Content

1 Special methodology for crisis scenarios 13
1.1 DYVELOP methodology 13
2 Special scenario construction, modelling and simulation 21
2.1 Crisis scenarios 32
2.2 Societal security and business continuity scenarios cycling 36
2.2.1 Business continuity management life cycle implementation 39
2.3 Threat/Peril crisis scenarios analysis, assessment, modelling and simulation 41
2.3.1 Threat/peril TERORIST's METABLAZON 50
3 Scenarios – continuity, use cases and applications 57
3.1 The scenarios use cases in NATO long time defence planning 57
3.1.1 NATO's case of scenario use 62
3.2 Exercise scenarios - International Atomic Energy Agency 66
3.2.1 Developing of the exercise crisis scenario 68
4 The Crisis scenarios and information safety – system of information safety management 73
4.1 Introduction 73
4.2 Information security 77
4.2.1 Confidentiality – preventing unauthorized access to data 78
4.2.2 Integrity – preventing unauthorized modification of data 79
4.2.3 Availability - preventing unauthorized non availability of data 79
4.3 Family of standards ISO/IEC 27xxx 84
4.3.1 Standards describing terminology 85
4.3.2 Standards describing requirements 85
4.3.3 Standards describing general guidelines ("best practices") 85
4.3.4 Standards describing sector – specific guidelines ("best practices") 87
4.3.5 Upcoming standards 87
4.4 Information security risk management (ISO/IEC 27005) 87
4.4.1 Defining the borders of risk analysis 90
4.4.2 Asset identification 90
4.4.3 Setting value and grouping of assets 91
4.4.4 Threats identification 92
4.4.5 Vulnerabilities identification 93
4.4.6 Risk Analysis - Assets Matrix 93
4.5 Information security management systems - ISO/IEC 27001 95
4.5.1 Model ISMS - PDCA cycle 95
4.6 Code of practice for information security management - ISO/IEC 27002:2005 99
4.6.1 Security policy 100
4.6.2 Organization of information security 101

4.6.3 Asset management ... 101
4.6.4 Human resources security ... 101
4.6.5 Physical and environmental security ... 101
4.6.6 Communications and operations management ... 102
4.6.7 Access control ... 102
4.6.8 Information systems acquisition, development and maintenance ... 102
4.6.9 Information security incident management ... 103
4.6.10 Business continuity management ... 103
4.6.11 Compliance ... 103
5 Societal Security Management System Standards as Crisis Management Implementation ... 105
5.1 Introduction ... 105
5.1.1 Implementing ISO 22301 ... 105
5.1.2 Comparing ISO 22301:2012 with BS 25999-2:2007 ... 106
5.1.3 History and mission ... 106
5.2 International Standard ISO 22313 ... 108
5.2.1 The Plan-Do-Check-Act cycle ... 109
5.2.2 Business continuity management system ... 109
5.3 Key Clauses of ISO22301:2012 ... 111
5.4 Implementing and operating the BCMS ... 120
5.4.1 Business impact analysis and risk assessment ... 121
5.4.2 Business Continuity Strategy and Planning Activities ... 122
5.4.3 Exercising and testing ... 123
5.5 Conclusion ... 124
6 Risks and Risk Scenarios in Insurance Assessing Systems ... 125
6.1 Solvency II Project ... 127
6.2 Potential risk classification procedures ... 128
6.3 Conclusion ... 133
7 Process-related risk according to ISO/IEC 15504 ... 135
7.1 Introduction ... 135
7.1.1 Background ... 135
7.1.2 Overview of ISO/IEC 15504 ... 135
7.2 Assessment process ... 138
7.2.1 Process reference model ... 138
7.2.2 Process assessment model ... 139
7.3 Process-related risk ... 140
7.3.1 Assessed process profile ... 140
7.3.2 Target process profile ... 141
7.3.3 Consequences of process attribute gaps ... 142

7.4 Risk analysis 143
7.4.1 Analysis approach 143
7.4.2 Problem probability 144
7.4.3 Consequences 145
7.4.4 Process-related risk 145
7.4.5 Processes with highest risk 146
7.4.6 Analysis procedure 146
7.4.7 Risk analysis examples 147
7.5 Risk management process 149
7.5.1 Risk management process overview 149
7.5.2 Risk management process activities 149
8 Nuclear and Radiological Emergency management, crisis scenarios, exercises and readiness in the Nuclear Power Plants 153
8.1 Exercise planning and development 154
8.2 Exercise conduct and evaluation 154
8.3 Conclusions 155
8.4 Strategic Aspects of Nuclear and Radiological Emergency Management 155
8.5 International recommendations and experience 157
8.5.1 Nuclear Regulatory Commission (NRC) 157
8.5.2 International Atomic Energy Agency (IAEA) 159
8.6 Types of exercises 160
8.6.1 Drills 160
8.6.2 Tabletop exercises 161
8.6.3 Partial and full-scale exercises 162
8.6.4 Field exercises 162
8.7 Methods of conducting an exercise 163
8.7.1 Time mode 163
8.7.2 Free play versus stimulation 164
8.7.3 Using a simulator during an exercise 164
8.8 Frequency of emergency exercises 165
8.9 Exercise programme 166
9 Assets Protection 167
9.1 Assets 167
9.1.1 Asset Security 168
9.1.2 Asset Evaluation 170
9.1.3 Risk Analysis 172
9.2 Protection of Organization Assets 172
9.3 Extraordinary Events and Asset Protection 174
9.3.1 Asset Protection from Floods 174

9.3.2 Asset Protection from Fires ... 175
9.3.3 Asset Protection from Earthquakes ... 176
9.3.4 Asset Protection from Landslides ... 176
9.3.5 Asset Protection from Avalanches ... 177
9.3.6 Information System Protection ... 177
9.4 Process Approach to Asset Protection ... 178
10 Crisis Scenarios and Simulation Technologies ... 181
10.1 Introduction ... 181
10.2 Modeling and Simulation Training ... 181
10.2.1 Basic concepts ... 181
10.2.2 Live, Virtual and Constructive (LVC) Simulation ... 185
10.3 CSTT Simulator in Czech Army ... 186
10.3.1 The means of live simulation by CSTT ... 186
10.3.2 The means of virtual simulation at CSTT ... 187
10.3.3 The means of constructive simulation ... 188
10.3.4 Possibilities of CSTT ... 190
10.4 Rules for the preparation, implementation and evaluation of employment and trainer simulation technique ... 193
10.4.1 Preparation period ... 193
10.4.2 Execution Period ... 194
10.4.3 Assessment period ... 194
10.5 Example of Crisis Scenarios ... 194
10.5.1 Basic Information ... 195
10.5.2 Detailed information ... 199
10.5.3 Head director's documentation ... 201
10.6 Plan MEL/MIL ... 203
10.6.1 Scenario: Disposal of and emergency disaster of an international express train ... 203
10.7 Advantages of the simulator ... 205
10.8 Interim conclusion ... 206
10.9 Formal appendix ... 206
10.9.1 Definitions, Acronyms, Abbreviations ... 206
10.9.2 Others (Revise Questions, ...) ... 208
11 Implementation of crisis scenarios to the training system of the Army of the Czech Republic ... 209
11.1 Current career education system of the Czech soldiers ... 209
11.2 Characteristics of incidents most often occured during the units deploymen abroad ... 214
11.2.1 The Improvized Explosive Device (IED, a roadside bomb) ... 215
11.2.2 The enemy's attacks on COB and FOB. ... 216

11.3 Crisis scenarios feasible in the career education 216
11.3.1 The IED explosion during patrols 216
11.3.2 Balistik trauma after enemy's attack 217
11.4 Possible ways of implementation of crisis scenarios to the tactics training of career education system 219
11.5 OPORD of commander of the 1st parachute company for the patrol 223
12 References 227
13 Figures 235
14 Tables 239