



# TECHNICAL REPORT



---

**Security for industrial automation and control systems –  
Part 2-3: Patch management in the IACS environment**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

---

ICS : 25.040.40; 35.040; 35.100

ISBN 978-2-8322-2768-8

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

## CONTENTS

|  |    |
|--|----|
| FOREWORD.....  | 5  |
| INTRODUCTION.....  | 7  |
| 1 Scope.....   | 8  |
| 2 Normative references.....  | 8  |
| 3 Terms, definitions, abbreviated terms and acronyms .....                     | 8  |
| 3.1 Terms and definitions .....  | 8  |
| 3.2 Abbreviated terms and acronyms.....  | 9  |
| 4 Industrial automation and control system patching.....                       | 11 |
| 4.1 Patching problems faced in industrial automation and control systems ..... | 11 |
| 4.2 Impacts of poor patch management .....                                     | 11 |
| 4.3 Obsolete IACS patch management mitigation.....                             | 12 |
| 4.4 Patch lifecycle state .....  | 12 |
| 5 Recommended requirements for asset owner .....                               | 13 |
| 6 Recommended requirements for IACS product supplier .....                     | 14 |
| 7 Exchanging patch information .....   | 14 |
| 7.1 General.....   | 14 |
| 7.2 Patch information exchange format.....                                     | 15 |
| 7.3 Patch compatibility information filename convention.....                   | 15 |
| 7.4 VPC file schema .....  | 15 |
| 7.5 VPC file element definitions.....  | 17 |
| Annex A (informative) VPC XSD file format .....                                | 21 |
| A.1 VPC XSD file format specification.....                                     | 21 |
| A.2 Core component types .....   | 23 |
| A.2.1 Overview .....   | 23 |
| A.2.2 CodeType .....   | 23 |
| A.2.3 DateTimeType .....   | 24 |
| A.2.4 IdentifierType.....  | 24 |
| A.2.5 IndicatorType.....   | 25 |
| A.2.6 TextType .....   | 25 |
| Annex B (informative) IACS asset owner guidance on patching.....               | 26 |
| B.1 Annex organization .....   | 26 |
| B.2 Overview.....  | 26 |
| B.3 Information gathering .....  | 27 |
| B.3.1 Inventory of existing environment .....                                  | 27 |
| B.3.2 Tools for manual and automatic scanning .....                            | 29 |
| B.3.3 IACS product supplier contact and relationship building .....            | 30 |
| B.3.4 Supportability and product supplier product lifecycle .....              | 32 |
| B.3.5 Evaluation and assessment of existing environment.....                   | 32 |
| B.3.6 Classification and categorization of assets/hardware/software.....       | 33 |
| B.4 Project planning and implementation .....                                  | 36 |
| B.4.1 Overview .....   | 36 |
| B.4.2 Developing the business case .....                                       | 37 |
| B.4.3 Establishing and assigning roles and responsibilities .....              | 38 |
| B.4.4 Testing environment and infrastructure .....                             | 40 |
| B.4.5 Implement backup and restoration infrastructure .....                    | 41 |
| B.4.6 Establishing product supplier procurement guidelines .....               | 42 |

|                       |  |    |
|-----------------------|--|----|
| B.5                   | Monitoring and evaluation .....  | 42 |
| B.5.1                 | Overview .....   | 42 |
| B.5.2                 | Monitoring and identification of security related patches.....                               | 43 |
| B.5.3                 | Determining patch applicability.....   | 43 |
| B.5.4                 | Impact, criticality and risk assessment.....   | 44 |
| B.5.5                 | Decision for installation .....  | 45 |
| B.6                   | Patch testing.....   | 45 |
| B.6.1                 | Patch testing process.....   | 45 |
| B.6.2                 | Asset owner qualification of security patches prior to installation.....                     | 46 |
| B.6.3                 | Determining patch file authenticity.....   | 46 |
| B.6.4                 | Review functional and security changes from patches.....                                     | 46 |
| B.6.5                 | Installation procedure.....  | 47 |
| B.6.6                 | Patch qualification and validation .....   | 48 |
| B.6.7                 | Patch removal, roll back, restoration procedures.....  | 48 |
| B.6.8                 | Risk mitigation alternatives.....  | 49 |
| B.7                   | Patch deployment and installation .....  | 50 |
| B.7.1                 | Patch deployment and installation process .....  | 50 |
| B.7.2                 | Notification of affected parties .....   | 50 |
| B.7.3                 | Preparation.....   | 51 |
| B.7.4                 | Phased scheduling and installation.....  | 51 |
| B.7.5                 | Verification of patch installation.....  | 52 |
| B.7.6                 | Staff training and drills .....  | 52 |
| B.8                   | Operating an IACS patch management program.....  | 53 |
| B.8.1                 | Overview .....   | 53 |
| B.8.2                 | Change management .....  | 53 |
| B.8.3                 | Vulnerability awareness.....   | 53 |
| B.8.4                 | Outage scheduling .....  | 54 |
| B.8.5                 | Security hardening.....  | 54 |
| B.8.6                 | Inventory and data maintenance.....  | 54 |
| B.8.7                 | Procuring or adding new devices .....  | 55 |
| B.8.8                 | Patch management reporting and KPIs.....   | 55 |
| Annex C (informative) | IACS product supplier / service provider guidance on patching .....                          | 56 |
| C.1                   | Annex organization .....   | 56 |
| C.2                   | Discovery of vulnerabilities.....  | 56 |
| C.2.1                 | General .....  | 56 |
| C.2.2                 | Vulnerability discovery and identification within the product.....                           | 57 |
| C.2.3                 | Vulnerability discovery and identification within externally sourced product components..... | 57 |
| C.3                   | Development, verification and validation of security updates .....                           | 58 |
| C.4                   | Distribution of cyber security updates .....   | 58 |
| C.5                   | Communication and outreach .....   | 58 |
| Bibliography          | .....  | 60 |
| Figure 1              | – Patch state model .....  | 13 |
| Figure 2              | – VPC file schema.....   | 16 |
| Figure 3              | – VPC file schema diagram format.....  | 17 |
| Figure B.1            | – IACS patch management workflow.....  | 27 |
| Figure B.2            | – Planning an IACS patch management process .....  | 36 |

|  |    |
|--|----|
| Figure B.3 – Sample responsibilities chart.....                    | 40 |
| Figure B.4 – Patch monitoring and evaluation process.....          | 42 |
| Figure B.5 – A patch testing process.....                          | 45 |
| Figure B.6 – A patch deployment and installation process.....      | 50 |
| Table 1 – Patch lifecycle states.....                              | 12 |
| Table 2 – VPC XSD PatchData file elements.....                     | 17 |
| Table 3 – VPC XSD PatchVendor file elements.....                   | 18 |
| Table 4 – VPC XSD Patch file elements.....                         | 18 |
| Table 5 – VPC XSD VendorProduct file elements.....                 | 20 |
| Table A.1 – CodeType optional attributes.....                      | 24 |
| Table A.2 – DateTimeType optional attributes.....                  | 24 |
| Table A.3 – IdentifierType optional attributes.....                | 25 |
| Table A.4 – IndicatorType optional attributes.....                 | 25 |
| Table A.5 – TextType optional attributes.....                      | 25 |
| Table B.1 – Sample product supplier profile.....                   | 31 |
| Table B.2 – Communication capabilities.....                        | 34 |
| Table B.3 – Sample software categorization.....                    | 35 |
| Table B.4 – Responsibility assignment definitions.....             | 39 |
| Table B.5 – Sample severity based patch management timeframes..... | 45 |

IECNORM.COM : Click to view the full PDF of IEC TR 62443-2-3 ed 1.0:2015

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

### SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

#### Part 2-3: Patch management in the IACS environment

#### 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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

Technical Report IEC 62443-2-3 has been prepared by ISA Technical Committee 99 in partnership with IEC technical committee 65: Industrial-process measurement, control and automation.

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

|               |                  |
|---------------|------------------|
| Enquiry draft | Report on voting |
| 65/554/DTR    | 65/564/RVC       |

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

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

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

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

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

A bilingual version of this publication may be issued at a later date.

**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.**

IECNORM.COM : Click to view the full PDF of IEC TR 62443-2-3 ed 1.0:2015