CONTENTS

INTRODUCTION 10
Definition of problematic area 11
Aims of the monograph 14
1. THEORY 16
1.1 Testing of Software 17
1.1.1 Verification and validation 18
1.1.2 Elementary attributes of software quality 19
1.2 Acceptance testing 19
1.2.1 Factory Acceptance Test (FAT) 20
1.2.2 Site Acceptance Test (SAT) 24
1.3 System testing 25
1.3.1 Stress Testing 27
1.3.2 Performance testing 30
1.3.3 Load testing 32
2. ANALYSIS OF PROBLEMATICS OF SAFETY-CRITICAL SYSTEMS 34
2.1 Safety and safety- critical systems 35
2.2 Safety Critical Computer Systems 36
2.3 Systems of Real Time 38
2.3.1 Time limits 40
2.3.2 Scheduling algorithm 42
2.4 Industrial Nets and their Safety 42
2.4.1 Types of Attacks in Communication 43
2.4.2 Requirements for Safety Protection 45
2.4.3 Application protocols 46
2.4.4 Fieldbus nets 47
3. DEFINITION OF DIFFERENCES AND SPECIFIC ASPECTS OF TRADITIONAL SOFTWARE SYSTEMS AND SAFETY--CRITICAL SYSTEMS 52
3.1 Analysis of the Standard IEEE 829 53
3.1.1 Summary of Results 54
3.2 Analysis of the Standard IEC 61508 55
3.2.1 Summary of Results 55

Bibliografische Informationen
http://d-nb.info/1046956221

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.3 Analysis of Regional and Product Standards of Safety-critical Systems 56
3.3.1 Summary of Results 59
3.4 Analysis of the Standards for Nuclear Power Equipment..... 60
3.4.1 Summary of Results 62
3.5 Analysis of Guideline GAMP..... 63
3.5.1 Summary of Results 63
3.6 Generalization of requirements for testing of safety-critical systems on the basis of analysis of standards and guidelines..... 64
4. DESIGN OF TESTING MODEL OF COMMUNICATION SUBSYSTEM BY SAFETY-CRITICAL CONTROL SYSTEMS..... 69
4.1 Importance of modelling 71
4.2 Design Process of Safety-critical Systems..... 72
4.2.1 System Testing in the Process of Design and Development of Safety-critical Systems..... 74
4.2.2 Requirements of System Testing from Perspective of Safety-critical Systems..... 77
4.3 Specification of the System Testing Type 82
4.4 Outputs for a Model Design of System Testing 84
4.5 A Model Design of the Performance Testing of a Communication Subsystem 86
4.5.1 Process of the Performance Testing of Communication Subsystem of Safety-critical Control Systems..... 86
4.5.2 Overview of Performance Testing States of Communication Subsystems of Safety-critical Control Systems 95
4.6 Design of Stress Testing Model by Testing of the Communication Subsystem 99
4.6.1 Modified Phases of Step Stress Testing..... 99
4.6.2 Process of the Step Stress Testing of a Communication Subsystem of Safety-critical Control Systems..... 101
4.6.3 State Overview of the Stress Testing of the Communication Subsystem of Safety-critical Control Systems..... 106
5. VERIFICATION OF THE DESIGNED TESTING MODELS..... 110
5.1 Metrics Proposal..... 111
5.1.1 Selection of Appropriate Metrics..... 111
5.1.2 Definition of Metrics 113

5.2 Verification of Designed Model of the Performance Testing 117
5.3 Verification of Designed Model of the Step Stress Testing 122
6. ACHIEVED RESULTS 128
CONCLUSION 131
REFERENCES 133
CONTENTS 138