Irish Standard Recommendation
S.R. CEN ISO/TR 12489:2016

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

S.R. CEN ISO/TR 12489:2016

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
CEN ISO/TR 12489:2016	2016-01-27

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2016-02-14	75.180.01 75.200
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

S.R. CEN ISO/TR 12489:2016 is the adopted Irish version of the European Document CEN ISO/TR 12489:2016, Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems (ISO/TR 12489:2013)

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

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

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

Contents

Page

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.

This page is intentionally left blank

TECHNICAL REPORT

ISO/TR 12489

First edition
2013-11-01

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

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

Reference number
ISO/TR 12489:2013(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

1 Scope

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

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

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

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

2 Analysis framework

2.1 Users of this Technical Report

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

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

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

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