ICS 25.040
CCS N10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 42445-2023

Industrial automation and control systems security - Patch management in the IACS environment

工业自动化和控制系统安全 IACS环境下的补丁管理

Issued on: March 17, 2023 **Implemented on: October 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents" drafting: This document is equivalent to IEC TR62443-2-3:2015 "Industrial Automation and Control System Safety Part 2-3: IACS environment Patch Management for : The file type is adjusted from the IEC technical report to the national standard of our country: The following minimal editorial changes have been made to this document:

---In order to coordinate with the existing standard, the name of the standard is changed to "Patch management in the context of industrial automation and control system security IACS reason": This document is proposed by China Machinery Industry Federation: This document is under the jurisdiction of the National Industrial Process Measurement Control and Automation Standardization Technical Committee (SAC/TC124): This document is drafted by: Dongfang Electric Group Science and Technology Research Institute Co:, Ltd:, Mechanical Industry Instrumentation Comprehensive Technical Economic Research Institute, General Electric Power Planning Institute Co:, Ltd:, Schneider Electric (China) Co:, Ltd:, Siemens (China) Co:, Ltd:, Beijing Sifang Relay Automation Co:, Ltd:, Beijing Guoneng Zhishen Control Technology Co:, Ltd:, North China Electric Power University, Chongqing Xin'an Network Security Level Evaluation Co:, Ltd:, State Power Investment Wuhu Power Generation Co:, Ltd:, PetroChina Tarim Oilfield Branch, Chongqing University of Posts and Telecommunications, Southwest University, Shenyang Institute of Automation, Chinese Academy of Sciences, Huazhong University of Science and Technology, the 30th Research Institute of China Electronics Technology Group Corporation, Shanghai Industrial Automation Instrument Research Institute Co:, Ltd:, the Fifth Electronic Research Institute of the Ministry of Industry and Information Technology, National Industrial Information Security Development Research Center, Rockway Seoul (Shanghai) Co:, Ltd:, Shanghai Electrical Apparatus Research Institute (Group) Co:, Ltd:, Hollysys Technology Group Co:, Ltd:, Ministry of Industry and Information Technology Computer and Microelectronics Development Research Center (China Software Evaluation Center), Xi'an Space Radio Technology Research Institute: The main drafters of this document: Yuan Xiaoshu, Wang

Yumin, Shang Yujia, Zhang Jinbin, Wang Yong, Yan Tao, Du Zhenhua, Zhu Jingling, Gong Gangjun, Zhou Yanhui, Cheng Jiarong, Yang Qizhan, Wei Min, Liu Feng, Zhao Jianming, Zhou Chunjie, Lan Kun, Liu Huifang, Liu Jie, Zhao Ran, Gao Jingmei, Ren Yue, Liu Ying, Guo Yongzhen, Wang Aipeng, Sang Zi, Wang Ying, Zhai Wanbo, Yang Xiaoqian, Zhang Yan, Xu Jin, Wang Jia, Hu Bo, Yang Chao:

IEC 62443 is a series of international standards applied to the safety of industrial automation and control systems: At present, my country has adopted this series of standards to develop Published GB/T 33007-2016 "Industrial Communication Network Network and System Security Establishing Industrial Automation and Control System Security Procedures" (IEC 62443-2-1:2010, IDT), GB/T 35673-2017 "Industrial Communication Network Network and System Security System Security Requirements and Security Level" (IEC 62443-3-3:2013, IDT), GB/T 40211-2021 "Industrial Communication Network Network and System Security Terms, Overview and Models Type" (IEC 62443-1-1:2009, IDT), GB/T 40218-2021 "Industrial Communication Network Network and System Security Industrial Automation and Control System Information Security Technology" (IEC TR62443-3-1:2009, IDT), GB/T 40682-2021 "Industrial Automation and Control System Network Cybersecurity Part 2-4: Security Program Requirements for IACS Service Providers (IEC 62443-2-4:2015, IDT) and this document, these standards The quasi-cooperatively constitute a series of national standards applied to the safety of industrial automation and control systems: Cybersecurity is an increasingly important topic in modern organizations: Many information technology (IT) and business organizations have sustained Focus on cyber security and comply with ISO /IEC 27001 and ISO /IEC 27002 to establish an Information Security Management System (ISMS): These management systems provide organizations with a means to protect their assets from cyber-attacks Methods: Currently, industrial automation and control system (IACS) suppliers and owners use in their daily activities commercial off-the-shelf (COTS) technology: As the COTS system is more widely known and used, its application in IACS also improves the quality of IACS equipment: Chances of being attacked by a network: New research on IACS security has also found vulnerabilities in many devices: Successful Attacks on Industrial Systems May cause health, safety and environmental (HSE) consequences: Organizations may attempt to address IACS security with commercial cybersecurity policies without understanding the consequences: Although the Many solutions can be applied to IACS, but they need to be applied in the correct way to eliminate unintended consequences: This document addresses the issue of patch management for IACS cybersecurity: Patch management is part of an overall network security strategy, it Increase network security by installing patches, which are also known as software updates, software upgrades, firmware upgrades, service packs, patches, Basic Input Output System (BIOS) updates and other digital electronic updates that address defects, operability, reliability, and cybersecurity vulnerabilities Program update: This document addresses the many issues and industries that asset owners and IACS product vendors have with regard to IACS patch management

Concerns, and the impact of poor patch management on the reliability and/or operability of the IACS: Industrial Automation and Control System Security Patch Management in IACS Environment

1 Scope

GB/T 42445-2023 deals with patching in industrial control systems, where the ordinary IT answer does not apply. In an office, patches are installed promptly and a reboot is an inconvenience. In a plant, the same patch may invalidate a supplier's validation of the system, and the reboot is a shutdown of a process that cannot simply be stopped - so control systems run for years on software with known vulnerabilities, not through negligence but because the risk of patching can genuinely exceed the risk of not patching. What makes that decision defensible is a documented process rather than an ad hoc judgement, and the information the asset owner needs to make it comes from the supplier, who is the only party who knows whether a patch has been tested against their product. This document describes the requirements for asset owners establishing and maintaining an IACS patch management plan and the corresponding requirements for IACS product suppliers, and recommends a defined format in which suppliers communicate patch information to asset owners. Under ICS 25.040 and CCS N10, it is written for plant operators, control system integrators and automation vendors.

This document describes the requirements for asset owners who have established and are maintaining an industrial automation and control system (IACS) patch management plan and IACS product supplier requirements: This document recommends a well-defined format for asset owners and IACS product vendors to distribute security patch information, and defines Some related activities such as the development of patch information by IACS product suppliers and the deployment and installation of patches by asset owners: determined The defined exchange format and activities are primarily used for security-related patches: Interchange formats and activities are defined for security-related patches, but can also be Can be applied to non-security related patches or updates: This document does not distinguish between operating system (OS), application, or device patches, nor does it differentiate between providing infrastructure components or IACS applications The product vendor of the program, but instead provides guidance for all patches applicable to IACS: In addition, patch types can be used to address defects, Reliability issues, operability issues, or security vulnerabilities:

Note 1: Discovering and disclosing security vulnerabilities affecting IACS is a general issue outside the scope of this document, and this document does not provide ethical standards and treatment in this regard: methodological guidance: Unless otherwise specified, "security" in this document refers to "information security": NOTE 2: This document does not provide guidance on how to mitigate a vulnerability from discovery to creation of a patch for the vulnerability: Multiple Compensation Measures to Mitigate Security Risks The

implementation is part of the IACS Safety Management System (IACS-SMS): If you need guidance on this content, please refer to B:4:5, Appendix B of this document: B:4:6 and B:8:5 and other parts of the IEC 62443 series of standards:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document: IEC TS62443-1-

1 Industrial communication network network and system security Part 1-1: Terms, concepts and models (Industrial els)

GB/T 40211-2021 Industrial Communication Network Network and System Security Terms, Concepts and Models (IEC TS62443-1-1:2009, IDT) IEC 62443-2-

1 Industrial communication network network and system security Part 2-1: Establishing industrial automation and control system security

GB/T 33007 industrial communication network network and system security establishes security procedures for industrial automation and control systems (

IEC 62443-2-1: 2010, IDT)

3 Terms, Definitions, Abbreviations and Abbreviations 3: