

# Contents

Preface.....	5
1 Introduction.....	9
Definition of “Industrial Security”.....	10
2 Scope and roles of IEC 62443 .....	11
3 Structure of IEC 62443.....	15
4 Concepts of IEC 62443.....	17
4.1 Defense in depth .....	17
4.2 Risk assessment according to VDI/VDE 2182 .....	19
4.3 The standard IEC 62443 in product and IACS lifecycles.....	24
Use of the standard in product lifecycles.....	24
Use of the standard in IACS lifecycles .....	25
4.4 PDCA cycles in product and IACS lifecycles.....	27
Product supplier lifecycles .....	27
IACS lifecycles .....	28
4.5 Security Levels according to IEC 62443-3-3.....	29
5 Holistic approach, Protection Levels.....	33
Security is about technology, processes, and people .....	33
Protection levels are addressing installations in operation .....	34
Protection Levels combine the evaluation of technical and organizational measures.....	35
5.1 Methodology to evaluate Protection Levels .....	37
5.2 PL values belong to security control classes or views .....	38
Security control classes.....	40
Views .....	44
5.3 Use of protection levels in a risk-based approach.....	46
5.4 Use of protection levels in the IACS lifecycle.....	47
5.5 Use of protection levels by product suppliers.....	49
6 How to proceed in the development of a protection concept .....	51
6.1 Overview .....	51
6.2 Plant security .....	52

6.3	Network security .....	56
6.4	System integrity.....	60
6.5	Role based access .....	62
6.6	Consideration of attack scenarios in product development and production.....	62
<b>Annex: Detailed description of the IEC 62443 documents.....</b>		<b>65</b>
<b>A</b>	<b>Main documents relevant for development and maintenance of a protection concept.....</b>	<b>67</b>
A.1	IEC 62443-2-1 / ISO/IEC 27001 .....	67
A.2	IEC 62443-2-4 .....	75
A.3	IEC 62443-3-3 .....	80
	FR 1 – Identification and access control .....	82
	FR 2 – Use control .....	84
	FR 3 – System integrity .....	85
	FR 4 – Data confidentiality .....	86
	FR 5 – Restricted data flow .....	87
	FR 6 – Timely response to events.....	88
	FR 7 – Resource availability .....	89
A.4	IEC 62443-4-1 .....	90
	Practice 1 – Security Management, SM .....	91
	Practice 2 – Specification of security requirements, SR .....	92
	Practice 3 – Secure by design, SD .....	92
	Practice 4 – Secure implementation, SI .....	93
	Practice 5 – Security verification and validation testing, SV .....	93
	Practice 6 – Security defect management, DM.....	94
	Practice 7 – Security update management, PM .....	94
	Practice 8 – Security guidelines, SG .....	95
A.5	IEC 62443-4-2 .....	95
<b>B</b>	<b>Other documents of IEC 62443 .....</b>	<b>103</b>
B.1	IEC 62443-1-1 .....	103
B.2	IEC 62443-1-2 .....	104
B.3	IEC 62443-1-3 .....	104
B.4	IEC 62443-2-3 .....	104
B.5	IEC 62443-3-1 .....	107
B.6	IEC 62443-3-2 .....	108
<b>Bibliography .....</b>		<b>111</b>
<b>Index .....</b>		<b>113</b>