IEC 63096

Edition 1.0 2020-10

INTERNATIONAL STANDARD

colour inside

Nuclear power plants – Instrumentation, control and electrical power systems – Security controls

This is a preview. Click here to purchase the full publication.

IEC 63096:2020-10(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

This is a preview. Click here to purchase the full publication.

IEC 63096

Edition 1.0 2020-10

INTERNATIONAL STANDARD

colour inside

Nuclear power plants – Instrumentation, control and electrical power systems – Security controls

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-8837-5

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

® Registered trademark of

This is a preview. Click here to purchase the full publication.

CONTENTS

FOREWORD 7
INTRODUCTION 9
1 Scope 11
1.1 General 11
1.2 Objectives 12
1.3 Application 12
1.4 Framework 13
2 Normative references 13
3 Terms, definitions and abbreviated terms 15
3.1 Terms and definitions 15
3.2 Abbreviated terms 22
4 Nuclear I&C programmable digital systems specific security controls 23
4.1 Target audience and related life-cycle activities 23
4.2 Source for definition of nuclear I&C programmable digital systems specific security controls 24
4.2.1 General 24
4.2.2 Security degrees and baseline requirements 25
4.2.3 Computer-based tools for I&C system– engineering, –maintenance and –diagnostic 26
4.2.4 Safety and security 26
4.3 Security controls catalogue 26
4.3.1 General 26
4.3.2 ISO/IEC 27002 is the basis for IEC 63096 security controls 26
4.3.3 Modification/ extension of the ISO/IEC 27002:2013 security control description 27
4.3.4 Structure of each security control description 27
4.4 Process of selecting security controls 30
4.4.1 General 30
4.4.2 Process of selecting and implementing security controls for the actual I&C platform and I&C system 32
4.4.3 Process of selecting and implementing security controls for D- activity → I&C Platform Development 36
4.4.4 Process of selecting and implementing security controls for E- activity → I&C system engineering 36
4.4.5 Process of selecting and implementing security controls for O- activity → Operation and Maintenance of I&C system 38
4.4.6 Additional process requirements valid for controls for the “actual I&C platform and I&C system” and for the D-, E- and O- activity 39
4.5 Documentation and traceability of security controls 40
4.5.1 Documentation of security controls selection (statement of applicability) 40
4.5.2 Traceability 40
5 *Cybersecurity* policies 40
5.1 Management direction for *cybersecurity* 41
5.1.1 Policies for *cybersecurity* 41
5.1.2 Review of the policies for *cybersecurity* 43
6 Organization of *cybersecurity* 44
6.1 Internal organization 44
6.1.1 *Cybersecurity* roles and responsibilities 44

This is a preview. Click here to purchase the full publication.

6.1.2 Segregation of duties 47
6.1.3 Contact with authorities 48
6.1.4 Contact with special interest groups 49
6.1.5 *Cybersecurity* to project management 49
6.2 Mobile devices and teleworking 50
6.2.1 Mobile device policy 50
6.2.2 Teleworking 53
7 Human resource security 56
7.1 Prior to employment 56
7.1.1 Screening 56
7.1.2 Terms and Conditions of Employment 58
7.2 During employment 58
7.2.1 Management responsibilities 58
7.2.2 *Cybersecurity* Awareness, Education and Training 59
7.2.3 Disciplinary process 59
7.3 Termination and change of employment 60
7.3.1 Termination or change of employment responsibilities 60
8 Asset management 60
8.1 Responsibility for assets 60
8.1.1 Inventory of assets 60
8.1.2 Ownership of assets 62
8.1.3 Acceptable use of assets 62
8.1.4 Return of assets 62
8.2 Information classification 63
8.2.1 Classification of information 63
8.2.2 Labelling of information 64
8.2.3 Handling of assets 65
8.3 Media handling 65
8.3.1 Management of removable media 65
8.3.2 Disposal of media 66
8.3.3 Physical media transfer 66
8.3.4 *NUC – Removable media management* 66
9 Access control 67
9.1 *Requirements* of access control 67
9.1.1 Access Control Policy 67
9.1.2 Access to network and network services 74
9.2 User access management 77
9.2.1 User registration and de-registration 77
9.2.2 User access provisioning 77
9.2.3 Management of privileged access rights 78
9.2.4 Management of secret authentication information of users 79
9.2.5 Review of user access rights 80
9.2.6 Removal or adjustment of access rights 80
9.3 User responsibilities 81
9.3.1 Use of secret authentication information 81
9.4 System and application access control 81
9.4.1 Information access restriction 82
9.4.2 Secure log-on procedures 82
9.4.3 Password management system 82

This is a preview. Click here to purchase the full publication.

9.4.4 Use of privileged utility programs 83
9.4.5 Access control to program source code 84
10 Cryptography 84
10.1 Cryptographic controls 84
10.1.1 Policy on the use of cryptographic control 85
10.1.2 Key management 89
11 Physical and environmental security 91
11.1 Secure areas 91
11.1.1 Physical security perimeter 91
11.1.2 Physical entry controls 93
11.1.3 Securing offices, rooms and facilities 94
11.1.4 Protecting against external and environmental threats 94
11.1.5 Working in secure areas 95
11.1.6 Delivery and loading areas *and ware houses* 95
11.2 Equipment 96
11.2.1 Equipment siting and protection 96
11.2.2 Supporting utilities 98
11.2.3 Cabling security 99
11.2.4 Equipment maintenance 99
11.2.5 Removal of assets 100
11.2.6 Security of equipment and assets off-premises 101
11.2.7 Secure disposal or re-use of equipment 102
11.2.8 Unattended user equipment 103
11.2.9 Clear desk and clear screen policy 104
12 Operations security 104
12.1 Operational procedures and responsibilities 105
12.1.1 Documented operating Procedures 105
12.1.2 Change management 106
12.1.3 Capacity management 107
12.1.4 Separation of development, testing and operational environments 107
12.2 Protection from malware 108
12.2.1 Controls against malware 108
12.3 Backup 110
12.3.1 Information backup 110
12.4 Logging and monitoring 111
12.4.1 Event logging 111
12.4.2 Protection of log information 113
12.4.3 Administrator and operator logs 113
12.4.4 Clock synchronisation 114
12.4.5 *NUC – Centralization of collected cybersecurity events* 115
12.4.6 *NUC – Logs correlation and cyberattack scenarios identification* 115
12.5 Control of operational software 116
12.5.1 Installation of software on operational systems 116
12.5.2 *NUC – Only needed software packages* 118
12.6 Technical vulnerability management 119
12.6.1 Management of technical vulnerabilities 119
12.6.2 Restrictions on software installation 121
12.6.3 *NUC – Technical vulnerabilities information sources and channels* 121
12.6.4 *NUC – Restrictions on software execution* 122

This is a preview. Click here to purchase the full publication.

12.7 *Systems* audit considerations 122
12.7.1 *Systems* audit controls 123
13 Communications security 123
13.1 Network security management 123
13.1.1 Network controls 123
13.1.2 Security of network services 130
13.1.3 Segregation in networks 132
13.2 Information transfer 136
13.2.1 Information transfer policies and procedures 136
13.2.2 Agreements on information transfer 138
13.2.3 Electronic messaging 138
13.2.4 Confidentiality or non-disclosure agreements 140
14 System acquisition, development and maintenance 141
14.1 Security requirements of information systems 141
14.1.1 *Cybersecurity* Requirements Analysis and Specification 141
14.2 Security in development and support processes 142
14.2.1 Secure development policy 142
14.2.2 System change control procedures 143
14.2.3 Technical review of applications after operating platform changes 144
14.2.4 Restrictions on changes to software packages 145
14.2.5 Secure system engineering principles 145
14.2.6 Secure development environment 146
14.2.7 Outsourced development 147
14.2.8 System security testing 148
14.2.9 System acceptance testing 148
14.3 Test data 149
14.3.1 Protection of test data 149
15 Supplier relationships 150
15.1 *Cybersecurity* in supplier relationships 150
15.1.1 *Cybersecurity* policy for supplier relationships 150
15.1.2 Addressing security within supplier agreements 151
15.1.3 Information and communication technology supply chain 153
15.2 Supplier service delivery management 154
15.2.1 *Cybersecurity* policy for supplier relationships 154
15.2.2 Managing changes to supplier services 155
16 *Cybersecurity* incident management 156
16.1 Management of *I&C cybersecurity* incidents and improvements 156
16.1.1 Responsibilities and procedures 156
16.1.2 Reporting *I&C cybersecurity* events 162
16.1.3 Reporting *I&C cybersecurity* weaknesses 162
16.1.4 Assessment of and decision on *I&C cybersecurity* events 163
16.1.5 Response to *I&C cybersecurity* incidents 164
16.1.6 Learning from *I&C cybersecurity* incidents 165
16.1.7 Collection of evidence *from I&C* 165
17 *Cybersecurity* aspects of business continuity management 167
17.1 Cybersecurity continuity 167
17.1.1 Planning *cybersecurity* continuity 167
17.1.2 Implementing *cybersecurity* continuity 168

This is a preview. Click here to purchase the full publication.

17.1.3 Verify, review and evaluate *cybersecurity* continuity 169
17.2 Redundancies 170
17.2.1 Availability of *I&C systems* 170
18 Compliance 170
18.1 Compliance with legal and contractual requirements 171
18.1.1 Identification of applicable legislation and contractual requirements 171
18.1.2 Intellectual property rights 172
18.1.3 Protection of records 172
18.1.4 Privacy and protection of personally identifiable information 173
18.1.5 Regulation of cryptographic controls 174
18.2 Information security reviews*, audits, and inspections* 175
18.2.1 Independent review of cybersecurity 176
18.2.2 Compliance with security policies and standards 177
18.2.3 Technical compliance reviewing 177
19 *NUC – Cybersecurity and architecture* 179
19.1 *NUC – Cybersecurity and architecture controls* 179
19.1.1 *NUC – Security levels* 179
19.1.2 *NUC – Security zones* 180
19.1.3 *NUC – Administration security zones* 181
19.1.4 *NUC – Data extraction and collection* 182
19.1.5 *NUC – Temporary elements introduction within a security zone* 182
20 *NUC – Virtualization environment and infrastructure* 183
20.1 *NUC – Virtualization environment and infrastructure controls* 183
20.1.1 *NUC virtualized I&C environments* 183
Annex A (informative) Security Controls by Security Degrees, activities, I&C platform or I&C system, preservation focus, control focus and ISO/IEC 27002 modification 185
Annex B (informative) Correspondence with IEC 62645:2019 235
Annex C (informative) Sample list for documentation of project specific security controls selections 240
Annex D (informative) Semi-formal representation and exchange of security controls 243
Annex E (informative) Cryptography 244
E.1 Risk categorization 244
E.2 Information to be provided for transporting data 244
E.3 Cybersecurity roles 244
E.4 Two-factor authentication process for key management system access 245
Bibliography 246

Figure 1 – E/E/PE items 17
Figure 2 – Overview 31
Figure 3 – Process of selecting and implementing security controls for the actual I&C platform and I&C system 33

Table A.1 – Security controls overview 186
Table B.1 – Correspondence between IEC 62645:2019 and IEC 63096 235
Table C.1 – Sample list for documentation of project specific security controls selections 241

This is a preview. Click here to purchase the full publication.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – SECURITY CONTROLS

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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 63096 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

The text of this standard is based on the following documents:

FDIS	Report on voting
45A/1346/FDIS	45A/1353/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

This document is based on ISO/IEC 27002:2013.

This is a preview. Click here to purchase the full publication.

Clause 5 through Clause 18 of this document follow ISO/IEC 27002:2013, Clause 5 through Clause 18.

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.

This is a preview. Click here to purchase the full publication.