IEC TR 62443-2-3

Edition 1.0 2015-06

TECHNICAL REPORT

colour inside

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

IEC TR 62443-2-3:2015-06(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 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.

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: csc@iec.ch.

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

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

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:

3.1.1
bug
flaw in the original development of software (such as a security vulnerability), which causes it to perform or behave in an unintended manner (such as cause reliability or operability issues)

3.1.2
patch
incremental software change in order to address a security vulnerability, a bug, reliability or operability issue (update) or add a new feature (upgrade)

Note 1 to entry: Patches may also be called software updates, software upgrades, firmware upgrades, service packs, hotfixes, basic input output system (BIOS) updates, security advisories and other digital electronic program updates.

3.1.3
patch lifecycle
period in time that a patch is recommended or created until the patch is installed

Note 1 to entry: In the context of this technical report, this lifecycle begins when the patch is created and made available.

Note 2 to entry: Some feel that the patching lifecycle begins when the vulnerability has been disclosed. However, it is not possible for this technical report to provide all possible guidance for the mitigation of vulnerabilities for the period between disclosure of a vulnerability, the decision to create a patch and the availability of a patch. It is also to the discretion of the software developer or product supplier to determine if they develop a patch.

3.1.4
patch management
set of processes used to monitor patch releases, decide which patches should be installed to which system under consideration (SuC), if the patch should be tested prior to installation on a production SuC, at which specified time the patch should be installed and of tracking the successful installation

3.2 Abbreviated terms and acronyms

ANSI	American National Standards Institute
BCP	Business continuity planning
BIA	Business impact assessment
BIOS	Basic input output system
CCTS	Core Components Technical Specification
CERT	Cyber Emergency Response Team, Computer Emergency Readiness Team or other regional/industry variant
CD	Compact disc
COTS	Commercial-off-the-shelf
CPNI	[UK] Centre for Protection of National Infrastructure
CPU	Central processing unit
DCS	Distributed control system
DHS	[US] Department of Homeland Security
DRP	Disaster recovery planning
DVD	Digital versatile disc
EULA	End user license agreement
FAT	Factory acceptance testing
HSE	Health, safety and environmental
HTML	Hypertext Markup Language
HTTP	Hypertext transfer protocol
ICS-CERT	[US DHS] Industrial Control Systems Cyber Emergency Response Team

IACS	Industrial automation and control system(s)
IACS-SMS	IACS security management system
IDS	Intrusion detection system
IEC	International Electro-technical Commission
IP	Internet protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information technology
KPI	Key performance indicator
MD5	Message digest 5
MES	Manufacturing execution system
MESA	Manufacturing Enterprise Solutions Association International
MSMUG	Microsoft Manufacturing Users Group
NERC	North American Electric Reliability Corporation
NISCC	[US] National Infrastructure Security Co-ordination Centre
NSA	[US] National Security Agency
OAGIS	Open Applications Group Integration Specification
OEM	Original equipment manufacturer
OS	Operating system
PLC	Programmable logic controller
RACI	Responsible, accountable, consulted, informed
RAID	Redundant array of independent disks
RASCI	Responsible, accountable, supportive, consulted and informed
RTU	Remote terminal unit
SAT	Site acceptance testing
SHA	Secure hash algorithm
SIS	Safety instrumented system
SMTP	Simple Mail Transfer Protocol
SPX	Sequenced packet exchange
SQL	Structured query language
SuC	System under consideration
TC	Technical committee
UN	United Nations
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
URI	Uniform resource identifier
USB	Universal serial bus
US-CERT	United States Computer Emergency Readiness Team
VPC	Vendor patch compatibility
WAN	Wide area network
XML	eXtensible Markup Language
XSD	XML schema definition

4 Industrial automation and control system patching

4.1 Patching problems faced in industrial automation and control systems

There are many challenges that asset owners face when attempting to implement a patch management program for their IACS. Patching an IACS means changing the IACS and changes can negatively affect its safety, operability or reliability if not performed correctly. Preparing an IACS to be patched can require a tremendous amount of work and asset owners may struggle for the necessary resources to address the added workload. For each patch and for each product they own, an asset owner will have to gather and analyze patch information for each device, install and verify on a test system, ensure backups are created before and after, ensure testing again before turning the system back over to operations and finally track all the necessary documentation of the changes.

Due to the resources and efforts recommended to patch an IACS most organizations schedule patch installations during other normal routine maintenance outages. Sometimes these outage windows are quarterly, yearly or even less frequently. Some extremely critical systems may not have outage windows available and can therefore not be patched if a system outage is required to do so.

Applying patches is a risk management decision. If the cost of applying patches is greater than the risk evaluated cost, then the patch may be delayed, especially if there are other security controls in place that mitigate the risk (such as disable or remove features).

The unintended consequences of a poor patch management program can include:

- incompatibility between patches and control system software;
- false positives due to antivirus and anti-malware; and
- degradation of system performance, reliability and operability with insufficient testing.

For additional information, see B.4.2.

4.2 Impacts of poor patch management

Adversaries (for example, malicious threat actors) will always have an advantage over their targets given the challenges product suppliers and asset owners face in keeping their systems up to date to minimize security risk caused by vulnerabilities. The moment a vulnerability is disclosed, whether by well-intentioned or malicious intent, the problem is then transferred primarily to the asset owner to apply the patch as quickly as possible. The asset owner may or may not be able to apply the patch and it becomes a risk-based decision on how to mitigate the vulnerability risk. Though it may never be possible to eliminate all software vulnerabilities, there should be no excuse for not evaluating the risk of the vulnerability and determining when and how patches should be applied.

The primary impact of poor IACS patch management is an increased risk of loss or compromise of an IACS system. Unlike for example office or enterprise systems, compromise of an IACS may have consequences beyond the loss of data or downtime of the system. A compromise of an IACS may impact system safety, the physical safety of operational personnel, the quality of produced products, the safety of produced products and the usability of produced products.

For additional information, see B.4.2.

NOTE 1 If critical documentation on the production of a product is lost, the product may have to be scrapped, even if there was no physical damage done to the product (such as pharmaceutical development, food production, etc.)

NOTE 2 Directed attacks of unpatched IACS systems may even result in the destruction of equipment. Undirected attacks of unpatched IACS systems, where the IACS system is not a primary target, may still cause the loss of control with resultant risks to safety and product quality. One example of such an attack is Structured Query Language (SQL) injection worms, which consume all central processing unit (CPU) and network resources.

4.3 Obsolete IACS patch management mitigation

Asset owners may experience the situation where products are no longer supported by their suppliers but have reported vulnerabilities. IACS systems are typically in production for decades and adversaries know these older systems are vulnerable. Asset owners need to consider other mitigations when patching is not an option.

For additional information on countermeasures to mitigate security risks as part of an IACS patch management process see Annexes B.4.5, B.4.6 and B.5.5, and other documents in the IEC 62443 series.

4.4 Patch lifecycle state

Patches have a defined lifecycle state model. They progress from available to authorized to effective and installed. Not all patches available are relevant to the IACS and not all patches are compatible with the IACS applications. It is important for an effective IACS patch management process to know the state of all available patches. Lifecycle states for patches are defined in Table 1.

Table 1 – Patch lifecycle states

Patch state	Patch state definition	Managed by
Available	The patch has been provided by a third party or an IACS supplier but has not been tested.	Asset owner Product supplier
In Test	The patch is being tested by an IACS supplier.	Product supplier
Not Approved	The patch has failed the testing of the IACS supplier and should not be used, unless and until the IACS supplier confirms that the patch has been Approved.	Product supplier
Not Applicable	The patch has been tested and is not considered relevant to IACS use.	Product supplier
Approved	The patch has passed testing by the IACS supplier.	Product supplier
Released	The patch is released for use by the IACS supplier or third party, or the patch may be directly applicable by the asset owner for their internally developed systems.	Asset owner Product supplier
In Internal Test	The patch is being tested by the asset owner testing team.	Asset owner
Not Authorized	The patch has failed internal testing, or may not be applicable.	Asset owner
Authorized	The patch is released by the asset owner and meets company standards for updatable devices, or by inspection did not need testing.	Asset owner
Effective	The patch is posted by the asset owner for use.	Asset owner
Installed	The patch is installed on the system.	Asset owner

The state model for lifecycle states is shown in Figure 1. The states maintained by the IACS product supplier are in the dark gray area in the left half of the figure. The states maintained by the IACS asset owner are in the light grey area in the right half of the figure. The transitions between states are activities of the asset owners or the product suppliers, as defined in the other parts of this report.

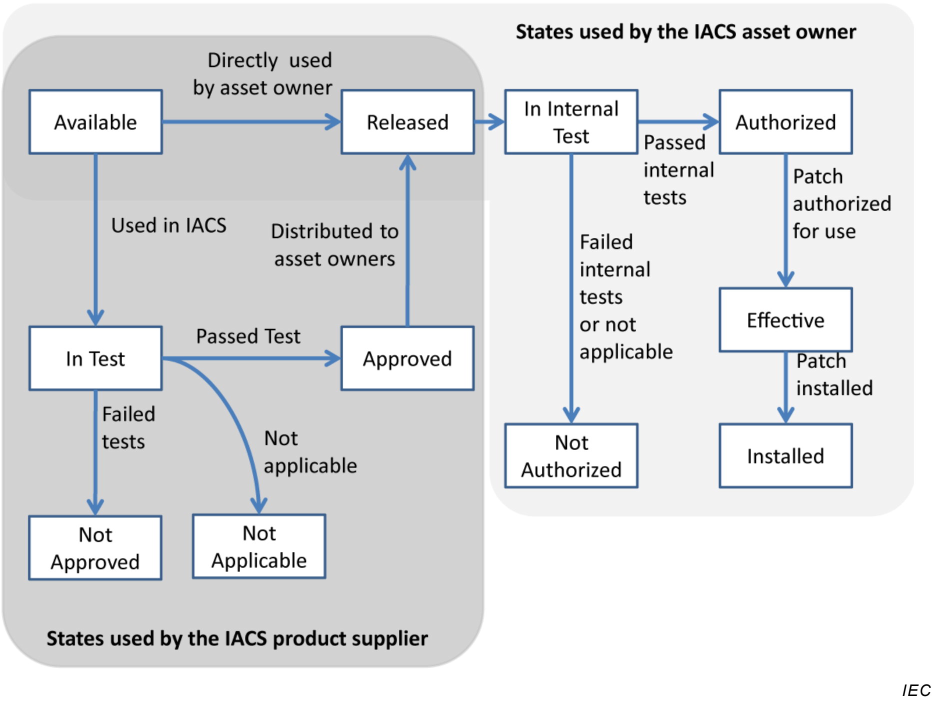

Figure 1 – Patch state model

5 Recommended requirements for asset owner

Asset owners have an implied obligation to uphold the safety, reliability, operability, security and quality of their operations. Achieving cyber security assurance, through patching IACS assets, is a critical part of that obligation.

IACS asset owners should:

a) establish and maintain an inventory of all electronic devices associated with the IACS, that may be updated by: modification of their functionality, configuration, operation, software, firmware, operating code, etc. These devices should be referred to as ‘updatable’ devices;

b) establish and maintain an accurate record of the currently installed versions for each device, called the ‘installed’ version;

c) determine on a regular schedule what upgrades and updates are available for each device, called the ‘latest’ version;

d) determine on a regular schedule the ‘released versions’ of upgrades and updates which are identified as compatible by the IACS product supplier and meet the asset owners standards for ‘updatable’ devices;

e) test the installation of IACS patches in a way that accurately reflects the production environment, so as to ensure that the reliability and operability of the IACS is not negatively affected when patches are installed on the IACS in the actual production environment. Patches which have successfully passed these tests are called the ‘authorized patches’;

f) schedule authorized, effective patches for installation at the next available opportunity within the constraints of system design (for example, redundancy, fault-tolerance, safety) and operational requirements (for example, unplanned outage, scheduled outage, on-process, etc.);

g) update records at a planned interval, at least on a quarterly basis, to include for each updateable device: installed versions, authorized versions, effective versions and released versions;