

# Contents

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| Preface.....                                                                                                      | 5  |
| 1      Introduction.....                                                                                          | 9  |
| 2      Cybersecurity involves process, people, and technology .....                                               | 11 |
| 3      Roles and responsibilities in IEC 62443 .....                                                              | 15 |
| 4      Structure of IEC 62443 .....                                                                               | 17 |
| 5      Concepts of IEC 62443.....                                                                                 | 21 |
| 5.1    Defense-in-depth .....                                                                                     | 21 |
| 5.2    The standard IEC 62443 in product and IACS lifecycles.....                                                 | 24 |
| 5.3    Risk assessment according to VDI/VDE 2182.....                                                             | 26 |
| 5.4    Security Levels.....                                                                                       | 32 |
| 6      Security Program (SP) and Security Protection Scheme (SPS).....                                            | 35 |
| 6.1    Relationship between Security Program (SP) and Security Protection Scheme (SPS) .....                      | 35 |
| 6.2    Development and operation of a SPS.....                                                                    | 36 |
| 7      Security Protection Ratings.....                                                                           | 41 |
| 7.1    Definition and methodology .....                                                                           | 41 |
| 7.2    Use of SPR in risk reduction .....                                                                         | 46 |
| 7.3    SPR and SL types .....                                                                                     | 47 |
| 7.4    Grouping of system security requirements .....                                                             | 49 |
| 8      Integrating IEC 62443 and ISO 27001 / ISO 27002<br>for Security Protection Schemes .....                   | 55 |
| 9      Role-based activities in the development, practice and maintenance<br>of a security protection scheme..... | 61 |
| 9.1    Specification.....                                                                                         | 62 |
| 9.2    Design .....                                                                                               | 65 |
| 9.3    Implementation.....                                                                                        | 72 |
| 9.4    Verification and validation .....                                                                          | 73 |
| 9.5    Operation and Maintenance .....                                                                            | 75 |
| 9.6    Update .....                                                                                               | 76 |
| 9.7    Decommissioning .....                                                                                      | 77 |

|                |                                                                                                                                             |            |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>10</b>      | <b>Holistic approach for product suppliers, using the example of the Siemens security concept for process and discrete industries .....</b> | <b>79</b>  |
| 10.1           | Overview .....                                                                                                                              | 79         |
| 10.2           | Holistic security concept (HSC).....                                                                                                        | 80         |
| 10.3           | Plant security.....                                                                                                                         | 81         |
| 10.4           | Network security.....                                                                                                                       | 84         |
| 10.5           | System integrity .....                                                                                                                      | 90         |
| 10.6           | Role based access .....                                                                                                                     | 92         |
| 10.7           | Consideration of attack scenarios in product development and production...                                                                  | 92         |
| <b>Annex A</b> | <b>Main documents to be considered for the SPS .....</b>                                                                                    | <b>93</b>  |
| A.1            | IEC 62443-2-1 Edition 2.....                                                                                                                | 93         |
| A.2            | IEC 62443-2-4 .....                                                                                                                         | 101        |
| A.3            | IEC 62443-3-3 .....                                                                                                                         | 106        |
| A.4            | IEC 62443-4-1 .....                                                                                                                         | 119        |
| A.5            | IEC 62443-4-2 .....                                                                                                                         | 124        |
| A.6            | IEC 62443-3-2 .....                                                                                                                         | 129        |
| A.7            | ISO 27001 and ISO 27002.....                                                                                                                | 132        |
| <b>Annex B</b> | <b>Supporting documents of IEC 62443 series .....</b>                                                                                       | <b>137</b> |
| B.1            | IEC 62443-1-1 .....                                                                                                                         | 137        |
| B.2            | IEC 62443-1-3 .....                                                                                                                         | 138        |
| B.3            | IEC 62443-2-3 .....                                                                                                                         | 138        |
| B.4            | IEC 62443-3-1 .....                                                                                                                         | 141        |
| <b>Annex C</b> | <b>Tracing of requirements to the elements of the asset owner security program (SP).....</b>                                                | <b>143</b> |
| C.1            | ORG 1 – Security related organization and policies.....                                                                                     | 143        |
| C.2            | ORG 2 – Security assessments and reviews .....                                                                                              | 146        |
| C.3            | ORG 3 – Security of physical access.....                                                                                                    | 147        |
| C.4            | CM 1 – Inventory management of IACS hardware/software components and network communications.....                                            | 148        |
| C.5            | NET 1 – System segmentation .....                                                                                                           | 149        |
| C.6            | NET 2 – Secure wireless access.....                                                                                                         | 151        |
| C.7            | NET 3 – Secure remote access.....                                                                                                           | 152        |
| C.8            | COMP 1 – Components and portable media.....                                                                                                 | 153        |
| C.9            | COMP 2 – Malware protection .....                                                                                                           | 155        |
| C.10           | COMP 3 – Patch management.....                                                                                                              | 156        |
| C.11           | DATA 1 – Protection of data .....                                                                                                           | 157        |
| C.12           | USER 1 – Identification and authentication.....                                                                                             | 160        |
| C.13           | USER 2 – Authorization and access control.....                                                                                              | 164        |
| C.14           | EVENT 1 – Event and incident management .....                                                                                               | 165        |
| C.15           | AVAIL 1 – System availability and intended functionality .....                                                                              | 167        |
| C.16           | AVAIL 2 – Backup/restore/archive.....                                                                                                       | 168        |
| C.17           | Abbreviations.....                                                                                                                          | 169        |
|                | <b>Bibliography .....</b>                                                                                                                   | <b>171</b> |
|                | <b>Index .....</b>                                                                                                                          | <b>173</b> |