



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of ISO/TR 12489:2013.

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 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 78308 1

ICS 75.180.01; 75.200

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

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

Amendments issued since publication

Date	Text affected
------	---------------

TECHNICAL
REPORT

ISO/TR
12489

First edition
2013-11-01

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

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



Reference number
ISO/TR 12489:2013(E)

© ISO 2013



COPYRIGHT PROTECTED DOCUMENT

© ISO 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

	Page
Foreword	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.....	3
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 systems 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 make 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 user 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,^[2] 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.