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 International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Licensee=University of Alberta/5966844001, User=sharabiani, shahramfs
Not for Resale, 11/18/2013 23:12:39 MST

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Licensee=University of Alberta/5966844001, User=sharabiani, shahramfs
Not for Resale, 11/18/2013 23:12:39 MST

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

--`,````````,,,``,`,,,,,`,```,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Licensee=University of Alberta/5966844001, User=sharabiani, shahramfs
Not for Resale, 11/18/2013 23:12:39 MST