PD IEC TR 63486:2024

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

National foreword

This Published Document is the UK implementation of IEC/TR 63486:2024.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Instrumentation, Control & Electrical Systems of Nuclear Facilities.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 33762 4

ICS 27.100; 27.120.20

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub

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 ... 144

AVA Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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

AVA Documents
Document Sharing Hub

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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.

Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

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.

AVA Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

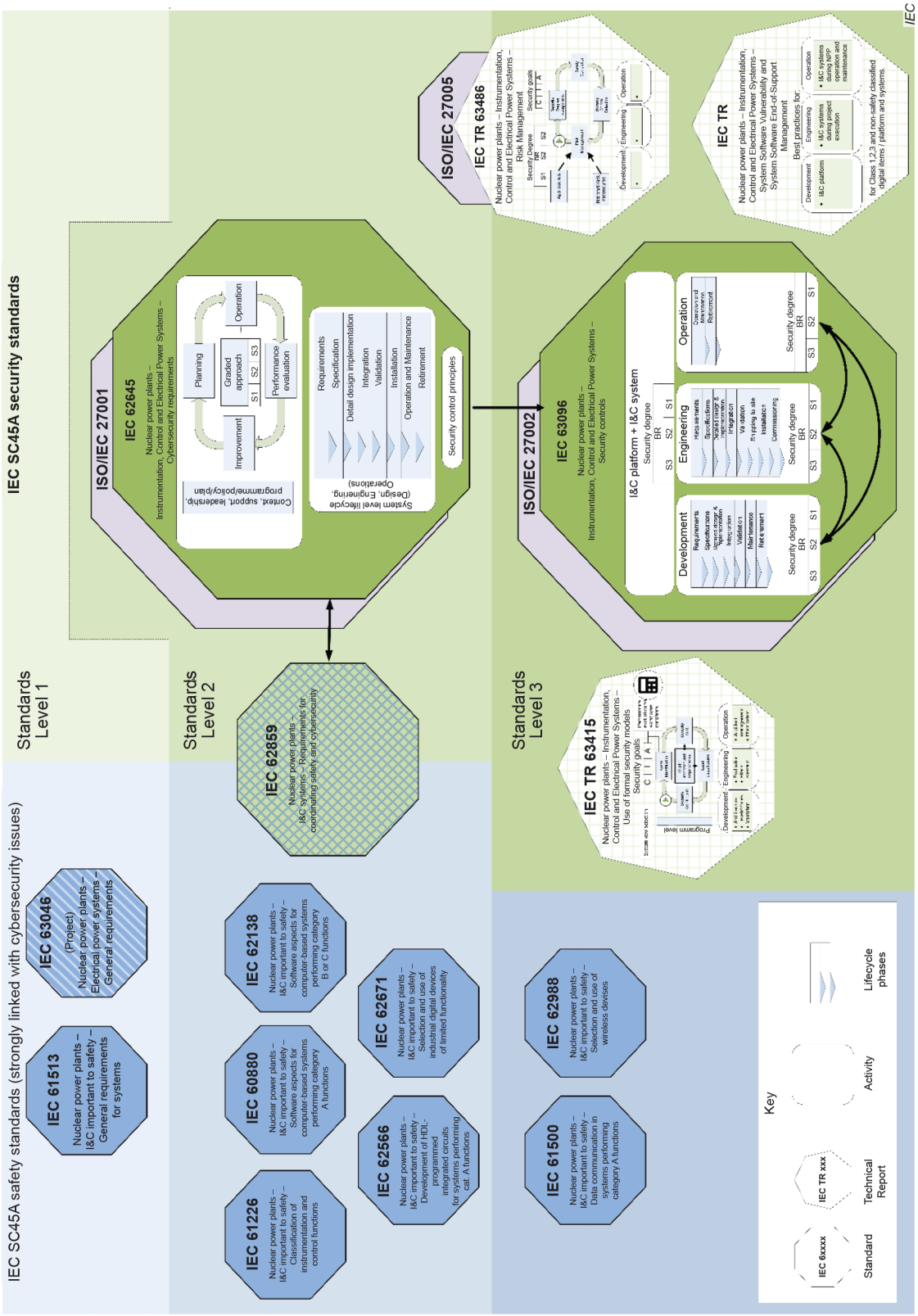

Figure 1 – Overview of the hierarchy of IEC SC 45A standards related to cyber security

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

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.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia [16]: available at http://www.electropedia.org/
- ISO Online browsing platform [17]: available at http://www.iso.org/obp
- IAEA Nuclear Safety and Security Glossary [18] available at https://www.iaea.org/publications/15236/iaea-nuclear-safety-and-security-glossary

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

3.1
attack pathway
path or *route* by which an attacker or malicious program can gain access to a computer-based system

Note 1 to entry: Examples of attack pathways are (1) physical access, (2) wired network connectivity, (3) wireless network connectivity, (4) portable media/mobile device connectivity, and (5) supply chain.

Note 2 to entry: Adapted from “attack vector” definition from IEC 62645:2019, 3.1.

3.2
attack vector
method or means by which an attacker or malicious program *performs tasks on a* computer-based system

Note 1 to entry: The attack vector enables the attacker to perform tasks after accessing an attack pathway.

[SOURCE: IEC 62645:2019, 3.1]

3.3
authorization
function of specifying access rights to resources, which is related to information security and computer security in general and access control in particular

[SOURCE: IEC 62645:2019, 3.2]

3.4
availability
property of being accessible and usable upon demand by an authorized entity

Note 1 to entry: This definition is specific to the context of security of nuclear information and is therefore different from the one used in other IEC/SC45A standards , which is “ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.”

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 Interim Edition]

3.5
computer-based item
item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: The term item can be replaced by the terms “system,” “equipment,” or “device.”

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to a software-based item.

[SOURCE: IEC 62138:2018, 3.8]

3.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: IAEA Safety and Security Glossary, 2022 Interim Edition]

3.7
cyberattack
malicious acts by digital means

[SOURCE: IEC 62645:2019, 3.6]

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

3.8
cybersecurity
set of activities and measures whose objective is to prevent, detect, and react to:

- *Malicious modifications* (integrity) of functions that may compromise the delivery or integrity of the required service by I&C system (including loss of control) or EPS, which could lead to an accident, an unsafe situation, or plant performance degradation;
- *Malicious withholding or prevention* of access to or communication of information, data, or resources (including loss of view) that could compromise the delivery of the required service by I&C systems or EPS (availability), which could lead to an accident, an unsafe situation or plant performance degradation;
- *Unauthorised disclosure of information* (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation, or plant performance degradation.

Note 1 to entry: This definition is tailored to reflect the IEC 62645 standard scope and the overall SC 45A document structure. It is recognized the term "cybersecurity" has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors, and protection against natural disasters, those aspects – except human errors that degrade cybersecurity protections – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A of IEC 62645:2019 for more detail regarding this document scope exclusions.

Note 2 to entry: Computer security and cybersecurity are considered synonymous in this document.

3.9
design
process and result of developing a concept, detailed plans, supporting calculations, and specifications for a facility and its parts

[SOURCE: IAEA Nuclear Safety and Security glossary, 2022 Interim Edition]

3.10
design basis threat
DBT
attributes and characteristics of potential insider or external adversaries who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated

Note 1 to entry: Cyberattacks and related adversaries are not considered in an equivalent manner in DBTs; this depends on each cyber-risk approach and legal framework. Moreover, the content of a nuclear DBT is treated as highly confidential.

Note 2 to entry: IAEA Nuclear Security Series publications leverage the concept of a physical protection system to protect against malicious acts targeting theft of nuclear material or resulting in radiological sabotage. Conversely, IEC SC 45A standards focus on protection against compromise of I&C systems and EPS of resulting in unacceptable impacts to the safety and security of an NPP.

[SOURCE: IAEA NSS No. 13, 2011 modified: notes 1 and 2 added]

3.11
electrical/electronic/programmable electronic item
E/E/PE item
item based on electrical (E) or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: This term and its definition, the word "item," can be replaced by the words: "system," "equipment," or "device."

Note 2 to entry: The definitions of the terms related to the technology: E/E/PE item, programmable digital item, computer-based item, hardwired item, programmable logic item provide a taxonomy that allows for a consistent and coherent means of classifying these items. Programmable digital items are susceptible to cyber-attacks.

[SOURCE: IEC 62138: 2018, 3.15]

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

3.12
Hardware Description Language-programmed device
HPD
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages (HDL) and related software tools

Note 1 to entry: HDLs and related tools (e.g., simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use pre-developed Blocks.

Note 3 to entry: HPDs are typically based on blank Field Programmable gate Arrays or similar micro-electronic technologies.

Note 4 to entry: HPD is a kind of programmable logic item.

Note 5 to entry: See the definition of “E/E/PE item” and the associated notes.

[SOURCE: IEC 62566: 2012, 3.7]

3.13
I&C function
function to control, operate or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.14
I&C system
system, based on E/E/PE items, performs plant instrumentation and control functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: A general term that encompasses all system elements such as internal power supplies, sensors, and other input devices, data highways and other communication paths, interfaces to actuators, and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the system’s boundaries.

Note 3 to entry: See also “electrical power system.” The terms “electrical power system” and “I&C system” are terms related to the main functions the systems perform, respectively, “electrical power generation, transmission and distribution” and “measurement, protection, control and HMI related to the NPP process.” They have to be considered in conjunction and are consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control, and electrical power systems for nuclear power plants.

Note 4 to entry: See also the definition of the E/E/PE item and the associated notes.

Note 5 to entry: According to their typical functionality, IAEA distinguishes between automation/control systems, HMI systems, interlock systems, and protection systems.

[SOURCE: IEC 62138: 2018, 3.26]

3.15
integrity
property of protecting the accuracy and completeness of assets

[SOURCE: ISO/IEC 27000:2018, 3.36, modified – the phrase “of assets” was added]

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

3.16
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment, or device.

Note 2 to entry: See also the definition of the E/E/PE item and the associated notes.

Note 3 to entry: The main kinds of programmable digital items are computer-based and programmable logic items.

Note 4 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined accordingly to IEC 61508.

[SOURCE: IEC 62138:2018, 3.34]

3.17
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.18
risk assessment
overall process of systematically identifying, estimating, analysing, and evaluating risk

[SOURCE: IAEA Nuclear: Safety and Security Glossary, 2022 Interim Edition, modified – the phrase “for the purpose of informing priorities, developing or comparing courses of action, and informing decision making of assets” was deleted]

3.19
security controls
means of managing security which can be technical, physical, or administrative

[SOURCE: IEC 62645:2019, 3.18]

3.20
security degree
gradation of security protection with associated sets of requirements assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance

Note 1 to entry: IEC 62645 defines three security degrees corresponding to S1, S2, and S3. The rationale behind the use of these three degrees for I&C systems is provided in Annex B. This document is limited to I&C systems and EPS and does not make any assumptions about the security degrees for other systems. Non-I&C systems (e.g., office computers) might be assigned to supplemental/different security degrees, leading to a graded approach with more than three security degrees from a global perspective. Moreover, some national practices involved the subdivision of security degrees.

Note 2 to entry: The term “security degree” is preferred to “security level” or avoid possible confusion with the concept of I&C levels commonly found in other standards and industry practices.

[SOURCE: IEC 62645:2019, 3.19]

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

3.21
security programme
set of interrelated or interacting elements of an organization to establish security policies and objectives, as well as processes and security plans to achieve those objectives

Note 1 to entry: Programme is a concept similar to a "management system" as defined in ISO/IEC 27000:2018.

Note 2 to entry: Computer security programme, cybersecurity programme, and security programme are considered synonymous in this document.

[SOURCE: IEC 62645:2019, 3.20]

3.22
threat
potential cause of an unwanted incident, which may result in harm to a system, organization, or people

Note 1 to entry: In the frame of this document (see IEC 62645), the considered events or occurrences are limited to malicious ones and to human errors that degrade cybersecurity – not include accidental aspects (e.g., natural hazards, human errors not impacting cybersecurity).

[SOURCE IEC 62645:2019, 3.22, modified – the phrase "harm to a system or organization" was amended to "harm to a system, organization, or people"]

3.23
vulnerability
weakness of an asset or a security control that can be exploited by a threat

[SOURCE: IEC 62645:2019, 3.23]

4 Abbreviated terms

CDA	Critical Digital Asset
CFR	Code for Regulation
CR	Component Requirement
CSP	Computer Security Policy
CERT	Computer Emergency Response Team
CIE	Cyber Informed Engineering
CSRM	Computer Security Risk Management
DBSy	Domain Based Security
DBT	Design Basis Threat
DCSA	Defensive Computer Security Architecture
DER	Detection and Reaction
DiD	Defense in Depth
DI&C	Digital Instrumentation and Control
DBT	Design Basis Threat
DOE	United States Department of Energy
EBIOS	Expression of needs and identification of security objectives
EPRI	Electric Power Research Institute
EPS	Electrical Power System
ES	Electrical System
FCSRM	Facility Computer Security Risk Management

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

FOI	Focus of Interest
FSTEC	Russian Federal Service for Technical and Export Control
FTA	Fault Tree Analysis
HAZCADS	Hazards and Consequences Analysis for Digital Systems
HAZOP	Hazard and Operability
HDL	Hardware Description Language
HMG	His Majesty's Government (UK)
HPD	HDL Programmed Device
HTRA	Harmonized Threat and Risk Assessment Methodology
I&C	Instrumentation and Control
IACS	Industrial Automated Control Systems
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
I&C	Instrumentation and Control
MFA	Multi-factor authentication
NEI	Nuclear Energy Institute
NM	Nuclear Material
NPP	Nuclear Power Plant
NRC	United States Nuclear Regulatory Commission
NSS	Nuclear Security Series
OT	Operational Technology
PRA	Probabilistic Risk Assessment
RE	Requirement Enhancement
RG	Regulatory Guide
RMF	Risk Management Framework
SCSRM	System Computer Security Risk Management
SD	Security Degree
SIEM	Security Information and Event Management
SL	Security Level
SL-T	Security Level – Target
SOC	Security Operations Centre
SR	System Requirement
SSEP	Safety, Security and Emergency Preparendess
STPA	Systems Theoretic Process Analysis
TR	Technical Report
UCA	Unsafe Control Actions
URC	Unacceptable Radiological Consequences
V&V	Verification & Validation

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

5 IEC 62645 risk management elements

5.1 General

IEC 62645:2019, 5.4 [1] provides a high-level outline of cyber security management processes, which are adapted from ISO/IEC 27001:2013 [2]. However, IEC 62645 [1] does not attempt to provide detailed guidance on how to perform a risk management process. IEC 62645 [1] scope is limited to establishing "requirements and provides guidance for the development and management of effective computer security programmes for I&C systems and EPS. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements."

The current approach of IEC 62645 [1] is to establish a cyber security programme that uses the risk assessment process from ISO/IEC 27005:2018 [5] and the risk assessment method adapted from ISO/IEC 27001 [2]. However, the ISO/IEC 27001 [2] and ISO/IEC 27005 [5] standards are not directly applicable to the cyber protection of NPP I&C systems and EPS. As a result, there is a need for further guidance to aid risk management approaches for NPP cybersecurity programmes similar to the relationship between ISO/IEC 27001 [2] and ISO/IEC 27005 [5] to further optimize the allocation of limited resources for cybersecurity at NPPs.

Risk is typically described as consequences times likelihood. However, applying this description in the nuclear domain tends to prioritize consequence over likelihood. This inherent pragmatic assumption as the potentially severe consequences associated with nuclear power plants is unacceptable, and risks associated with these consequences cannot be accepted under any circumstances. Therefore, for instrumentation, control, and electrical systems critical to safety, a near-total reliance on consequence determines the level of effort to ensure these risks are mitigated/reduced to the greatest extent possible.

5.2 Assignment of security degrees in the management of risk

IEC 62645:2019, [1] 5.4.3.1.1.2 outlines a risk classification scheme that is based upon:

a) the consequences of a cyberattack;

b) functional assessment; and

c) consequence-based assignment approach that is rigorous and repeatable.

IEC 62645 [1] requires the application of a graded approach where sets of requirements (i.e., Security Degrees) are imposed on I&C systems and EPS based upon an analysis that identifies and evaluates the potential consequences resulting from compromise of these systems. The three security degrees from most demanding (i.e., most significant consequence) to least demanding are (SD1, SD2, and SD3) and baseline requirements (i.e., requirements that result in generic measures applied to all I&C systems and EPS).

The evaluation of consequences and SD assignments are dependent upon the following risk elements and activities:

- External Context (Regulation, Laws, Safety Classification);
- Internal Context (Operational Performance, Organization Objectives);
- Risk Identification (identification of consequences: ISO/IEC 27005:2018, [5] 8.2.6); and
- Risk Analysis (assessment of consequences: ISO/IEC 27005:2018, [5] 8.3.2).

IEC 62645 [1], however, gives no detailed description of how to implement risk management processes in conjunction with the security degrees and safety classification.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

5.3 Safety correlation

IEC 62645:2019 [1], 5.4.3.1.2 provides guidance on the link between safety categories, safety classes, and SDs. The assignment of the appropriate SD to a system shall consider the effects of a compromise with its safety class. Consequently, the assignment of SD without critical thought based on the safety categories is not recommended as there is no strict one-to-one mapping between safety classes and security degrees for instrumentation, control, and electrical systems. If there is a potential for a cyberattack to increase the consequence severity of the system not operating as expected an assignment to a higher security degree may be warranted.

Typically, the final determination of the SDs is based on the function category or the maximum consequences of a malicious act or event on any part of the function. Concurrence by the personnel responsible for safety and those responsible for security on the determined SD is necessary to ensure that both perspectives are incorporated. This agreement is a necessity to provide the appropriate protection based on the maximum severity associated with the potential safety and security consequences. The agreement shall account for differences in measures put in place for safety that may not provide protection for security. For example, safety systems implement redundant components and systems to increase reliability and avoid potential safety consequences resulting from the failure of these components and systems, thereby ensuring availability. However, implementing identical redundant digital components that contain the same vulnerabilities will provide cyber security protection. The vulnerabilities can be exploited if the primary or secondary systems are active, and the attack can potentially impact integrity and confidentiality.

6 NPP cyber risk management challenges and analyses

6.1 General

This document identifies challenges considered not adequately covered by IEC 62645 [1]. The following sections of this document, summarize and provide analyses of cyber-risk approaches to risk management that could provide insight into these specific challenges affecting NPP operators when managing cybersecurity risks. Challenges affect effective cyber risk management. Challenges can increase uncertainty of elements necessary to measure or estimate risks, increasing complexity or ambiguity in relationships between related risks, activities, or systems, or involve different organizations or methods in risk management activities. The analyses were structured to align the cyber-risk approaches' elements with ISO/IEC 27005:2018 [5], Clauses 7 through 12.

The challenges evaluated in this document are listed in Table 1. Challenges impact risk management activities and increase uncertainty in risk management outputs, but do not represent specific cybersecurity risks (like those associated with theft or sabotage) that are identified, analyzed, evaluated, treated and managed by a nuclear facility operator,

Table 1 – Risk management challenges

#	Description	Rationale
1	**Aggregate risk of multiple units / locations:** There is a need for additional ways to evaluate levels beyond Security Degree assignment for aggregate risk of multiple units / locations.	The analysis focuses on multiple locations (not co-located), and some clauses of IEC 62645 [1] do not address multiple co-located units.
2	**Complexity of interdependencies and interactions:** Identifying and analyzing risks associated with attacks that target more significant functions through their interdependencies and/or interactions with less significant functions.	The NPP may not directly manage risks associated with interdependencies between systems and functions. For example, an attack on a diesel fuel supply may impact standby generator operation or external offsite power.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

#	Description	Rationale
3	**Incident likelihood determination (leading to extremely rare but unacceptable events):** Estimating the likelihood of an extremely rare but unacceptable event is challenging.	Severe accidents at NPPs are extremely rare and can result in unacceptable radiological consequences. Accidents for which the initiating event is a cyberattack are rare and lack statistical data that would allow for likelihood to be considered in risk analysis and evaluation.
4	**Unknown or lacking sufficient detail for pre-developed components:** Pre-developed components that make up digital I&C systems have not been individually identified and evaluated for risks associated with NPP applications. In these cases, the Operator performs the risk assessment and may incur extra effort to treat risk.	Modern supply chains that result in digital I&C system components are complex. Specifically, the NPP operator is not provided a complete bill of materials and software provenance. This gap in information increases uncertainty in risk management activities.
5	**Differences in cyber-risk management:** Many differing risk management processes are used across or within member states.	The differences between member states' regulations or between organizations within a member state with respect to risk management are significant, especially where the level of abstraction is low (e.g., asset).
6	**Lack of abstract analysis methods:** There exists a general lack of guidance on risk management applied to conceptual facilities, systems, and processes where the technology or operational environment is not completely known. The risk impact has a greater dependence on the controlled process (e.g., primary asset; Domain Based Security) that may be unknown. There is a need to provide additional guidance on performing cybersecurity risk management at an abstract level.	Standard processes that provide for abstract analysis, where functions and levels are considered, are not available for this level of risk assessment. IAEA FCSRM [6] and NIST Risk Management Framework (RMF NIST SP800-37 [19]) provide for multiple levels of risk management processes based on the level of abstraction to separate the nature and source of risks to simplify tasks and activities associated with risk management.
7	**Uncertainty in vulnerability / susceptibility analysis:** Significant uncertainty is associated with the use of vulnerability / susceptibility analysis / documents necessary for effective risk management.	An unacceptable degree of uncertainty in the quality of vulnerability analysis of an I&C system increases the difficulty in performing effective risk management.
8	**Adversary characterization uncertainty:** Applying a cyber DBT/Adversary analysis to formal risk management of cybersecurity for NPPs is difficult due to the degree of uncertainty associated with adversary analysis in the DBT.	The application of cyber DBT within risk management and the degree of uncertainty associated with adversary analysis (e.g., DBT) increases the difficulty in performing effective risk management.
9	**Excessive information volume:** Effective and timely analysis of the large volume of information to assess risk is not practical (reasonable).	Modern digital information systems and cybersecurity risk management rely upon a tremendous volume of input data. Rationalizing this amount of information is challenging and could lead to ineffective risk management
10	**Lack of a common and comprehensive risk management process:** There exists a need for a common and comprehensive process that manages all significant risks, both regulatory and organizational objectives.	Significant risks are associated with consequences that will not result in radioactive release or theft of nuclear material (i.e., not required by regulation). The risks that lead to these consequences may not be identified and effectively managed.
11	**Advanced security capabilities incompatibility:** Security controls that provide advanced security capabilities (e.g., Cyber SOC or SIEM, cryptography, virtualization) are unsupported or incompatible with isolated or legacy systems reducing defense in depth and increasing risk.	Contemporary and effective technical measures cannot be implemented on legacy and/or physically isolated systems.

The cyber-risk approaches evaluated to determine whether effective guidance exists to address each of the challenges are listed in Table 2.

AVA Documents
Document Sharing Hub

Table 2 – Cyber-risk approaches

Approach	Description	Entity
Facility Computer Security Risk Management (FCSRM) [6]	The FCSRM [6] assesses the impacts of compromise on facility functions and strategic risks.	IAEA
System Computer Security Risk Management (SCSRM) [6]	The SCSRM assesses the assets, systems, security controls, attack pathways, and tactical risks.	IAEA
EBIOS [11], [12]	EBIOS provides a formalized approach for assessing and treating risks within the field of information systems security, including support tools for contracting authorities, drafting documents, and raising awareness	Agence nationale de la sécurité des systèmes d'information (ANSSI)[4]
YVLA.12 [20]	YVLA.12 [20] sets out requirements for the management of information security at a nuclear facility, and it specifies in more detail the design requirements outlined in the STUK Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020) [20]	Finland
IEC 62443 [14]	IEC 62443 [14] provides a series of standards with a focus on Operational Technology (OT). The IEC 62443 considers systems and components in risk informing requirements and implementation of security controls.	IEC
Cyber Informed Engineering (CIE) [10]	CIE [10] provides a framework for understanding and addressing cyber threats to NPP systems and facilities.	US Department of Energy (DOE)
Hazards and Consequences Analysis for Digital Systems (HAZCADS [9])	HAZCADS [9] leverages Systems Theoretic Process Analysis (STPA) [21] to identify Unsafe Control Actions (UCAs) within control systems that may result from faults including those caused by cyberattacks. This analysis allows for risk-informed hazard analysis and selection of security controls.	Electric Power Research Institute (EPRI)
Harmonized Threat Risk Assessment (HTRA) [8]	HTRA [8] provides a scalable framework to address strategic and tactical risks. HTRA provides several tools and tables to simplify the risk management processes.	Canada
Malicious Acts Guidelines for Computer-Based Systems (SEWD) [22]	These guidelines are “classified information – for official use only” and not publicly available. They cover the whole IT-security framework for the nuclear field with some parts for cyber risks.	Germany
Information Security Technology—Implementation Guide to Risk Assessment of Industrial Control Systems GB/T 36466 [23]	The national standard GB/T 36466-2018 [23] “Information security technology—Implementation guide to risk assessment of industrial control systems” provides guidelines for cyber security assessment for industrial control systems.	China
Regulatory Guide (RG) 5.71 [24]	RG 5.71 provides one acceptable approach regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by Title 10 Code of Federal Regulations (CFR) Part 73.1 [25]	US Nuclear Regulatory Commission (NRC)

[4] EBIOS [11][12] is a risk analysis method recommended by ANSSI but is not the national approach for France which is detailed in [14]. This approach consists of an approved procedure for information systems of vital importance. This procedure requires NPP operators to periodically perform risk analysis (which can be performed using EBIOS) as well as security audits and formal management of the associated risks to information systems of vital importance.

AVA Documents Document Sharing Hub

Approach	Description	Entity
Russian Federal Service for Technical and Export Control (FSTEC) [26], [27], [28], [29], [30], [31], [32], [33]	FSTEC [26], [27], [28], [29], [30], [31], [32], [33] provides a series of documents with a focus on the security of the control systems for the critical infrastructure. The FSTEC classifies the systems using risk-oriented approach and assign the set of the security controls to protect the control system.	Russia
His Majesty's Government (HMG) Information Assurance Standard Numbers 1 & 2 and Domain Based Security (DBSy) [34] [35]	Provides a methodology for technical risk assessment and risk treatment for implementation by Central Government Departments and Agencies. It was also recommended for the wider public sector. The technical risk assessment is supported the DBSy modelling technique. The standard has been withdrawn but is still in use by NPPs.	United Kingdom

This document was developed through the execution of four tasks:

a) Identification and description of NPP operator-specific challenges associated with risk management are detailed in Table 1.

b) Identification and analysis of cyber-risk approaches that may offer insights into reducing the challenges; the cyber-risk approaches are detailed in Table 2.

c) Using ISO/IEC 27005:2018 [5] as the base:

   1) Associate the Challenges (Table 1) with specific ISO/IEC 27005:2018 [5] Risk Phases and Clauses (process shown in green in Figure 2).

   2) Associate the cyber-risk approaches with ISO/IEC 27005:2018 [5] Risk Phases and Clauses (process shown in blue in Figure 2).

d) Combine the challenges and cyber-risk approaches, leveraging ISO/IEC 27005:2018 [5] Clause numbers as an index and summarize the combined data.

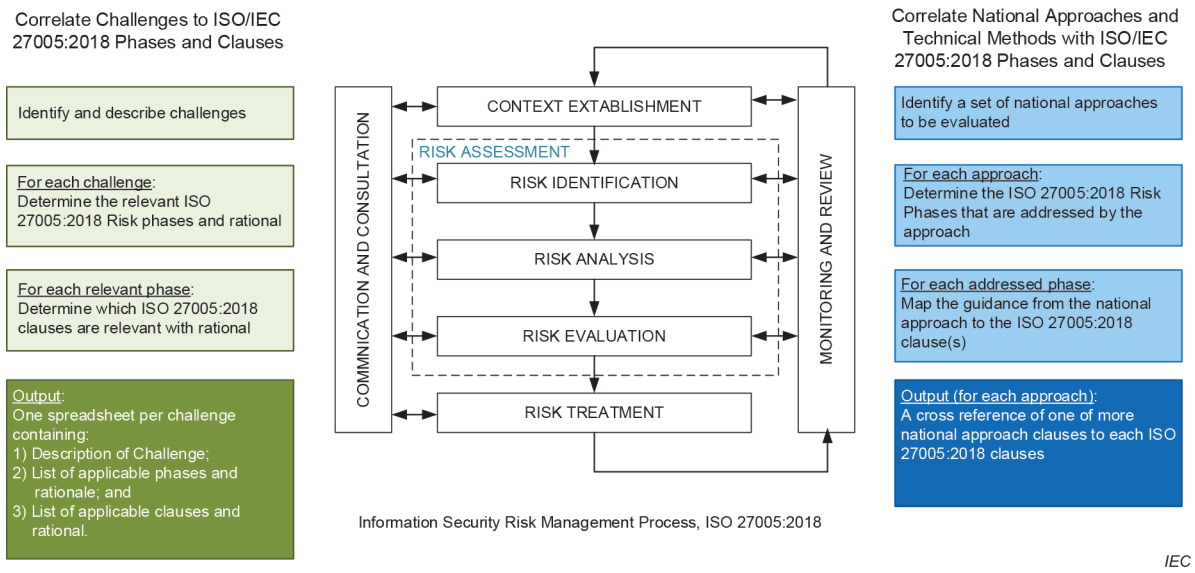

Figure 2 – Technical report development approach

6.2 Challenge 1: Aggregate risk of multiple units / locations

There is a need for additional ways to evaluate levels beyond security degree assignment for aggregate risk of multiple units/locations. For example, a system can be installed on several units or multiple locations. Current analyses do not focus on multiple installations of the same unit with identical, similar, or common design, configuration, and functionality.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

While the impact of a compromise of a single system would affect a single unit or location, the attack could propagate to other identical systems, or an additional attack could be performed targeting like systems. For example, an adversary could leverage a supply chain attack to compromise a vulnerable system located at all units and locations. The current approach to risk management may not consider these strategic risks.

In many current approaches, risk analysis focuses on multiple locations (not co-located), and some clauses in IEC 62645 [1] do not address multiple co-located units. However, both Canada's HTRA [8] and Finland's YVLA12 [20] provide flexibility when setting the scope and context of the risk management process.

6.3 Challenge 2: Complexity of interdependencies and interactions

Identifying and analyzing risks associated with attacks that target more significant functions through their interdependencies and/or interactions with less significant functions is a challenge.

An example of this challenge is the Colonial Pipeline attack that disrupted gasoline supplies to the US Northeast. This attack affected IT systems that interfaced with I&C systems that controlled delivery of gasoline. The attack led to prolonged disruption of gasoline supplies.

Prolonged and widespread disruption of fuel supplies to an NPP may have cascading effects leading to increased risks to NPP systems and processes that depend on fuel supply (e.g., emergency generators).

A non-malicious event that supports this challenge was the loss of bulk electrical supply in the northeast of North America in 2003 (i.e., Northeast blackout of 2003). The complexity of the bulk electrical supply resulted in a latent design deficiency where a failure mode and effects were not anticipated and accounted for resulting in severe consequences. Similarly, latent design deficiencies can lead to flaws that may be exploited by adversaries by cyber-attack leading to consequences and affecting risk management.

Challenge 2 differs from Challenge 1. The interdependencies are targeted in Challenge 2, whereas Challenge 1 addresses a common vulnerability or weakness in multiple locations.

6.4 Challenge 3: Incident likelihood determination

Estimating the likelihood of an extremely rare but unacceptable event is challenging as likelihood values are associated with large uncertainty. A specific example is performing a risk analysis, including the likelihood, of sabotage at NPPs where the initiating event is a cyber-attack.

The example postulated scenario is assumed to be extremely unlikely as it would involve multiple and persistent access to various systems, complex interactions, and other difficult elements for a potential adversary to achieve radiological sabotage.

6.5 Challenge 4: Unknown or lacking sufficient detail for pre-developed components

Pre-developed and purchased components that make up digital I&C systems have not been individually identified and evaluated for risks associated with NPP applications. In these cases, the Operator performs the risk assessment and may incur extra effort to treat the risk.

This challenge differs from Challenge 2: Complexity of Interdependencies and Interactions. This challenge occurs when the NPP operator does not have sufficient resources or the capability (e.g., as in reverse engineering) to span the information gap that is necessary to perform effective risk management.

Additionally, the NPP operator may be restricted by legal obligations (e.g., EULA) prohibiting them from performing these activities. Or, if there are sufficient resources and the capability is

AVA Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

present to gather sufficient information to perform effective risk management, the supplier may have limited information about a proprietary product upon which the supplied item depends.

6.6 Challenge 5: Differences in cyber-risk management

There are many different risk management processes used across Member States. Reasons for this difference can come from:

a) differing regulatory constraints on risk management or risk methodologies across Member States; and

b) accreditation of (risk analysis, risk treatment) defensive architecture, zones, or libraries of common controls for risk modification to sensitive systems and digital assets, and associated V&V processes.

This challenge is particularly impactful to the system or asset-level risk management. At the system/asset level, it is difficult to accredit common controls, DCSA elements, and associated V&V processes. The greater the specificity needed to perform risk management tasks and activities, the greater the potential for modifications to the process to account for national differences.

6.7 Challenge 6: Lack of abstract analysis methods

There exists a general lack of guidance on risk management applied to conceptual facilities, systems, and processes where the technology or “asset” is unknown. There is a need to provide additional direction on performing cybersecurity risk management at an abstract level.

The lack of abstract analysis methods increases the difficulty when comparing cyber versus non-cyber risks. For example, it is challenging to :

a) compare and rationalize these risks (i.e., equate cyber versus non-cyber risks and treat them in an equivalent manner) within the NPP operator’s management system; and

b) establish the context for assessing the comparable risks.

For new power plants, some approaches require two risk assessment phases – Facility Level and Systems Level.

First level – Facility Level: systems technology is unknown (could be analogue), validates the DCSA zone/level model; differing risk decision criteria (established context is different) and

Second level – System Level: SD is informed/established by the DCSA model; the system shall comply with SD requirements.

6.8 Challenge 7: Uncertainty in vulnerability / Susceptibility analysis

There is a challenge with accommodating uncertainty associated with vulnerability/susceptibility analysis/documents necessary for effective risk management.

Vulnerability analysis is based on known vulnerabilities, susceptibilities, weaknesses, or adversary tactics, techniques and procedures. This analysis does not account for unknown or unreported weaknesses or exposures. Example: I&C systems that utilize general purpose operating systems rely on a “Penetrate and Patch” approach for security that is not readily accommodated by nuclear I&C configuration management processes.

At any operational time, any operating system has more than several hundred open vulnerabilities, and many of these are critical (i.e., ease of exploitation with high potential impact(s) from compromise).

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

I&C project management has long lead times and is frequently delayed. The time between design approval, installation, commissioning, and placing into service is significant. Risk assessments completed at earlier stages of this process may be significantly impacted by new weaknesses or vulnerabilities that become known during this period.

6.9 Challenge 8: Adversary characterization uncertainty

There is a challenge in applying DBT/Adversary analysis to formal risk management of cybersecurity for NPPs.

Challenge 8 is similar to Challenge 5 above but differs in the focus on uncertainty with adversary analysis and not the differences in applying this analysis and regulatory requirements.

Adversary analysis is based upon incomplete intelligence informed largely by expert opinion and relies upon the application of sense-making loops to “fill in” missing details concerning adversary capabilities, resources, motivation, opportunity, and intent.

In many national regulations, the DBT is an instrument that delineates the risk-sharing/transfer arrangement for security between state and operator. However, States have not reported, or have not disclosed, a robust or proven capability to detect, intercept, infiltrate, and disrupt cyber adversaries that exceed the DBT.

The developed adversary analysis does not clearly bind threats associated with identified risks because they are too vague or have too much uncertainty when considering the potential consequences of NPP operations. This lack of certainty may not allow for efficient risk management.

6.10 Challenge 9: Excessive information volume

There exists a challenge for the NPP personnel to analyze large volumes of information and assess risk in an effective and practical (reasonable) time period during both the design phase(s) and operations. Additional analysis is required to leverage the safety analysis when considering specific impacts of cyberattacks (i.e., maloperation) by using the safety analysis on each system. Cybersecurity risk management can benefit from these safety analyses (e.g., non-malicious threats like floods). However, safety analysis may not consider specific failure modes and effects associated with cyberattacks. For example, a safety-related air operated valve and high-pressure instrument air unexpected modes of operation (mal-operation) are not considered within the safety analysis.

The resources required to perform a more in-depth analysis that requires additional time and information place excessive demands above the resources available to NPP operators. Additionally, the sensitivity of disclosing information regarding cybersecurity risks results in limiting the personnel who can provide critical review and analysis. Restricted access to sensitive information coupled with a lack of advancement/availability of risk support tools/technology (i.e., modelling and simulation) to ease the challenge associated with data input/analysis and rationalization results in significant reliance on expert opinion or experience.

6.11 Challenge 10: Lack of a common and comprehensive risk management process

There is a need for a common and comprehensive process that manages all significant risks and regulatory and organizational objectives. Other risks may include the long-term impact on production (See Challenge 2 main transformer example), reputation, political, and reduction of public support for nuclear power (e.g., the cyber attack on Korea Hydro and Nuclear Power Co. Ltd, in 2014). For example, a unit outage impacts the maintenance schedule.

A common repeatable process has the potential to reduce effort and errors while providing a comprehensive approach to risk management.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

6.12 Challenge 11: Advanced security capabilities incompatibility

There exists a challenge whereby security controls that provide advanced security capabilities (e.g., cyber-SOC or SIEM, cryptography, virtualization) are unsupported or incompatible with isolated or legacy I&C systems reducing defence in depth and increasing risk.

“Air Ggp”, and/or isolated systems and networks impairs network security and real-time (or continuous) monitoring and response. Air gaps eliminate the potential for holistic, comprehensive Security Information and Event Management (SIEM) systems that provide real-time alerting, perform threat hunting, as well as fail to prevent or detect insider threats. The reliance on isolation assumes that placement within Vital Areas is sufficient risk modification for cyberattacks. However, it does not protect against malicious actions (witting or unwitting) of individuals with authorized physical and portable media / mobile device access, and supply chain attacks. Additionally, legacy I&C systems and protocols do not support contemporary (non-deprecated) cryptographic mechanisms.

Use of fail-secure, deterministic, unidirectional data communication pathways (e.g., data diodes) may provide logical isolation while still allowing for real-time operation and continuous monitoring.

7 Cyber-risk approaches versus challenges by ISO/IEC 27005

7.1 General

Cyber-risk approaches (see Annex A through Annex K) were evaluated to determine whether their guidance addressed one or more of the identified challenges (see Clause 7). The evaluation was structured based on the ISO/IEC 27005:2018 [5] clauses to simplify subsequent analysis and summary.

Each of the subclauses below applies to a specific ISO/IEC 27005:2018 [5] clause and provides:

- A summary of the ISO clause
- Applicable challenges to which the clause applies
- Summary of the cyber-risk approaches based on the evaluations (see Annex A through Annex K)
- The cross-reference table legend is below:
  - “Key” – approach contains key insight(s). Key insights are those elements of a cyber-risk approach that have significant benefit to cyber security risk management, and which could be considered for inclusion in a potential new standard for cyber risk management.
  - “X” – approach contains guidance but is not a key insight.
  - Blank – approach does not address the challenge.

7.2 ISO/IEC 27005:2018, 7.1 General considerations

7.2.1 Summary

ISO/IEC 27005:2018, [5] 7.1 requires that an external and internal context for cybersecurity risk management be established. This context involves:

a) setting the basic criteria necessary for information security risk management (ISO/IEC 27005:2018 [5], 7.2);

b) defining the scope and boundaries (ISO/IEC 27005:2018 [5], 7.3), and

c) establishing an appropriate organization operating the information security risk management (ISO/IEC 27005:2018 [5], 7.4).

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

7.2.2 Applicable challenges

The external and internal context is particularly important for challenges impacted by events and information from inside and outside the organization. For example, the internal context is vital for Challenge 11 (advanced security capabilities incompatibility), as a facility's technology and modification processes would demand specific approaches to obsolescence and the feasibility of integrating advanced technologies. Similarly, the external context is essential for Challenge 10 (common and comprehensive risk process), as national risk approaches may influence the scope and boundaries of risk management. See Table 3.

Table 3 – ISO/IEC 27005:2018, 7.1: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Incompatibility

7.2.3 Summary of key approaches

Cyber-risk approaches with key insights for Challenge 2 are:

- HAZCADS [9] relies upon scenario-informed fault trees, modified fault trees that allow fault tree analysis (FTA). FTA provides a structured manner to analysis systems and interactions.
- IAEA CSRM [6] identifies interdependencies and interactions that need to be considered.
- US NRC [24] addresses the identification and analysis of risks associated with attacks that target safety, security, and emergency preparedness (SSEP) functions and associated systems through their interdependencies and / or interactions with less significant functions / systems.

Key approaches for Challenge 4 are:

- HAZCADS [9] use of FTA will minimize the impact of pre-developed components if there exists a traditional FTA (e.g., existing operating fleets that leverage probabilistic risk assessment (PRA)).
- IEC 62443 [14] has a layered series of standards that specifically address Component layer requirements (IEC 62443 Part 4 [36], [37]).

Key approaches for Challenge 6 are:

- HAZCADS [9] demands a control structure model abstraction to allow for effective STPA [21] analysis to identify UCAs and inform fault tree analysis.
- IEC 62443 [14] leverages a tiered approach focused on different types of organizations. IEC 62443-2 [38], [39].
- is focused on operating the organization's programmes, IEC 62443-3 [40], [41] focuses on architectural analysis, and IEC 62443-4-2 [37] is focused on component analysis.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

Key approach for Challenge 9 is:

- IAEA CSRM [6] provides a tiered analysis approach (facility, system) with compartmentalized activities to reduce the amount of information needed for each activity.
- HAZCADS [9] leverages a type of FTA that can provide a pathway to utilize PRA. PRA is associated with many tools and processes to simplify or support analysis than can reduce excessive information.

Key approaches for Challenge 10 are:

- Germany's cyber-risk approach [22] allows different State authorities to authorize differing risk management processes while being compliant with federal guidelines.
- IAEA CSRM [6] allows for all risks to be considered in a common and comprehensive manner. The facility covers strategic risks with unacceptable (major/severe) consequences to the operator, whereas the system covers tactical risks associated with graded consequences impacting the correct operation of a system.
- IEC 62443 [14] provides lists of risk sources that can provide a basis for a common and comprehensive risk process.
- Russia's FSTEC [29], [30], [31], [32] approach provides common ground for challenge 10 by enforcing the same approach for all critical infrastructure.

7.2.4 Cross-reference table (Table 4)

Table 4 – ISO/IEC 27005:2018, 7.1: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X		X	X		X		X	X	X
Germany		X			X		X		X	Key	
HAZCADS		Key		Key		Key			Key		
IAEA CSRM		Key							Key	Key	
IEC 62443		X		Key		Key				Key	
Russia				X		X			X	Key	
US NRC		Key		X	X		X		X	X	X

7.3 ISO/IEC 27005:2018, 7.2 Basic criteria

7.3.1 Summary

Risk management basic criteria involve identifying an approach, evaluation, impact, and acceptance criteria. Examples of basic criteria are the significance of sensitive digital assets and the importance of their confidentiality, integrity, and availability. Different risk approaches and/or acceptance criteria can also apply to different risk classes (e.g., strategic, tactical, nuclear safety, and security).

7.3.2 Applicable challenges

Risk management basic criteria are particularly important for challenges that affect risk criteria. Specifically, the type of approach, evaluation, impact, and acceptance criteria significantly contribute to Challenges 2, 3, 5, 7, and 10. For example, interdependencies (Challenge 2) or vulnerabilities of pre-developed components (Challenge 7) may be difficult to assess at a higher level of complexity or detail with the potential to bring about Challenge 9 (excessive information). National differences in risk tolerance/acceptance (Challenge 5) also need to be considered when applying a common and comprehensive process, especially for organizations operating in multiple national jurisdictions (Challenge 10).

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

Additionally, the sequence or timing of when specific risk management activities are conducted could impact these challenges. See Table 5.

Table 5 – ISO/IEC 27005:2018, 7.2: Applicable challenges

Challenge	Description
1	Aggregate risk of multiple units/locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Volume of Information
10	Lack of a Common and Comprehensive Risk Management Process

7.3.3 Key approaches

Key approach for Challenge 1 is:

- A key step of UK IS/DBSy [34], [35] is the requirement to create a model of the I&C assessment scope. The model can include a full plant with many Units or can be extended to other plants, although in practice the assessment is done on a plant basis.

Key approaches for Challenge 2 are:

- HAZCADS [9] uses STPA [21] to identify UCAs and link them to hazards and losses (i.e., consequences). This linkage requires deliberate analysis of interactions and interdependencies.
- IAEA CSRM [6] listed interdependencies and interactions that can be used to support risk evaluation criteria and impact criteria identification.
- IEC 62443 [14] tiered approach covers the interactions and interdependencies between different types of organizations, all managed by the operating organization.
- UK IS/DBSy [34], [35] requires the modelling and analysis of requirements for exchanging data between systems and the impact of those interactions in the evaluation of risk.

Key approach for Challenge 3 is:

- CIE [10] focuses on consequences to reduce the impact of uncertainty on incident likelihood. Additionally, CIE accredits cybersecurity culture and planned resilience in protecting against incidents, reducing the likelihood.

Key approaches for Challenge 4 are:

- IEC 62443 Part 4 [36], [37] provides requirements on components that suppliers provide. These requirements identify key attributes of acquired components to support the cybersecurity objectives of the operating organization.
- UK IS/DBSy [34], [35] requires the modelling of assets within the scope of the technical risk assessment to consider the systems that support the evaluated assets, this will include the need to assess components delivered by supply chain.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

Key approaches for Challenge 6 are:

- HAZCADS [9] uses abstraction to simplify the STPA [21] efforts. STPA simplifies the cybersecurity analysis by only considering the impact of the cyberattack to cause a system to mal-operate.
- IEC 62443-2 [38], [39] provides abstract analysis to allow an organization to develop and implement its cybersecurity management system (i.e., programme).
- UK IS/DBSy [34], [35] provides a modelling methodology that allows for the creation of a plant abstract model based on I&C systems significance rather than specific technology or system architecture.

Key approach for Challenge 7 is:

- Canada's HTRA [8] provides pre-compiled lists of these vulnerabilities to minimize uncertainty, especially in reducing unknown or missing vulnerability/susceptibility analysis considerations.

Key approach for Challenge 9 is:

- IAEA CSRM [6] leverages existing information and analysis to reduce the information necessary to be considered/re-evaluated to perform cybersecurity risk management. The key activity is the facility characterization which leverages the Facility's safety analysis and other documents.
- The tiered approach of IEC 62443 [14] compartmentalizes the necessary information to perform key risk activities in each tier.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [11], [12] does not exclude considering other systems not directly associated with the consequences of theft of NM or radiological sabotage. The French cyber-risk approach allows NPP operators to apply a common and comprehensive risk management approach to significant and other systems.
- Germany's cyber-risk approach [22] pre-classifies systems and their risks under regulatory requirements by the competent authority.
- IAEA CSRM [6] provides an ordered list of the effects of a system compromise on functions. This approach can provide a basis for setting risk evaluation, impact, and acceptance criteria to support a common and comprehensive risk management process.
- IEC 62443 [14] is an international standard for industrial automated control systems (IACS) or operational technology (OT) systems. It broadly addresses risks associated with critical infrastructure and can inform a common and comprehensive approach.
- Russia's cyber-risk approach [29], [30], [31], [32] provides common ground for challenge 10 by enforcing the same approach for whole all critical infrastructure.US NRC guidance was primarily developed for risks associated with consequences that will result in radioactive release. It could be used as a starting point for developing a cybersecurity framework for addressing risks not required by regulation.
- UK's IS/DBSy [34], [35] provides a very detailed and repeatable stepped process to perform the technical risk assessment, with guidance and templates for use at each step.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

7.3.4 Cross-reference table (Table 6)

Table 6 – ISO/IEC 27005:2018, 7.2: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X			X		X		X	X	
CIE		X	Key	X		X			X	X	
France		X					X			Key	
Germany		X	X	X	X					Key	
HAZCADS		Key		X		Key				X	
HTRA		X			X		Key		X	X	
IAEA CSRM		Key			X		X		Key	Key	
IEC 62443		Key		Key		Key	X		Key	Key	
Russia	X	X								Key	
US NRC		X			X		X		X	Key	
UK IS/DBSy	Key	X		X		Key		X	X	Key	

7.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

7.4.1 Summary

Scope and boundaries need to be defined to ensure effective cybersecurity risk management. The assessment scope needs to account for all relevant assets and bounded to ensure risks are considered both within and through them.

Scope and boundaries rely on an organization's policies, risk management approach, functions and structure, sensitive digital assets, DCSA, and stakeholders' expectations.

7.4.2 Applicable challenges

These challenges affect how scope and boundaries are set. For example, boundaries need to consider risks that may arise through interdependencies and interactions (i.e., Challenge 2) between other organizations or systems that may not be directly assessed. The scope of the risk assessment may affect Challenge 5 and Challenge 10. Specifically, differences in national risk management typically reflect different national stakeholders (e.g., national regulators). Additionally, scope and boundaries are associated with Challenges 4, 7, and 9. A wide scope with limited abstraction would lead to uncertainty in vulnerability analysis and/or lack of sufficient detail or excess volume of information. See Table 7.

Table 7 – ISO/IEC 27005:2018, 7.3: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Method
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

7.4.3 Key approaches

Key approach for Challenge 1 is:

- A key step of UK IS/DBSy [34], [35] is the requirement to create a DBSy model that defines of the I&C assessment scope. The model can include a full plant with many units or can be extended to other plants.

Key approaches for Challenge 2 are:

- IAEA FCSRM [6] provides a list of interdependencies to be considered within the risk process. This list could be used to set the scope and boundaries of risk assessments and leverage a tiered analysis, and this would reduce the impact of lacking sufficient detail (Challenge 4) and excessive information volume (Challenge 9).
- IEC 62443-3-2 [40] provides a process to investigate the interdependencies and interactions with other systems.
- UK IS/DBSy [34], [35] requires the definition of the specific Focus of Interest (FOI) that defines the scope of the technical risk assessment, as well as to identify any interconnections with other systems outside the FOI.

Key approaches for Challenge 4 are:

- Russia [29], [30], [31], [32] provides guidance to investigate software, firmware and hardware vulnerabilities related to pre-developed components.
- UK IS/DBSy [34], [35] as part of defining the scope allows the modelling of interactions between systems and organisations, including those responsible for system design and development i.e., assessment of the supply chain.

Key approach for Challenge 5 is:

- Germany's cyber-risk approach [22] provides two frameworks (BSI 200-3 [42] and ISO/IEC 27005 [5]). These frameworks are not fully compatible but generally lead to similar outcomes. Application of either framework provides a path to compliance with regulatory requirements. The framework used is dependent upon the utility/operator and vendors or integrators need to be able to comply with either.

Key approaches for Challenge 7 are:

- Canada's HTRA [8] allows for smaller modular assessments that may limit the level of uncertainty in the analysis.
- IEC 62443 [14] specifically addresses component layer requirements (62443-4 [36], [37]) to identify and describe a component's vulnerabilities and addresses vulnerabilities of components provided by the vendor.

Key approaches for Challenge 9 are:

- Canada's HTRA [8] provides pre-compiled lists of these criteria (e.g., asset valuation, safeguard (control measures) listing, threat (sources) listing, impacts, etc.), hierarchical structures, taxonomy, and an extensive glossary to allow for modular assessments that can compartmentalize information, thereby alleviating the challenge of excessive information.
- IAEA CSRM [6] tiered analysis sets the scopes and boundaries to prioritize and compartmentalize information to ease excessive information challenges.
- UK IS/DBSy [34], [35] modelling allows for identification of focus of interest (FOI) from the overall model. Each FOI is then assessed independently, helping to manage the large amount of information.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

Key approaches for Challenge 10 are:

- France's cyber-risk approach [11], [12] allows NPP operators to set the scope and boundaries of risk management. It only requires a minimum set of significant systems that shall be considered.
- Canada's HTRA [8] provides a list of risk sources that can provide a basis for a common and comprehensive risk process. These resources can help NPPs address stakeholders' expectations, the socio-cultural environment, and other constraints affecting the organization.
- Russia's approach [29], [30], [31], [32] provides a common and comprehensive approach to set the scope and boundaries of risk management for all critical infrastructure.

7.4.4 Cross-reference table (Table 8)

Table 8 – ISO/IEC 27005:2018, 7.3: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X		X	X		X		X	X	
CIE		X	X	X		X			X		
France		X		X			X		X	Key	
Germany					Key					X	
HAZCADS		X		X		X			X	X	
HTRA		X		X	X		Key		Key	Key	
IAEA CSRM		Key		X	X		X		Key	X	
IEC 62443		Key		X		Key					
Russia		X		Key		X	X		X	Key	
UK IS/DBSy	Key	Key		Key	X	Key	X		Key		

7.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management

7.5.1 Summary

The organization and responsibilities of the cybersecurity risk management process shall be established and maintained. Development of the process, identifying stakeholders, defining the roles and responsibilities of entities, and other key aspects of the process shall be managed.

7.5.2 Applicable challenges

Challenges 2, 4, and 9 are impacted by how the risk management process is organized. A common risk process, organization, and experts shall provide a consistent approach to address these challenges. Challenges 5 and 10 would benefit from a single risk process and responsible organization, thereby reducing variance through centralized control and the conduct of a risk management programme. Challenge 7 may result in the need to address this within decision escalation paths or external parties to supplement analysis. See Table 9.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

Table 9 – ISO/IEC 27005:2018, 7.4: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.5.3 Key approaches

Key approaches for Challenge 9 are:

- Canada's HTRA [8] outlines how organizational structure may be too large and complex to handle excessive information coherently. HTRA details how to define roles and responsibilities to ensure excessive information is distributed across several roles to a manageable level.
- IAEA CSRM [6] specifies key outputs and outcomes of the risk management process. This method may allow for redundant or unnecessary information to be filtered out.

Key approach for Challenge 10 is:

- France's cyber-risk approach [11], [12] mandates the involvement of specific multi-disciplinary personnel and roles for security approval allowing for consequences to be identified that are impactful but not regulatory.
- In Russia's cyber-risk approach [29], [30], [31], [32], the security approval involves the regulator, the owner and operator (usually it is the same), the security officer as well as technical experts. That provides a key insight to dealing with challenge 10 in detecting consequences that are significant but are not regulatory.

7.5.4 Cross-reference table (Table 19)

Table 10 – ISO/IEC 27005:2018, 7.4: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
France		X		X			X		X	Key	
HTRA		X		X	X		X		Key	X	
IAEA CSRM		X		X	X		X		Key	X	
IEC 62443		X		X	X		X		X	X	
Russia		X		X					X	Key	
US NRC		X	X	X		X			X		
UK IS/DBSy		X		X		X			X	X	

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

7.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

7.6.1 Summary

A general description of information security risk is needed to identify, quantify, or qualitatively describe and prioritize risks. The risk assessment consists of risk identification, analysis, and evaluation and needs to be consistent with established criteria.

7.6.2 Applicable challenges

These challenges require a risk assessment process described with inputs, actions, and implementation guidance. Particularly, Challenge 1 needs to consider strategic risks differently, possibly by application of abstract analysis methods, whereas more detailed analysis may experience Challenges 2, 4, and 7.

A general description of the risk assessment process considers the need to be consistent regardless of the necessary level of detail (i.e., challenge 10). See Table 11.

Table 11 – ISO/IEC 27005:2018, 8.1: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.6.3 Key approaches

Key approach for Challenge 1 is:

- UK IS/DBSy [34][35] methodology consisting of well-defined steps can be applied to different scope of assessment, including an assessment of the overall NPP I&C.

Key approach for Challenge 2 is:

- The Chinese cyber-risk approach [23] recommends that a mock-up of the system be built. This process could be of benefit in identifying a system's functional interdependencies and interactions with less significant functions.
- IAEA [6] specifically indicates that the operator shall set the scope to include an assessment inclusive of those risks associated with this challenge.

Key approaches for Challenge 4 are:

- US NRC approved the methodology in NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," [43] that could help the Operator when identifying and prioritizing risks to SSEP functions and systems associated with pre-developed components during the risk assessment.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

Key approach for Challenge 6 is:

- IAEA CSRM [6] prioritizes analysis of facility functions to address strategic risks in compromising or altering these functions. Functions are an emergent property (abstraction) resulting from the complex interactions and organizations of a set of elements within a system. This analysis technique is widely used for safety analysis.

Key approach for Challenge 7 is:

- IEC 62443 [14] application of common measures, such as DCSA implementing defense in depth reduces the impact of uncertainty in Vulnerability/Susceptibility Analysis on risk management.

Key approach for Challenge 8 is:

- IEC 62443 [14] leverages an attack pathway analysis approach that aims to deny access of the adversary to I&C and EPS by implementing a DCSA. The DCSA may limit the effect of uncertainty on risk management. IEC 62443-3-2 [40] contains a staged risk analysis, first to implement a DCSA and a second more detailed assessment to modify unacceptable residual risks.

Key approach for Challenge 9 is:

- IEC 62443 [14] leverages a tiered approach to manage the facility, system, and supplier risks. Categorizing the information in this way reduces the amount of information required for each activity.

Key approaches for Challenge 10 are:

- IAEA CSRM [6] leverages functions as a common and comprehensive means to assess all risks. Correct performance of functions is necessary for an organization to achieve all objectives.
- UK IS/DBSy [34], [35] applies a consistent risk assessment process that is common and comprehensive for all risks impacting the NPP I&C systems.

7.6.4 Cross-reference table (Table 12)

Table 12 – ISO/IEC 27005:2018, 8.1: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	Key		X		X	X			X	
Germany		X		X			X				
IAEA CSRM		Key		X		Key	X			Key	
IEC 62443		X		X		X	Key	Key	Key	X	
US NRC	X	X		Key		X	X			X	
UK IS/DBSy	Key	X		X	X		X	X	X	Key	

7.7 ISO/IEC 27005:2018, 8.2 Risk identification

7.7.1 Summary

Risk identification involves the identification of assets; threats; existing controls; vulnerabilities; and consequences. The purpose of risk identification as it relates to cybersecurity risk for NPPs is to understand the impacts of compromise, how and why the impact could arise from cyberattacks, and existing mitigations to prevent or protect against these impacts.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024

7.7.2 Applicable challenges

Subclause 7.7 (i.e. Risk identification) is associated with all challenges.

For example, the identification of assets and vulnerabilities is associated with Challenges 1 (multiple locations), 2 (inter-dependencies), 4 (pre-developed components), 5 (national differences), 7 (uncertainty vulnerabilities), and 9 (excessive information) as the number of assets and their vulnerabilities could be significant.

The identification of threats is associated with Challenge 8 and Challenge 11. Challenge 11 also pertains to existing controls. Advanced technologies can enable techniques such as threat-hunting and behaviour-based detection. Incompatibility with these technologies reduces information regarding threat sources on an organization's networks and systems and may increase uncertainty in threat identification and adequacy of the control measures. See Table 13.

Table 13 – ISO/IEC 27005:2018, 8.2: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.7.3 Key approaches

Key approaches for challenge 1 are:

- UK IS/DBSy [34], [35] methodology uses a threat-based risk assessment, also allows for modelling of an entire facility, making it easier to identify threats that could impact whole plant.

Key approaches for Challenge 2 are:

- CIE [10] principles are effective in supporting challenges but are very general. However, CIE-related literature leverages HAZAOP analysis to complement risk analysis that considers information and data flow that could harm systems.
- Canada's HTRA [8] provides detailed lists within its annexes to identify risks and identify and describe the potential interdependencies and interactions between items on these lists via grading tables.
- IAEA CSRM [6] considers interactions and interdependencies at the facility level (via functions) and system level (e.g., information flows, engineering/resources) to identify risks in a similar manner but through independent processes.
- IEC 62443-3-2 [40] demands special attention to safety-related systems, wireless, internet-connected devices, mobile devices, and assets that other organizations manage. These are key interdependencies and interactions that increase complexity.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

- UK IS/DBSy [34], [35] step 1 includes as part of the asset identification, the modelling of systems and organisations interdependencies.

Key approaches for Challenge 4 are:

- CIE [10] and related literature (see Clause B.13) provides categories of attacks and points of entry within the supply chain. This literature helps analyze key risks within the supply chain and establish the requirements for the level of detail for the pre-developed of components necessary to support effective risk management.
- IEC 62443-4 [36] [37] imposes requirements on suppliers to ensure components can provide the required level of security to meet operator needs.
- UK IS/DBSy [34], [35] step 1 allows for modelling supply chain organisations and systems, therefore providing the opportunity to assess pre-developed components used in the I&C systems.

Key approaches for Challenge 6 are:

- HAZCADS [9] abstraction of the control system structure associates risks with UCAs that are then linked to hazards and losses. This process simplifies the identification of risks. However, in large interconnected systems, a large number of UCAs may be identified.
- IAEA CSRM [6] prioritizes a high degree of abstraction (functions) to identify strategic risks at the facility level.
- UK IS/DBSy [34], [35] step 1 uses an abstract modelling approach that can be used even when the systems are not deployed (i.e., plant under construction).

Key approach for Challenge 7 is:

- Canada's HTRA [8] lists vulnerabilities that aid in identifying risks associated with these vulnerabilities. These lists ensure that vulnerabilities are carefully and systematically considered, reducing the uncertainty associated with deficiencies in identifying vulnerabilities.
- The Chinese cyber-risk approach [23] provides detailed vulnerability risks and provides ways to identify them, reducing the uncertainty in identifying vulnerabilities.
- IAEA CSRM [6] treats functions as targeted by threats. The threat analysis does not consider the vulnerability the adversary would exploit to cause the impact, only that the adversary can do so if they obtain access.

Key approaches for Challenge 8 are:

- Canada's HTRA [8] uses an extensive catalogue of threats, including natural and physical threats. Using this type of catalogue reduces the uncertainty associated with the failure to consider certain types of threats.
- UK IS/DBSy [34], [35] Steps 2 and 4 detail the approach for threat evaluation, uncertainty exists but is reduced by requirements for the use of various government and industry sources to evaluate threat levels as well as the identification of threat actors levels within the NPP.

Key approaches for Challenge 9 are:

- IAEA CSRM [6] identifies risks in modular activities, such as facility characterization and threat characterization in facility-level processes and deeper analysis in system-level processes.
- UK IS/DBSy [34], [35] Step 3 provides the mean for splitting the overall NPP security model into Focus of Interest areas where risks can be identified and assessed, reducing the amount of information into manageable sets.

Documents
Document Sharing Hub

Full document details: PD IEC TR 63486:2024

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] does not restrict the risk management approach to radiological sabotage or theft of NM. This approach allows other risks to be identified where the impact is graded from minor to critical.
- Germany's cyber-risk approach [22] allows for variance between State regulation and implementation by differing NPP operators.
- HAZCADS [9] risk evaluation is consistent with PRA.
- Canada HTRA [8] identifies all risks to the objectives of an organization. Types of risks, such as safety, security, economic, and cybersecurity, are all identified and managed similarly.
- IAEA CSRM [6] recommends evaluating all significant functions of an organization and provides a 5-level example that accounts for all digital assets associated with a facility.
- US NRC [45] protection of SSEP functions could be a starting point for including other functions and a common and comprehensive approach to risk management.

Key approach for Challenge 11 is:

- The Chinese cyber-risk approach [23] describes the process of choosing and tailoring the security controls, including the advanced security capabilities, for industrial control systems.

7.7.4 Cross-reference table (Table 14)

Table 14 – ISO/IEC 27005:2018, 8.2: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	X		X	X		Key	X	X	X	Key
CIE		Key	X	Key		X			X		
France		X		X			X	X		Key	X
Germany		X			X		X	X	X	Key	
HAZCADS		X		X		Key	X	X	X	Key	
HTRA		Key		X	X		Key	Key	X	Key	X
IAEA CSRM		Key		X	X	Key	Key	X	Key	Key	
IEC 62443		Key		Key	X	X	X	X	X	X	
Russia		X		X				X	X	X	X
USNRC	X	X		X	X		X	X	X	Key	X
UK IS/DBSy	Key	Key		Key		Key	X	Key	Key	X	X

7.8 ISO/IEC 27005:2018, 8.3 Risk analysis

7.8.1 Summary

Risk analysis involves the assessment of incident likelihood, consequences, and level of risk. The purpose of risk analysis as it relates to cybersecurity risk for NPPs is to understand the severity of impacts related to compromise. Conservative decision-making and the lack of statistical data necessary to determine incident likelihood has limited risk analysis associated with the 'worst case' impacts of compromise.

Documents
Document Sharing Hub
Full document details: PD IEC TR 63486:2024