

Kazimierz T. Kosmowski

Functional safety and reliability analysis methodology for hazardous industrial plants

Applicable to functional safety management in life cycle
in the process industry sector and nuclear power plants

Gdańsk 2013

PRZEWODNICZĄCY KOMITETU REDAKCYJNEGO
WYDAWNICTWA POLITECHNIKI GDAŃSKIEJ
Janusz T. Cieśliński

REDAKTOR PUBLIKACJI NAUKOWYCH
Michał Szydłowski

RECENZENCI
Kazimierz Lebecki
Jacek Marecki

Wydano za zgodą
Rektora Politechniki Gdańskiej

Oferta wydawnicza Politechniki Gdańskiej jest dostępna pod adresem
<http://pg.gda.pl/wydawnictwo/oferta>

© Copyright by Wydawnictwo Politechniki Gdańskiej
Gdańsk 2013

Utwór nie może być powielany i rozpowszechniany, w jakiegokolwiek formie
i w jakikolwiek sposób, bez pisemnej zgody wydawcy

ISBN 978-83-7348-499-3

WYDAWNICTWO POLITECHNIKI GDAŃSKIEJ

Wydanie I. Ark. wyd. 9,5, ark. druku 11,5, 137/774

Druk i oprawa: *EXPOL* P. Rybiński, J. Dąbek, Sp. Jawna
ul. Brzeska 4, 87-800 Włocławek, tel. 54 232 37 23

CONTENTS

LIST OF SYMBOLS AND ACRONYMS	9
PREFACE.....	15
1. INTRODUCTION.....	17
1.1. Importance of functional safety and reliability aspects in industrial hazardous plants	17
1.2. Selected publications, monographs, reports and research works concerning reliability and safety of technical systems and hazardous plants	18
1.3. Functional safety standards and safety-related documents issued by international organisations.....	23
1.4. Scope of this monograph	24
2. FUNCTIONAL SAFETY CONCEPT AND CHALLENGES	28
2.1. Functional safety of electrical/electronic/programmable electronic systems	28
2.1.1. Safety functions and safety-related systems.....	28
2.1.2. Safe and danger failures of elements, subsystems and systems	30
2.1.3. Common cause failures	32
2.1.4. Probabilistic modelling of E/E/PE systems.....	34
2.1.5. Basic requirements concerning the E/E/PE safety-related systems.....	35
2.2. Risk assessment and reduction	36
2.2.1. Necessary risk reduction.....	36
2.2.2. Individual and societal risk assessment for decision making.....	37
2.3. Issues of safety integrity analysis and risk reduction.....	39
2.3.1. Safety integrity of E/E/PE systems and operation modes	39
2.3.2. Risk reduction for low demand mode applications	40
2.3.3. Risk reduction for high demand mode applications	42
2.3.4. Risk reduction for continuous mode applications	43
2.3.5. Risk of protection system spurious operation.....	43
2.3.6. Mitigation systems and risk reduction.....	44
2.4. Allocation of safety integrity requirements and challenges	45
2.4.1. Allocation of safety integrity requirements to E/E/PE safety-related systems.....	45
2.4.2. Safety integrity levels and software-related requirements	45
2.4.3. Risk reduction in case of multiple layers of protection	46
2.4.4. Challenges in consistent treating of dependent failures	47
3. DETERMINATION AND VERIFICATION OF THE SAFETY INTEGRITY LEVELS	50
3.1. Relevant methods supporting analyses	50
3.2. Quantitative method for determination of safety integrity level.....	51
3.3. Determination of SIL based on defined risk matrix and ALARP principle	52
3.4. Determination of SIL based on defined risk graph.....	54
3.4.1. Defining the risk graph.....	54
3.4.2. Risk graph calibration.....	55
3.4.3. Extended risk matrix including information from risk graph and remarks	57
3.5. Safety-related system design and SIL hardware verification using qualitative method....	59
3.5.1. The architectural constraints.....	59
3.5.2. Qualitative verification of the SIL of safety-related system.....	61
3.6. Quantitative verification of the SIL of safety-related system	62
3.7. Estimation of failure rates and parameters of quantitative models.....	66
3.7.1. Estimation of failure rates.....	66
3.7.2. The issue of reliability data for probabilistic modelling of functional safety components and systems	67

4. LAYER OF PROTECTION ANALYSIS INCLUDING HUMAN FACTORS.....	71
4.1. Remark on contribution of human factors in safety of hazardous plants	71
4.2. Layers of protection in the process industry	72
4.3. Defense in depth in nuclear power plants and defining the main protection functions	76
4.4. Human-centered design of the control room	78
4.5. Human reliability analysis in the context of safety functions	81
4.5.1. Operator behaviour and human reliability analysis	81
4.5.2. Examples of human error probability evaluation	84
4.6. Treating of dependencies in layer of protection analysis.....	87
4.7. Requirements and criteria concerning the design of protection layers	90
4.8. Requirements and criteria concerning the alarm system and operator interface	92
4.9. Selected topics of functional safety analysis in nuclear power plants	95
4.9.1. General requirements concerning the safety-related systems.....	95
4.9.2. Requirements for the safety-related systems in the context of basic safety issues of nuclear power plants.....	99
4.10. Basic design issues of protection systems in nuclear power plants.....	100
4.10.1. Classification of safety functions, structures and safety systems	100
4.10.2. Safety classification process	104
4.10.3. Safety categories to be assigned to plant specific safety functions and SSCs.....	107
4.10.4. Remarks on safety barriers and protection levels	109
4.10.5. Application of engineering rules for SSCs including I&C	112
5. COST-BENEFIT ANALYSIS OF FUNCTIONAL SAFETY IMPROVEMENTS	115
5.1. Individual risk criteria and ALARP principle.....	115
5.2. Individual risk levels and cost-benefit analysis	117
5.3. Combining ALARP framework for individual risk and cost-benefit analysis	119
5.4. Social risk criteria	120
5.5. Cost-benefit analysis and indirect effects of potential accidents	123
5.6. Cost-benefit analysis of the risk control options.....	124
5.7. Evaluation of justified costs for improvement of safety-related systems	125
5.8. Remarks on requirements and criteria for supporting safety-related decision making of nuclear power plants	128
5.8.1. Individual risk evaluation issues in hazardous industry	128
5.8.2. The criteria for the individual risk and societal risk of potential accidents.....	130
5.8.3. Selected safety related criteria and requirements for nuclear power plants	132
5.8.4. Examples of selected European safety criteria and requirements for nuclear power plants.....	133
6. FUNCTIONAL SAFETY MANAGEMENT AND RISK-INFORMED DECISION MAKING.....	139
6.1. Scope of the functional safety management in lifecycle	139
6.2. Concept and principles of risk-informed decision making	141
6.3. Sources of uncertainty in functional safety analyses	142
6.4. Factors and uncertainties related to determining required safety integrity levels	144
6.5. Software ProSIL for supporting the functional safety management.....	145
6.6. Evaluation of life cycle costs for design variants of safety-related systems.....	147
6.7. Security problems of safety-related industrial computer systems and networks.....	149
6.8. Key role of competences and safety culture	151
6.8.1. Shaping and managing safety-related competences	151
6.8.2. A system for certification of competences in the domain of functional safety	153
6.8.3. Safety culture and responsibility for functional safety	156
6.9. Remarks on functional safety analysis and verifying safety integrity level under uncertainty.....	159
6.9.1. Frameworks for uncertainty representation and treating.....	159

6.9.2. Uncertainty treating concept at relevant levels of probabilistic modelling of complex systems	160
7. CONCLUSIONS	164
REFERENCES	167
Summary in English	182
Summary in Polish	183