Figure B.1).