ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 42457—2023/IEC 62443-4-1:2018

工业自动化和控制系统信息安全 产品安全开发生命周期要求

**Security for industrial automation and control systems—
Secure product development lifecycle requirements**

（IEC 62443-4-1:2018,Security for industrial automation and control systems—
Part 4-1:Secure product development lifecycle requirements,IDT）

2023-03-17 发布　　2023-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件等同采用IEC 62443-4-1:2018《工业自动化和控制系统信息安全　第4-1部分:产品安全开发生命周期要求》。

本文件做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《工业自动化和控制系统信息安全　产品安全开发生命周期要求》。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位:北京威努特技术有限公司、机械工业仪器仪表综合技术经济研究所、电力规划总院有限公司、施耐德电气(中国)有限公司、西门子(中国)有限公司、北京四方继保自动化股份有限公司、北京国能智深控制技术有限公司、华北电力大学、重庆信安网络安全等级测评有限公司、重庆邮电大学、西南大学、华中科技大学、中国电子科技集团公司第三十研究所、北京广利核系统工程有限公司、辽宁大唐国际新能源有限公司、国网辽宁省电力有限公司检修分公司、中车株洲电力机车研究所有限公司、北京西南交大盛阳科技股份有限公司、交控科技股份有限公司、杭州电子科技大学、中国第一汽车集团有限公司、西安热工研究院有限公司、上海工业自动化仪表研究院有限公司、工业和信息化部电子第五研究所、国家工业信息安全发展研究中心、罗克韦尔(上海)有限公司、上海电器科学研究所(集团)有限公司、和利时科技集团有限公司、西安空间无线电技术研究所。

本文件主要起草人:黄敏、王玉敏、尚羽佳、王春霞、张晋宾、杨建平、龙国东、张东旗、王勇、闫韬、杜振华、朱镜灵、龚钢军、周彦晖、魏旻、刘枫、周纯杰、兰昆、莫昌瑜、赵志鹏、汪心明、曾阳、王锦、唐军、邹智荣、杨滨茂、杨雪涛、杨清雯、徐向华、王然、李雷、张子佳、杨渊、刘慧芳、刘杰、赵冉、高镜媚、任悦、刘盈、王爱鹏、王英、张焱、徐进、王佳、胡博、杨超。

引　言

IEC 62443 是应用于工业自动化和控制系统安全的系列国际标准。目前我国已采用该系列标准发布了 GB/T 33007—2016《工业通信网络　网络和系统安全　建立工业自动化和控制系统安全程序》(IEC 62443-2-1:2010,IDT)、GB/T 35673—2017《工业通信网络　网络和系统安全　系统安全要求和安全等级》(IEC 62443-3-3:2013,IDT)、GB/T 40211—2021《工业通信网络　网络和系统安全　术语、概述和模型》(IEC 62443-1-1:2009,IDT)、GB/T 40218—2021《工业通信网络　网络和系统安全　工业自动化和控制系统信息安全技术》(IEC/TR 62443-3-1:2009,IDT)、GB/T 40682—2021《工业自动化和控制系统网络安全　第 2-4 部分:IACS 服务提供商的安全程序要求》(IEC 62443-2-4:2015,IDT)和本文件。这些标准共同构成应用于工业自动化和控制系统安全的系列国家标准。

本文件是解决工业自动化和控制系统(IACS)安全问题的系列标准的一部分。本文件介绍工业自动化和控制系统环境中使用的产品的信息安全相关开发生命周期要求,并就如何满足每个要素描述的要求提供指导。

本文件大部分来自 ISA 安全合规研究所(ISCI)的安全开发生命周期评估(SDLA)认证要求[26]。SDLA 程序基于以下来源:

——ISO/IEC 15408-3(通用标准)[18];

——开放式 Web 应用程序安全项目(OWASP),全面轻量级应用程序安全性过程(CLASP)[36];

——迈克尔·霍华德和史蒂夫·利普纳[43]的安全开发生命周期;

——IEC 61508 电气/电子/可编程电子的安全相关系统的功能安全[24];和

——RCTA DO-178B 机载系统和设备认证中的软件考虑[28]。

因此,所有这些都可以被认为是本文件的来源。

本文件包含的信息安全要求,可以作为任何自动化和控制产品的开发人员考虑信息安全问题时的指导。

图 1 说明了 IEC 62443 不同部分之间的关系。

图 1　IEC 62443 系列各部分

图 2 说明了已开发的产品如何与 IEC 62443-2-4 中定义的维护和集成能力以及资产所有者的操作相关联。产品供应商使用符合本文件的过程开发产品。这些产品可能是单个组件,例如嵌入式控制器,或作为系统或子系统一起工作的一组组件。系统集成商使用符合 IEC 62443-2-4 的过程将产品集成到一个自动化解决方案中。自动化解决方案随后被部署在特定的现场,并成为 IACS 的一部分。其中一些功能参考了 IEC 62443-3-3 [10]中定义的安全措施,服务提供商确保在自动化解决方案(作为产品特性或补偿机制)中支持这些安全措施。本文件仅涉及用于开发产品的过程;它不涉及自动化解决方案或 IACS 的设计、部署或操作。

在图 2 中,自动化解决方案包含一个或多个子系统和可选的支持组件,如先进控制组件。虚线框表示这些组件是“可选的”。

自动化解决方案通常包含一个产品,但不限于此。在一些行业中,可能存在分层次的产品结构。一般而言,自动化解决方案是一套不依赖于产品包装的硬件和软件,用于控制资产所有者定义的物理过程(例如连续过程或制造过程)。

如果服务提供商提供自动化解决方案中使用的产品,则服务提供商在图 2 中履行产品供应商的职责。

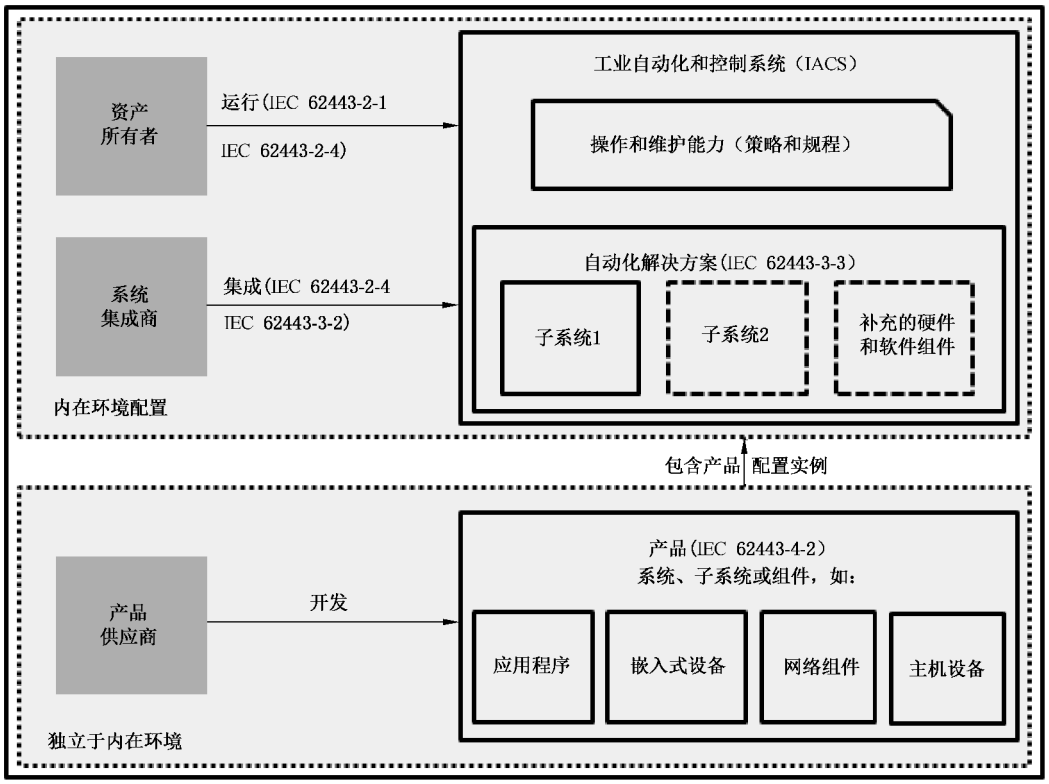

图 2 产品生命周期示例

工业自动化和控制系统信息安全 产品安全开发生命周期要求

1 范围

本文件规定了用于工业自动化和控制系统产品的信息安全开发的过程要求。它定义了一个用于开发和维护安全的产品的安全开发生命周期(SDL)。这个生命周期包括安全需求定义、安全设计、安全实现(包括编码准则)、验证和确认、缺陷管理、补丁管理和产品退役。这些需求可以应用于新的或现有的过程,以开发、维护和淘汰新的或现有的产品硬件、软件或固件。这些需求适用于产品的开发人员和维护人员,但不适用于产品的集成人员或用户。本文件的需求摘要清单见附录B。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

IEC 62443-2-4 工业自动化和控制系统信息安全 第2-4部分:IACS服务提供商信息安全程序需求(Security for industrial automation and control systems—Part 2-4:Security program requirements for IACS service provides

注:GB/T 40682—2021 工业自动化和控制系统安全 IACS服务提供商的安全程序要求(IEC 62443-2-4:2015,IDT)

IEC TR 62443-1-2 工业自动化和控制系统安全 第1-2部分:术语和缩略语的基本词汇(Security for industrial automation and control systems—Part 1-2:Master glossary of terms and abbreviations)

3 术语、定义、缩略语和惯例

ISO和IEC的术语数据库可以通过下述网址访问:

——IEC:http://www.electropedia.org/;

——ISO:http://www.iso.org/obp。

3.1 术语和定义

IEC TR 62443-1-2界定的以及下列术语和定义适用于本文件。

3.1.1

滥用用例 abuse case

用于执行负面操作的测试用例。

注:滥用用例测试通常是基于威胁模型的模拟攻击。滥用用例是一个系统与一个或多个行动者之间完全相互作用的一种类型,其中交互的结果是故意地对系统、行为者之一或系统中的一个利益相关者有害。

3.1.2

访问控制<保护> access control <protection>

保护系统资源免受未经授权的访问。

3.1.3

访问控制<过程> access control<process>

根据安全策略对系统资源的使用进行管理的过程,并且只有符合该策略的授权用户才被允许。