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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR FACILITIES – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY RISK MANAGEMENT APPROACHES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TR 63486 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear Instrumentation. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
45A/1522/DTR	45A/1541/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This document focuses on methods for implementing cybersecurity risk management processes for instrumentation and control (I&C) systems and electrical power systems (EPS) at NPPs, resulting in various cyber-risk approaches. The goal of this document applies a common analysis process to each of the cyber-risk approaches to identify and evaluate key insights for cyber-risk management for I&C systems and EPS of NPPs to support potential development of an international standard based upon common elements.

This report considers eleven challenges for applying ISO/IEC 27005:2018 cybersecurity risk management to I&C systems and EPS of NPPs. The report compares how the cyber-risk approaches address these challenges. This report identifies common elements, if any, between these approaches. These common elements will be further analyzed to determine if there is sufficient consensus to recommend developing an IEC risk management standard for I&C Systems and EPS at NPPs.

It is intended that this standard be used by operators of NPPs (utilities), systems evaluators and by licensors.

b) Situation of the current standard in the structure of the IEC SC 45A standard series

IEC TR 63486 is a fourth level IEC SC 45A document. Within the general principles defined by IEC 62645 as the entry level document for IEC SC 45A security standards, this document summarizes an evaluation of cyber-risk approaches that are in use by NPP operators to manage cybersecurity risks.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the standard

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

To ensure that the standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The IEC SC 45A standard series comprises a hierarchy of four levels. The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046.

IEC 61513 provides general requirements for instrumentation and control (I&C) systems and equipment that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems.

IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical power systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general requirements for specific topics, such as categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, human factors engineering, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific requirements for specific equipment, technical methods, or activities. Usually these documents, which make reference to second-level documents for general requirements, can be used on their own.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1 , establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs, the IAEA safety guide SSG-51 dealing with human factors engineering in the design of NPPs and the implementing guide NSS42-G for computer security at nuclear facilities. The safety and security terminology and definitions used by the SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework, IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 and IEC 63046 refer to ISO 9001 as well as to IAEA GSR part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards, IEC 63351 is the entry document for the human factors engineering standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards), international or national standards would be applied.

NOTE 2 IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A standards series and of its relationship with other standards bodies and standards.

NUCLEAR FACILITIES – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY RISK MANAGEMENT APPROACHES

1 Scope

1.1 General

IEC 62645 [1][1] provides a cybersecurity framework for digital I&C programmable systems[2]. IEC 62645 [1] aligns strongly with the information security management system (ISMS) elements detailed within ISO/IEC 27001:2013 [2]. The “I&C digital programmable system security programme” (as defined in 5.2.1 of IEC 62645:2019 [1]) align with the ISMS programme.

The framework for this programme assigns security degrees (SD) to I&C systems and EPS and defines cybersecurity requirements based upon these SDs. The assignment of an SD corresponds heavily to the safety categorization of IEC 61513 [3] and IEC 61226 [4].

IEC 62645 [1] does not provide detailed guidance on risk management. The only guidance outlined in IEC 62645:2019 [1] is in 5.4.3.2.2.4, and it states, that ISO/IEC 27005 [5] “provides a generic framework for information security risk assessment, but the specific implementation methodology is up to the organization, depending on its organizational, industrial, and regulatory context.”

IEC 62645:2019 [1] also references risk in 5.4.3.2.2.5, stating:

> “The specific risk assessment methodologies and tools shall be identified and kept up to date. Risk re-assessments shall be performed periodically throughout the whole life cycle of the I&C systems, when modifications to the system occur and when changes to the threat landscape are identified, such as new threats or new vulnerabilities that can affect the installed I&C programmable digital system. The number of potential threats and vulnerabilities usually increases with progress from stand-alone to interconnected systems.”

In recent years, there have been advances in NPP cybersecurity risk management nationally and internationally. For example, International Atomic Energy Agency (IAEA) publications Nuclear Security Series (NSS) 17-T [6] and NSS 33-T [7], propose a framework for computer security risk management that implements a risk management program at both the facility and individual system levels. These international approaches (i.e., IAEA), national approaches (e.g., Canada’s HTRA [8]) and technical methods[3] (e.g., HAZCADS [9], Cyber Informed Engineering [10], EBIOS [11] [12]) have advanced risk management within NPP cybersecurity programmes that implement international and national standards.

The scope of this document is to capture the national and international cyber-risk approaches employed to manage cybersecurity risks associated with Instrumentation and Control (I&C) and Electrical Power Systems (EPS) at a Nuclear Power Plant (NPP).

---

1 Numbers in square brackets refer to the Bibliography.

2 The terms I&C system and EPS in this document refers to those systems which are digital and thus susceptible to cyber-attacks.

3 The term “cyber-risk approaches” is used in this document to refer to international approaches, national approaches and technical methods.

This report inherits the scope from IEC 62645 [1], which defines adequate measures for the prevention of, detection of, and reaction to malicious acts by digital means (cyberattacks) on I&C systems and EPS. This scope includes any malicious act that creates an unsafe situation, equipment damage, or plant performance degradation, such as:

- Malicious modifications affecting system integrity;
- Malicious interference with information, data, or resources that could compromise the delivery of or performance of the required I&C system's programmable digital functions;
- Malicious interference with information, data, or resources that could compromise operator displays or lead to loss of management of I&C systems or EPS; and
- Malicious hardware, firmware, or software changes at the programmable logic controller level.

Human errors leading to violation of the security policy and those impacting the performance of cybersecurity controls are key risks to be assessed by risk management processes evaluated for this document.

This document summarizes an evaluation of cyber-risk approaches that are in use by nuclear facility operators to manage cybersecurity risks.

The scope of this document generally follows the exclusions of IEC 62645 [1] which are:

- Non-malevolent actions and events such as accidental failures, human errors (except those stated above, such as impacting the performance of cybersecurity controls), and natural events. In particular, good practices for managing applications and data, including backup and restoration related to accidental failure, are out of scope.

NOTE 1 Although security programs in other normative contexts often cover such aspects (e.g., in the ISO/IEC 27000 series [13] or IEC 62443 series [14]), this document is only focused on evaluating risk management processes that manage risks associated with malicious acts by digital means (cyberattacks) on digital I&C systems (I&C) and Electrical Power Systems (EPS). The main reason for the limitation in scope is that in the nuclear generation domain, other standards and practices already cover accidental failures, unintentional human errors, natural events, etc. The focus of this document is to provide the maximum consistency and the minimum overlap with these other nuclear standards and practices, especially IEC 62645 [1].

- Site physical security, access control (site and specific locations within the site), and site security surveillance systems. While not explicitly addressed in IEC 62645 [1], these systems are generally covered by plant operating procedures and programmes.

NOTE 2 This exclusion does not deny that cybersecurity has clear dependencies on the security of the physical environment (e.g., physical protection, or heating/ventilation/air-conditioning systems). However, this exclusion is based on the scope of IEC subcommittee and the working group that developed this document.

- Confidentiality of information regarding I&C systems and EPS is not within the scope of IEC 62645 [1] (see IEC 62645:2019 [1], 5.4.3.2.3). However, unauthorized disclosure of sensitive information regarding I&C systems or EPS can lead to changes in risks associated with those systems. Loss of confidentiality and its impact on risks were considered within this evaluation.

Standards such as ISO/IEC 27001:2013 [2] and ISO/IEC 27005:2018 [5] are not directly applicable to the cyber protection of NPP I&C systems and EPS. The regulatory and safety requirements needed for the safe operation of systems within an NPP render much of the ISO/IEC 27001:2013 [2] and ISO/IEC 27005:2018 [5] content immaterial or inadequate. However, IEC 62645 [1] builds upon the valid high-level principles and main concepts of ISO/IEC 27001:2013 [2], adapts them, and completes them to fit into the nuclear context. In a similar manner, this document aims to evaluate and summarize key insights within ISO/IEC 27005:2018 [5] risk management elements for possible adaptation for a potential standard under IEC 62645 [1] NPP cybersecurity programmes.

An overview of the hierarchy of IEC SC 45A standards related to cybersecurity is shown in Figure 1.

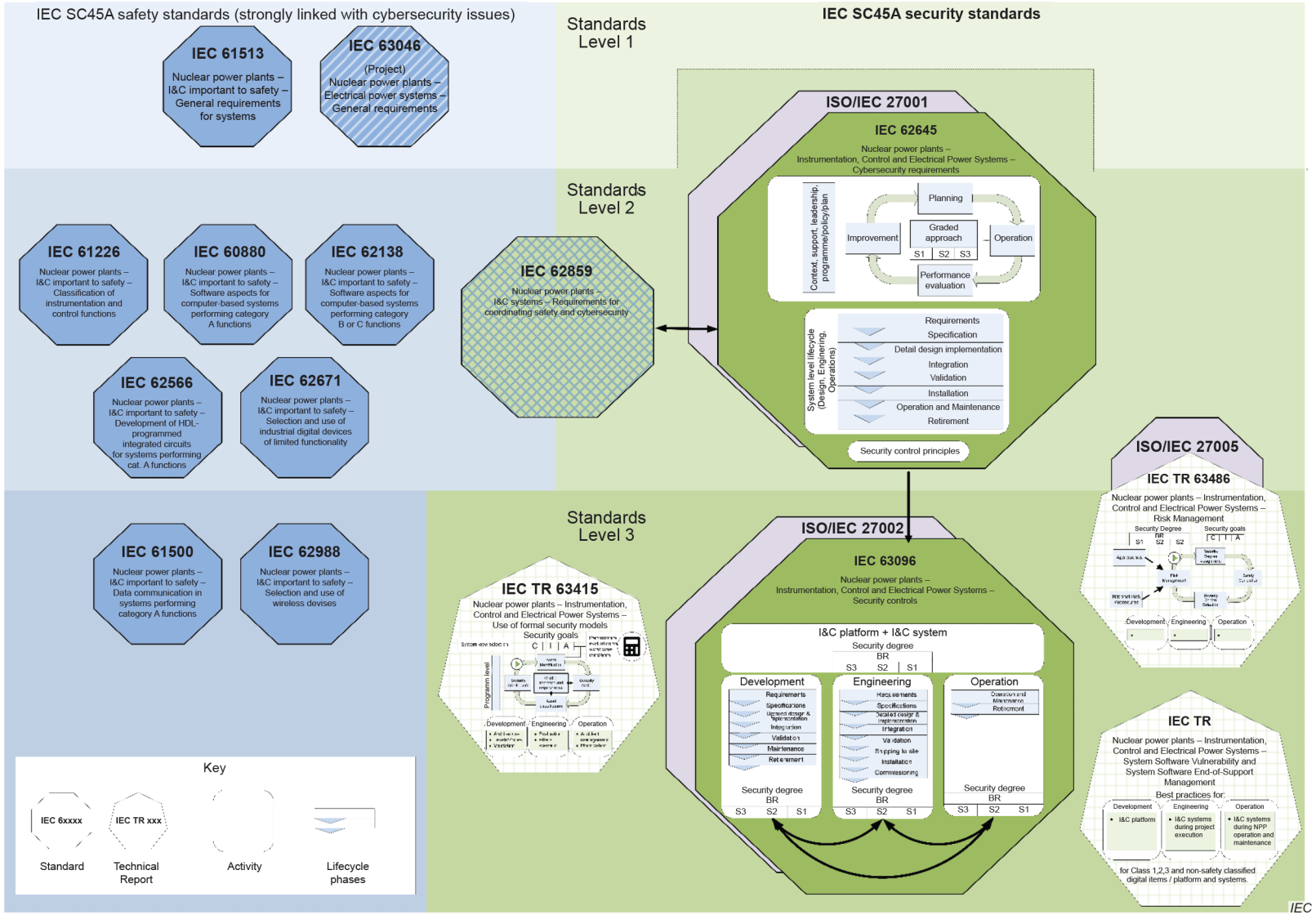

Figure 1 – Overview of the hierarchy of IEC SC 45A standards related to cyber security

1.2 Framework

This document summarizes key insights of the international and cyber-risk approaches used at NPPs regarding the application of ISO/IEC 27005:2018 [5]. The evaluation is based on 11 challenges to cybersecurity risk management and their applicability to NPP risk management. The challenges are detailed in Clause 7.

The risk management elements within ISO/IEC 27005:2018 [5] considered within the evaluation are listed below:

- Context Establishment (external and internal)
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Decision Point 1 (Assessment satisfactory)
- Risk Treatment
- Risk Decision Point 2 (Treatment satisfactory)
- Risk Acceptance
- Risk Communication and Consultation
- Monitoring and Review

This document also relates the risk management elements of IEC 62645 [1] and IEC 63096 [15].

1.3 Limitations

This document is limited to the scope defined in IEC 62645 [1]. Therefore, this document assumes that I&C systems and EPS do not directly contribute to the potential theft of nuclear material. The risk of theft of nuclear material and its consequence is covered through the design, implementation, and operation of Physical Protection Systems and the design and operation of these are unique for each NPP.

2 Normative references

There are no normative references in this document.