TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN ISO/TR 12489

January 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

Ref. No. CEN ISO/TR 12489:2016 E

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

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.