

ISA-TR62443-2-3-2015

**Security for industrial automation
and control systems**

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

Approved 1 July 2015

.....

ISA-TR62443-2-3-2015

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

ISBN: 978-1-941546-64-2

Copyright © 2015 by ISA. All rights reserved. Not for resale.

ISA
67 Alexander Drive
P. O. Box 12277
Research Triangle Park, NC 27709 USA

PREFACE

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR62443-2-3-2015.

This technical report has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the fields of industrial automation and instrumentation. To be of real value, this technical report should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices and technical reports to the greatest extent possible. Standard for Use of the International System of Units (SI): The Modern Metric System, published by the American Society for Testing and Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA or of any of the standards, recommended practices and technical reports that ISA develops.

CAUTION – ISA adheres to the policy of the American National Standards Institute with regard to patents. If ISA is informed of an existing patent that is recommended for use of the standard, it will require the owner of the patent to either grant a royalty-free license for use of the patent by users complying with the standard or a license on reasonable terms and conditions that are free from unfair discrimination.

Even if ISA is unaware of any patent covering this Standard, the user is cautioned that implementation of the standard may require use of techniques, processes or materials covered by patent rights. ISA takes no position on the existence or validity of any patent rights that may be involved in implementing the standard. ISA is not responsible for identifying all patents that may require a license before implementation of the standard or for investigating the validity or scope of any patents brought to its attention. The user should carefully investigate relevant patents before using the standard for the user's intended application.

However, ISA asks that anyone reviewing this standard who is aware of any patents that may impact implementation of the standard notify the ISA Standards and Practices Department of the patent and its owner.

Additionally, the use of this standard may involve hazardous materials, operations or equipment. The standard cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this standard must exercise sound professional judgment concerning its use and applicability under the user's particular circumstances. The user must also consider the applicability of any governmental regulatory limitations and established safety and health practices before implementing this standard.

The following people served as active members of ISA99 Working Group 06 since 2011 for the preparation of this technical report and the patch reporting format:

Name	Company	Contributor	Reviewer
William "Bill" Cotter WG/TG co-Chair	3M	X	
Florian Ott WG/TG co-Chair	Siemens AG	X	
Donovan Tindill WG/TG co-Chair, Editor	Honeywell / Matrikon	X	
Michael Coden Editor	NextNine Inc, and MIT-(IC)3	X	
Marc Ayala	aeSolutions	X	
Bruce Billedeaux	Maverick Technologies	X	
Eric Boice	Honeywell	X	
Dennis Brandl	BR&L Consulting	X	
Seth Carpenter	Honeywell	X	
Eric Cosman	ISA, ARC, ISA99 Committee Co-Chair		X
Ratna Kanth Dittakavi	ABB	X	
Earl Eiland	New Mexico Institute of Mining and Technology	X	
Jim Gilsinn	Kenexis, ISA99 Committee Co-Chair		X
Tom Good	DuPont	X	
Erik Goode		X	
Bruce Honda	Weyerhaeuser	X	
Larry McArthur			X
Glenn Merrell	Freelance Consulting	X	
Susan Peterson	GE Oil & Gas		X
Tom Phinney	IEC Liaison	X	X
Michael Piccalo	Industrial Defender	X	
Charley Robinson	ISA		X
Ragnar Schierholz	ABB		X
Walter Sikora	Industrial Defender	X	
Graham Speake NISCC/CPNI Liaison	Yokogawa		
Tatsaki Takebe	Yokogawa Electric		X
Randy Woods	Dow	X	

CONTENTS

PREFACE	3
FOREWORD	9
INTRODUCTION	10
1 Scope	11
2 Normative references	11
3 Terms, definitions, abbreviated terms, acronyms and conventions	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms and acronyms	12
4 Industrial automation and control system patching	14
4.1 Patching problems faced in industrial automation and control systems	14
4.2 Impacts of poor patch management.....	14
4.3 Obsolete IACS patch management mitigation	15
4.4 Patch lifecycle state.....	15
5 Recommended requirements for asset owner	16
6 Recommended requirements for IACS product supplier	17
7 Exchanging patch information.....	17
7.1 Introduction	17
7.2 Patch information exchange format	18
7.3 Patch compatibility information filename convention	18
7.4 VPC file schema	18
7.5 VPC file element definitions	20
Annex A (Informative) VPC XSD file format	25
A.1 VPC XSD file format specification	25
A.2 Core component types	27
A.2.1 Overview	27
A.2.2 CodeType.....	28
A.2.3 DateTimeType	28
A.2.4 IdentifierType	29
A.2.5 IndicatorType	29
A.2.6 TextType	29
Annex B (Informative) IACS asset owner guidance on patching	31
B.1 Annex organization	31
B.2 Overview	31
B.3 Information gathering	32
B.3.1 Inventory of existing environment.....	32
B.3.2 Tools for manual and automatic scanning.....	34
B.3.3 IACS product supplier contact and relationship building	35
B.3.4 Supportability and product supplier product lifecycle.....	37
B.3.5 Evaluation and assessment of existing environment	37
B.3.6 Classification and categorization of assets/hardware/software	38
B.4 Project planning and implementation	41
B.4.1 Overview	41

B.4.2	Developing the business case	41
B.4.3	Establishing and assigning roles and responsibilities	43
B.4.4	Testing environment and infrastructure	45
B.4.5	Implement backup and restoration infrastructure	46
B.4.6	Establishing product supplier procurement guidelines	47
B.5	Monitoring and evaluation	47
B.5.1	Overview	47
B.5.2	Monitoring and identification of security related patches	48
B.5.3	Determining patch applicability	49
B.5.4	Impact, criticality and risk assessment	49
B.5.5	Decision for installation	50
B.6	Patch testing	50
B.6.1	Patch testing process	50
B.6.2	Asset owner qualification of security patches prior to installation	51
B.6.3	Determining patch file authenticity	51
B.6.4	Review functional and security changes from patches	51
B.6.5	Installation procedure	52
B.6.6	Patch qualification and validation	53
B.6.7	Patch removal, roll back, restoration procedures	53
B.6.8	Risk mitigation alternatives	54
B.7	Patch deployment and installation	55
B.7.1	Patch deployment and installation process	55
B.7.2	Notification of affected parties	56
B.7.3	Preparation	56
B.7.4	Phased scheduling and installation	56
B.7.5	Verification of patch installation	57
B.7.6	Staff training and drills	57
B.8	Operating an IACS patch management program	58
B.8.1	Overview	58
B.8.2	Change management	58
B.8.3	Vulnerability awareness	58
B.8.4	Outage scheduling	59
B.8.5	Security hardening	59
B.8.6	Inventory and data maintenance	59
B.8.7	Procuring or adding new devices	60
B.8.8	Patch management reporting and KPIs	60
Annex C	(Informative) IACS product supplier / service provider guidance on patching	61
C.1	Annex organization	61
C.2	Discovery of vulnerabilities	61
C.2.1	Vulnerability discovery and identification within the product	62
C.2.2	Vulnerability discovery and identification within externally sourced product components	62
C.3	Development, verification and validation of security updates	62
C.4	Distribution of cyber security updates	63

C.5 Communication and outreach	63
BIBLIOGRAPHY	65
Figure 1 – Patch state model	16
Figure 2 – VPC file schema	19
Figure 3 – VPC file schema diagram format	20
Figure B.1 – IACS patch management workflow	32
Figure B.2 – Planning an IACS patch management process.....	41
Figure B.3 – Sample responsibilities chart.....	45
Figure B.4 – Patch monitoring and evaluation process.....	48
Figure B.5 – A patch testing process.....	50
Figure B.6 – A patch deployment and installation process	55
Table 1 – Patch lifecycle states	15
Table 2 – VPC XSD PatchData file elements	20
Table 3 – VPC XSD PatchVendor file elements	20
Table 4 – VPC XSD Patch file elements	21
Table 5 – VPC XSD VendorProduct file elements	23
Table A.1 – CodeType optional attributes.....	28
Table A.2 – DateTimeType optional attributes	28
Table A.3 – IdentifierType optional attributes	29
Table A.4 – IndicatorType optional attributes	29
Table A.5 – TextType optional attributes	29
Table B.1 – Sample product supplier profile	36
Table B.2 – Communication capabilities	39
Table B.3 – Sample software categorization.....	39
Table B.4 – Responsibility assignment definitions	44
Table B.5 – Sample severity based patch management timeframes	50

This page intentionally left blank.

Document ID: ISA-TR62443-2-3-2015

FOREWORD

This technical report is part of a multipart standard that addresses the issue of security for industrial automation and control systems (IACS). It has been developed by Working Group 06 of the ISA99 committee.

This technical report describes a format for the exchange of information about the status of patches and their applicability, and providing guidance on planning and building a patch management program within asset owner and IACS product supplier organizations.

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.

NOTE The format of this technical report follows the ISO/IEC requirements discussed in ISO/IEC Directives, Appendix H of Part 2 [13]¹. The ISO/IEC Directives specify the format of this technical report as well as the use of terms like “shall”, “should” and “may”. The use of those terms for the requirements specified in this technical report use the conventions discussed in the ISO/IEC Directives, Appendix H.

¹ Numbers in brackets indicate references in the Bibliography.

1 Scope

ISA-TR62443-2-3 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 ISA-62443 series.

2 Normative references

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

ANSI/ISA-62443- 1- 1 (99.00.01) – *Security for industrial automation and control systems Part 1-1: Terminology, concepts and models* [1]

ISA- TR62443- 1- 2 – *Security for industrial automation and control systems, Part 1-2: Master glossary of terms and abbreviations* [2]

ANSI/ISA-62443- 2- 1 (99.02.01) – *Security for industrial automation and control systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* [1]

3 Terms, definitions, abbreviated terms, acronyms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the normative references specified in clause 2 apply, in addition to the following.

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 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 Electrotechnical 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 for 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 ISA-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.

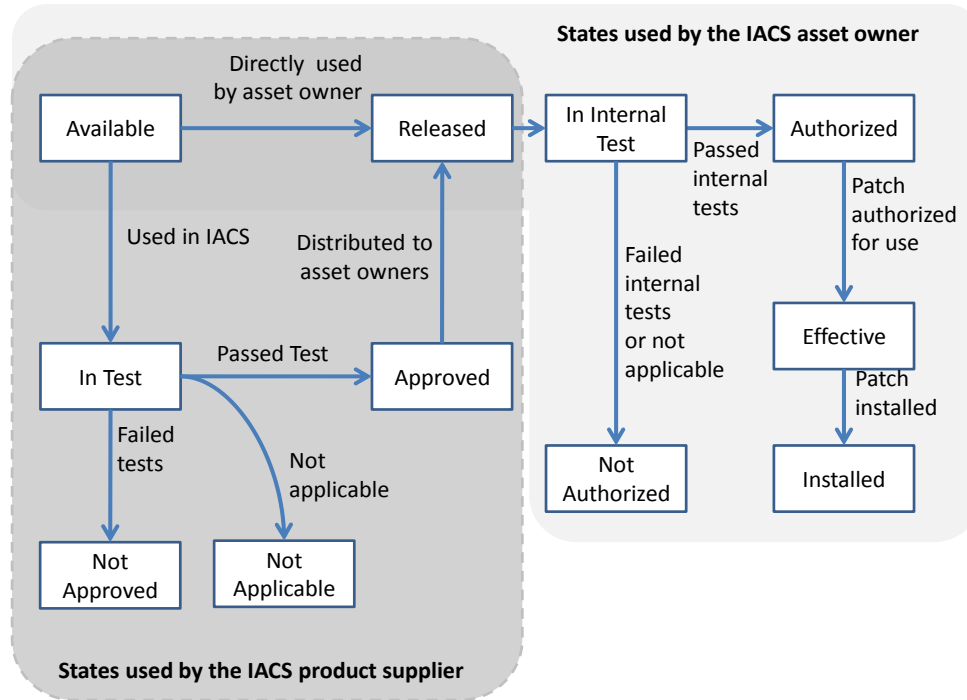


Figure 1 – Patch state model

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:

- 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;
- establish and maintain an accurate record of the currently installed versions for each device, called the 'installed' version;
- determine on a regular schedule what upgrades and updates are available for each device, called the 'latest' version;
- 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;
- 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';
- 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;
- h) identify a planned interval for installation of patches, such as: when patches are available, or at least on an annual basis; and
- i) install patches and/or implement compensating countermeasures to mitigate security vulnerabilities that exist in the IACS.

Additional guidance that can be used to achieve these requirements is provided in Annex B.

6 Recommended requirements for IACS product supplier

Security of the IACS on a running facility is very important and proactive measures are needed to reduce the probability of the plant being compromised, therefore determining which patches apply to, and should be tested on, a product is a critical responsibility of the IACS product supplier.

IACS product suppliers should:

- a) provide documentation describing the software patching policy for the products and systems they supply;
- b) qualify in terms of applicability and compatibility, all patches, by analyzing and verifying the patches, including patches that are released by the supplier of the OS that is used, and all suppliers of third-party software, that may be used by the IACS products;
- c) provide a list of all patches and their approval status, including the information and data in the format described in clause 7 and Annex A;
- d) inform the asset owners, and update the list of patches described in: clause 6 b) above, clause 7, and Annex A periodically, and ideally within 30 days after a patch is released by the supplier of the OS or third-party software;
- e) provide adequate warning (at least two years in advance) about the components reaching 'end of life,' or for which cyber security patches will no longer be made available; and
- f) provide information to IACS users regarding the policy of supporting IACS products, including security updates.

Additional guidance that can be used to achieve these requirements is provided in Annex C.

7 Exchanging patch information

7.1 Introduction

Patch information is required because a complete IACS is usually based on commercial OSs, commercial application systems, such as distributed control systems (DCSs), historian and manufacturing execution systems (MESs) and application specific software programs using commercial IT tools, such as databases and libraries. All of these software elements require periodic updates to correct newly discovered errors or to correct newly discovered security deficiencies.

Implementing a system to manage patches requires knowledge of: what patches are available, if the patches are applicable to installed systems, if the patches have been tested against the installed products, and if the IACS product supplier recommends that the patches should be installed.

Determining the compatibility of patches can be a complex task. IACS product suppliers perform tests of their products against OS and library patches in order to determine if the patch should be used with their automation products. Because failures in automation products due to incompatibility with patches may result in the loss of life, property or product, there is often a requirement that all

related automation products have been tested with the patch prior to installation of the patch in a production system.

IACS users often have various IACS product supplier systems in their facilities and managing the patch compatibility information from multiple IACS product suppliers is difficult because the patch information is usually available in each IACS product supplier's specific format. This clause defines a standard format for the exchange of patch information necessary to identify a product, patch and status of the patch. The exchanged information includes:

- g) an identification of the IACS product supplier providing the product;
- h) an identification of the IACS supplier's product and version;
- i) an identification of the product supplier providing the patch, such as the company providing the OS;
- j) an identification of the patch supplier's product, such as the OS version;
- k) the patch supplier's identification of the patch;
- l) an indication if the patch is applicable to the IACS product;
- m) an indication of status of testing of the patch against the IACS product; and
- n) an indication of the results of testing of the patch against the IACS product.

This information allows end users to make informed decisions before they decide to install the patch. The exchange information defines if a specific patch from an IACS system supplier, an OS supplier or a third party software product supplier has been tested against a specific version of the IACS software, with an indication that the tested patch works with that version of the IACS software.

7.2 Patch information exchange format

The format for the minimal patch compatibility information is based on eXtensible Markup Language (XML) technology and is defined using an XML schema definition (XSD) file. The patch information file is identified as vendor patch compatibility (VPC).

7.3 Patch compatibility information filename convention

The filename of a VPC file should be defined according to the following syntax:

```
<filename> = <vendor_name> "_patch_compatibility_" <date> "_" <number> ".xml"
```

where

<vendor_name>	the generally recognized short name of the IACS company
<date>	the date the compatibility file was released by the IACS product supplier (formatted according to ISO 8601 [18])
<number>	a number identifying the file if the IACS product supplier releases more than one file on a single date.
EXAMPLE 1	SomeCompany_patch_compatibility_2010-01-08_01.xml
EXAMPLE 2	OtherCompany_patch_compatibility_2010-01-08_02.xml

Note: Since the recipient will use the contents of this file to manage whether a patch is to be applied, there is a need to ensure that its contents are authentic. The means by which source authentication and integrity protection of this file is attained is outside the scope of this Technical Report.

7.4 VPC file schema

The VPC format allows for the exchange of patch information about multiple patches and IACS product supplier products in the same VPC exchange file.

Figure 2 illustrates the VPC file schema definition.

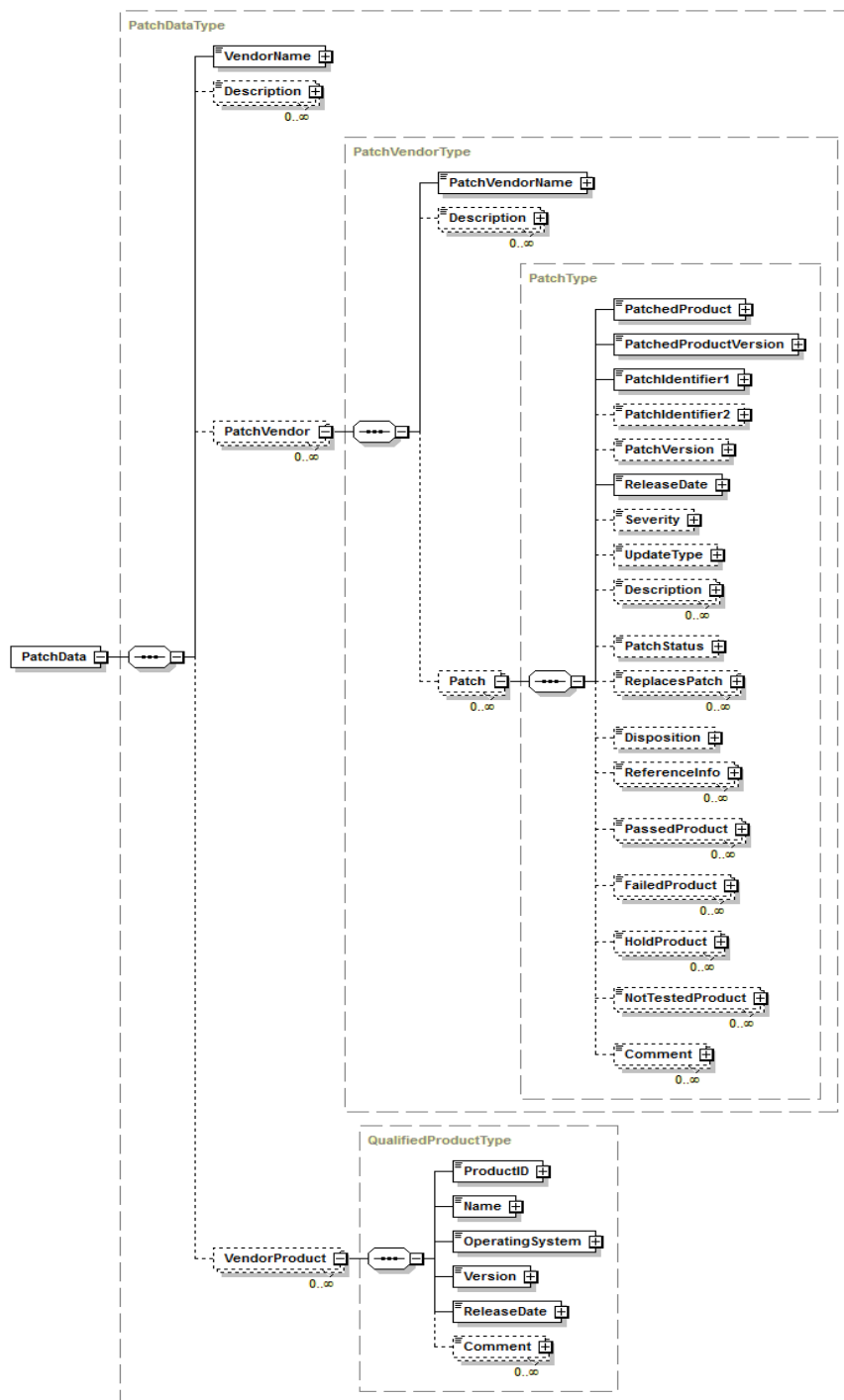


Figure 2 – VPC file schema

Figure 3 illustrates the VPC file schema diagram format.

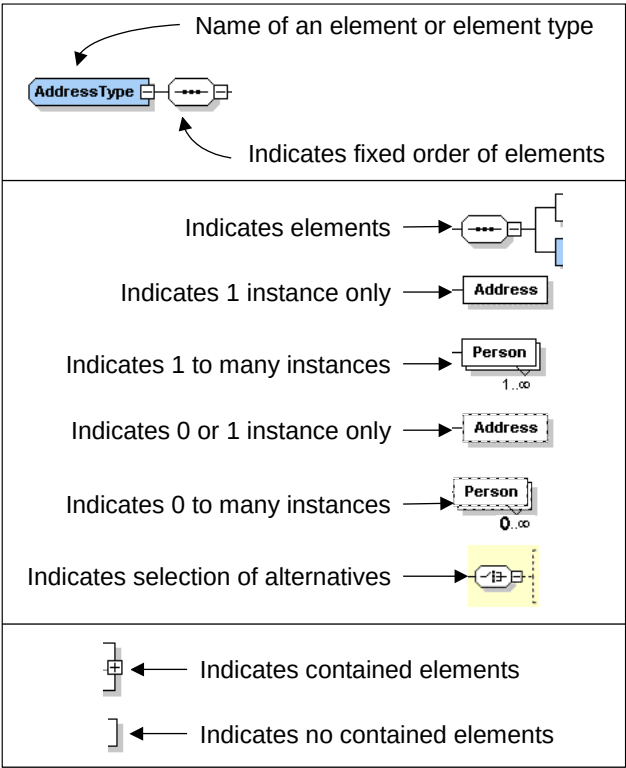


Figure 3 – VPC file schema diagram format

7.5 VPC file element definitions

Table 2 through Table 5 define each element in the VPC XSD file. Only the enumerations, defined in the “Definition” column, for the applicability, test result and test status should be used in the exchange file.

Table 2 – VPC XSD PatchData file elements

Element	Type	Definition
VendorName	IdentifierType	A required string containing the name of the vendor that is providing the patch information. EXAMPLES: “DCS vendor”, “MES vendor”
Description	TextType	An optional string containing a description of the vendor information.

Table 3 – VPC XSD PatchVendor file elements

Element	Type	Definition
PatchVendorName	IdentifierType	A required string containing the name of the vendor that is providing the patch. EXAMPLES: “OS Vendor”, “DCS Vendor”, “Protocol Stack Vendor”
Description	TextType	An optional string containing a description of the vendor.

Table 4 – VPC XSD Patch file elements

Element	Type	Definition
PatchedProduct	IdentifierType	A required string containing the patch product supplier's name of the product that the patch is targeting. EXAMPLES: "SQL Server", "Microsoft Windows"
PatchedProductVersion	IdentifierType	A required string containing the version of the product the patch is for. EXAMPLES: "Service Pack 2", "7.15", "A", "R23.9"
PatchIdentifier1	IdentifierType	A required string containing the patch product supplier defined primary identification of the patch. EXAMPLE: "KB1234567"
PatchIdentifier2	IdentifierType	An optional string containing a patch product supplier defined secondary identification of the patch.
PatchVersion	IdentifierType	An optional string containing the version number of the patch. EXAMPLES: "1", "1.0", "1.2" NOTE This may be needed if multiple versions of the patch are released due to errors in the previous patch version.
ReleaseDate	DateTimeType	A required string containing the released date of the patch. EXAMPLE: "2014-01-17" NOTE: Format this string according to ISO 8601 [18].
Severity	CodeType	An optional string containing the severity of the patch. The value should be one of the items in the following enumeration: • Critical – The patch should be installed. It corrects a vulnerability whose exploitation could allow code execution without user interaction. These scenarios include for example: self-propagating malware (such as network worms) and unavoidable common use scenarios where code execution occurs without warnings or prompts. • Important – The patch should be installed. The patch corrects a vulnerability whose exploitation could result in compromise of the confidentiality, integrity or availability of data, or of the integrity or availability of processing resources, but which requires a user action. • Optional – The patch may be installed. The patch corrects a vulnerability that requires unique or uncommon user actions.
UpdateType	CodeType	A required string value containing the type of patch. The value should be one of the items in the following enumeration: • Non_Security – This update is related to a non-security related issue and updates a known issue that is not related to security. • Security – This update is related to a security issue and repairs a known security problem.
Description	TextType	An optional string value that contains a description of the update and/or patch.