

# Contents

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.....	23
5.3	Risk assessment according to VDI/VDE 2182.....	26
5.4	Security Levels.....	32
6	Holistic protection scheme .....	35
7	Security Program 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	Views .....	48
8	Role-based activities and contributions in the development, practice and maintenance of a holistic protection scheme .....	53
8.1	Specification.....	54
8.2	Design .....	57
8.3	Implementation.....	64
8.4	Verification and validation .....	65
8.5	Operation and Maintenance .....	67
8.6	Update .....	68
8.7	Decommissioning.....	69
9	Holistic approach for product suppliers using the example of the Siemens security concept for process and discrete industries .....	71
9.1	Overview.....	71
9.2	Holistic security concept (HSC).....	72
9.3	Plant security.....	73
9.4	Network security.....	76
9.5	System integrity .....	81

9.6	Role based access .....	83
9.7	Consideration of attack scenarios in product development and production.....	83
<b>A</b>	<b>Detailed description of the IEC 62443 documents .....</b>	<b>85</b>
A.1	Main documents relevant for the development and practice of a holistic protection scheme .....	85
A.1.1	IEC 62443-2-1 .....	85
A.1.2	IEC 62443-2-4 .....	93
A.1.3	IEC 62443-3-2 .....	98
A.1.4	IEC 62443-3-3 .....	101
A.1.5	IEC 62443-4-1 .....	112
A.1.6	IEC 62443-4-2 .....	117
A.1.7	ISO/IEC 27001 .....	123
A.2	Other documents of IEC 62443.....	133
A.2.1	IEC 62443-1-1 .....	133
A.2.2	IEC 62443-1-2 .....	134
A.2.3	IEC 62443-1-3 .....	134
A.2.4	IEC 62443-2-3 .....	134
A.2.5	IEC 62443-3-1 .....	137
<b>B</b>	<b>Tracing of requirements to the elements of the new organizational structure .....</b>	<b>139</b>
B.1	SM, Security Management.....	140
B.2	LF, Security Life Cycle.....	142
B.3	RM, Risk Management .....	143
B.4	AC, Access Control.....	146
B.5	SI, System Integrity .....	149
B.6	AS, System Availability .....	153
B.7	DC, Data Confidentiality.....	154
B.8	AM, Asset Management .....	156
B.9	IM, Incident Management .....	158
	<b>Bibliography .....</b>	<b>161</b>
	<b>Index .....</b>	<b>163</b>