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)