IEC TR 63486

Edition 1.0 2024-09

TECHNICAL REPORT

colour inside

Nuclear facilities – Instrumentation, control and electrical power systems – Cybersecurity risk management approaches

IEC TR 63486:2024-09(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 63486

Edition 1.0 2024-09

TECHNICAL REPORT

colour inside

Nuclear facilities – Instrumentation, control and electrical power systems – Cybersecurity risk management approaches

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20; 27.100

ISBN 978-2-8322-9380-5

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 13
INTRODUCTION 15
1 Scope 17
1.1 General 17
1.2 Framework 20
1.3 Limitations 20
2 Normative references 20
3 Terms and definitions 20
4 Abbreviated terms 25
5 IEC 62645 risk management elements 27
5.1 General 27
5.2 Assignment of security degrees in the management of risk 27
5.3 Safety correlation 28
6 NPP cyber risk management challenges and analyses 28
6.1 General 28
6.2 Challenge 1: Aggregate risk of multiple units / locations 31
6.3 Challenge 2: Complexity of interdependencies and interactions 32
6.4 Challenge 3: Incident likelihood determination 32
6.5 Challenge 4: Unknown or lacking sufficient detail for pre-developed components 32
6.6 Challenge 5: Differences in cyber-risk management 33
6.7 Challenge 6: Lack of abstract analysis methods 33
6.8 Challenge 7: Uncertainty in vulnerability / Susceptibility analysis 33
6.9 Challenge 8: Adversary characterization uncertainty 34
6.10 Challenge 9: Excessive information volume 34
6.11 Challenge 10: Lack of a common and comprehensive risk management process 34
6.12 Challenge 11: Advanced security capabilities incompatibility 35
7 Cyber-risk approaches versus challenges by ISO/IEC 27005 35
7.1 General 35
7.2 ISO/IEC 27005:2018, 7.1 General considerations 35
7.2.1 Summary 35
7.2.2 Applicable challenges 36
7.2.3 Summary of key approaches 36
7.2.4 Cross-reference table (Table 4) 37
7.3 ISO/IEC 27005:2018, 7.2 Basic criteria 37
7.3.1 Summary 37
7.3.2 Applicable challenges 37
7.3.3 Key approaches 38
7.3.4 Cross-reference table (Table 6) 40
7.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries 40
7.4.1 Summary 40
7.4.2 Applicable challenges 40
7.4.3 Key approaches 41
7.4.4 Cross-reference table (Table 8) 42
7.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management 42

7.5.1 Summary 42
7.5.2 Applicable challenges 42
7.5.3 Key approaches 43
7.5.4 Cross-reference table (Table 10) 43
7.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 44
7.6.1 Summary 44
7.6.2 Applicable challenges 44
7.6.3 Key approaches 44
7.6.4 Cross-reference table (Table 12) 45
7.7 ISO/IEC 27005:2018, 8.2 Risk identification 45
7.7.1 Summary 45
7.7.2 Applicable challenges 46
7.7.3 Key approaches 46
7.7.4 Cross-reference table (Table 14) 48
7.8 ISO/IEC 27005:2018, 8.3 Risk analysis 48
7.8.1 Summary 48
7.8.2 Applicable challenges 49
7.8.3 Key approaches 49
7.8.4 Cross-reference table (Table 16) 51
7.9 ISO/IEC 27005:2018, 8.4 Risk evaluation 51
7.9.1 Summary 51
7.9.2 Applicable challenges 51
7.9.3 Key approaches 52
7.9.4 Cross-reference table (Table 18) 53
7.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment 54
7.10.1 Summary 54
7.10.2 Applicable challenges 54
7.10.3 Key approaches 54
7.10.4 Cross-reference table (Table 20) 55
7.11 ISO/IEC 27005:2018, 9.2 Risk modification 55
7.11.1 Summary 55
7.11.2 Applicable challenges 56
7.11.3 Key approaches 56
7.11.4 Cross-reference table (Table 22) 57
7.12 ISO/IEC 27005:2018, 9.3 Risk retention 58
7.12.1 Summary 58
7.12.2 Applicable challenges 58
7.12.3 Key approaches 58
7.12.4 Cross-reference table (Table 23) 59
7.13 ISO/IEC 27005:2018, 9.4 Risk avoidance 59
7.13.1 Summary 59
7.13.2 Applicable challenges 59
7.13.3 Key approaches 60
7.13.4 Cross-reference table (Table 25) 60
7.14 ISO/IEC 27005:2018, 9.5 Risk sharing 60
7.14.1 Summary 60
7.14.2 Applicable challenges 60
7.14.3 Key approaches 61

7.14.4 Cross-reference table (Table 27) 61
7.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 61
7.15.1 Summary 61
7.15.2 Applicable challenges 62
7.15.3 Key approaches 62
7.15.4 Cross-reference table (Table 29) 63
7.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 63
7.16.1 Summary 63
7.16.2 Applicable challenges 63
7.16.3 Key approaches 64
7.16.4 Cross-reference table (Table 31) 65
7.17 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 65
7.17.1 Summary 65
7.17.2 Applicable challenges 65
7.17.3 Key approaches 66
7.17.4 Cross-reference table (Table 33) 67
7.18 Overall summary of approaches to challenges 67
8 Conclusions 68
Annex A (informative) Chinese approach 71
A.1 Summary of general approach 71
A.2 ISO/IEC 27005:2018, 7.1 Context establishment 71
A.3 ISO/IEC 27005:2018, 7.2 Basic criteria 72
A.4 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 72
A.5 ISO/IEC 27005:2018, 8.2 Risk identification 72
A.6 ISO/IEC 27005:2018, 8.3 Risk analysis 74
A.7 ISO/IEC 27005:2018, 8.4 Risk evaluation 74
A.8 ISO/IEC 27005:2018, 9.1 General description of risk treatment 74
A.9 ISO/IEC 27005:2018, 9.2 Risk modification 75
A.10 ISO/IEC 27005:2018, 9.3 Risk retention 75
A.11 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 75
A.12 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 76
Annex B (informative) Cyber informed engineering 77
B.1 Summary of general approach 77
B.2 ISO/IEC 27005:2018, 7.1 General considerations 78
B.3 ISO/IEC 27005:2018, 7.2 Basic criteria 78
B.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries 79
B.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 79
B.6 ISO/IEC 27005:2018, 8.2 Risk identification 79
B.7 ISO/IEC 27005:2018, 8.3 Risk analysis 80
B.8 ISO/IEC 27005:2018, 9.2 Risk modification 80
B.9 ISO/IEC 27005:2018, 9.4 Risk avoidance 81
B.10 ISO/IEC 27005:2018, 9.5 Risk sharing 81
B.11 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 81
B.12 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 82
B.13 Reference documents 82

Annex C (informative) French approach 83
C.1 Summary of general approach 83
C.2 EBIOS 83
C.2.1 General 83
C.2.2 EBIOS 2010 83
C.2.3 EBIOS RM 85
C.2.4 Mapping between modules/workshops from EBIOS methods and challenges 86
C.3 ISO/IEC 27005:2018, 7.2 Basic criteria 87
C.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries 87
C.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management 88
C.6 ISO/IEC 27005:2018, 8.2 Risk identification 88
C.7 ISO/IEC 27005:2018, 8.3 Risk analysis 89
C.8 ISO/IEC 27005:2018, 8.4 Risk evaluation 89
C.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment 90
C.10 ISO/IEC 27005:2018, 9.2 Risk modification 90
C.11 ISO/IEC 27005:2018, 9.3 Risk retention 91
C.12 ISO/IEC 27005:2018, 9.4 Risk avoidance 92
C.13 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 92
C.14 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 93
C.15 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 93
Annex D (informative) German approach 95
D.1 Summary of general approach 95
D.2 ISO/IEC 27005:2018, 7.1 General considerations 95
D.3 ISO/IEC 27005:2018, 7.2 Basic criteria 95
D.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries 96
D.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 96
D.6 ISO/IEC 27005:2018, 8.2 Risk identification 96
D.7 ISO/IEC 27005:2018, 8.3 Risk analysis 97
D.8 ISO/IEC 27005:2018, 8.4 Risk evaluation 97
D.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment 97
D.10 ISO/IEC 27005:2018, 9.2 Risk modification 97
D.11 ISO/IEC 27005:2018, 9.3 Risk retention 98
D.12 ISO/IEC 27005:2018, 9.4 Risk avoidance 98
D.13 ISO/IEC 27005:2018, 9.5 Risk sharing 98
D.14 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 98
D.15 ISO/IEC 27005 :2018,Clause 11 Information security risk communication and consultation 99
D.16 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 99
Annex E (informative) Harmonized threat and risk assessment (Canada) 100
E.1 ISO/IEC 27005:2018, 7.2 Basic criteria 100
E.2 ISO/IEC 27005:2018, 7.3 Scope and boundaries 100
E.3 ISO/IEC 27005:2018, 7.4 Organization for information security risk management 101
E.4 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 101
E.5 ISO /IEC 27005:2018, 8.2 Risk identification 102

E.6 ISO/IEC 27005:2018, 8.3 Risk analysis 104
E.7 ISO/IEC 27005:2018, 8.4 Risk evaluation 104
E.8 ISO/IEC 27005:2018, 9.1 General description of risk treatment 104
E.9 ISO/IEC 27005:2018, 9.2 Risk modification 105
E.10 ISO/IEC 27005:2018, 9.3 Risk retention 105
E.11 ISO/IEC 27005:2018, 9.4 Risk avoidance 105
E.12 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 105
E.13 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 106
E.14 ISO/IEC 27005:2018, 12 Security risk monitoring and review 106
E.15 Reference document 107
Annex F (informative) HAZCADS approach 108
F.1 Summary of general approach 108
F.2 ISO/IEC 27005:2018, 7.1 General considerations 109
F.3 ISO/IEC 27005:2018, 7.2 Basic criteria 110
F.4 ISO/IEC 27005:2018,7.3 Scope and boundaries 110
F.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 111
F.6 ISO/IEC 27005:2018, 8.2 Risk identification 111
F.7 ISO/IEC 27005:2018, 8.3 Risk analysis 112
F.8 ISO/IEC 27005:2018, 8.4 Risk evaluation 113
F.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment 113
F.10 ISO/IEC 27005:2018, 9.2 Risk modification 113
F.11 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 113
F.12 Reference documents 114
Annex G (informative) IAEA computer security risk management 115
G.1 Summary of general approach 115
G.2 ISO/IEC 27005:2018, 7.1 General considerations 116
G.3 ISO/IEC 27005:2018, 7.2 Basic criteria 116
G.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries 117
G.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management 118
G.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 118
G.7 ISO/IEC 27005:2018, 8.2 Risk identification 118
G.8 ISO/IEC 27005:2018, 8.3 Risk analysis 119
G.9 ISO/IEC 27005:2018, 8.4 Risk evaluation 120
G.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment 120
G.11 ISO/IEC 27005:2018, 9.2 Risk modification 121
G.12 ISO/IEC 27005:2018, 9.3 Risk retention 121
G.13 ISO/IEC 27005:2018, 9.4 Risk avoidance 121
G.14 ISO/IEC 27005:2018, 9.5 Risk sharing 121
G.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 122
G.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 122
G.17 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 122
Annex H (informative) IEC 62443 123
H.1 Summary of general approach 123
H.2 ISO/IEC 27005:2018, 7.1 General considerations 124

H.3 ISO/IEC 27005:2018, 7.2 Basic criteria ... 125
H.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries ... 125
H.5 ISO/IEC 27005:2018,7.4 Organization for information security risk management ... 125
H.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment ... 126
H.7 ISO/IEC 27005:2018, 8.2 Risk identification ... 126
H.8 ISO/IEC 27005:2018, 8.3 Risk analysis ... 127
H.9 ISO/IEC 27005:2018, 8.4 Risk evaluation ... 128
H.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment ... 128
H.11 ISO/IEC 27005:2018, 9.2 Risk modification ... 128
H.12 ISO/IEC 27005:2018, 9.3 Risk retention ... 129
H.13 ISO/IEC 27005:2018, 9.4 Risk avoidance ... 129
H.14 ISO/IEC 27005:2018, 9.5 Risk sharing ... 129
H.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance ... 129
H.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation ... 129
H.17 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review ... 130
Annex I (informative) Russian approach ... 131
I.1 Summary of general approach ... 131
I.2 ISO/IEC 27005:2018, 7.1 General considerations ... 132
I.3 ISO/IEC 27005:2018, 7.2 Basic criteria ... 132
I.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries ... 133
I.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management ... 133
I.6 ISO/IEC 27005:2018, 8.2 Risk identification ... 134
I.7 ISO/IEC 27005:2018, 8.3 Risk analysis ... 134
I.8 ISO/IEC 27005:2018, 8.4 Risk evaluation ... 135
I.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment ... 135
I.10 ISO/IEC 27005:2018, 9.2 Risk modification ... 136
I.11 ISO/IEC 27005:2018, 9.3 Risk retention ... 136
I.12 ISO/IEC 27005:2018, 9.4 Risk avoidance ... 136
I.13 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance ... 137
I.14 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation ... 137
I.15 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review ... 138
I.16 Reference documents ... 138
Annex J (informative) US NRC ... 139
J.1 Summary of general approach ... 139
J.2 ISO/IEC 27005:2018, 7.1 Context establishment ... 139
J.3 ISO/IEC 27005:2018, 7.2 Basic criteria ... 140
J.4 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment ... 140
J.5 ISO/IEC 27005:2018, 8.2 Risk identification ... 141
J.6 ISO/IEC 27005:2018, 8.3 Risk analysis ... 142
J.7 ISO/IEC 27005:2018, 8.4 Risk evaluation ... 142
J.8 ISO/IEC 27005:2018, 9.1 General description of risk treatment ... 143
J.9 ISO/IEC 27005:2018, 9.2 Risk modification ... 144
J.10 ISO/IEC 27005:2018, 9.3 Risk retention ... 144
J.11 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance ... 145

J.12 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 146
J.13 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 147
Annex K (informative) United Kingdom 148
K.1 Summary of general approach 148
K.2 ISO/IEC 27005:2018, 7.2 Basic criteria 148
K.3 ISO/IEC 27005:2018,7.3 Scope and boundaries 149
K.4 ISO/IEC 27005:2018, 7.4 Organization for information security risk management 151
K.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment 151
K.6 ISO/IEC 27005:2018, 8.2 Risk identification 152
K.7 ISO/IEC 27005:2018, 8.3 Risk analysis 152
K.8 ISO/IEC 27005:2018, 8.4 Risk evaluation 153
K.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment 154
K.10 ISO/IEC 27005:2018, 9.2 Risk modification 154
K.11 ISO/IEC 27005:2018, 9.3 Risk retention 155
K.12 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance 155
K.13 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation 155
K.14 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review 156
Bibliography 157

Figure 1 – Overview of the Hierarchy of IEC SC 45A Standards Related to Cyber Security 19
Figure 2 – Technical Report Development Approach 31
Figure C.1 – EBIOS 2010 Process Overview 84
Figure C.2 – EBIOS Risk Manager Overview [11] 85
Figure E.1 – HTRA Risk Formula (Figure B-4 of [8]) 102
Figure F.1 – Overview of HAZCADS Method (See Reference documents, EPRI 2018) 109
Figure H.1 – Parts of the ISA/IEC 62443 Series [39] 124
Figure I.1 – Overview the Relation of the FSTEC Approach for Risk Assessment and ISO/IEC 27005 131
Figure K.1 – UK IS/DBSy approach: Example InfoSec model 150

Table 1 – Risk management challenges 28
Table 2 – Cyber-risk approaches 30
Table 3 – ISO/IEC 27005 Clause 7.1: Applicable challenges 36
Table 4 – ISO/IEC 27005 Clause 7.1: Cross reference table 37
Table 5 – ISO/IEC 27005 Clause 7.2: Applicable challenges 38
Table 6 – ISO/IEC 27005 Clause 7.2: Cross reference table 40
Table 7 – ISO/IEC 27005 Clause 7.3: Applicable challenges 40
Table 8 – ISO/IEC 27005 Clause 7.3: Cross reference table 42
Table 9 – ISO/IEC 27005 Clause 7.4: Applicable challenges 43
Table 10 – ISO/IEC 27005 Clause 7.4: Cross reference table 43
Table 11 – ISO/IEC 27005 Clause 8.1: Applicable challenges 44
Table 12 – ISO/IEC 27005 Clause 8.1: Cross reference table 45

Table 13 – ISO/IEC 27005 Clause 8.2: Applicable challenges 46
Table 14 – ISO/IEC 27005 Clause 8.2: Cross reference table 48
Table 15 – ISO/IEC 27005 Clause 8.3: Applicable challenges 49
Table 16 – ISO/IEC 27005 Clause 8.3: Cross reference table 51
Table 17 – ISO/IEC 27005 Clause 8.4: Applicable challenges 52
Table 18 – ISO/IEC 27005 Clause 8.4: Cross reference table 53
Table 19 – ISO/IEC 27005 Clause 9.1: Applicable challenges 54
Table 20 – ISO/IEC 27005 Clause 9.1: Cross reference table 55
Table 21 – ISO/IEC 27005 Clause 9.2: Applicable challenges 56
Table 22 – ISO/IEC 27005 Clause 9.2: Cross reference table 57
Table 23 – ISO/IEC 27005 Clause 9.3: Cross reference table 59
Table 24 – ISO/IEC 27005 Clause 9.4: Applicable challenges 60
Table 25 – ISO/IEC 27005 Clause 9.4: Cross reference table 60
Table 26 – ISO/IEC 27005 Clause 9.5: Applicable challenges 61
Table 27 – ISO/IEC 27005 Clause 9.5: Cross reference table 61
Table 28 – ISO/IEC 27005 Clause 10: Applicable challenges 62
Table 29 – ISO/IEC 27005 Clause 10: Cross reference table 63
Table 30 – ISO/IEC 27005 Clause 11: Applicable challenges 63
Table 31 – ISO/IEC 27005 Clause 11: Cross reference table 65
Table 32 – ISO/IEC 27005 Clause 12: Applicable challenges 66
Table 33 – ISO/IEC 27005 Clause 12: Cross reference table 67
Table 34 – Summary of approaches to challenges 68
Table A.1 – Chinese approach: Challenges addressed 71
Table A.2 – Chinese approach: Insights for ISO/IEC Clause 7.1 71
Table A.3 – Chinese approach: Insights for ISO/IEC Clause 7.2 72
Table A.4 – Chinese approach: Insights for ISO/IEC Clause 8.1 72
Table A.5 – Chinese approach: Insights for ISO/IEC Clause 8.2 73
Table A.6 – Chinese approach: Insights for ISO/IEC Clause 8.3 74
Table A.7 – Chinese approach: Insights for ISO/IEC Clause 8.4 74
Table A.8 – Chinese approach: Insights for ISO/IEC Clause 9.1 75
Table A.9 – Chinese approach: Insights for ISO/IEC Clause 9.2 75
Table A.10 – Chinese approach: Insights for ISO/IEC Clause 9.3 75
Table A.11 – Chinese approach: Insights for ISO/IEC Clause 10 75
Table A.12 – Chinese approach: Insights for ISO/IEC Clause 12 76
Table B.1 – Cyber-Informed Engineering: Key challenges addressed 77
Table B.2 – Cyber-Informed Engineering: Challenges indirectly addressed 78
Table B.3 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 7.2 79
Table B.4 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 7.3 79
Table B.5 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 8.2 80
Table B.6 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 8.3 80
Table B.7 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 9.2 81
Table B.8 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 9.4 81
Table B.9 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 9.5 81

Table B.10 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 11 81
Table B.11 – Cyber-Informed Engineering: Insights for ISO/IEC Clause 12 82
Table C.1 – French approach: Challenges addressed 86
Table C.2 – French approach: Insights for ISO/IEC Clause 7.2 87
Table C.3 – French approach: Insights for ISO/IEC Clause 7.3 87
Table C.4 – French approach: Insights for ISO/IEC Clause 7.4 88
Table C.5 – French approach: Insights for ISO/IEC Clause 8.2 88
Table C.6 – French approach: Insights for ISO/IEC Clause 8.3 89
Table C.7 – French approach: Insights for ISO/IEC Clause 8.4 89
Table C.8 – French approach: Insights for ISO/IEC Clause 9.1 90
Table C.9 – French approach: Insights for ISO/IEC Clause 9.2 91
Table C.10 – French approach: Insights for ISO/IEC Clause 9.3 91
Table C.11 – French approach: Insights for ISO/IEC Clause 9.4 92
Table C.12 – French approach: Insights for ISO/IEC Clause 10 93
Table C.13 – French approach: Insights for ISO/IEC Clause 11 93
Table C.14 – French approach: Insights for ISO/IEC Clause 12 94
Table D.1 – German approach: Insights for ISO/IEC Clause 7.1 95
Table D.2 – German approach: Insights for ISO/IEC Clause 7.2 95
Table D.3 – German approach: Insights for ISO/IEC Clause 7.3 96
Table D.4 – German approach: Insights for ISO/IEC Clause 8.1 96
Table D.5 – German approach: Insights for ISO/IEC Clause 8.2 96
Table D.6 – German approach: Insights for ISO/IEC Clause 8.3 97
Table D.7 – German approach: Insights for ISO/IEC Clause 8.4 97
Table D.8 – German approach: Insights for ISO/IEC Clause 9.1 97
Table D.9 – German approach: Insights for ISO/IEC Clause 9.2 97
Table D.10 – German approach: Insights for ISO/IEC Clause 9.3 98
Table D.11 – German approach: Insights for ISO/IEC Clause 9.4 98
Table D.12 – German approach: Insights for ISO/IEC Clause 9.5 98
Table D.13 – German approach: Insights for ISO/IEC Clause 10 98
Table D.14 – German approach: Insights for ISO/IEC Clause 11 99
Table D.15 – German approach: Insights for ISO/IEC Clause 12 99
Table E.1 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 7.2 100
Table E.2 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 7.3 101
Table E.3 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 7.4 101
Table E.4 – HTRA: Relationship between threat capability and gravity [8] 103
Table E.5 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 8.2 103
Table E.6 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 8.3 104
Table E.7 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 8.4 104
Table E.8 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 9.1 104
Table E.9 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 9.2 105
Table E.10 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 9.3 105
Table E.11 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 9.4 105
Table E.12 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 10 106

Table E.13 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 11 106
Table E.14 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 12 106
Table F.1 – HAZCADs approach: Key challenges addressed 108
Table F.2 – HAZCADs approach: Challenges indirectly addressed 108
Table F.3 – HAZCADs approach: Insights for ISO/IEC Clause 7.1 109
Table F.4 – HAZCADs approach: Insights for ISO/IEC Clause 7.2 110
Table F.5 – HAZCADs approach: Insights for ISO/IEC Clause 7.3 111
Table F.6 – HAZCADs approach: Insights for ISO/IEC Clause 8.2 112
Table F.7 – HAZCADs approach: Insights for ISO/IEC Clause 8.3 112
Table F.8 – HAZCADs approach: Insights for ISO/IEC Clause 8.4 113
Table F.9 – HAZCADs approach: Insights for ISO/IEC Clause 9.2 113
Table F.10 – HAZCADs approach: Insights for ISO/IEC Clause 11 114
Table G.1 – IAEA approach: Key challenges addressed 115
Table G.2 – IAEA approach: Challenges indirectly addressed 115
Table G.3 –IAEA approach: Insights for ISO/IEC Clause 7.1 116
Table G.4 – IAEA approach: Insights for ISO/IEC Clause 7.2 117
Table G.5 – IAEA approach: Insights for ISO/IEC Clause 7.3 117
Table G.6 – IAEA approach: Insights for ISO/IEC Clause 7.4 118
Table G.7 – IAEA approach: Insights for ISO/IEC Clause 8.1 118
Table G.8 – IAEA approach: Insights for ISO/IEC Clause 8.2 119
Table G.9 – IAEA approach: Insights for ISO/IEC Clause 8.3 119
Table G.10 – IAEA approach: Insights for ISO/IEC Clause 8.4 120
Table G.11 – IAEA approach: Insights for ISO/IEC Clause 9.1 120
Table G.12 – IAEA approach: Insights for ISO/IEC Clause 9.2 121
Table G.13 – IAEA approach: Insights for ISO/IEC Clause 9.3 121
Table G.14 – IAEA approach: Insights for ISO/IEC Clause 11 122
Table G.15 – IAEA approach: Insights for ISO/IEC Clause 12 122
Table H.1 – IEC 62443: Key challenges addressed 123
Table H.2 – IEC 62443: Challenges indirectly addressed 124
Table H.3 – IEC 62443: Insights for ISO/IEC Clause 7.1 124
Table H.4 – IEC 62443: Insights for ISO/IEC Clause 7.2 125
Table H.5 – IEC 62443: Insights for ISO/IEC Clause 7.3 125
Table H.6 – IEC 62443: Insights for ISO/IEC Clause 7.4 125
Table H.7 – IEC 62443: Insights for ISO/IEC Clause 8.1 126
Table H.8 – IEC 62443: Insights for ISO/IEC Clause 8.2 127
Table H.9 – IEC 62443: Insights for ISO/IEC Clause 8.3 127
Table H.10 – IEC 62443: Insights for ISO/IEC Clause 8.4 128
Table H.11 – IEC 62443: Insights for ISO/IEC Clause 9.1 128
Table H.12 – IEC 62443: Insights for ISO/IEC Clause 9.2 128
Table H.13 – IEC 62443: Insights for ISO/IEC Clause 9.5 129
Table H.14 – IEC 62443: Insights for ISO/IEC Clause 11 129
Table H.15 – IEC 62443: Insights for ISO/IEC Clause 12 130
Table I.1 – FSTEC Document References 132

Table I.2 – Russian approach: Insights for ISO/IEC Clause 7.1 132
Table I.3 – Russian approach: Insights for ISO/IEC Clause 7.2 133
Table I.4 – Russian approach: Insights for ISO/IEC Clause 7.3 133
Table I.5 – Russian approach: Insights for ISO/IEC Clause 7.4 133
Table I.6 – Russian approach: Insights for ISO/IEC Clause 8.2 134
Table I.7 – Russian approach: Insights for ISO/IEC Clause 8.3 134
Table I.8 – Russian approach: Insights for ISO/IEC Clause 8.4 135
Table I.9 – Russian approach: Insights for ISO/IEC Clause 9.1 135
Table I.10 – Russian approach: Insights for ISO/IEC Clause 9.2 136
Table I.11 – Russian approach: Insights for ISO/IEC Clause 9.3 136
Table I.12 – Russian approach: Insights for ISO/IEC Clause 9.4 136
Table I.13 – Russian approach: Insights for ISO/IEC Clause 10 137
Table I.14 – Russian approach: Insights for ISO/IEC Clause 11 137
Table I.15 – Russian approach: Insights for ISO/IEC Clause 12 138
Table J.1 – US NRC: Insights for ISO/IEC Clause 7.1 139
Table J.2 – US NRC: Insights for ISO/IEC Clause 7.2 140
Table J.3 – US NRC: Insights for ISO/IEC Clause 8.1 141
Table J.4 – US NRC: Insights for ISO/IEC Clause 8.2 142
Table J.5 – US NRC: Insights for ISO/IEC Clause 8.3 142
Table J.6 – US NRC: Insights for ISO/IEC Clause 8.4 143
Table J.7 – US NRC: Insights for ISO/IEC Clause 9.1 144
Table J.8 – US NRC: Insights for ISO/IEC Clause 9.2 144
Table J.9 – US NRC: Insights for ISO/IEC Clause 9.3 145
Table J.10 – US NRC: Insights for ISO/IEC Clause 10 146
Table J.11 – US NRC: Insights for ISO/IEC Clause 11 146
Table J.12 – US NRC: Insights for ISO/IEC Clause 12 147
Table K.1 – UK IS/DBSy approach: Insights for ISO/IEC Clause 7.2 148
Table K.2 – UK IS/DBSy approach: Examples of object types 149
Table K.3 – UK IS/DBSy approach: Insights for ISO/IEC Clause 7.3 150
Table K.4 – UK IS/DBSy approach: Insights for ISO/IEC Clause 7.4 151
Table K.5 – UK IS/DBSy approach: Insights for ISO/IEC Clause 8.1 151
Table K.6 – UK IS/DBSy approach: Insights for ISO/IEC Clause 8.3 152
Table K.7 – UK IS/DBSy approach: Insights for ISO/IEC Clause 8.3 153
Table K.8 – UK IS/DBSy approach: Insights for ISO/IEC Clause 8.4 153
Table K.9 – UK IS/DBSy approach: Insights for ISO/IEC Clause 9.1 154
Table K.10 – UK IS/DBSy approach: Insights for ISO/IEC Clause 9.2 154
Table K.11 – UK IS/DBSy approach: Insights for ISO/IEC Clause 9.3 155
Table K.12 – UK IS/DBSy approach: Insights for ISO/IEC Clause 10 155
Table K.13 – UK IS/DBSy approach: Insights for ISO/IEC Clause 12 156