



**SLOVENSKI STANDARD**  
**oSIST prEN IEC 62443-2-1:2019**  
**01-november-2019**

---

**Zaščita industrijske avtomatizacije in kontrolnih sistemov - 2-1. del: Zahteve za program varnosti zaščite za lastnike sredstev IACS**

Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners

**iTeh STANDARD PREVIEW**

Réseaux industriels de communication - Sécurité dans les réseaux et les systèmes -  
Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes  
d'automatisation et de commande industrielles

<https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-8615bf2d800/osist-pr-en-iec-62443-2-1-2019>

**Ta slovenski standard je istoveten z: prEN IEC 62443-2-1:2019**

---

**ICS:**

|           |   |  |
|-----------|---|--|
| 25.040.01 | Sistemi za avtomatizacijo v industriji na splošno | Industrial automation systems in general |
| 35.030    | Informacijska varnost                             | IT Security                              |

**oSIST prEN IEC 62443-2-1:2019**                      **en,fr,de**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[oSIST prEN IEC 62443-2-1:2019](https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-8615bfb2d800/osist-pren-iec-62443-2-1-2019)

<https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-8615bfb2d800/osist-pren-iec-62443-2-1-2019>



PROJECT NUMBER:

**IEC 62443-2-1 ED2**

DATE OF CIRCULATION:

**2019-08-23**

CLOSING DATE FOR VOTING:

**2019-11-15**

SUPERSEDES DOCUMENTS:

**65/692A/RR**

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

SECRETARIAT:

France

SECRETARY:

Mr Rudy BELLIARDI

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 44, SC 45A, TC 57, SC 62A; ISO/IEC/JTC1/SC 27

PROPOSED HORIZONTAL STANDARD:

Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

 EMC ENVIRONMENT QUALITY ASSURANCE SAFETY SUBMITTED FOR CENELEC PARALLEL VOTING NOT SUBMITTED FOR CENELEC PARALLEL VOTING**Attention IEC-CENELEC parallel voting**

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

iTech STANDARD PREVIEW  
(standards.iteh.ai)

oSIST prEN IEC 62443-2-1:2019  
<http://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-8615fb2d800/osist-pr-en-iec-62443-2-1-2019>

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

**Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners**

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

**Copyright © 2019 International Electrotechnical Commission, IEC.** All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

## CONTENTS

|   |    |
|---|----|
| FOREWORD.....   | 9  |
| INTRODUCTION .....  | 11 |
| 1 Scope .....   | 13 |
| 2 Normative references .....  | 14 |
| 3 Terms, definitions, abbreviated terms, acronyms and conventions .....     | 14 |
| 3.1 Terms and definitions.....  | 14 |
| 3.3 Abbreviated terms and acronyms .....                                    | 17 |
| 4 Concepts.....   | 19 |
| 4.1 Use of IEC 62443-2-1.....   | 19 |
| 4.1.1 Applicable roles .....  | 19 |
| 4.1.2 Use of IEC 62443-2-1 by asset owners.....                             | 20 |
| 4.1.3 Use of IEC 62443-2-1 by service providers and product suppliers ..... | 22 |
| 4.2 Maturity model.....   | 22 |
| 4.3 Security levels (SLs) .....   | 24 |
| 4.4 Requirements definitions.....   | 25 |
| 4.4.1 Requirements organization.....  | 25 |
| 4.4.2 Requirements mappings .....   | 25 |
| 4.4.3 Requirement conventions.....  | 25 |
| 5 Conformity .....  | 25 |
| 5.1 Overview.....   | 25 |
| 5.2 Requirements selection.....   | 26 |
| 6 SPE 1 – Organizational security measures .....                            | 28 |
| 6.1 Purpose.....  | 28 |
| 6.2 ORG 1 – Security related organization and policies .....                | 28 |
| 6.2.1 ORG 1.1: Information security management system (ISMS) .....          | 28 |
| 6.2.2 ORG 1.2: Background checks.....                                       | 29 |
| 6.2.3 ORG 1.3: Security roles and responsibilities .....                    | 29 |
| 6.2.4 ORG 1.4: Security awareness training.....                             | 30 |
| 6.2.5 ORG 1.5: Security responsibilities training.....                      | 30 |
| 6.2.6 ORG 1.6: Supply chain security .....                                  | 31 |
| 6.3 ORG 2 – Security assessments and reviews .....                          | 32 |
| 6.3.1 ORG 2.1: Security risk mitigation .....                               | 32 |
| 6.3.2 ORG 2.2: Processes for discovery of security anomalies .....          | 33 |
| 6.3.3 ORG 2.3: Secure development and support .....                         | 33 |
| 6.3.4 ORG 2.4: SP reviews .....   | 34 |

|        |   |    |
|--------|---|----|
| 6.4    | ORG 3 – Security of physical access .....   | 35 |
| 6.4.1  | ORG 3.1: Physical access control.....   | 35 |
| 7      | SPE 2 – Configuration management.....   | 35 |
| 7.1    | Purpose.....  | 35 |
| 7.2    | CM 1 – Inventory management of IACS hardware/software components and<br>network communications..... | 35 |
| 7.2.1  | CM 1.1: Asset inventory baseline.....   | 35 |
| 7.2.2  | CM 1.2: Infrastructure drawings/documentation.....  | 36 |
| 7.2.3  | CM 1.3: Configuration settings.....   | 37 |
| 7.2.4  | CM 1.4: Change control.....   | 37 |
| 8      | SPE 3 – Network and communications security.....  | 38 |
| 8.1    | Purpose.....  | 38 |
| 8.2    | NET 1 – System segmentation.....  | 38 |
| 8.2.1  | NET 1.1: Segmentation from non-IACS networks .....  | 38 |
| 8.2.2  | NET 1.2: Documentation of network segment interconnections .....                                    | 39 |
| 8.2.3  | NET 1.3: Network segmentation from safety systems.....  | 39 |
| 8.2.4  | NET 1.4: Network autonomy.....  | 40 |
| 8.2.5  | NET 1.5: Network disconnection from external networks.....  | 40 |
| 8.2.6  | NET 1.6: Internal network access control .....  | 41 |
| 8.2.7  | NET 1.7: Device connections.....  | 41 |
| 8.2.8  | NET 1.8: Network accessible services .....  | 42 |
| 8.2.9  | NET 1.9: User messaging.....  | 43 |
| 8.2.10 | NET 1.10: Network time distribution .....   | 43 |
| 8.3    | NET 2 – Secure wireless access .....  | 44 |
| 8.3.1  | NET 2.1: Wireless protocols .....   | 44 |
| 8.3.2  | NET 2.2: Wireless network segmentation.....   | 44 |
| 8.3.3  | NET 2.3: Wireless properties and addresses.....   | 45 |
| 8.4    | NET 3 – Secure remote access.....   | 45 |
| 8.4.1  | NET 3.1: Remote access applications.....  | 45 |
| 8.4.2  | NET 3.2: Remote access connections.....   | 46 |
| 8.4.3  | NET 3.3: Remote access termination .....  | 47 |
| 9      | SPE 4 – Component security .....  | 47 |
| 9.1    | Purpose.....  | 47 |
| 9.2    | COMP 1 – Devices and media.....   | 48 |
| 9.2.1  | COMP 1.1: Device hardening .....  | 48 |
| 9.2.2  | COMP 1.2: Dedicated portable media .....  | 48 |
| 9.3    | COMP 2 – Malware protection.....  | 49 |
| 9.3.1  | COMP 2.1: Malware free.....   | 49 |

|         |   |    |
|---------|---|----|
| 9.3.2   | COMP 2.2: Malware protection .....                                      | 50 |
| 9.3.3   | COMP 2.3: Malware protection software validation and installation ..... | 50 |
| 9.4     | COMP 3 – Patch management.....  | 51 |
| 9.4.1   | COMP 3.1: Security patch authenticity/integrity .....                   | 51 |
| 9.4.2   | COMP 3.2: Security patch validation and installation.....               | 51 |
| 9.4.3   | COMP 3.3: Security patch status.....                                    | 52 |
| 9.4.4   | COMP 3.4: Security patching retention of security.....                  | 52 |
| 9.4.5   | COMP 3.5: Security patch mitigation .....                               | 53 |
| 10      | SPE 5 – Protection of data.....   | 53 |
| 10.1    | Purpose.....  | 53 |
| 10.2    | DATA 1 – Protection of data .....                                       | 54 |
| 10.2.1  | DATA 1.1: Data classification.....                                      | 54 |
| 10.2.2  | DATA 1.2: Protection of data .....                                      | 54 |
| 10.2.3  | DATA 1.3: Safety system configuration mode.....                         | 55 |
| 10.2.4  | DATA 1.4: Failure-state .....   | 56 |
| 10.2.5  | DATA 1.5: Data retention .....  | 56 |
| 10.2.6  | DATA 1.6: Data purging .....  | 57 |
| 10.2.7  | DATA 1.7: Cryptographic mechanisms.....                                 | 57 |
| 10.2.8  | DATA 1.8: Key management .....  | 58 |
| 10.2.9  | DATA 1.9: Public key infrastructure (PKI).....                          | 58 |
| 11      | SPE 6 – User access control.....  | 59 |
| 11.1    | Purpose.....  | 59 |
| 11.2    | USER 1 – Identification and authentication .....                        | 59 |
| 11.2.1  | USER 1.1: User identity assignment .....                                | 59 |
| 11.2.2  | USER 1.2: User identity removal .....                                   | 60 |
| 11.2.3  | USER 1.3: User identity persistence .....                               | 61 |
| 11.2.4  | USER 1.4: Access rights assignment .....                                | 61 |
| 11.2.5  | USER 1.5: Least privilege .....   | 62 |
| 11.2.6  | USER 1.6: Software service authentication.....                          | 62 |
| 11.2.7  | USER 1.7: Software services interactive login rights.....               | 63 |
| 11.2.8  | USER 1.8: User authentication .....                                     | 63 |
| 11.2.9  | USER 1.9: Multifactor authentication .....                              | 64 |
| 11.2.10 | USER 1.10: Mutual authentication.....                                   | 65 |
| 11.2.11 | USER 1.11: Password protection.....                                     | 65 |
| 11.2.12 | USER 1.12: Shared and disclosed/compromised passwords .....             | 66 |
| 11.2.13 | USER 1.13: User login display information.....                          | 66 |
| 11.2.14 | USER 1.14: User login failure displays.....                             | 67 |
| 11.2.15 | USER 1.15: Consecutive login failures.....                              | 67 |
| 11.2.16 | USER 1.16: Session integrity.....                                       | 68 |

|              |  |    |
|--------------|--|----|
| 11.2.17      | USER 1.17: Concurrent sessions.....                                | 68 |
| 11.2.18      | USER 1.18: Screen lock.....  | 69 |
| 11.3         | USER 2 – Authorization and access control.....                     | 69 |
| 11.3.1       | USER 2.1: Authorization.....                                       | 69 |
| 11.3.2       | USER 2.2: Administrative rights authorization.....                 | 70 |
| 11.3.3       | USER 2.3: Multiple approvals.....                                  | 70 |
| 11.3.4       | USER 2.4: Manual elevation of privileges.....                      | 71 |
| 12           | SPE 7 – Event and incident management.....                         | 71 |
| 12.1         | Purpose.....   | 71 |
| 12.2         | EVENT 1 – Event and incident management.....                       | 71 |
| 12.2.1       | EVENT 1.1: Event detection.....                                    | 71 |
| 12.2.2       | EVENT 1.2: Event reporting.....                                    | 72 |
| 12.2.3       | EVENT 1.3: Event reporting interfaces.....                         | 73 |
| 12.2.4       | EVENT 1.4: Logging.....  | 73 |
| 12.2.5       | EVENT 1.5: Log entries.....  | 74 |
| 12.2.6       | EVENT 1.6: Log access.....   | 74 |
| 12.2.7       | EVENT 1.7: Event analysis.....                                     | 75 |
| 12.2.8       | EVENT 1.8: Incident handling and response.....                     | 75 |
| 12.2.9       | EVENT 1.9: Vulnerability handling.....                             | 76 |
| 13           | SPE 8 – System integrity and availability.....                     | 77 |
| 13.1         | Purpose.....   | 77 |
| 13.2         | AVAIL 1 – System availability and intended functionality.....      | 77 |
| 13.2.1       | AVAIL 1.1: Continuity management.....                              | 77 |
| 13.2.2       | AVAIL 1.2: Resource management.....                                | 77 |
| 13.2.3       | AVAIL 1.3: DoS attacks.....  | 78 |
| 13.3         | AVAIL 2 – Backup/restore/archive.....                              | 78 |
| 13.3.1       | AVAIL 2.1: Backup.....   | 78 |
| 13.3.2       | AVAIL 2.2: Backup non-interference.....                            | 79 |
| 13.3.3       | AVAIL 2.3: Backup verification.....                                | 79 |
| 13.3.4       | AVAIL 2.4: Backup media.....                                       | 80 |
| 13.3.5       | AVAIL 2.5: Backup restoration.....                                 | 80 |
| Annex A      | (Informative) Cross references to other standards.....             | 81 |
| A.1          | Requirements relationship to IEC 62443-2-4.....                    | 81 |
| A.2          | Requirements relationship to IEC 62443-3-3.....                    | 84 |
| A.3          | Requirements relationship to IEC 62443-4-2.....                    | 86 |
| A.4          | Requirements relationship to ISO/IEC 27001 and ISO/ IEC 27002..... | 88 |
| A.5          | Requirements relationship to the NIST CSF.....                     | 90 |
| BIBLIOGRAPHY | .....  | 92 |

|  |    |
|--|----|
| Figure 1 – Parts of the IEC 62443 Series.....            | 11 |
| Figure 2 – Roles and responsibilities in IEC 62443 ..... | 14 |
| Table 1 – Maturity model.....                            | 24 |
| Table 2 – Typical conformity evidence types .....        | 26 |
| Table 3 – ORG 1.1 related references .....               | 28 |
| Table 4 – ORG 1.2 related references .....               | 29 |
| Table 5 – ORG 1.3 related references .....               | 30 |
| Table 6 – ORG 1.4 related references .....               | 30 |
| Table 7 – ORG 1.5 related references .....               | 31 |
| Table 8 – ORG 1.6 related references .....               | 32 |
| Table 9 – ORG 2.1 related references .....               | 33 |
| Table 10 – ORG 2.2 related references .....              | 33 |
| Table 11 – ORG-2.3 related references .....              | 34 |
| Table 12 – ORG 2.4 related references .....              | 34 |
| Table 13 – ORG 3.1 related references .....              | 35 |
| Table 14 – CM 1.1 related references.....                | 36 |
| Table 15 – CM 1.2 related references.....                | 37 |
| Table 16 – CM 1.3 related references .....               | 37 |
| Table 17 – CM 1.4 related references .....               | 38 |
| Table 18 – NET 1.1 related references .....              | 39 |
| Table 19 – NET 1.2 related references .....              | 39 |
| Table 20 – NET 1.3 related references .....              | 40 |
| Table 21 – NET 1.4 related references .....              | 40 |
| Table 22 – NET 1.5 related references .....              | 41 |
| Table 23 – NET 1.6 related references .....              | 41 |
| Table 24 – NET 1.7 related references .....              | 42 |
| Table 25 – NET 1.8 related references .....              | 42 |
| Table 26 – NET 1.9 related references .....              | 43 |
| Table 27 – NET 1.10 related references .....             | 43 |
| Table 28 – NET 2.1 related references .....              | 44 |
| Table 29 – NET 2.2 related references .....              | 45 |
| Table 30 – NET 2.3 related references .....              | 45 |
| Table 31 – NET 3.1 related references .....              | 46 |

STANDARD PREVIEW  
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-86156b2d800/osist-pr-en-iec-62443-2-1-2019>

<https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-86156b2d800/osist-pr-en-iec-62443-2-1-2019>

<https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-86156b2d800/osist-pr-en-iec-62443-2-1-2019>



|   |    |
|---|----|
| Table 32 – NET 3.2 related references .....   | 47 |
| Table 33 – NET 3.3 related references .....   | 47 |
| Table 34 – COMP 1.1 related references.....   | 48 |
| Table 35 – COMP 1.2 related references.....   | 49 |
| Table 36 – COMP 2.1 related references.....   | 49 |
| Table 37 – COMP 2.2 related references.....   | 50 |
| Table 38 – COMP 2.3 related references.....   | 51 |
| Table 39 – COMP 3.1 related references.....   | 51 |
| Table 40 – COMP 3.2 related references.....   | 52 |
| Table 41 – COMP 3.3 related references.....   | 52 |
| Table 42 – COMP 3.4 related references.....   | 53 |
| Table 43 – COMP 3.5 related references.....   | 53 |
| Table 44 – DATA 1.1 related references.....   | 54 |
| Table 45 – DATA 1.2 related references.....   | 55 |
| Table 46 – DATA 1.3 related references.....   | 56 |
| Table 47 – DATA 1.4 related references.....   | 56 |
| Table 48 – DATA 1.5 related references.....   | 57 |
| Table 49 – DATA 1.6 related references.....   | 57 |
| Table 50 – DATA 1.7 related references.....   | 58 |
| Table 51 – DATA 1.8 related references.....   | 58 |
| Table 52 – DATA 1.9 related references.....   | 59 |
| Table 53 – USER 1.1 related references .....  | 60 |
| Table 54 – USER 1.2 related references .....  | 60 |
| Table 55 – USER 1.3 related references .....  | 61 |
| Table 56 – USER 1.4 related references .....  | 61 |
| Table 57 – USER 1.5 related references .....  | 62 |
| Table 58 – USER 1.6 related references .....  | 63 |
| Table 59 – USER 1.7 related references .....  | 63 |
| Table 60 – USER 1.8 related references .....  | 64 |
| Table 61 – USER 1.9 related references .....  | 64 |
| Table 62 – USER 1.10 related references ..... | 65 |
| Table 63 – USER 1.11 related references ..... | 65 |
| Table 64 – USER 1.12 related references ..... | 66 |
| Table 65 – USER 1.13 related references ..... | 66 |
| Table 66 – USER 1.14 related references ..... | 67 |

ITeH STANDARD PREVIEW  
(standards.iteh.ai)

oSIST prEN IEC 62443-2-1:2019

[https://standards.iteh.ai/catalog/standards/sist/c44504e1-6fcc-4d18-b2ca-](https://standards.iteh.ai/catalog/standards/sist/c44504e1-6fcc-4d18-b2ca-8615bf2d800/osist-pr-en-iec-62443-2-1-2019)

[8615bf2d800/osist-pr-en-iec-62443-2-1-2019](https://standards.iteh.ai/catalog/standards/sist/c44504e1-6fcc-4d18-b2ca-8615bf2d800/osist-pr-en-iec-62443-2-1-2019)

|  |    |
|--|----|
| Table 67 – USER 1.15 related references .....            | 67 |
| Table 68 – USER 1.16 related references .....            | 68 |
| Table 69 – USER 1.17 related references .....            | 68 |
| Table 70 – USER 1.18 related references .....            | 69 |
| Table 71 – USER 2.1 related references .....             | 70 |
| Table 72 – USER 2.2 related references .....             | 70 |
| Table 73 – USER 2.3 related references .....             | 71 |
| Table 74 – USER 2.4 related references .....             | 71 |
| Table 75 – EVENT 1.1 related references .....            | 72 |
| Table 76 – EVENT 1.2 related references .....            | 72 |
| Table 77 – EVENT 1.3 related references .....            | 73 |
| Table 78 – EVENT 1.4 related references .....            | 74 |
| Table 79 – EVENT 1.5 related references .....            | 74 |
| Table 80 – EVENT 1.6 related references .....            | 75 |
| Table 81 – EVENT 1.7 related references .....            | 75 |
| Table 82 – EVENT 1.8 related references .....            | 76 |
| Table 83 – EVENT 1.9 related references .....            | 76 |
| Table 84 – AVAIL 1.1 related references .....            | 77 |
| Table 85 – AVAIL 1.2 related references .....            | 77 |
| Table 86 – AVAIL 1.3 related references .....            | 78 |
| Table 87 – AVAIL 2.1 related references .....            | 79 |
| Table 88 – AVAIL 2.2 related references .....            | 79 |
| Table 89 – AVAIL 2.3 related references .....            | 79 |
| Table 90 – AVAIL 2.4 related references .....            | 80 |
| Table 91 – AVAIL 2.5 related references .....            | 80 |
| Table A.1 – IEC 62443-2-4 cross-references .....         | 81 |
| Table A.1 – IEC 62443-2-4 cross-references (cont'd)..... | 82 |
| Table A.2 – IEC 62443-3-3 cross-references .....         | 84 |
| Table A.2 – IEC 62443-3-3 cross-references (cont'd)..... | 85 |
| Table A.3 – IEC 62443-4-2 cross-references .....         | 86 |
| Table A.3 – IEC 62443-4-2 cross-references (cont'd)..... | 86 |
| Table A.4 – ISO/IEC 27001 cross-references .....         | 88 |
| Table A.4 – ISO/IEC 27001 cross-references (cont'd)..... | 89 |
| Table A.5 – NIST CSF cross-references .....              | 90 |
| Table A.5 – NIST CSF cross-references (cont'd).....      | 91 |

iTech STANDARD PREVIEW  
(standards.iteh.ai)

oSIST prEN IEC 62443-2-1:2019

[https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-](https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-86156b2d800/osist-pr-en-iec-62443-2-1-2019)

86156b2d800/osist-pr-en-iec-62443-2-1-2019

# INTERNATIONAL ELECTROTECHNICAL COMMISSION

## Security for industrial automation and control systems –

### Part 2-1: Security program requirements for IACS asset owners

## 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 62443-2-1 has been prepared by subcommittee TC65: Industrial process measurement, control and automation, in cooperation with the ISA99 liaison.

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

|            |                  |
|------------|------------------|
| FDIS       | Report on voting |
| XX/XX/FDIS | XX/XX/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.

43 A list of all parts in the IEC 62443 series, published under the general title Security for  
44 industrial automation and control systems, can be found on the IEC website.

45 Future standards in this series will carry the new general title as cited above. Titles of existing  
46 standards in this series will be updates at the time of the next edition.

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

- 50 • reconfirmed,
- 51 • withdrawn,
- 52 • replaced by a revised edition, or
- 53 • amended.

54

55 The National Committees are requested to note that for this document the stability date  
56 is ....

57 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE  
58 DELETED AT THE PUBLICATION STAGE.

59

## iTeh STANDARD PREVIEW (standards.iteh.ai)

60

| Edition | Year | Changes  |
|---------|------|--|
| 1       | 2010 | Original Document<br><a href="https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-36128b2d6993/osist-pr-en-iec-62443-2-1-2019">https://standards.iteh.ai/catalog/standards/sist/e44504c1-6fec-4d18-b2ca-36128b2d6993/osist-pr-en-iec-62443-2-1-2019</a> |
| 2       | 2019 | Reformatted and revised document to create a set of requirements for asset owners to apply to their IACS.  |

61

62

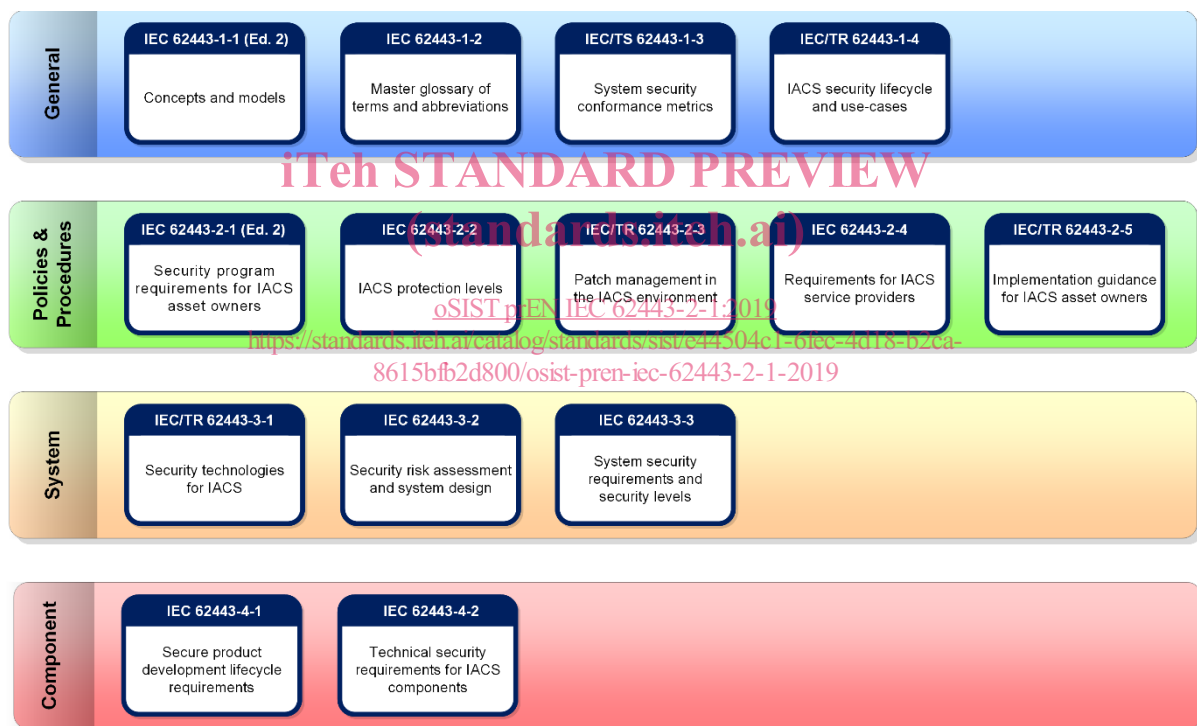
63

## INTRODUCTION

64 NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2. [13]<sup>1</sup> The ISO/IEC  
 65 Directives specify the format of this document as well as the use of terms like “shall”, “should” and “may”. The use of those  
 66 terms for the requirements specified in the numbered clauses of this document use the conventions discussed in the ISO/IEC  
 67 Directives, Appendix H.

68 This document is the part of the IEC 62443 series that contains security requirements for  
 69 industrial automation and control system (IACS) asset owners. In the context of this  
 70 document, asset owner also includes the operator of the IACS. It has been developed by  
 71 Working Group 02 of the International Society of Automation (ISA) committee on Security for  
 72 industrial automation and control systems, ISA99, in collaboration with Working Group 10 of  
 73 the International Electrotechnical Commission (IEC) Technical Committee 65. Its requirements  
 74 focus on cyber security and allow security capabilities that meet them to be provided as a  
 75 combination of technical, physical and procedural measures and compensating capabilities.

76 Figure 1 illustrates the relationship of the different parts of IEC 62443 that have been or are  
 77 being developed. Those that are normatively referenced are included in the list of normative  
 78 references in clause 2. All the parts are referenced in the Bibliography for informational  
 79 purposes.



80

81

**Figure 1 – Parts of the IEC 62443 Series**

82 Cyber security is an increasingly important topic in modern organizations. The term cyber  
 83 security is generally used to describe the set of countermeasures or practices taken to protect  
 84 a computer or computer system against unauthorized access or attack. In IACS, the concern  
 85 is that unwanted access or attack may result in the IACS not performing the critical functions  
 86 in the required timeframe.

87 Industrial organizations have begun using commercial-off-the-shelf (COTS) technology  
 88 developed for business systems in their IACS. Such products are often not ruggedized or

-----  
<sup>1</sup> Numbers in square brackets refer to the Bibliography.

89 rigorously engineered enough for IACS environments, where they can introduce additional  
90 vulnerabilities and threats to the IACS.

91 When COTS technologies are used in an IACS, they are often configured to meet IACS  
92 specific functional needs and operational constraints. For example, security event handling in  
93 COTS products may be configured differently for IACS applications than they are for  
94 traditional information technology (IT) applications. Typical COTS equipment is designed for  
95 environments where the primary objective is the protection of information. In an IACS  
96 environment, the primary objectives are the protection of the health, safety and environment  
97 (HSE) of the plant and the minimization of the operational and business impact on plant  
98 operation.

99 Some organizations may attempt to use pre-existing IT and business cyber security solutions  
100 to address security for IACS without understanding the consequences. While many of these  
101 solutions can be applied to IACS, they need to be applied in the correct way to eliminate  
102 inadvertent and undesired consequences.

103 A very common engineering approach when faced with a challenging problem is to break the  
104 problem into smaller pieces and address each piece in a disciplined manner. This approach is  
105 a sound one for addressing cyber security risks with IACS. However, a frequent mistake is to  
106 deal with cyber security one system at a time. Cyber security is a much larger challenge that  
107 should address all IACS components as well as the policies, procedures, practices and  
108 personnel that surround and utilize those IACS. Implementing such a wide-ranging  
109 management system may require a cultural change within the organization.

110 Addressing cyber security on an organization-wide basis may seem like a daunting task.  
111 There is no simple cookbook for security, nor is there a one-size-fits-all set of security  
112 practices. Absolute security may be achievable, but is probably undesirable because of the  
113 loss of functionality that would be necessary to achieve this near perfect state. Security is a  
114 balance of risk versus cost.

115 All situations will be different. In some situations, the risk may be related to HSE factors rather  
116 than purely economic impact. The risk may have an unrecoverable consequence rather than a  
117 temporary financial setback. Therefore, a predetermined set of mandatory security practices  
118 can either be overly restrictive and likely quite costly to implement or be insufficient to  
119 address the risk.

120 This document supports the need to address cyber security for an IACS by providing  
121 requirements for establishing, implementing, maintaining and continually improving an IACS  
122 security program (SP). These requirements, when implemented conscientiously, provide  
123 security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These  
124 requirements are written to be implementation independent, allowing asset owners to select  
125 approaches most suitable to their needs. IEC 62443-3-2 [9] describes a standard  
126 methodology for addressing cyber security risks in an IACS system design and can assist in  
127 the identification of risks and the selection of appropriate security requirements and  
128 associated capabilities for an IACS SP.

129 Asset owners may wish to apply their IACS SP across the organization to address the  
130 organization's needs and objectives, security requirements, business and work processes, as  
131 well as the organization's size and structure. All of these influencing factors are dynamic and  
132 will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the  
133 organization.

134 The effectiveness of an IACS SP is often enhanced through coordination or integration with  
135 the organization's processes and overall information security management system (ISMS).  
136 For example, security can be added to the organization's supply chain processes to require  
137 security in the design of processes, systems and controls. It is also expected that IACS SP  
138 will be scaled in accordance with the needs of the IACS and the organization.

139

## 140 1 Scope

141 IEC 62443-2-1 specifies asset owner security program (SP) requirements for an industrial  
142 automation and control system (IACS). This document uses the broad definition and scope of  
143 what constitutes an IACS as described in IEC 62443-1-1. In the context of this document,  
144 asset owner also includes the operator of the IACS.

145 This document recognizes that the lifespan of an IACS can exceed twenty years, and that  
146 many legacy systems contain hardware and software that are no longer supported. Therefore,  
147 the SP for a legacy system may address only a subset of the requirements defined in this  
148 document. For example, if its software is no longer supported, security patching requirements  
149 cannot be met. Similarly, backup software for older systems may not be available for all  
150 components of the IACS. As a result, this document recognizes that not all requirements can  
151 be met by legacy systems. In situations where specific requirements or subsets of  
152 requirements are applicable but unable to be implemented in legacy systems, then  
153 compensating countermeasures should be implemented where possible.

154 This document also recognizes that not all requirements specified in this document apply to  
155 all IACSs. For example, requirements associated with wireless technology or safety systems  
156 will not apply to IACSs that do not include wireless technology or safety systems technology.  
157 Similarly, malware protection requirements may not all apply to systems for which anti-  
158 malware software is not available for any of their devices. Therefore, the asset owner should  
159 identify the IACS security requirements that are applicable to its IACSs in their specific  
160 operating environments.

161 The elements of an IACS SP described in this document define required security capabilities  
162 that apply to the secure operation of an IACS. Although the asset owner is ultimately  
163 accountable for the secure operation of an IACS, implementation of these security capabilities  
164 often includes support from its service providers and product suppliers. For this reason, this  
165 document provides guidance for an asset owner when stating security requirements for their  
166 service providers and product suppliers, referencing other parts of the IEC 62443 series.

167 Figure 2 illustrates the security capabilities of the asset owner, service provider(s) and  
168 product supplier(s) of an IACS and their relationships to each other and to the  
169 Automation Solution. The Automation Solution is a technical solution implementing the  
170 functional capabilities necessary for the IACS. It is composed of hardware and software  
171 components that have been installed and configured to operate in the IACS. The IACS is a  
172 combination of the Automation Solution and the organizational measures necessary for its  
173 design, deployment, operation and maintenance.

174 Some of these capabilities rely on the appropriate application of integration maintenance  
175 capabilities defined in IEC 62443-2-4 [6] and technical security capabilities defined in  
176 IEC 62443-3-3 [10] and IEC 62443-4-2 [12].