Table of contents

Introduction 7

1. SAFETY IN RAIL TRANSPORT – AN OVERVIEW OF THE STATE OF THE ART ... 11

1.1. Technical approach to safety in rail transport 11
1.2. Refining the technical approach based on gained experience 13
1.3. Contribution of statistical analyses to the safety improvement in rail transport 14
1.4. Comprehensive approach to safety through safety management 14
1.5. Data communication systems in rail transport 15
1.6. Cybersecurity – the new dimension of safety not to be ignored 16
1.7. Objective and structure of the monograph 17

2. SAFETY AND SECURITY IN RAILWAY TRANSPORT 19

2.1. Technical approach to safety in technical solution approval procedures 23
2.1.1. Failure safety 23
2.1.2. Construction safety 24
2.1.3. Electrical safety 24
2.1.4. Access and fire protection 25
2.1.5. The effect of rolling stock forces on the track and wheel-rail interaction 25
2.1.6. Signalling systems (primary signalling and control command trackside and on-board installations 26
2.1.7. Interferences in signalling and control command systems from traction power supply systems 27
2.1.8. Operating rules and personnel qualifications 28
2.1.9. Panic prevention 28
2.1.10. IT support for railway transport safety 29
2.2. Supplementation of the technical approach with fields related to the protection of life, health, and property 29
2.2.1. Passenger healthcare aids 29
2.2.2. Vandalism protection 30
2.2.3. Protection against terrorism 30
2.2.4. Property protection 31
2.2.5. Protection against disasters and adverse weather conditions 31
2.3. Railway transport safety management covering operation and maintenance processes 32
2.3.1. Safety policy 33
2.3.2. Maintenance safety 35
2.3.3. Operational safety 36
2.3.4. Risk assessment 37
2.3.5. Risk assessment monitoring 38
2.3.6. Access to safety-related data 39

2.3.7. Emergency response ... 40
2.3.8. Documenting and analysing accidents and incidents ... 40
2.3.9. Internal safety system monitoring ... 41
2.3.10. Safety improvement programmes ... 42
2.4. Cybersecurity in railway transport ... 43
2.5. External safety system supervision ... 45
2.6. Summary of the railway transport safety review ... 46

3. SYSTEMS WITH DATA TRANSMISSION RELEVANT FOR SAFETY AND SECURITY IN RAILWAY TRANSPORT ... 49
3.1. Signalling systems ... 52
3.1.1. Primary signalling systems ... 53
3.1.2. Systems providing operational communication ... 66
3.1.3. Control-Command Trackside Systems ... 73
3.1.4. Alarm Signal Propagation and Emergency Braking Systems ... 81
3.1.5. Railway automation systems ... 85
3.2. Fire and access safety systems and equipment ... 88
3.3. Electrical safety systems and equipment ... 88
3.4. Failure and malfunction detection systems and equipment for rolling stock ... 90
3.5. Panic and rescue support systems and equipment ... 93
3.6. Safety integrity of the systems supporting traffic safety and transport security ... 93
3.6.1. Overall approach to RAMS ... 94
3.6.2. Maintenance conditions ... 96
3.6.3. Operating conditions ... 97
3.6.4. System conditions – basic concept ... 98
3.6.5. System conditions – environmental conditions, external disturbances, cyberattracts ... 98
3.6.6. System conditions – systematic failures safety integrity ... 99
3.6.7. System conditions – random failures safety integrity ... 100
3.7. The RAMS tasks in the life cycle phases ... 100
3.7.1. Concept phase of the lifecycle ... 102
3.7.2. System and operational context definition phase of the lifecycle ... 107
3.7.3. Risk analysis and evaluation phase of the lifecycle ... 107
3.7.4. Specification of the system requirements phase of the lifecycle ... 108
3.7.5. Architecture and apportionment of the system requirements phase of the lifecycle ... 109
3.7.6. Design and implementation phase of the lifecycle ... 110
3.7.7. Manufacture phase of the lifecycle ... 110
3.7.8. Integration phase of the lifecycle ... 110
3.7.9. System validation phase of the lifecycle ... 111
3.7.10. System acceptance phase of the lifecycle ... 111
3.7.11. Operation, maintenance and performance monitoring phase of the lifecycle ... 112
3.7.12. Decommissioning phase of the lifecycle ... 112
3.8. Cooperation between stakeholders and safety cases proving Safety Integrity Levels SILs ... 113
3.8.1. Hourglass model representing safety edge between industry and railway ... 113
3.8.2. The safety cases proving safety integrity levels ... 116
3.8.3. Three different types of safety cases versus lifecycle phases ... 120

4. REFERENCE FUNCTIONAL MODEL FOR SUPPORTING RAILWAY TRANSPORT SAFETY AND SECURITY THROUGH DATA COMMUNICATION SYSTEMS ... 121
4.1. Procedural protection means against safety hazards to ensure safe railway operation ... 122

4.2. Technical protection means against safety hazards to ensure safe railway operation – primary signalling and control command systems 123
4.3. Procedural protection means against security hazards to ensure railway transport security 128
4.4. Technical protection means against life, health, and property hazards to ensure railway transport security 129
4.5. Railway safety-related technical solutions intentionally not included in the RFM model 139

5. CYBERSECURITY – THE E-RFM MODEL 141
5.1. Threats and protection means in data communication systems relevant to safety and/ or security 141
5.1.1. Accurate records of data processing and communication systems relevant to safety and security – sender and receiver, input and output, source and outlet 142
5.1.2. Protection measures in transmission systems........ 144
5.1.3. Reference between transmission safety and the ISO OSI model 145
5.2. Complementing the reference functional model to highlight cybersecurity issues – the e-RFM model 149

6. DETERMINATION OF THE FUNCTIONAL INTEGRITY LEVEL OF THE SAFETY, SECURITY AND CYBERSECURITY 153
6.1. Safety, security and cybersecurity check sheets 154
6.2. Determining the functional integrity level of safety, security, and cybersecurity 166
6.3. Identification of homogenous transport systems for the purpose of determining the *FIL* level and drawing conclusions for non-homogenous transport systems........ 168

7. AN EXAMPLE OF THE RFM AND e-RFM MODEL APPLICATION AND THE *FIL* LEVEL DETERMINATION 173
7.1. Separate homogenous rail transport system selected for assessment 173
7.2. Example application of RFM and e-RFM models........ 174
7.3. Example determination of the functional integrity level of safety, security and cybersecurity based on safety and security factors in the RFM model and transmission cybersecurity conditions in the e-RFM model........ 181
7.4. Functional integrity level of safety, security and cybersecurity in Solidarity Transport Hub reference requirements........ 184

8. A HOLISTIC APPROACH TO CYBERSECURITY 187
8.1. The extent of the cyber threat challenge according to the UIC 187
8.2. Formal commitment to cybersecurity 187
8.3. The extent of the cyber threat challenge according to ENISA 188
8.4. Overview of reference documents 190
8.5. Infrastructure managers' and railway undertakings' systems exposed to cyber threats..... 191
8.5.1. Background cybersecurity-relevant functionalities........ 193
8.5.2. Cybersecurity-relevant functionalities of signalling, control command and operational communication systems 195
8.5.3. Cybersecurity-relevant functionalities of OT systems excluding signalling, control command and operational communication systems 198
8.5.4. Cybersecurity-relevant functionalities of railway IT systems........ 200
8.5.5. Cybersecurity-relevant functionalities of other IT systems 202
8.5.6. Cybersecurity-relevant functionalities of OT systems on trains 204

8.6. Identification of critical risks 205
8.7. Identification of locations requiring security measures to be defined 208
8.8. Support to railway managers and operators in countering cyber threats 210

Summary 213
References 217
List of figures 225
List of terms used in the monograph 227