

PD CEN ISO/TR 12489:2016



BSI Standards Publication

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

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This Published Document is the UK implementation of CEN ISO/TR 12489:2016. It is identical to ISO/TR 12489:2013. It supersedes PD ISO/TR 12489:2013 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PSE/17, Materials and equipment for petroleum, petrochemical and natural gas industries.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 88682 9

ICS 75.180.01; 75.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2013.

Amendments/corrigenda issued since publication

Date	Text affected
29 February 2016	This corrigendum renumbers PD ISO/TR 12489:2013 as PD CEN ISO/TR 12489:2016.

ICS 75.200; 75.180.01

English Version

**Petroleum, petrochemical and natural gas industries -
Reliability modelling and calculation of safety systems
(ISO/TR 12489:2013)**

Pétrole, pétrochimie et gaz naturel - Modélisation et
calcul fiabilistes des systèmes de sécurité (ISO/TR
12489:2013)

Erdöl-, petrochemische und Erdgasindustrie -
Zuverlässigkeit der Modellierung und Berechnung von
Sicherheitssystemen (ISO/TR 12489:2013)

This Technical Report was approved by CEN on 28 March 2015. It has been drawn up by the Technical Committee CEN/TC 12.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

This document (CEN ISO/TR 12489:2016) has been prepared by Technical Committee ISO/TC 67 “Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries” in collaboration with Technical Committee CEN/TC 12 “Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of ISO/TR 12489:2013 has been approved by CEN as CEN ISO/TR 12489:2016 without any modification.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Analysis framework	2
2.1 Users of this Technical Report	2
2.2 ISO/TR 12489 with regard to risk and reliability analysis processes	2
2.3 Overview of the reliability modelling and calculation approaches considered in this Technical Report	4
2.4 Safety systems and safety functions	7
3 Terms and definitions	8
3.1 Basic reliability concepts	8
3.2 Failure classification	20
3.3 Safety systems typology	24
3.4 Maintenance issues	25
3.5 Other terms	28
3.6 Equipment-related terms	29
4 Symbols and abbreviated terms	30
5 Overview and challenges	33
5.1 General considerations about modelling and calculation challenges	33
5.2 Deterministic versus probabilistic approaches	35
5.3 Safe failure and design philosophy	35
5.4 Dependent failures	36
5.5 Human factors	37
5.6 Documentation of underlying assumptions	40
6 Introduction to modelling and calculations	41
6.1 Generalities about safety systems operating in “on demand” or “continuous” modes	41
6.2 Analytical approaches	44
7 Analytical formulae approach (low demand mode)	47
7.1 Introduction	47
7.2 Underlying hypothesis and main assumptions	47
7.3 Single failure analysis	48
7.4 Double failure analysis	50
7.5 Triple failure analysis	55
7.6 Common cause failures	56
7.7 Example of implementation of analytical formulae: the PDS method	57
7.8 Conclusion about analytical formulae approach	57
8 Boolean and sequential approaches	58
8.1 Introduction	58
8.2 Reliability block diagrams (RBD)	58
8.3 Fault Tree Analysis (FTA)	59
8.4 Sequence modelling: cause consequence diagrams, event tree analysis, LOPA	61
8.5 Calculations with Boolean models	61
8.6 Conclusion about the Boolean approach	64
9 Markovian approach	65
9.1 Introduction and principles	65
9.2 Multiphase Markov models	68
9.3 Conclusion about the Markovian approach	69
10 Petri net approach	69
10.1 Basic principle	69
10.2 RBD driven Petri net modelling	71

10.3	Conclusion about Petri net approach	74
11	Monte Carlo simulation approach.....	74
12	Numerical reliability data uncertainty handling.....	74
13	Reliability data considerations	75
13.1	Introduction	75
13.2	Reliability data sources.....	76
13.3	Required reliability data.....	78
13.4	Reliability data collection	80
14	Typical applications.....	80
14.1	Introduction	80
14.2	Typical application TA1: single channel.....	82
14.3	Typical application TA2: dual channel.....	97
14.4	Typical application TA3: popular redundant architecture.....	110
14.5	Typical application TA4: multiple safety system	119
14.6	Typical application TA5: emergency depressurization system (EDP)	124
14.7	Conclusion about typical applications.....	135
Annex A (informative) Systems with safety functions		136
Annex B (informative) State analysis and failure classification		146
Annex C (informative) Relationship between failure rate, conditional and unconditional failure intensities and failure frequency		152
Annex D (informative) Broad models for demand mode (reactive) safety systems		160
Annex E (informative) Continuous mode (preventive) safety systems.....		167
Annex F (informative) Multi-layers safety systems/multiple safety systems.....		170
Annex G (informative) Common cause failures		173
Annex H (informative) The human factor		180
Annex I (informative) Analytical formulae		186
Annex J (informative) Sequential modelling.....		207
Annex K (informative) Overview of calculations with Boolean models.....		213
Annex L (informative) Markovian approach		221
Annex M (informative) Petri net modelling.....		239
Annex N (informative) Monte Carlo simulation approach.....		248
Annex O (informative) Numerical uncertainties handling		252
Bibliography.....		255

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.

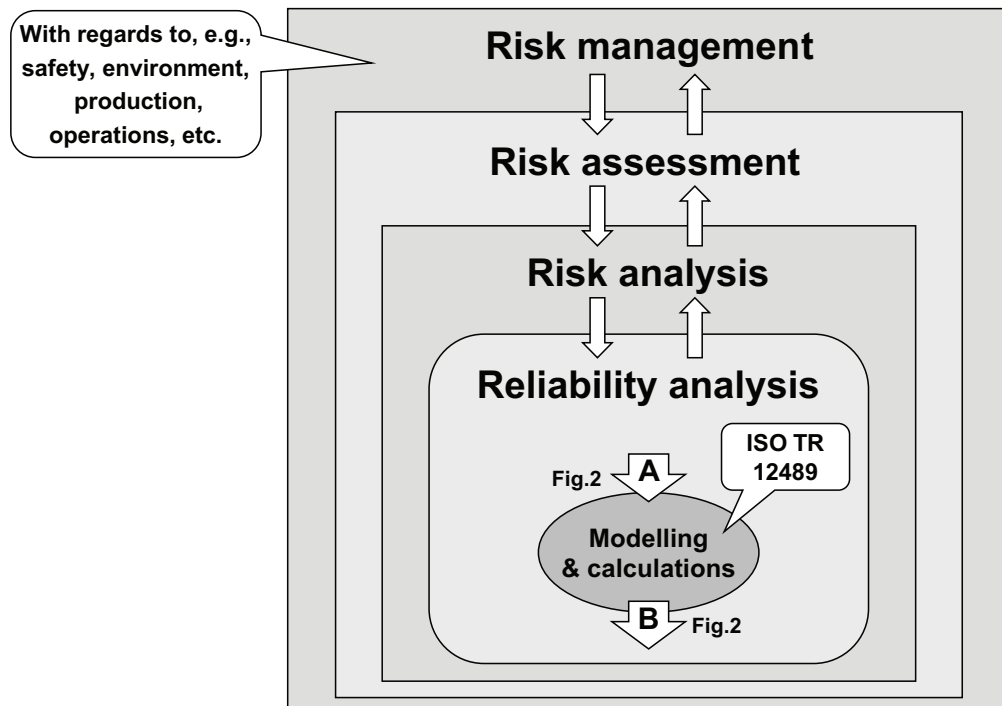


Figure 1 — ISO/TR 12489 within the framework of risk management

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.

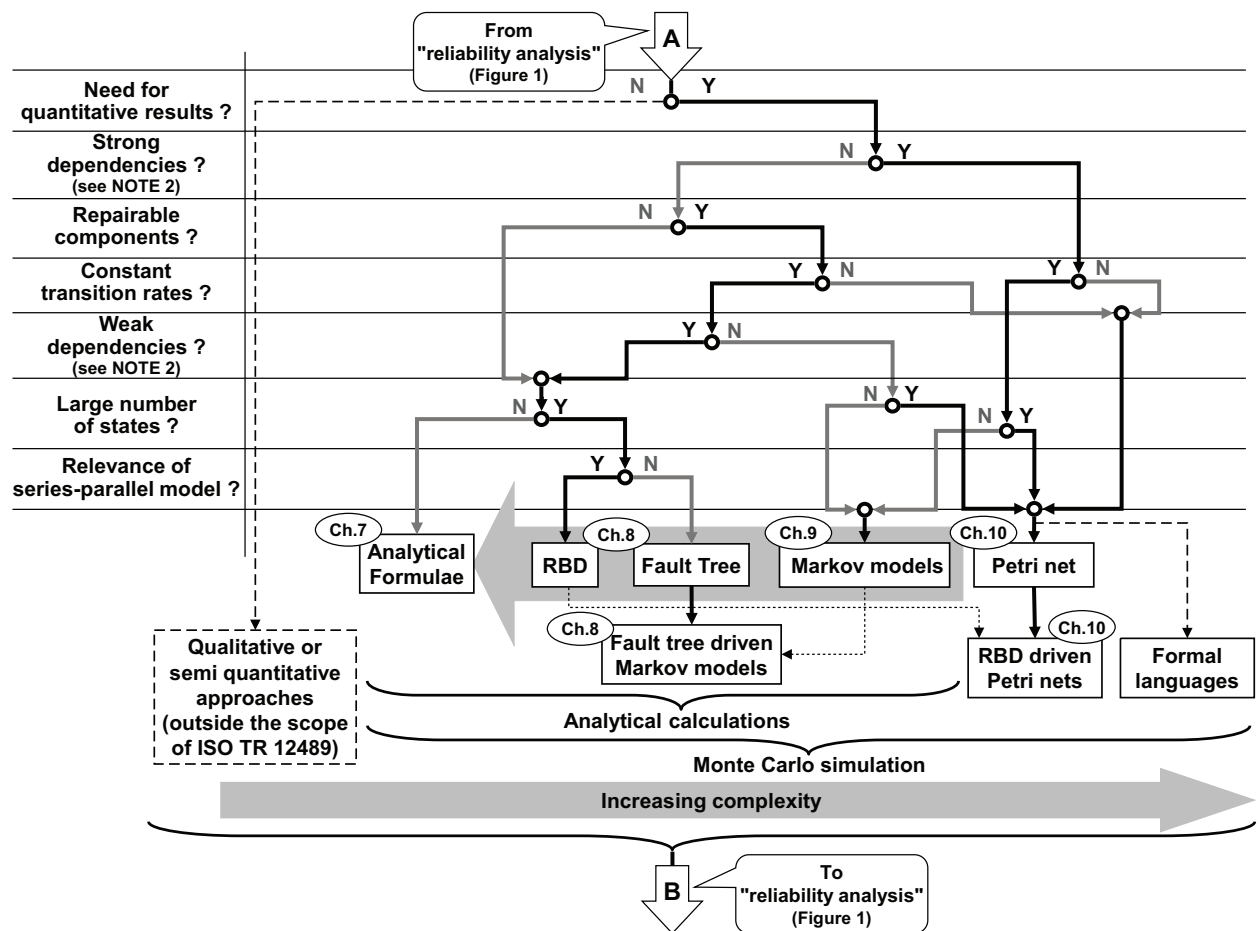
f) **Final results** (weak points, failure contributors, failure probabilities, interpretation, specifications, etc.).

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:

- 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.
- 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.
- 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](#)).
- 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](#)).
- 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](#)).

3.1.6

safety function

function which is intended to achieve or maintain a safe state, in respect of a specific hazardous event

Note 1 to entry: This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.1.7

safety system

system which realizes one or more safety functions

3.1.8

reliability

$R(t)$

⟨measure⟩ probability for an item to perform a required function under given conditions over a given time interval $z = \frac{S-m}{\sigma}$

Note 1 to entry: This is a time-dependent parameter.

Note 2 to entry: This parameter is related on a continuous functioning from 0 to t .

Note 3 to entry: For non-repairable items, Reliability and Availability are identical.

Note 4 to entry: In IEC 60500-191^[14], the reliability is defined both as ability and as measure.

3.1.9

unreliability

$F(t)$

⟨measure⟩ probability for an item to fail to perform a required function under given conditions over a given time interval $[0, t]$

Note 1 to entry: $F(t)$ is also the probability that the time of the first failure t_f is lower than t : $F(t) = P(t_f \leq t)$. This is in relationship with the occurrence of the first failure.

Note 2 to entry: $F(t)$ is the cdf (cumulative distribution function) of the time to the first failure t_f of the item. It ranges from 0 to 1 when t goes from 0 to infinity.

Note 3 to entry: The unreliability is the complementary of the reliability: $F(t) = 1 - R(t)$

Note 4 to entry: When dealing with safety, $F(t)$ is generally small compared to 1 and this property is used to develop approximated formulae (see [Clause 7](#)).

Note 5 to entry: Unreliability is better to communicate than MTTF.

3.1.10

failure probability density

$f(t)$

⟨measure⟩ probability for an item to fail between t and $t+dt$

Note 1 to entry: $f(t)$ is the classical pdf (probability density function) of the time to the first failure t_f of the item: $f(t) = P(t < t_f \leq t + dt)$

Note 2 to entry: $f(t)$ is the derivative of $F(t)$: $f(t) = \frac{dF(t)}{dt}$

Note 3 to entry: The failure density is linked to the failure rate by the following relation:

Note 4 to entry: $f(t) = \lambda(t)R(t) = \lambda(t)[1 - F(t)]$ (see [Annex C](#) for more details).

3.1.11

instantaneous availability

point availability

$A(t)$

probability for an item to be in a state to perform as required at a given instant

Note 1 to entry: In this Technical Report the word “availability” used alone stands for “instantaneous availability”.

Note 2 to entry: This is a time-dependent parameter.

Note 3 to entry: No matter if the item has failed before the given instant if it has been repaired before.

Note 4 to entry: For non-repairable items, Availability and Reliability are identical.

Note 5 to entry: When dealing with safety, $A(t)$ is generally close to 1 and this property is used to develop approximated formulae (see [Clause 7](#)).

3.1.12

unavailability

instantaneous unavailability

point unavailability

$U(t)$

(measure) probability for an item not to be in a state to perform as required at a given instant

Note 1 to entry: The unavailability is the complementary of the availability: $U(t) = 1 - A(t)$

Note 2 to entry: The unavailability is called “Probability of Failure on Demand” (PFD) by the standards related to the functional safety of safety related/instrumented systems (e.g. IEC 61508[2]).

Note 3 to entry: Note 3 to entry: When dealing with safety $U(t)$ is generally small compared to 1 and this property is used to develop approximated formulae (see [Clause 7](#)).

3.1.13

$\bar{A}(t_1, t_2)$

average availability

(measure) average value of the availability $A(t)$ over a given interval $[t_1, t_2]$

Note 1 to entry: The mathematic definition is the following: $\bar{A}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(\tau) d\tau$

Note 2 to entry: When $t_1 = 0$ and $t_2 = T$ the average availability becomes $\bar{A}(T) = \frac{1}{T} \int_0^T A(\tau) d\tau$

Note 3 to entry: Mathematically speaking, the average availability is the mathematical expectation of the availability. It does not have the mathematical property of a normal probability and cannot be handled as such.

3.1.14

average unavailability

$\bar{U}(t_1, t_2)$

(measure) average value of the unavailability $U(t)$ over a given interval

Note 1 to entry: The average unavailability is the complementary of the average availability:

Note 2 to entry: $\bar{U}(t_1, t_2) = 1 - \bar{A}(t_1, t_2)$ or $\bar{U}(T) = 1 - \bar{A}(T)$

Note 3 to entry: The average unavailability is called “average Probability of Failure on Demand” (PFD_{avg}) by the standards related to functional safety of safety related/instrumented systems (e.g. IEC 61508[2]): $\text{PFD}_{\text{avg}} = \bar{U}(T)$ where T is the overall life duration of the system.

Note 4 to entry: Mathematically speaking, the average unavailability is the mathematical expectation of the unavailability. It does not have the mathematical property of a normal probability and cannot be handled as such.

Note 5 to entry: When dealing with safety $\bar{U}(T)$ is generally small compared to 1 and this property is used to develop approximated formulae (see [Clause 7](#)).

3.1.15 probability of failure on demand PFD

unavailability as per [3.1.12](#) in the functional safety standard terminology (e.g. IEC 61508[2])

Note 1 to entry: “Failure on demand” means here “failure likely to be observed when a demand occurs”. This encompasses both the failure occurred before the demand and the failure occurring due to the demand itself. Then this term needs not to be mixed up with the probability of a failure due to a demand (see [3.2.13](#)).

3.1.16 average probability of failure on demand PFD_{avg}

average unavailability as per [3.1.12](#) in the functional safety standard terminology (e.g. IEC 61508[2])

Note 1 to entry: “Failure on demand” means here “failure likely to be observed when a demand occurs”. PFD_{avg} encompasses both the failure occurred before the demand and the failure occurring due to the demand itself. Then this term needs not to be mixed up with the probability of a failure due to a demand (see [3.2.13](#)).

3.1.17 steady state availability asymptotic availability $\bar{A}$ or A_{as}

(measure) limit, when it exists, of the availability $A(t)$ when t goes to infinity

Note 1 to entry: The mathematical definition is the following: $\bar{A} = \lim_{t \rightarrow \infty} A(t)$

Note 2 to entry: Mathematically speaking, the steady-state availability is a probability and can be handled as such.

Note 3 to entry: When it exists, the steady-state availability is also the average availability over the interval $[0, \infty[$:

Note 4 to entry: $\bar{A} \equiv A(\infty) \equiv \bar{A}(T \rightarrow \infty) \equiv \bar{A}(t_1, t_2 \rightarrow \infty)$

Note 5 to entry: Average and steady-state availability should not be confused. The average availability exists in any cases but components with immediately revealed and quickly repaired failures reach quickly a steady-state; periodically tested components have no steady-state.

3.1.18 failure rate $\lambda(t)$

conditional probability per unit of time that the item fails between t and $t + dt$, provided that it works over $[0, t]$

Note 1 to entry: $\lambda(t)$ is the hazard rate of a reliability function: $R(t) = \exp(-\int_0^t \lambda(\tau) d\tau)$ and $\lambda(t) = -\frac{dR(t)}{R(t)dt} = \frac{f(t)}{1 - F(t)}$

Note 2 to entry: $\lambda(t)dt$ is the probability that the item fails between t and $t + dt$, provided that it has working over $[0, t]$. Therefore the failure rate is in relationship with the first failure of the related item.

Note 3 to entry: $\lambda(t)$ is a time-dependent parameter. It is generally accepted that it evolves accordingly a “bathtub” curve: decreasing during the early failures period, becoming (almost) constant during the useful life and increasing during the wear out period.

Note 4 to entry: When the failure rate is constant the following relationship holds: $\lambda(t) \equiv \lambda = \frac{1}{MTTF}$

Note 5 to entry: An individual component with a constant failure rate remains permanently “as good as new” until it fails suddenly, completely and without warnings. This is the characteristic of the so-called catalectic failures (see definition 3.2.9).

Note 6 to entry: The failure rate is linked to the failure density by the following relation:

Note 7 to entry: $\lambda(t) = f(t)/R(t) = w(t)/[1 - F(t)]$ (see [Annex C](#) for more details).

3.1.19

average failure rate

$\bar{\lambda}(t_1, t_2)$, $\bar{\lambda}(T)$

average value of the time-dependent failure rate over a given time interval

Note 1 to entry: The mathematical definition is the following: $\bar{\lambda}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \lambda(\tau) d\tau$ or $\bar{\lambda}(T) = \frac{1}{T} \int_0^T \lambda(\tau) d\tau$

Note 2 to entry: Mathematically speaking, the average failure rate is the mathematical expectation of the failure rate. It does not have the mathematical property of a failure rate as per 3.1.18 and cannot be handled as such.

3.1.20

asymptotic failure rate

λ^{as}

limit, when it exists, of the failure rate $\lambda(t)$ when t goes to infinity

Note 1 to entry: The mathematic definition is the following: $\lambda^{\text{as}} = \lim_{t \rightarrow \infty} \lambda(t)$

Note 2 to entry: Mathematically speaking, the asymptotic failure rate is a failure rate and it can be handled as such.

Note 3 to entry: When it exists, the asymptotic failure rate is also the average failure rate over the interval $[0, \infty[$:

Note 4 to entry: $\lambda^{\text{as}} \equiv \lambda(\infty) \equiv \bar{\lambda}(T \rightarrow \infty) \equiv \bar{\lambda}(t_1, t_2 \rightarrow \infty)$

Note 5 to entry: Average and asymptotic failure rate should not be confused. The average failure rate exists in any case, but:

— components with immediately revealed and quickly repaired failures reach quickly a steady-state corresponding to a constant asymptotic failure rate which is both, on the long term, an average failure rate as per [3.1.19](#) and a failure rate as per [3.1.18](#).

— periodically tested components have no steady-state and therefore the asymptotic failure rate just does not exist. The average of the failure rate can still be evaluated but this average has not the mathematical properties of a failure rate as per 3.1.18 (see also [Figure 32](#), [Figure 33](#) and [Figure 34](#)).

3.1.21

Vesely failure rate

conditional failure intensity

$\lambda_V(t)$

conditional probability per unit of time that the item fails between t and $t+dt$, provided that it was working at time 0 and at time t

Note 1 to entry: The Vesely failure rate is linked to the failure frequency by the following relation:

Note 2 to entry: $\lambda_V(t) = w(t)/A(t) = w(t)/[1 - U(t)]$ (see [Annex C](#) for more details)

Note 3 to entry: In the general case, the Vesely failure rate is not a failure rate as per 3.1.18 and cannot be used as such.

Note 4 to entry: In special cases (e.g. system with immediately revealed and quickly repaired failures), the Vesely failure rate reaches an asymptotic value which is also a good approximation of the asymptotic failure rate

$\lambda^{\text{as}} \approx \lambda_V^{\text{as}}$. In this case it can be used as a failure rate as per 3.1.18.

3.1.22

failure frequency

unconditional failure intensity

$w(t)$

conditional probability per unit of time that the item fails between t and $t+dt$, provided that it was working at time 0

Note 1 to entry: The failure frequency is linked to the Vesely failure rate by the following relation: $w(t) = \lambda_V(t)A(t) = \lambda_V(t)[1 - U(t)]$ (see [Annex C](#) for more details).

Note 2 to entry: $\lambda(t)$, $\lambda_V(t)$ and $w(t)$ should not be confused even if in particular cases they have the same numerical values.

Note 3 to entry: For highly available systems, $A(t) \approx 1$, the following relationship holds: $w(t) \approx \lambda_V(t)$

Note 4 to entry: When the Vesely failure rate reaches an asymptotic value the following relationship holds: $w^{as} \approx \lambda_V^{as} \approx \lambda^{as}$

3.1.23

average failure frequency

$\bar{w}(t_1, t_2)$, $\bar{w}(T)$, $\bar{w}$

average value of the time-dependent failure frequency over a given time interval

Note 1 to entry: The mathematical definition is the following: $\bar{w}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} w(\tau) d\tau$ or $\bar{w}(T) = \frac{1}{T} \int_0^T w(\tau) d\tau$

Note 2 to entry: The average failure frequency is also called "Probability of Failure per Hour" (PFH) by the standards related to functional safety of safety related/instrumented systems (e.g. IEC 61508^[2]): $PFH = \bar{w}(T)$ where T is the overall life duration of the system.

Note 3 to entry: Mathematically speaking, this is the mathematical expectation of the failure frequency. It does not have the mathematical property of a failure frequency as per 3.1.22 and cannot be handled as such.

3.1.24

PFH

DEPRECATED: probability of failure per hour

average failure frequency as [3.1.23](#) in the functional safety standard terminology (e.g. IEC 61508^[2] or IEC 61511^[3])

Note 1 to entry: The old meaning "Probability of Failure per Hour" is obsolete and replaced by "average failure frequency". Nevertheless PFH is still in use to keep the consistency with the previous versions of functional safety standards.

3.1.25

hazardous event frequency

accident frequency

$\Phi(t)$

failure frequency as [3.1.23](#) related to the hazardous event (or to the accident)

3.1.26

average hazardous event frequency

average accident frequency

$\bar{\Phi}(t_1, t_2)$, $\bar{\Phi}(T)$, $\bar{\Phi}$

average frequency as [3.1.23](#) related to of the hazardous event (or to the accident)

3.1.27

mean up time

MUT

expectation of the up time

Note 1 to entry: See [Figure 3](#) and also ISO 14224^[15] or IEC 60050-191^[14] for definitions of up time and down time.

[SOURCE: IEC 60050-191]

3.1.28 mean down time MDT expectation of the down time

Note 1 to entry: See [Figure 3](#) and also ISO 14224[15] or IEC 60050-191[14] for definitions of up time and down time.

[SOURCE: IEC 60050 -191]

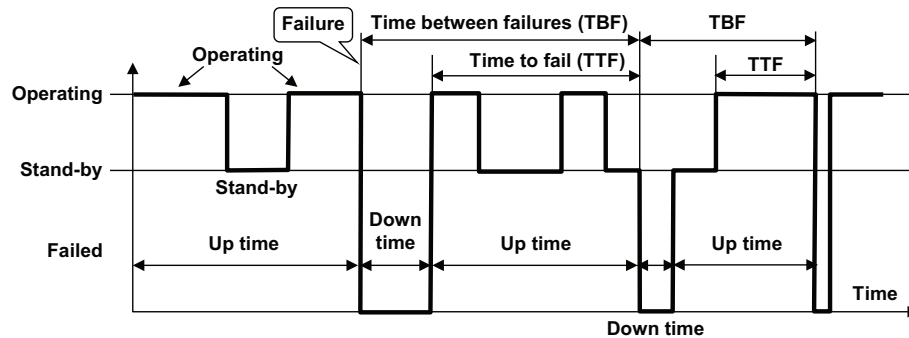


Figure 3 — Illustration of the general behaviour of an item over its lifetime

3.1.29 mean time to failure MTTF expected time before the item fails

Note 1 to entry: The MTTF is classically used to describe the time to failure for a non-repairable item or to the first failure for a repairable item. When the item is as good as new after a repair, it is also valid for the further failures (see [Figure 4](#)).

Note 2 to entry: In the cases illustrated by [Figure 4](#), the MTTF may be calculated by the following formulae:

$$MTTF = \int_0^{\infty} f(t) \cdot t \cdot dt = \int_0^{\infty} R(t) \cdot dt$$

Note 3 to entry: The following relationship holds when the failure rate is constant: $MTTF = 1/\lambda$.

Note 4 to entry: In the case illustrated by [Figure 3](#) where operating and stand-by failures are mixed, the formulae described in Note 2 to entry are no longer valid.

Note 5 to entry: The MTTF should not be mixed up with the design life time of the item.

Note 6 to entry: Sometimes it may be more understandable to express lifetime in probability of failure (i.e. unreliability, see [3.1.9](#)) during a certain lifespan.

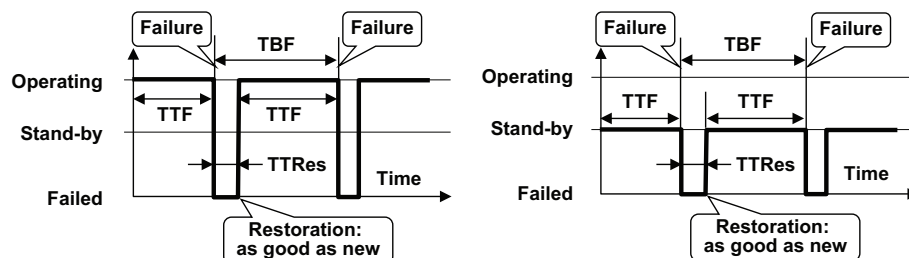


Figure 4 — Particular cases of the behaviour of an item over its lifetime

3.1.30

mean time between failures

MTBF

expected time between successive failures of a repairable item

Note 1 to entry: In the cases illustrated in [Figure 4](#), the MTBF is linked with MTTF and MTTRes by the following relationship: $MTBF = MTTF + MTTRes$. More generally It is also linked to the MUT and MDT by $MTBF = MUT + MDT$.

Note 2 to entry: The acronym MTBF is sometimes defined as the mean *operating* time between failures (e.g. in IEV191[14]). This is not at all the same and, in this case, the formula described in Note 1 to entry is no longer valid. This is very confusing, therefore the traditional definition of the MTBF is retained in this Technical Report.

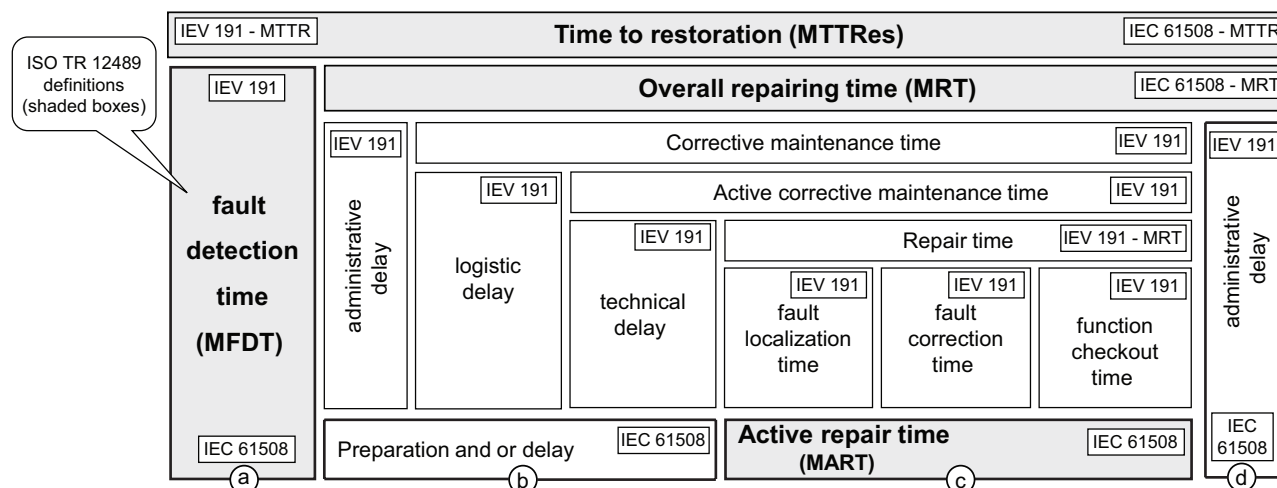


Figure 5 — Repair time taxonomies as per IEV 191[14], IEC 61508[2] and ISO/TR 12489

3.1.31

mean time to repair

MTTR

expected time to achieve the repair of a failed item

Note 1 to entry: This term MTTR is used in ISO 14224[15] and ISO 20815[16] where the fault detection time is not really considered: ISO 14224[15] deals with detected faults (in fact, the actual time spent to detect the fault is never known and cannot be collected); ISO 20815[16] deals mainly with immediately revealed failure where the time spent to detect the faults is close to 0 (i.e. negligible). As the fault detection time is very important for the purpose of this Technical Report there is a need to clearly distinguish between the two following times (cf. [Figure 5](#)):

- 1) the time elapsing from the actual occurrence of the failure of an item to its detection (cf. [3.1.35](#), MFDT);
- 2) the time elapsing from the detection of the failure of an item to the restoration of its function (cf. [3.1.33](#), MRT).

Note 2 to entry: The acronym MTTR is defined as the mean time to restore in the IEC 60500-191[14] or in the IEC 61508[2]. This is not the same as in ISO 14224[15] or ISO 20815[16]. Therefore, in order to avoid any mixed-up, the acronym MTTRes is used in this Technical Report instead of MTTR (cf. [3.1.32](#)).

3.1.32

mean time to restoration

MTTRes

expected time to achieve the following actions: (see [Figure 5](#), [Figure 6](#) and [Figure 7](#)):

- the time to detect the failure a; and,
- the time spent before starting the repair b; and,
- the effective time to repair c; and,
- the time before the component is made available to be put back into operation d

Note 1 to entry: [Figure 5](#) illustrates how the times a, b, c and d defined in the IEC 61508[2] standard are linked to the delays defined in the IEC 60050-191[14] standard. Time b starts at the end of a; time c starts at the end of b; time d starts at the end of c.

Note 2 to entry: [Figure 5](#), [Figure 6](#) and [Figure 7](#) can be used to understand the differences between the definitions of MTTRes, MRT and MART used in this Technical Report.

Note 3 to entry: The MTTRes is linked to the MRT and the MFDT by the following formula: $MTTRes = MFDT + MRT$.

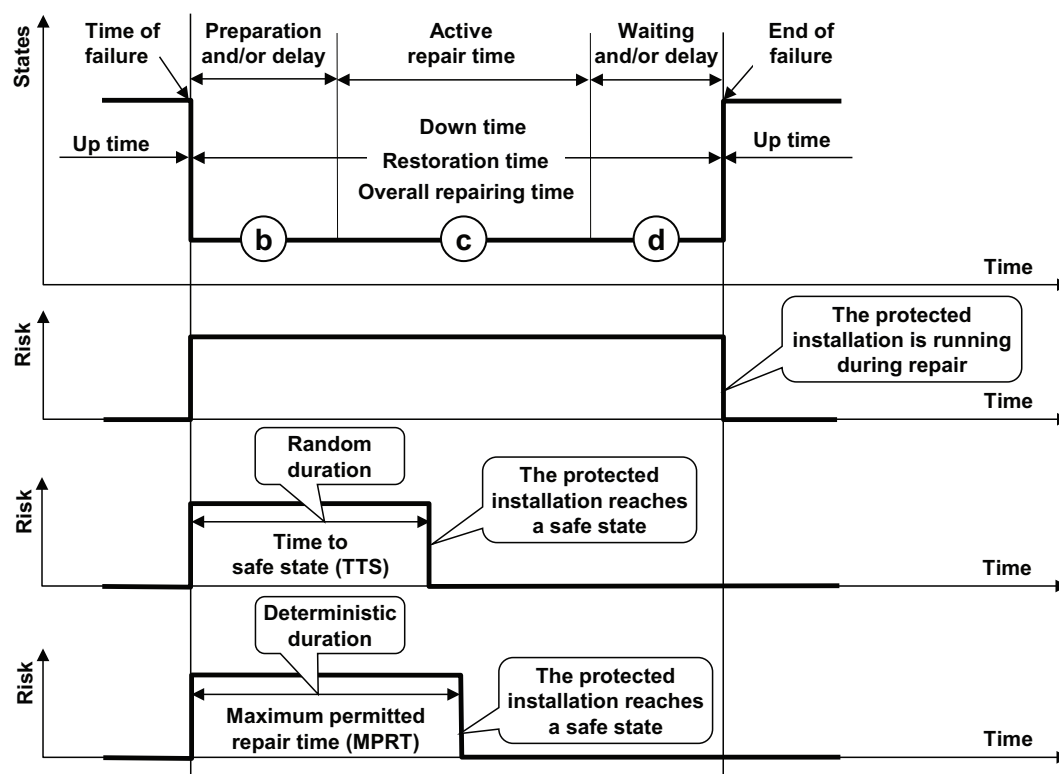


Figure 6 — Illustration of the restoration time and of the risk exposure for immediately revealed failures of an item

3.1.33

MRT

mean overall repairing time

expected time to achieve the following actions:

- the time spent before starting the repair b; and,
- the effective time to repair c; and,
- the time before the component is made available to be is put back into operation d

Note 1 to entry: See [Figure 5](#), [Figure 6](#) and [Figure 7](#).

Note 2 to entry: The terms “repair”, “repairable”, “repaired” used in this Technical Report, unless otherwise specified, are related to the overall repairing time (see [Figure 5](#)).

Note 3 to entry: When a safety system operating in demand mode is faulty, the risk disappears as soon as the protected installation is placed in a safe state (e.g. stopped). In this case (see [Figure 6](#) and [Figure 7](#)) the MTTS replaces the MRT (see [3.1.36](#)) with regard to the probabilistic calculations.

Note 4 to entry: This definition is in line with IEC 61508[2] but not with IEC 60050-191.[14]

3.1.34

mean active repair time

MART

expected active repair time

Note 1 to entry: The MART is the expected effective time to repair c, (see [Figure 5](#), [Figure 6](#) and [Figure 7](#)).

3.1.35

mean fault detection time

MFDT

expected time needed to detect a fault

Note 1 to entry: The MFDT is the time a) in [Figure 5](#), [Figure 6](#) and [Figure 7](#).

Note 2 to entry: The MFDT is equal to zero for immediately revealed failure; (see [Figure 6](#)) generally negligible for quickly detected failures; (see [Figure 6](#)) depending of the test policy for the hidden failures. In this case it may be the main part of the item down time (see [Figure 7](#)).

Note 3 to entry: The MFDT used in this Technical Report should not be mixed-up with the mean fractional dead time which has the same acronym.

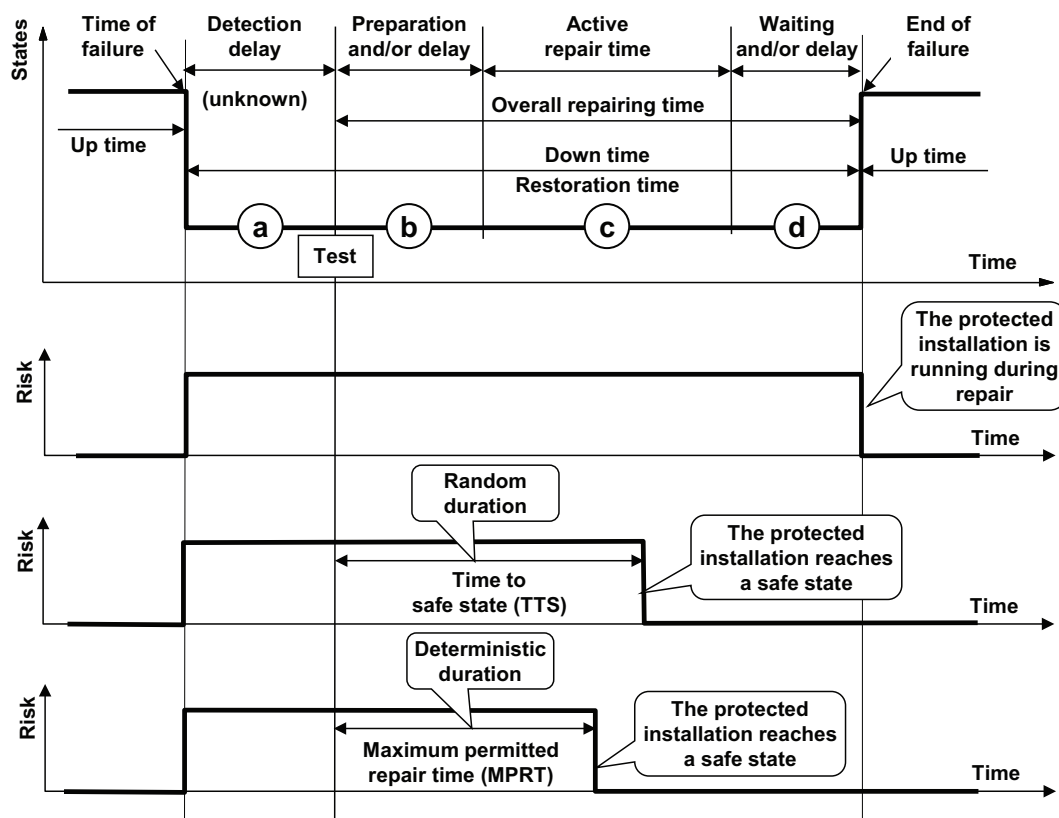


Figure 7 — Illustration of the restoration time and of the risk exposure for the hidden failures of an item

3.1.36

MTTS

mean time to safe state

expected time needed for the protected installation to reach a safe state after a dangerous failure of a safety system has been detected

EXAMPLE When a dangerous fault is revealed for a safety system operating in demand mode, it may be decided to reach a safe state rather than undertake the repair of the fault and this may take some time: a MTTS of 8 h means, for example, that, on average, 8 h are needed to shut down the process. After the shut down, a safe state is reached, the fault is no longer dangerous and it is not necessary to take into account the remaining time spent to complete the repair. This is illustrated in [Figure 6](#), [Figure 7](#) and [Figure B.1](#).

Note 1 to entry: When the MTTS is defined as a maintenance procedure it is necessary to take it into consideration for the probabilistic calculations of hazardous events. In this case the MTTS replaces the MRT (see [3.1.33](#)) with regard to the probabilistic calculations. Reciprocally it is necessary to verify that this MTTS is respected during the actual repair actions in order to keep the probabilistic calculations valid.

Note 2 to entry: The role of the MTTS is close to the role of the MPRT. The difference is that the MPRT is a maximum duration allowed to reach a safe state when the MTTS is the average of the random duration of the TTS needed to reach the safe state when a dangerous fault is revealed (see [Figure 6](#) and [Figure 7](#)). The methods developed in this Technical Report have been focused on average random values (MTTRes, MRT, MTTS) rather than on deterministic values (MPRT), but the MPRT can be easily handled by using Petri nets and Monte Carlo simulations.

3.1.37

maximum permitted repair time

MPRT

maximum time allowed to repair a fault before undertaking an action to make the risk disappearing

EXAMPLE When a dangerous fault is revealed for a safety system operating in demand mode, it may be decided to reach a safe state when a maximum duration has elapsed: a MPRT of 8 h means, for example, that if the repair is not completed after 8 h, the process is shut down. Then a safe state is reached, the fault is no longer dangerous, and it is not necessary to take into account the remaining time spent to complete the repair. This is illustrated in [Figure 6](#), [Figure 7](#) and [Figure B.1](#). When the fault may result of several failure modes, the MPRT allows to repair those within short MRT without shutdown of the process.

Note 1 to entry: When a MPRT is defined as a maintenance procedure it is necessary to take it into consideration for the probabilistic calculations of hazardous events. Reciprocally it is necessary that this MPRT be respected during the actual repair actions in order to keep the probabilistic calculations valid.

Note 2 to entry: The role of the MPRT is close to the role of the MTTS (see 0). The difference is that the MPRT is a maximum duration allowed to reach a safe state and the MTTS is the average duration needed to reach the safe state when a dangerous fault is revealed (see [Figure 6](#) and [Figure 7](#)). The methods developed in this Technical Report have been focused on random repair values (MTTRes, MRT, MTTS) rather than on deterministic values (MPRT), but the MPRT can be easily handled by using Petri nets and Monte Carlo simulations.

3.1.38

mean time to demand

MTTD

expected time before the demand on the safety system occurs

3.1.39

restoration rate

μ

conditional probability per unit of time that the restoration of a failed item ends between t and $t+dt$, provided that it was not finished over $[0, t]$

Note 1 to entry: The following relationship holds when the restoration rate is constant: $MTTRes = 1/\mu$.

Note 2 to entry: The “restoration” rate is in relationship with the restoration time. Similarly the “repairing” rate can be defined in relationship with the “overall repairing” time and the “active repair” rate in relationship with the “active repair” time.

Note 3 to entry: The restoration rate has the same mathematical properties for the restoration as the failure rate for the failures.

3.2 Failure classification

Explanations about the various states and the various failures of a safety system are developed in [Annex B](#).

3.2.1

failure

loss of ability to perform as required

Note 1 to entry: A failure of an item is an event, as distinct from a fault of an item, which is a state (see [Figure 8](#)).

[SOURCE: IEC 60050 –191]

3.2.2

fault

inability to perform as required

Note 1 to entry: A fault of an item is a state, as distinct from a failure of an item which is an event (see [Figure 8](#)).

Note 2 to entry: A fault of an item may result from a failure of the item or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance.

Note 3 to entry: Qualifying terms may be used to indicate the cause of a fault, such as specification, design, manufacture, maintenance or misuse.

Note 4 to entry: Inability to perform due to preventive maintenance, other planned actions, or lack of external resources does not constitute a fault.

Note 5 to entry: [Figure 8](#) illustrate the relationship between the concepts of failure and fault:

- The *Failure x* occurs at stage 1 and leads to the state *Fault x* which is not detected.
- from stage 2 point of view *Fault x* is a pre-existing fault.
- The *Failure y* occurs at stage 2 and lead to the state *Faults x,y* which is not detected.
- From stage 3 point of view *Fault x,y* is a pre-existing fault.
- and so on.

[SOURCE: IEC 60050 –191]

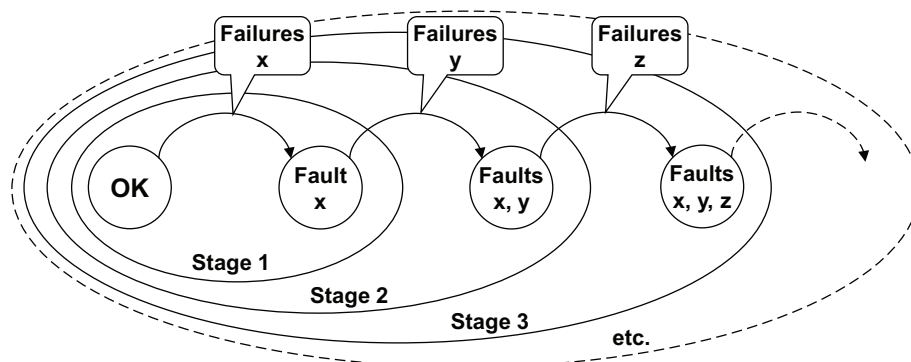


Figure 8 — Relationship between failure and fault concepts

3.2.3

dangerous failure

unsafe failure

failure of a safety system which tends to impede a given safety action

Note 1 to entry: This is a systemic failure in relationship with a given safety action performed by the safety system. Therefore this concept is irrelevant for an individual item on the shelves.

Note 2 to entry: See [Figure B.1](#).

3.2.4

critical dangerous failure

dangerous failure leading to the complete inhibition of the safety action (i.e. leading to a dangerous situation for the protected system)

Note 1 to entry: This is a systemic failure in relationship with a given safety action performed by the safety system. Therefore this concept is irrelevant for an individual item on the shelves.

Note 2 to entry: The same failure of a component belonging to a safety system with internal redundancy may be dangerous or critical dangerous depending on the system state from which it occurs.

Note 3 to entry: The critical dangerous failures that are undetected (e.g. those revealed by periodic tests) are sometimes called *safety critical failures* (cf. ISO 14224[15]). The equipment subject to such potential failures can be identified within a plant and monitored, and the ratio between the number of safety critical failures detected by periodic tests and the corresponding number of tests performed (commonly called "*failure fraction*") is being used for that purpose. This indicator of the average unavailability (PFDavg) due to dangerous undetected failures is established by using test reports. It is important not to mix such failure fraction with other reliability terms.

3.2.5

safe failure

failure of a safety system which tends to favour a given safety action

Note 1 to entry: The concept of safe failure is illustrated in [Figure B.1](#).

Note 2 to entry: A failure is safe only with regard to a given safety function. This is a systemic failure in relationship with a given safety action performed by the safety system. This concept is irrelevant for an individual item on the shelves.

Note 3 to entry: The non-critical safe failures basically increase the probability of success of the safety function. The critical safe failures initiate the related safety actions when this is not needed (see spurious failures).

3.2.6

spurious failure

failure triggering an action in an untimely manner

Note 1 to entry: Critical safe failures (see [Figure B.1](#)) are the typical spurious failures related to safety systems.

Note 2 to entry: A spurious failure does not necessarily imply a spurious trip ([3.4.14](#)) but a spurious trip is always the result of a spurious failure.

3.2.7

critical safe failure

spurious failure of a safety system, due to safe failure(s) of its component(s), triggering the safety action and leading to a spurious safety action

Note 1 to entry: The concept of critical safe failure is illustrated in [Figure B.1](#).

Note 2 to entry: This is a systemic failure in relationship with a given safety action performed by the safety system. This concept is irrelevant for an individual item on the shelves.

Note 3 to entry: The same failure of a component belonging to a safety system may be safe or spurious (critical safe) depending of the system state from which it occurs (e.g. the safe failure of a sensor belonging to 2oo3 is only safe when it occurs in 1st position. It is critical when it occurs in 2nd position).

3.2.8 systemic failure

holistic failure

failure at system level which cannot be simply described from the individual component failures of the system

Note 1 to entry: Systemic/holistic principles have been concisely summarized by Aristotle by "*The whole is more than the sum of its parts*".

Note 2 to entry: Components have only failure modes. Those failure modes become dangerous, safe or spurious only when the components are implemented into a safety "system". This is why dangerous, safe or spurious failures are typical systemic failures. For example the failure "fail to close" of a valve is dangerous only if it belongs to a safety system closing this valve on demand. Otherwise this failure mode does not matter.

Note 3 to entry: "Systematic" failures (i.e. occurring in a deterministic way when given conditions are encountered, see [3.2.17](#)) and "systemic" failures should not be confused.

3.2.9 catalectic failure

sudden and complete failure

Note 1 to entry: This term has been introduced by analogy with the catalectic verses (i.e. a verse with seven feet instead of eight) which stop abruptly. Then, a catalectic failure occurs without warning and is more or less impossible to forecast by examining the item. It is the contrary of failures occurring progressively and incompletely.

Note 2 to entry: Catalectic failures characterize simple components with constant failure rates (exponential law): they remain permanently "as good as new" until they fail suddenly, completely and without warning. Most of the probabilistic models used in reliability engineering are based on catalectic failures of the individual component of the system under study (e.g. Markovian approach).

3.2.10 immediately revealed failure

overt failure

detected failure

evident failure

failure which is immediately evident to operations and maintenance personnel as soon as it occurs

Note 1 to entry: The immediately revealed failures show themselves immediately, but the hidden failures which are quickly detected by specific diagnostic tests are generally considered as immediately revealed failures.

Note 2 to entry: The repair of immediately revealed failures may begin immediately after they have occurred.

Note 3 to entry: The failures which are detected by periodic tests are not considered as immediately revealed failures.

3.2.11 hidden failure

covert failure

dormant failure

unrevealed failure

undetected failure

failure which is not immediately evident to operations and maintenance personnel

Note 1 to entry: Hidden failures do not show themselves when they occur. The occurrence of a hidden failure gives a latent fault which may be revealed by specific tests (e.g. periodic tests) or by the failure of the item to perform its function when required.

Note 2 to entry: The repair of hidden failures cannot begin as long as they have not been detected. The unknown times spent between the failures and their detections belong to the MTTRes.

3.2.12

time-dependent failure

failure occurring with a probability depending of the time

Note 1 to entry: The unreliability $F(t)$ is a typical probability function describing time-dependent failures

3.2.13

failure due to demand

failure occurring on demand

γ , ψ

failure of one item due to a change of its state triggered by an external event (the so-called “demand”)

EXAMPLE 1 Obtaining 2 when launching a dice is an event occurring on demand. The probability of this event is 1/6. It does not depend on the elapsing time but only of the demand itself (i.e. the fact that the dice is launched).

EXAMPLE 2 The failure of an electromechanical relay (e.g. rupture of the spring) when it changes state depends on the number of operations (cycles) rather on the operating time (see IEC 61810-2[49]) and this is the same for the failure of an electronic device due to over voltage when it is switched or the blocking of a diesel engine when it is started, etc.: these are typical examples of failures due to demands (or cycles).

Note 1 to entry: In this Technical Report two kinds of demand are considered: the periodic tests and the demand for an actual safety action. The probability of a failure due to periodic test is a constant number noted γ and the probability of a failure due to one actual demand of the safety action is a constant number noted ψ . Over a given time interval, those probabilities of failure do not depend on the duration but on the number of demands or tests occurring within this interval. The use of γ and ψ is explained in 7.3.

Note 2 to entry: This should not be confused with the “failure on demand” appearing in the term “probability of failure on demand” (see 3.1.14, Note 2 to entry) used in functional safety standards[2] for low demand mode safety systems. In those standards this means “failures *likely to be observed when* a demand occurs”.

3.2.14

common cause failures

CCF

failures of different items, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: It is generally accepted that the failures occur simultaneously or within a short time of each other.

Note 2 to entry: Common cause failures can lead to common mode failures.

Note 3 to entry: Common cause failures reduce the effect of system redundancy.

Note 4 to entry: Explicit and implicit CCF are defined in 5.4.2.

3.2.15

common mode failures

CMF

failures of different items, occurring in the same way

Note 1 to entry: Common mode failures may have different causes.

Note 2 to entry: Common mode failures can be due to common cause failures.

3.2.16

random failure

failure, occurring in a random way

Note 1 to entry: A random failure may be time or demand dependent. Whether it occurs or not is not predictable with certainty but the corresponding failure rate (see 3.1.18) or probability of a failure due to demand (see 3.2.13) may be predictable and this allows probabilistic calculations.

EXAMPLE Examples of failure mechanisms leading to unpredictable failure occurrence are: hardware random failures resulting from degradation mechanisms; human random failure resulting from error in routine operation, lack of attention, stress, tiredness, etc.

Note 2 to entry: From the probabilistic point of view, the random failures are the contrary of systematic failures (see [3.2.17](#)) which occur in a deterministic way (i.e. with a probability equal to 1) when some conditions are met.

3.2.17

systematic failure

failure that consistently occurs under particular conditions of handling, storage or use

Note 1 to entry: The cause of a systematic failure originates in the specification, design, manufacture, installation, operation or maintenance. Its occurrence is precipitated by particular conditions of handling, storage, use or maintenance (see [Figure G.3](#))

Note 2 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 3 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, e.g. in verifying the failure cause (from IEC 60050-191 ed3[14]). Systematic failures are non-random failures (see [3.2.16](#)).

Note 4 to entry: In operation, a systematic failure is a manifestation of a systematic fault (i.e. a pre-existing state of the system).

Note 5 to entry: The software systematic failures, called “bugs”, are example of systematic failures: they are due to pre-existing bugs (i.e. faults) and they occur when the input data activate them.

Note 6 to entry: Systematic and systemic (which means “at system level”) failures (see [3.2.8](#)) should not be confused.

[SOURCE: IEC 60050-191]

3.3 Safety systems typology

3.3.1

demand mode of operation safety systems

safety system designed to achieve its safety action only when receiving a specific request from its surrounding environment

Note 1 to entry: Such systems spend most of their time in stand-by position but need nevertheless to be ready to work as soon as a demand occurs.

Note 2 to entry: Such systems are subject to hidden failures. Diagnostic and periodic tests are generally implemented in order to reveal the corresponding latent faults.

Note 3 to entry: When the demand frequency increases, an on-demand mode safety system may be assimilated to a continuous mode of operation systems.

3.3.2

continuous mode of operation safety system

safety system designed to achieve its safety action permanently

Note 1 to entry: With a continuous mode safety system the hazardous event occurs as soon as the safety system fails. This is illustrated in [Figure B.1](#) where the systems states “KO” and “hazardous event” are gathered into a single state.

3.3.3

multiple safety systems

safety system comprising several sub safety systems operating one after the other when the prior ones have failed

Note 1 to entry: Industrial processes often implement multiple safety systems (safety layers). In this case the failure of an intermediate safety layer provokes a demand on the proximate succeeding safety layer and so on. The accident occurs only if the demand is transmitted until the ultimate safety layer and it fails to operate.

3.4 Maintenance issues

3.4.1

maintenance

combination of all technical and administrative actions, including supervisory actions, intended to retain an item in, or restore it to, a state in which it can perform a required function

Note 1 to entry: There are two basic categories of maintenance: corrective maintenance done after a failure has occurred and preventive maintenance (testing, inspection, condition monitoring, periodic) done before a failure has occurred. See also ISO 14224^[15], 9.6.

Note 2 to entry: Maintenance activities of either preventive or corrective maintenance category type, is shown in ISO 14224:2006^[15], Table B.5.

[SOURCE: ISO 14224]

3.4.2

maintenance concept

definition of the maintenance echelons, indenture levels, maintenance levels, maintenance support, and their interrelationships

Note 1 to entry: The maintenance concept provides the basis for maintenance planning, determining supportability requirements and developing logistic support.

Note 2 to entry: A maintenance echelon is a position in an organization where specified levels of maintenance are to be carried out (e.g. field, repair shop, manufacturer facility).

[SOURCE: IEC 60050-191]

3.4.3

preventive maintenance

PM

maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item

[SOURCE: ISO 14224]

3.4.4

corrective maintenance

maintenance carried out after fault detection to effect restoration

Note 1 to entry: Corrective maintenance of software invariably involves some modification.

Note 2 to entry: Sometimes the *corrective maintenance* is also called *curative maintenance*.

[SOURCE: IEC 60050-191-46-06]

3.4.5

detection method

method or activity by which a failure is discovered

Note 1 to entry: A categorization of detection methods (e.g. periodic testing or continuous condition monitoring) is shown in ISO 14224:2006^[15], Table B.4.

3.4.6

maintenance plan

structured and documented set of tasks that include the activities, procedures, resources and the time scale required to carry out maintenance

Note 1 to entry: The maintenance plan should be thoroughly analysed and modelled to produce relevant probabilistic results.

Note 2 to entry: The forecasted probabilistic results established at the design stage are no longer valid if the maintenance plan which has been considered is not thoroughly applied in operation.

Note 3 to entry: The maintenance plan should cover policies for both preventive maintenance (e.g. testing) and corrective maintenance (e.g. minimize downtime, restore lost redundancy).

Note 4 to entry: The maintenance plan is part of an overall Operations and Maintenance plan. It is sometimes called "*maintenance policy*".

[SOURCE: EN 13306]

3.4.7 test policy

set of procedures describing the various test operations (frequencies and procedures) scheduled to reach the safety requirements of a given safety system

Note 1 to entry: The test policy should be thoroughly analysed and modelled to produce relevant probabilistic results.

Note 2 to entry: The forecasted probabilistic results established at the design stage are no longer valid if the test policy which has been considered is not thoroughly applied in operation.

3.4.8 periodic tests

proof tests

planned operation performed at constant time interval in order to detect the potential hidden failures which may have occurred in the meantime

Note 1 to entry: The unsafe hidden failures of a safety system which are not detected by the diagnostic tests may be detected by periodic tests. Such tests are named "proof tests" in the standards dealing with functional safety (e.g. IEC 61508[2]).

[SOURCE: IEC 61508]

3.4.9 diagnostic tests

automatic operations performed at high frequency in order to detect the potential hidden failures as soon as possible when they occur

Note 1 to entry: The unsafe failures of safety system are generally hidden and diagnostic tests may be implemented to detect the larger part of them. As the diagnostic cycle is normally short, the hidden failures detected by diagnostic tests are assimilated to immediately revealed failures.

[SOURCE: IEC 61508]

3.4.10 staggered testing (of redundant items)

test of several items with the same test interval but not at the same time

EXAMPLE [Figure 9](#) shows staggered tests for two item A and B.

Note 1 to entry: When the redundant components of a system are tested at the same time (i.e. when the tests are synchronous) their availabilities are good (just after a test) and bad (just before a test) at the same time. This correlation means that the unavailabilities of the components peak simultaneously. This has a detrimental effect on the system availability which can be cancelled by de-synchronizing the tests. A practical way to do that is staggering the tests (e.g. testing one component in the middle of the test interval of the other); the unavailability peaks are also staggered and this improves the average availability of the system.

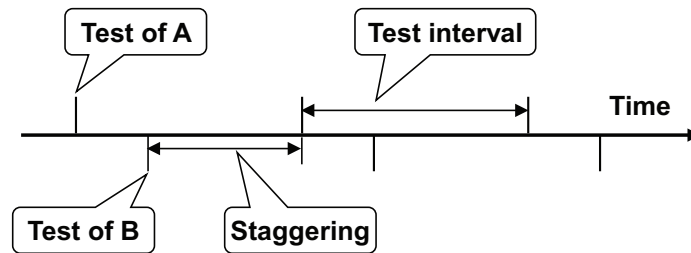


Figure 9 — Example of test staggering for a system made of two redundant items A and B

3.4.11

redundancy

existence of more than one means for performing a required function

Note 1 to entry: The aim of redundancy is to provide backup in case of one or several failures of the means performing a required function.

Note 2 to entry: Redundancy definitions for passive (cold) standby, active (hot) standby and mixed are given in ISO 14224[15], C.1.2.

Note 3 to entry: Redundancy is sometimes (in IEC 61508[2] and IEC 61511[3]) called “fault tolerance”.

[SOURCE: ISO 14224]

3.4.12

spurious activation (of a safety function)

untimely demand of a safety function when this is not needed

Note 1 to entry: The spurious activation of a safety function may be due to the occurrence of one or several safe failures.

3.4.13

spurious action (of a safety system)

result of a spurious activation of a safety function

Note 1 to entry: A spurious safety action is not necessary safe. An example of spurious action is a spurious trip.

3.4.14

trip

shutdown of machinery from normal operating condition to full stop

Note 1 to entry: Two types of shutdown can be identified:

- a) Trip: the shutdown is activated automatically by the control/monitoring system.
 - Real trip: the shutdown is activated as a result of a monitored (or calculated) value in the control system exceeding a pre-set limit.
 - Spurious trip: unexpected shutdown resulting from failure(s) in the control/monitoring system or error(s) imposed by on control/monitoring system originating from the environment or people.
- b) Manual shutdown: the machinery is stopped by an intended action of the operator (locally or from the control room).

Note 2 to entry: Sometimes statements like “equipment trip” or “spurious trip” can be misleading terminology used for failures causing (rotating) equipment shutdown, especially when it is treated as failure mode in reliability data or modelling. A failure mechanism (see Table B.2 of ISO 14224[15]) can be of various types (e.g. mechanical, instrument) and should not be mixed with the term failure modes (of which one is spurious trip). Failure modes are not necessarily instrument-related failures, but could be mechanical failures. See for example failure modes in Table B.6 of ISO 14224[15] for rotating equipment.

[SOURCE: ISO 14224]

3.4.15

reliability data

data for reliability, maintainability and maintenance support performance

Note 1 to entry: Reliability and maintainability (RM) data is the term applied by ISO 14224[15].

[SOURCE: ISO 20815]

3.4.16

generic reliability data

reliability data covering families of similar equipment

Note 1 to entry: See ISO 14224[15] for further details on equipment boundaries and equipment taxonomies that define these families of equipment within the petroleum, petrochemical and natural gas industries.

Note 2 to entry: Plant-specific data on specific equipment could be part of generic reliability databases, but could differ a lot from generic data and should not be mixed with those.

[SOURCE: ISO 14224]

3.5 Other terms

3.5.1

critical state

in a states-transitions model, state belonging to a given class of states and which is distant from the failure class of states by only one transition

Note 1 to entry: This is a mathematical concept in relationship with e.g. Markovian process or Petri nets models.

EXAMPLE The states of a safety system can be sorted out into two classes: class OK when the safety action is available and KO when the safety action is inhibited. In this case a critical state with regards to the safety system failure belongs to the class *OK* and only one failure (i.e. on event) is needed to have a transition to the class *KO*.

3.5.2

dysfunction

impaired or abnormal functioning of an item

Note 1 to entry: This term is built from the Greek prefix “dys” (i.e. “with difficulty”) and the Latin term “functio” (i.e. an activity with a given aim). Primarily used in the medical field, this term is now often used within the technological field as a more generic term than “failure” or “fault”.

3.5.3

dysfunctioning analysis

set of activities aiming to analyse the dysfunctions of an item

Note 1 to entry: This is the counterpart of the functioning analysis which aims to analyse how an item works when the dysfunctioning analysis aims to analyse how an item fails by e.g. identifying, sorting out, characterizing and/or evaluating the probability of occurrence of the dysfunctions.

Note 2 to entry: The term “dysfunctional” analysis is often used as a synonym of “dysfunctioning” analysis.

3.5.4

formal language

set of words, semantics and logical rules with sound mathematical properties

Note 1 to entry: Programming languages are an example of formal language with mathematical properties allowing them to be compiled into computer executable code.

Note 2 to entry: Every reliability model has an underlying formal language behind the graphical elements (e.g. the Binary logic for Boolean models).

Note 3 to entry: Specific formal languages have been developed to model the functioning and the dysfunctioning of industrial systems (e.g. AltaRica^{[11][12]}). According to their powerfulness of modelling and their mathematical properties they can be compiled toward event trees, fault trees, Markov graphs, Petri nets, accident sequences, etc. Some of them can also be directly used for Monte Carlo simulation.

3.5.5

functioning analysis

set of activities aiming to analyse how an item performs as required

Note 1 to entry: This is the counterpart of the dysfunctioning analysis which aims to analyse how an item fails when the functioning analysis aims to analyse how an item works by, e.g. identifying, sorting out and characterizing the various functions related to the item.

Note 2 to entry: The term “functional” analysis is often used as a synonym of “functioning” analysis. However, the term “functional analysis” which has several meanings is not used in this Technical Report to avoid confusion.

3.6 Equipment-related terms

3.6.1

high integrity protection system

HIPS

non-conventional autonomous safety instrumented system with sufficiently high safety integrity (see [3.2.1](#)) to protect equipment against exceeding the design parameters

Note 1 to entry: Deviations from industry standards describing mechanical protection systems (e.g. ISO 23251^[31] = API STD 521^[32], ISO 10418^[33], API RP 14C^[58]) are treated as HIPS. An ultimate protection relying solely on Safety Instrumented Systems (SIS) is qualified as HIPS, irrespective of its required Safety Integrity Level (SIL).

3.6.2

high integrity pressure protection system

HIPPS

HIPS exclusively devoted to protection against overpressure

Note 1 to entry: Alternative terminology: over pressure protection system (OPPS).

Note 2 to entry: A HIPPS can be used as an alternative to, e.g.:

- full pressure rating of downstream equipment, or
- adequately sized mechanical pressure relief devices, or
- design the disposal system for simultaneous reliefs.

3.6.3

HIPPS valve

valve used as a final element in a HIPPS system

3.6.4

subsea isolation valve

SSIV

SIV

valve which closes within a defined time limit derived from the risk assessment in order to reduce consequences of pipeline/riser leak or rupture

Note 1 to entry: The SSIV can be an actuated valve (e.g. remotely controlled subsea valve) or a non-activated valve (subsea check valve). An activated valve is normally designed as fail safe (i.e. closes and remains closed on all failures external to the valve and actuator themselves).

Note 2 to entry: Where the flexible risers are connected directly to the subsea wellhead, the master and wing valve may be considered to represent the SSIV function.

[SOURCE: ISO 14723]

3.6.5

subsurface safety valve

SSSV

device installed in a well below the wellhead with the design function to prevent uncontrolled well flow when actuated

Note 1 to entry: These devices can be installed and retrieved by wireline (Wireline retrievable) and/or pump down methods (TFL-Thru Flow Line) or be integral part of the tubing string (Tubing retrievable).

3.6.6

surface-controlled subsurface safety valve

SCSSV

SSSV controlled from the surface by hydraulic, electrical, mechanical or other means

Note 1 to entry: The SCSSV is sometimes called DHSV (downhole safety valve).

[SOURCE: ISO 14723]

3.6.7

subsurface-controlled subsurface safety valve

SSCSV

SSSV actuated by the characteristics of the well itself

Note 1 to entry: Note 1 to entry: These devices are usually actuated by the differential pressure through the SSCSV (velocity type) or by tubing pressure at the SSCSV (high or low pressure type).

[SOURCE: ISO 14723]

3.6.8

SSSV system equipment

components which include the surface-control system, control line, SSSV, safety valve lock, safety valve landing nipple, flow couplings and other downhole control components

[SOURCE: ISO 10417]

4 Symbols and abbreviated terms

Table 2 — Acronyms used in ISO/TR 12489

Acronyms	Meaning
AC, DC, UPS	Alternative or Direct Current, Uninterruptible Power Supply
APJ	Absolute Probability Judgement
ATHEANA	A Technique for Human Error Analysis
CCF	Common Cause Failure
CMF	Common Mode Failure
CREAM	Cognitive Reliability and Error Analysis Method
FMECA	Failure Modes, Effects and Criticality Analysis
FMEA	Failure Modes and Effects Analysis
FT, FTA	Fault Tree, Fault Tree Analysis
HAZID, HAZOP	HAZard IDentification, HAZard and OPerability study
HIPS	High Integrity Protection System
HIPPS	High Integrity Pressure Protection System
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability

Table 2 (continued)

Acronyms	Meaning
HRA	Human Reliability Analysis
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISO	International Organization for Standardization
LOPA	Layer Of Protection Analysis
MDT	Mean Down Time
MART, MRT	Mean Active Repair Time, Mean Repairing Time
MFDT	Mean Fault Detection Time
MPRT	Maximum Permitted Repair Time
MTBF	Mean Time Between Failures
MTTD	Mean Time to Demand
MTTE, MTTR, MTTRes	Mean Time to Fail, Mean Time to Repair, Mean Time To Restore
MTTS	Mean Time To Safe state
MUT	Mean Up Time
OPPS	Over Pressure Protection System
PC	Paired Comparisons
PDS	Reliability of computer-based safety systems (Norwegian)
PFD, PFD _{avg}	Probability of Failure on Demand, Average PFD
PFH	Probability of Failure per Hour (average dangerous failure frequency)
PHA	Preliminary Hazard Analysis
PN	Petri net
RBD	Reliability Block Diagram
SCSSV	Surface-Controlled Subsurface Safety Valve
SDT	Signal Detection Theory
SDV	Shut Down Valve
SIL, SIS	Safety Integrity Level, Safety Instrumented Systems
SLIM-MAUD	Success Likelihood Index Method using Multi-Attribute Utility Decomposition
SSCSV	Subsurface-controlled Subsurface Safety Valve
SSSV	Subsurface Safety Valve
SSIV, SIV	SubSea Isolation Valve
THERP	Technique for Human Error Rate Prediction
TR	Technical Report
TBF, TTF, TTRes	Time Between failures, Time To Failure, Time To Restore
TTS	Time to Safe State

Table 3 — Symbols used in ISO/TR 12489

Symbol	Definition
Time-related symbols	
T	Duration
$t, t_i, [t_1, t_2]$	Instants and interval of time
Event-related symbols	

Table 3 (continued)

Symbol	Definition
C (any letter)	Components C
E (any letter)	Event
$\bar{E}$ or $\neg E$	Complementary event
$e = \text{"true"} \text{ or } \text{"false"}$	Boolean variable indicating the state of an event.
$\{A\}, \{A, B\}, \{A, B, C\}, \dots$ $A \cap B, A \cap B \cap C, \dots$ $A \bullet B, A \bullet B \bullet C$	Combination of events
$??x == Fct(y, z, \dots)$ $??x > Fct(y, z, \dots)$	"Predicates" used in Petri net (see M.1): general form (x: any kind of variable, $Fct(.)$: any kind of function of other variable)
$??E == \text{"true"} \text{ or } ?E,$ $??E == \text{"false"} \text{ or } ?\neg E,$	"Predicates" used in Petri nets for Boolean variable (see M.1)
$!!x = Fct(y, z, \dots)$	"Assertions" used in Petri net (see M.1): general form (x: any kind of variable, $Fct(.)$: any kind of function of other variable)
$!!E = \text{"true"} \text{ or } !E,$ $!!E = \text{"false"} \text{ or } !\neg E,$	"Assertions" used in Petri nets for Boolean variable (see M.1)
Probabilistic-related symbols	
$P(.), P(A), P(t)$	Probability function, Probability of the event A, Probability at time t
$A(t), U(t), R(t), F(t)$	Availability, unavailability, reliability and unreliability at time t
$f(t)$	Failure probability density
$w, w(t), \bar{w}(T)$	Unconditional failure intensity (failure frequency)
$\Phi, \Phi_a, \Phi(t), \Phi_a(t), \Phi_{st}(t)$	Event frequency (accident, spurious safety actions)
$\bar{\Phi}, \bar{\Phi}_a, \bar{\Phi}(T), \bar{\Phi}_a(T), \bar{\Phi}_{st}(T)$	Average event frequency (accident, spurious safety actions)
$N_a, N_a(t), N_f, N_f(t)$	Number of accident or failures
$\Theta_z(T)$	Mean sojourn times in state Z over [0, T]
General notations and subscripts	
$\bar{X}(t_1, t_2), \bar{X}(T), \bar{X}$	Average values over $[t_1, t_2]$, over $[0, T]$ and over $[0, \infty[$
X_{as}	Asymptotic value of X
$X_{du}, X_{dd}, X_{sf}, X_{st},$	X related to <i>dangerous undetected, dangerous detected, safe failures, spurious safety actions (spurious trip)</i> .
$X_a, X_{a,du}, X_{a,dd}, \text{ etc.}$	X related to an hazardous event (accident)
$X_S, X_A, X_{AB}, \text{ etc.}$	X related to a safety system, a component A, a group of component A,B
X_{fs}, X_{ps}	X related to full or partial stroking (valve modelling)

Table 3 (continued)

Symbol	Definition
X_i, X_i^j	i, j indexes used when X is split in several parts.
$X^k, (X_i)^k, (X_i^j)^k$	Power k when k is an integer
$X_{Z,A,du}^3, X_{S,du}^{as}$, etc.	Indexes, (i, j) , (as, dd, du, sf, st), (S, A, AB) can be mixed
Parameters	
$\lambda, \lambda(t)$	Failure rates (component level)
$\Lambda, \Lambda(t), \Lambda_{eq}, \Lambda_{eq}(t)$	Equivalent failure rates (system level)
$\lambda_v, \lambda_v(t)$	Conditional failure intensity (Vesely failure rate)
λ_d	Demand rate
μ	Repair / restoration rates
γ, ψ	probability of failure due the test itself, Probability of failure due to a demand of the safety action
τ, θ	test interval, first test interval
π	test duration
ω	probability of human error
States	
KO	Class of states where a system is available
OK	Class of states where a system is unavailable
CS	Class of critical states

5 Overview and challenges

5.1 General considerations about modelling and calculation challenges

Reliability modelling and calculations constitute a delicate area because of the human perception, the technical difficulties, the potential “conflicting” interests between safety and production and the cross-functional organizational aspects of this activity within the overall hierarchy of the organization.

Challenges related to the human perception:

- Reluctance to use probabilistic calculations: they are more difficult to comprehend than deterministic rules and many people are circumspect in using them.
- Probabilistic reasoning: it is rather difficult and what seems obvious with a superficial analysis may appear to be inadequate when a sound analysis is performed.
- Working with time constraints leading to (over)simplifications which:
 - promotes superficial quick analyses of individual parts rather than detailed analysis of the system as a whole;
 - encourages practitioners to think that reliability modelling and calculations can be properly made just by applying analytical formulae or using black boxes without really understanding the underlying assumptions and limitations;

- convinces that additions and multiplications is a sufficient mathematical background to undertake probabilistic calculations.
- Poor dissemination of the advances in reliability modelling and calculations and belief that new tools are more difficult to use than formulae - when, actually, the contrary may be the case. A denial of usefulness can even be observed.

Difficulties related to technical issues:

- The basic concepts of reliability engineering seem simple when they conceal difficulties that non reliability experts may not be aware of.
- A system cannot properly be analysed by the simple juxtaposition of its parts: it is important to consider it as a whole. This implies “systemic” approaches and the size of such models may need the use of computers.
- The periodic tests introduce the following key challenges to be addressed:
 - approximations commonly used may not be conservative;

NOTE When periodic tests are implemented, the current approximations become worse when the probability decreases (i.e. when the redundancy increases). This behaviour is contrary to what happens in the usual situation where the approximations are generally better as the probability decreases.

- average probabilities of periodically tested components cannot be directly used to calculate the average probabilities at system level because the average of a product of quantities is not the product of the averages of these quantities.
- systemic dependencies are induced by periodic tests between safety systems working in sequence (see the Note 1 to entry of [3.4.10](#)). This implies that the requirement of independent safety layers is rarely met.
- awareness of the limitations inherent in software tools on the above matters.
- The handling of uncertainties should be done properly. These issues are further addressed in [Clauses 12](#) and [13](#), and also in ISO 20815[16] (D.3.7 and E.2). This relates to:
 - the importance of qualified input data (technical and operational assumptions and reliability data),
 - the quality of the modelling itself (the major focus in this Technical Report) and applicability of software tools used to facilitate calculation,
 - the final calculated result parameters and the need to reveal how robust and sensitive these results are in the above-mentioned framework, requiring possible use of statistical methods.

The traditional split between safety and production in the industrial organizations as well as in international standardization makes it more difficult to handle properly the tight links between safety and production: improving the first one generally damages the other one and reciprocally. Improving safety without production availability considerations is likely to lead to architectures subject to spurious safety actions. Then the safety is achieved to the detriment of the production availability of the installation. This is not the right way to design safety systems because even if the safety aspects constitute the dominant factor, the spurious actions have also to be considered to determine the best compromises. Moreover in the oil and gas industries, a spurious safety action is not necessarily safe: restarting after a spurious trip is often a perilous operation and a safety system provoking too many spurious trips is likely to be promptly disconnected. This may lead to dangerous situations especially when reconnecting the safety system is forgotten. Then combined systemic approaches where both safety and production are thoroughly considered are recommended by the present Technical Report which analyse both the inhibitions and spurious actions of the safety systems.

The probability of failure of the safety systems themselves is obviously a very important topic but it often tends to hide the primary problem which is to bring the probability of accident (or of the hazardous event frequency) below an acceptable level. This cannot be achieved properly just by calculating some

probabilistic measures on individual safety systems. Of course, the implementation of reliable safety systems (e.g. with high SIL requirements) helps to achieve the accident target but only a systemic analysis where all the safety layers are included is able to verify that the accident target is met.

The software tools necessary to accomplish the calculations related to the methods described in this Technical Report should in appropriate manner take into account the issues addressed in this report.

5.2 Deterministic versus probabilistic approaches

Since the beginning of the industrial era in the 19th century, the engineering philosophy has been to design the future systems by using the knowledge accumulated step by step during the past. This know-how built through a “trial and error approach” is now compiled into various state-of-the-art documents: good practices, rules, regulations, standards, etc. It is permanently improved according to the adverse events (failures, incident or accident) occurring in industry.

Waiting for negative experiences to improve the state-of-the-art is not really adequate for high risk industries where the consequences of the accidents are so large that they should be absolutely avoided. This is why alternative complementary methods have been investigated in aeronautics which has used “statistics” to compare the types of planes since World War I and “probabilities” to predict their number of expected accidents since the 1930s. The aeronautics field has been followed by rocket technology during World War II and later by the space industry and telecommunications field, the US army and the nuclear field. More recently it was the turn of the chemical, petrochemical and transportation fields to join this approach which is now in use in the main industrial areas.

The “deterministic” and “probabilistic” approaches are therefore available to design new systems. They are, indeed, very much complementary: it would not be possible to design a new system from scratch just by using the probabilistic approach, but oppositely the deterministic approach is not sufficient to prevent accidents which have not been observed yet. The result is that the deterministic rules constitute the basis of industrial systems design whereas the probabilistic approach provides effective means for in depth analyses, verification and improvement: the aim of the probabilistic approach is not to make the system run properly but to analyse how a system which is reputed to run properly can fail. Therefore the basic assumption of this Technical Report is that the safety systems have been designed according to the current state-of-the-art and run properly, before the probabilistic approaches are undertaken.

5.3 Safe failure and design philosophy

There are two philosophies to design safety systems:

- 1) a loss of energy provokes the safety action (“de-energize to trip” safety systems);
- 2) an emission of energy provokes the safety action (“energize to trip” safety systems).

With regard to the safety action, the first case is more reliable than the second one because the safety action occurs any time the energy is lost somewhere in the safety system. All failures related to energy or signal losses are safe and don’t need to be considered when evaluating the probability of dangerous failures. Therefore, this simplifies very much the analysis to be performed as well as the safety systems modelling.

This philosophy seems perfect and this is the solution which is the most widely implemented in the oil and gas sector. Nevertheless the counterpoint is that it increases the probability of spurious action.

This may be critical when there is no state where the risk completely disappears or when spurious actions have detrimental effects on the installation (e.g. water hammer). In this case, the spurious actions should be limited and the second philosophy could be used for this purpose.

When dealing with de-energize to trip safety system, only the components undergoing dangerous failures are considered within the safety analysis and the other components are generally ignored. Nevertheless they may participate in spurious actions and it is important to consider them when performing the safe or spurious failures analysis. This encompasses, but is not limited to:

- a) loss of power supply, e.g.:

- electric power supply (AC or DC);
- hydraulic power supply (i.e. the isolation valve is “fail-safe close”);
- b) loss of auxiliary supply (UPS, compressed air, etc.);
- c) rupture of the links between the sensors and the logic solvers;
- d) rupture of the links between the logic solvers and the final elements;
- e) any dangerous detected failure which is transformed into a safe failure by the self diagnostic tests.
- f) human actions following false alarms

Then the safe or spurious failure studies of “de-energize to trip” safety system need more detailed analysis than the dangerous failure analysis.

5.4 Dependent failures

5.4.1 Introduction

From a technological point of view (i.e. excluding the human factor considerations dealt in [5.5](#)), there are three main ways to decrease the probability of failure of a given system (including safety systems):

- 1) using more reliable components,
- 2) improving the maintenance strategy (e.g. increasing the test frequency of hidden failures),
- 3) introducing more redundancy to increase “fault tolerance” (see definition [3.4.9](#)).

The first one is practicable only if more reliable components are available on the market, the second one is usable to a small extent (e.g. because tests are costly and may have detrimental effects when their frequency is too high) and therefore the third one is generally implemented. It is effective to the extent that the redundant parts fail independently from each others. Therefore the identification and analysis of dependent failures (i.e. common cause failures and systematic failures) is an important topic when dealing with redundant (or fault tolerant) safety systems.

5.4.2 Common cause failures

From an academic point of view, if the probability of failure of a single component is p , the probability of failure of two independent redundant similar components (e.g. 1oo2) is p^2 , of three independent redundant similar components (e.g. 1oo3) is p^3 , of four independent redundant similar components (e.g. 1oo4) is p^4 , etc. Therefore it seems, in theory, possible to reduce the probability of failure to any level just by implementing the right level of redundancy. Let us take an example where the probability of failure of one component over one year is $p = 10^{-3}$. Over the same period of time this would lead respectively to 10^{-6} , 10^{-9} and 10^{-12} for 1oo2, 1oo3 and 1oo4 systems. These results are correct from a mathematical point of view but completely unrealistic from a physical point of view: in fact 10^{-9} is more or less the probability that system fails due to the collision with a meteorite over one year and 10^{-12} is about 100 times lower than the probability that the failure occurs because the Universe disappears!

Therefore some factors exist which limit the potential probability reduction expected from redundancy: they are linked to the potential for common cause (CCF), common mode (CMF) and systematic failures to cause multiple components to fail.

CCF can be split into the following categories:

- Explicit CCF: an event or mechanism that can cause more than one failure simultaneously is obviously a CCF. Such CCF can generally be explicitly known, analysed and treated as individual failures (e.g. meteorite collision, loss of power supply, fire, flooding).

- **Implicit CCF:** an event or mechanism that only increases the probability of failure of several components is obviously also a CCF. This kind of CCF does not induce the immediate failures of components but only degrade them so that their joint probability of simultaneous failure is increased (e.g. corrosion, premature wear out, over strength, unexpected systemic effects, design error, installation error). Such CCF cannot generally explicitly be known and remains implicit.

Implicit CCFs are far more difficult to identify, analyse and treat than the explicit CCF. It is very likely that some of them will remain ignored until they manifest themselves. They constitute a part of the epistemic uncertainties. ISO 14224^[15] advises how such data can be obtained (see ISO 14224^[15], Table B.3).

This Technical Report develops three of the pragmatic CCF approaches developed to establish effective safeguards in order to prevent over optimistic evaluations. They are presented in 5.4.2 and Annex G: β factor, shock model and PDS approaches.

NOTE Redundancy is more efficient to fight against CCFs which do not induce immediate failures because, provided that the relevant procedures are implemented to detect those CCFs, they can be discovered and repaired before all the redundant components are affected.

5.4.3 Systematic failures

It is outside the scope of this Technical Report to deal with the systematic failures (see 3.2.17) and the standards dealing with *functional safety* provide valuable information on this subject. A systematic failure results from a pre-existing fault (see 3.2.2) and occurs every time some given conditions are encountered. Then the systematic failures are perfect common cause failures which, like other CCFs do, limit the usefulness of redundancy. Beyond a certain level of redundancy (e.g. two or three channels) the benefit is illusory, especially if the software implemented in the redundant part has been developed on the same specification bases.

Further details are provided in Annex G.

5.5 Human factors

5.5.1 Introduction

The operator is sometimes defined as an unreliable agent of reliability. That means that, on one hand he/she is prone to commit simple action slips as well as more serious (cognitive) errors due to inadequate understanding of the system design and operation when on the other hand it is also acknowledged that he/she is sometimes the only element able, with sufficient understanding, to make good decisions when unscheduled situations occur i.e. improvising when suitable procedures have not been thought out beforehand.

Another interesting issue is that human beings can learn from their errors. Even if the operational situation stays constant the level of experience that the operators have of their interaction with it can affect their performance. They can improve their mental model of the world such that the operational situation is more predictable. Alternatively poor information and experience can result in applying incorrect mental models of the operational situation.

The role of the human operator is predominantly:

- part of the condition monitoring system;
- restoring to the appropriate system state in response to signalled deviations;
- activator of safety systems.

With regard to this Technical Report, there are several situations where the human function is appropriate for carrying out such tasks, e.g.:

- periodic testing;
- calibration;

- inhibition management;
- routine inspection and maintenance;
- repair of failed components;
- restoration / reconfiguration after repair;
- restarting of the process (e.g. restoring a system after a shut down/spurious trip);
- alarm detection and actions following alarms;
- recovery of a failed condition.

NOTE The human operator can be an initiator of unwanted events that make demands on safety systems. This contributes to the demand frequency of those safety systems and this out of the scope of this Technical Report.

In these roles the human operator is not only performing a function but is also a source of undesirable events. For that reason there are pros and cons for having a human in the system. It is therefore of value to model and quantify the effect of this.

Further information can be found in [Annex H](#) and in references[36],[37],[38],[39],[40],[41],[42],[43],[44] and.[45]

5.5.2 Human performance considerations

Human error is generally considered to be of three types:

- memory and attention lapses and action slips;
- mistakes in planning actions;
- rule violations.

In addition, three levels of human performance can be considered:

- skill based;
- rule based;
- knowledge based.

These levels are hierarchical. Performance at the knowledge-based level will call upon rule-based procedures which will call upon skill-based operations to execute the procedure. Human performance is most reliable at the skill-based level and least at the knowledge-based level.

When an operator has to assess a given condition such as in inspection and testing (e.g. periodic testing of a safety system) or in monitoring a system state where there is a certain degree of uncertainty a *signal detection* model can be used with four classes of response to the evidence:

- Hit – the operator correctly detects the signal.
- Miss – the operator missed the signal.
- False alarm – the operator identifies a noise event as a signal.
- Correct reject – the operator identifies a noise event as noise.

In human reliability assessment the primary focus is on eliminating systematic causes of human error at these different levels of performance. This is not discussed further in this Technical Report which is more focused on human random failures.

NOTE Systematic causes exist in equipment, man-machine interface and task design, training, procedures, information, communication, stress and fatigue, workload, and underlying organizational and management factors. Other factors to be taken into account are dependencies, for example when the same operator carries out the same task on otherwise independent systems.

5.5.3 Human error modelling

Human errors can be modelled as:

- omissions (omitting to do something);
- commission errors (doing things wrongly);
- acting too late or too early (a subset of commission error).

They are identified by examining procedures associated with a specified task, the initiation of a blow down for example. Commission errors not associated with a requirement for the operator to act and acts of sabotage are not generally modelled.

With regards to this Technical Report, the only human errors of interest are those which affect the functioning of the safety system in some way according to the intended design and operation. So, the analysis begins with the task performed within that function. Thereafter, understanding the task in terms of the performance requirements of the operator, both psychologically and physically, and the capacity of the operator to respond are important for quantification.

The probability of occurrence of a human error is measured by:

HEP = Numbers of human errors occurred/Number of opportunities for error, where HEP is the Human Error Probability.

The operator's opportunity for error can be identified as the whole task or it can be broken down to identify all the opportunities for human error which could result in a failure of interest. An opportunity for error might be, for example, the requirement to return gas detectors to service after maintenance or to close a valve before starting up a system

An operator may forget to close a valve, improvise by not replacing like with like or miss or dismiss signals to act. Such human errors can be identified from historical data but also can be surmised when there is a requirement for human action which could affect system performance. Some human reliability analysis (HRA) methods have human error identification prompts such as:

Can the signal be perceived as unreliable? → Signal ignored → Action omitted.

These undesirable events can be modelled as human error probabilities per demand for action or per task for example, the probability that the operator will not initiate the appropriate safety function in time on the occurrence of a particular blow out indicator.

It is important that the justification behind the quantification describes the conditions under which the operator undertakes the task as changes in these conditions can violate the assumptions made about the human error probability.

These concepts of human performance and human error modelling are important for linking the human performance into the safety system. It is outside the scope of this Technical Report to deal in detail with the human factor but further details may be found in [Annex H](#).

5.5.4 Human Reliability Analysis Methods

See also IEC 61508^[2] [Annex A](#) which gives examples of HRA methods.

Because of a lack of real data for the HEP calculation a number of methods have been developed. First generation methods were developed to help provide HEPs required in risk assessment. The most notable publically available methods include:

- THERP: Technique for Human Error Rate Prediction;
- HEART: Human Error Assessment and Reduction Technique.

and expert judgement methods:

- APJ: Absolute probability judgement;
- PC: Paired comparisons;
- SLIM-MAUD: Success likelihood index method using multi-attribute utility decomposition.

Second generation methods start around 1990 and were developed to better model the context in which the operator is working:

- ATHEANA: A Technique for Human Error Analysis;
- CREAM: Cognitive Reliability and Error Analysis Method.

Direct measurement of human failures is also possible.

- Within the framework of SDT - Signal detection theory;
- Conducting experiments on human performance under controlled conditions;
- Use of simulators.

Analysis of past incidents can also identify where human error contributed but not the number of opportunities for error.

Some HEPs and a worked example of the Paired Comparisons method are given in [Annex H](#).

5.6 Documentation of underlying assumptions

For further use of the reliability studies it is of utmost importance to keep the trace of every document which has been used as well as all prerequisites and underlying assumptions which have been adopted during the studies. This is an important part of the reliability analysis. It is often insufficiently done and should be more thoroughly considered.

Documenting underlying assumptions is important in order to:

- Highlight what technical, operational and analytic assumptions the results are based on and the consequences of these assumptions.
- Highlight measures and activities that are important to follow up and implement in design and operation – often being of more importance than the quantitative results themselves.
- Enhance the possibility of understanding the analysis results and the importance of the assumptions.
- Establish a good foundation to evaluate the validity of the results or for future use of the analysis, e.g. when updating the analysis.

Types of assumptions that are important to highlight are for example:

- The sources where the input reliability and maintenance data are taken from, and to what extent the data has been qualified and adjusted to account for a particular application. See ISO 20815^[16], [E.2](#).
- Any assumptions that have been made for the data concerning diagnostic coverage, critical failure modes, safe state, and so on, which are normally not presented (or presented in the same way) in

many data sources. In particular it is important to document and justify/substantiate failure rates that are significantly better than average generic data.

- Any assumptions that have been made in relation to periodic tests and maintenance, including required intervals and specific methods and/or tools to be applied.
- Any assumptions that have been made regarding operating environment.
- Any assumptions and analyses that have been made for evaluating the common cause failures (e.g. β factors) and for reducing them, e.g. diversity or staggered testing.
- All relevant assumptions related to procedures for inhibits and overrides, degraded operation, maximum repair times (if any), and assumptions concerning set points and required human interaction.
- Any assumptions that need to be validated during operation and how often such validation needs to be performed.

6 Introduction to modelling and calculations

6.1 Generalities about safety systems operating in “on demand” or “continuous” modes

A safety system is a *protection* system which protects another system - the *protected* system - against incident or accident. When the protection and the protected systems are not fully separated, it is essential to analyse them together as a whole. The protected system is sometime called “Equipment Under Control” (EUC) (e.g. in IEC 61508[2])

Two different modes of operation are generally considered with regard to how the safety system protects the protected system:

- **demand mode of operation:** the safety system spends most of its time to wait for a demand which occurs randomly when, due to hazardous events, a given physical parameter of the protected system exceeds a pre-established threshold. Reactive safety systems (also called curative safety system) operate on demand mode of operation.
- **continuous mode of operation:** a hazardous event occurs on the protected system as soon as the safety system fails. Preventive safety systems are operating in continuous mode of operation.

Let us consider an overpressure protection system which protects a pipe downstream by closing a valve when the upstream pressure exceeds a given threshold. During normal operation the upstream pressure fluctuates according to the process operation, hazardous events (e.g. overpressure) may occur and the safety system has to be ready to isolate the pipe (e.g. by closing a Shut Down Valve) as soon as a pre-established pressure threshold is reached. It performs its safety action just before the protected system enters in the dangerous zone: this is a typical reactive safety system working on demand mode of operation.

After the overpressure protection system has reacted to a demand by closing a SDV, the dynamic pressure drop decreases and the pressure increases upstream the valve closed between the pressure source and the pipe. After a while this pressure may become higher than the pressure strength of the downstream pipes and a spurious opening of this valve may lead to a dangerous situation. Because of the speed of the pipe pressurization in case of spurious opening, a reactive system may not be fast enough to close another valve before the overpressure occurs. Then another safety system is needed to prevent the spurious reopening of the valve. Its safety action is to continuously maintain the valve in the closed position until the pressure has dropped below a safe value: this is a typical preventive safety system working on continuous mode of operation.

Reactive safety systems are commonly used whereas preventive safety systems have just begun to be implemented in the oil and gas industries.

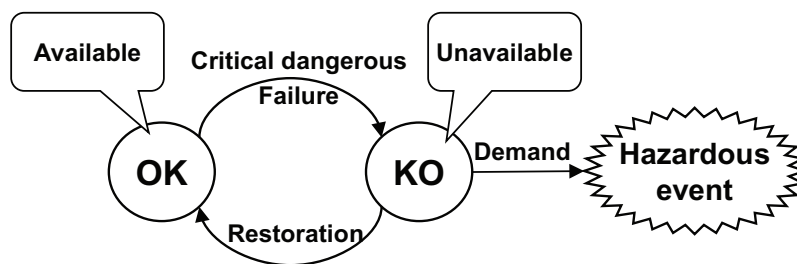


Figure 10 — Broad model for ultimate-on-demand mode safety system

As shown in Figure 10 a safety system working on demand mode may have failed before the occurrence of the demand and has not been repaired in the meanwhile, for a hazardous event occurring. What is important to prevent the hazardous event is that it is ready to operate at the time that the demand occurs. This does not matter if it has previously failed provided it has been repaired in the meanwhile: the “availability” (see definition 3.1.11, 3.1.12, 3.1.13) is the adequate probabilistic parameter to characterize such a safety system. Therefore, if the safety system is unavailable when the demand occurs and if no other succeeding safety system is able to respond, then the hazardous event occurs.

When the average unavailability $\bar{U} = \text{PFD}_{\text{avg}}$ of the safety system is small and the demand rate λ_d is low, then the hazardous event frequency can be calculated as: $\Phi_a(T) \approx \bar{U} \cdot \lambda_d = \text{PFD}_{\text{avg}} \cdot \lambda_d$. This is a widely used formula which is valid with some limitations analysed in Annex D.

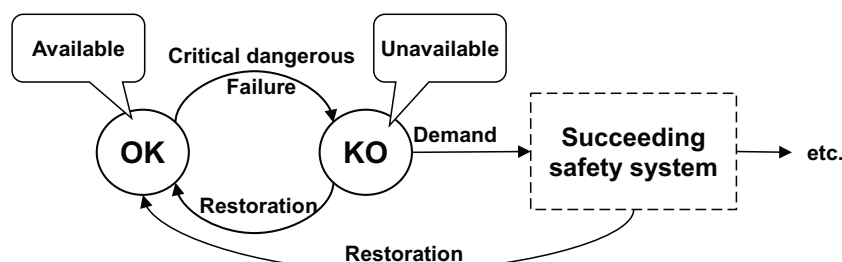


Figure 11 — Broad model for non-ultimate-on-demand mode safety system

In case of multiple safety-systems (see 3.3.3) another succeeding safety system may be able to respond, then, in this case, a new demand is generated to this safety system and the first one may be restored as shown in Figure 11. In this case the above formula gives the demand frequency on the succeeding safety system. The multiple safety systems are analysed in more detail in Annex F.

It is not allowed for a safety system working in continuous mode to fail as long as it is in use (e.g. as long as the pressure has not been lowered behind a safe threshold): the “reliability” (see definitions 3.1.8 and 3.1.9) is the adequate probabilistic parameter to characterize such a safety system.

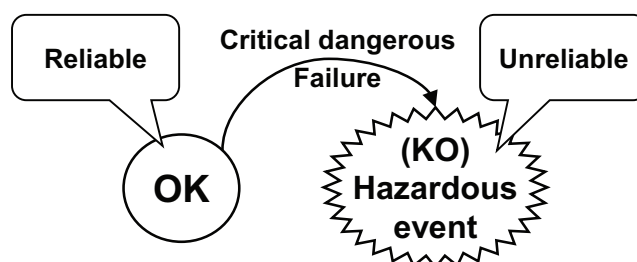


Figure 12 — Broad model for ultimate-continuous mode safety system

As shown in Figure 12 the hazardous event occurs as soon as the safety system fails if no other succeeding safety system is able to respond. Therefore, the critical dangerous failure rate of the safety system is