PD IEC/TR 62443-2-3:2015

BSI Standards Publication

Security for industrial automation and control systems

Part 2-3: Patch management in the IACS environment

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of IEC/TR 62443-2-3:2015.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 83544 5
ICS 25.040.40; 35.040; 35.100

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2015.

Amendments/corrigenda issued since publication

Date	Text affected

IEC TR 62443-2-3

Edition 1.0 2015-06

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

CONTENTS

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.

INTRODUCTION

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established information security management systems (ISMS) in place as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), in ISO/IEC 27001 and ISO/IEC 27002. These management systems provide an organization with a well-established method for protecting its assets from cyber-attacks.

Industrial Automation and Control Systems (IACS) suppliers and owners are using commercial-off-the-shelf (COTS) technology developed for business systems in their everyday processes. This provides an increased opportunity for cyber-attack against the IACS equipment, since COTS systems are more widely known and used. There has also been new interest in ICS security research that has uncovered numerous device vulnerabilities as well. Successful attacks against industrial systems may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the business cyber security strategy to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent consequences.

This technical report addresses the patch management aspect of IACS cyber security. Patch management is part of a comprehensive cyber security strategy that increases cyber security through the installation of patches, also called software updates, software upgrades, firmware upgrades, service packs, hotfixes, basic input output system (BIOS) updates and other digital electronic program updates that resolve bugs, operability, reliability and cyber security vulnerabilities. This technical report introduces to the reader many of the problems and industry concerns associated with IACS patch management for asset owners and IACS product suppliers. It also describes the impacts poor patch management can have on the reliability and/or operability of the IACS.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-3: Patch management in the IACS environment

1 Scope

This part of IEC 62443, which is a Technical Report, describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program.

This Technical Report recommends a defined format for the distribution of information about security patches from asset owners to IACS product suppliers, a definition of some of the activities associated with the development of the patch information by IACS product suppliers and deployment and installation of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however, it may also be applicable for non-security related patches or updates.

The Technical Report does not differentiate between patches made available for the operating systems (OSs), applications or devices. It does not differentiate between the product suppliers that supply the infrastructure components or the IACS applications; it provides guidance for all patches applicable to the IACS. Additionally, the type of patch can be for the resolution of bugs, reliability issues, operability issues or security vulnerabilities.

NOTE 1 This Technical Report does not provide guidance on the ethics and approaches for the discovery and disclosure of security vulnerabilities affecting IACS. This is a general issue outside the scope of this report.

NOTE 2 This Technical Report does not provide guidance on the mitigation of vulnerabilities in the period between when the vulnerability is discovered and the date that the patch resolving the vulnerability is created. For guidance on multiple countermeasures to mitigate security risks as part of an IACS security management system (IACS-SMS), refer to, Annexes B.4.5, B.4.6 and B.8.5 in this Technical Report and other documents in the IEC 62443 series.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the normative references specified in Clause 2, as well as the following, apply: