# Contents

1 Scope ..... 13
2 Normative references ..... 14
3 Terms, definitions, abbreviated terms, acronyms, and conventions ..... 15
3.1 Terms and definitions ..... 15
3.2 Abbreviated terms and acronyms ..... 19
3.3 Conventions ..... 21
4 Elements of a cyber security management system ..... 22
4.1 Overview ..... 22
4.2 Category: Risk analysis ..... 24
4.2.1 Description of category ..... 24
4.2.2 Element: Business rationale ..... 24
4.2.3 Element: Risk identification, classification, and assessment ..... 25
4.3 Category: Addressing risk with the CSMS ..... 26
4.3.1 Description of category ..... 26
4.3.2 Element group: Security policy, organization, and awareness ..... 27
4.3.3 Element group: Selected security countermeasures ..... 31
4.3.4 Element group: Implementation ..... 39
4.4 Category: Monitoring and improving the CSMS ..... 44
4.4.1 Description of category ..... 44
4.4.2 Element: Conformance ..... 44
4.4.3 Element: Review, improve, and maintain the CSMS ..... 45
Annex A (informative) Guidance for developing the elements of a CSMS ..... 47
A.1 Overview ..... 47
A.2 Category: Risk analysis ..... 48
A.2.1 Description of category ..... 48
A.2.2 Element: Business rationale ..... 49
A.2.3 Element: Risk identification, classification, and assessment ..... 54
A.3 Category: Addressing risk with the CSMS ..... 77
A.3.1 Description of category ..... 77
A.3.2 Element group: Security policy, organization, and awareness ..... 77
A.3.3 Element group: Selected security countermeasures ..... 94
A.3.4 Element group: Implementation ..... 118
A.4 Category: Monitoring and improving the CSMS ..... 147
A.4.1 Description of category ..... 147
A.4.2 Element: Conformance ..... 147
A.4.3 Element: Review, improve, and maintain the CSMS ..... 150
Annex B (informative) Process to develop a CSMS ..... 155
B.1 Overview ..... 155
B.2 Description of the Process ..... 155
B.3 Activity: Initiate CSMS program ..... 157

Copyright 2009 ISA. All rights reserved.

B.4 Activity: High-level risk assessment ..... 158
B.5 Activity: Detailed risk assessment ..... 158
B.6 Activity: Establishing Security Policy, Organization, and Awareness ..... 159
B.7 Activity: Select and implement countermeasures ..... 162
B.8 Activity: Maintain the CSMS ..... 162

Figure 1 – Graphical view of elements of a cyber security management system ..... 23
Figure 2 – Graphical view of category: Risk analysis ..... 24
Figure 3 – Graphical view of element group: Security policy, organization, and awareness ... 27
Figure 4 – Graphical view of element group: Selected security countermeasures ..... 32
Figure 5 – Graphical view of element group: Implementation ..... 39
Figure 6 – Graphical view of category: Monitoring and improving the CSMS ..... 44
Figure A.1 – Graphical view of elements of a cyber security management system ..... 48
Figure A.2 – Graphical view of category: Risk analysis ..... 49
Figure A.3 – Reported attacks on computer systems through 2004 (source: CERT) ..... 53
Figure A.4 – Sample logical IACS data collection sheet ..... 68
Figure A.5 – Example of a graphically rich logical network diagram ..... 70
Figure A.6 – Graphical view of element group: Security policy, organization, and awareness ..... 77
Figure A.7 – Graphical view of element group: Selected security countermeasures ..... 94
Figure A.8 – Reference architecture alignment with an example segmented architecture .... 102
Figure A.9 – Reference SCADA architecture alignment with an example segmented architecture ..... 105
Figure A.10 – Access control: Account administration ..... 107
Figure A.11 – Access control: Authentication ..... 110
Figure A.12 – Access control: Authorization ..... 116
Figure A.13 – Graphical view of element group: Implementation ..... 119
Figure A.14 – Security level lifecycle model: Assess phase ..... 122
Figure A.15 – Corporate security zone template architecture ..... 125
Figure A.16 – Security zones for an example IACS ..... 126
Figure A.17 – Security level lifecycle model: Develop and implement phase ..... 130
Figure A.18 – Security level lifecycle model: Maintain phase ..... 134
Figure A.19 – Graphical view of category: Monitoring and improving the CSMS ..... 147
Figure B.1 – Top level activities for establishing a CSMS ..... 155
Figure B.2 – Activities and dependencies for activity: Initiate CSMS program ..... 157
Figure B.3 – Activities and dependencies for activity: High-level risk assessment ..... 158
Figure B.4 – Activities and dependencies for activity: Detailed risk assessment ..... 159
Figure B.5 – Activities and dependencies for activity: Establish policies and procedures .... 160
Figure B.6 – Training and assignment of organization responsibilities ..... 161

Copyright 2009 ISA. All rights reserved.

Figure B.7 – Activities and dependencies for activity: Select and implement countermeasures ..... 162
Figure B.8 – Activities and dependencies for activity: Maintain the CSMS ..... 163

Table A.1 – Typical likelihood scale ..... 61
Table A.2 – Typical consequence scale ..... 63
Table A.3 – Typical risk level matrix ..... 64
Table A.4 – Example countermeasures and practices based on IACS risk levels ..... 120
Table A.5 – Example IACS asset table with assessment results ..... 123
Table A.6 – Example IACS asset table with assessment results and risk levels ..... 124
Table A.7 – Target security levels for an example IACS ..... 126

Copyright 2009 ISA. All rights reserved.