Contents

Preface 5

1 Introduction 11

2 Cybersecurity involves process, people, and technology

3 Roles and responsibilities in IEC 62443 17

4 Structure of IEC 62443

5 Concepts of IEC 62443 23
5.1 Defense in depth 23
5.2 The standard IEC 62443 in product and IACS lifecycles 25
5.3 Risk assessment according to VDI/VDE 2182 28
5.4 Security Levels 34

6 Security Program (SP) and Security Protection Scheme (SPS) 37
6.1 Relationship between Security Program (SP) and Security Protection Scheme (SPS) 37
6.2 Development and operation of a SPS 38

7 Security Protection Ratings 43
7.1 Definition and methodology 43
7.2 Use of SPR in risk reduction 48
7.3 SPR and SL types 49
7.4 Grouping of system security requirements 51

8 Role-based activities in the development, practice and maintenance of a security protection scheme 57
8.1 Specification 58
8.2 Design 62
8.3 Implementation 69
8.4 Verification and validation 70
8.5 Operation and Maintenance 72
8.6 Update 73
8.7 Decommissioning 74

9 Holistic approach for product suppliers, using the example of the Siemens security concept for process and discrete industries ... 77
9.1 Overview ... 77
9.2 Holistic security concept (HSC) ... 78
9.3 Plant security ... 79
9.4 Network security ... 82
9.5 System integrity ... 87
9.6 Role based access ... 89
9.7 Consideration of attack scenarios in product development and production ... 89

Annex A: Detailed description of the IEC 62443 documents ... 91
A1 Main documents relevant for the development and practice of a security protection scheme ... 91
A1.1 IEC 62443-2-1 ... 91
A1.2 IEC 62443-2-4 ... 99
A1.3 IEC 62443-3-2 ... 103
A1.4 IEC 62443-3-3 ... 106
A1.5 IEC 62443-4-1 ... 116
A1.6 IEC 62443-4-2 ... 121
A1.7 ISO/IEC 27001 ... 127
A2 Other documents of IEC 62443 ... 137
A2.1 IEC 62443-1-1 ... 137
A2.2 IEC 62443-1-2 ... 138
A2.3 IEC 62443-1-3 ... 138
A2.2 IEC 62443-2-3 ... 138
A2.5 IEC 62443-3-1 ... 141

Annex B: Tracing of requirements to the elements of the asset owner security program (SP) ... 143
B1 ORG 1 – Security related organization and policies ... 143
B2 ORG 2 – Security assessments and reviews ... 145
B3 ORG 3 – Security of physical access ... 146
B4 CM 1 – Inventory management of IACS hardware/software components and network communications ... 147
B5 NET 1 – System segmentation ... 148
B6 NET 2 – Secure wireless access ... 150
B7 NET 3 – Secure remote access ... 151
B8 COMP 1 – Components and portable media ... 152
B9 COMP 2 – Malware protection ... 153
B10 COMP 3 – Patch management ... 155
B11 DATA 1 – Protection of data ... 156
B12 USER 1 – Identification and authentication ... 158
B13 USER 2 – Authorization and access control ... 161

B14 EVENT 1 – Event and incident management 163
B15 AVAIL 1 – System availability and intended functionality 165
B16 AVAIL 2 – Backup/restore/archive 166

Bibliography 169

Index 171