ICS 25.040.40
N 10

中华人民共和国国家标准

GB/T 33007—2016/IEC 62443-2-1:2010

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

Industrial communication networks—Network and system security—Establishing an industrial automation and control system security program

(IEC 62443-2-1:2010,Industrial communication networks—Network and system security—Part 2-1:Establishing an industrial automation and control system security program,IDT)

2016-10-13 发布　　2017-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分:标准的结构和编写》和 GB/T 20000.2—2009《标准化工作指南　第 2 部分:采用国际标准》给出的规则起草。

本标准使用翻译法等同采用 IEC 62443-2-1:2010《工业通信网络　网络和系统安全　第 2-1 部分:建立工业自动化和控制系统安全程序》(英文版)。其技术内容、文本结构以及表达形式与 IEC 62443-2-1:2010 完全等同。

为了方便使用,本标准作了下列编辑性修改:

——删除了原文中的前言;

——将介绍部分的内容作为本标准的引言;

——如果不做说明,文中的“安全”都是指“网络安全”。

本标准由中国机械工业联合会提出。

本标准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)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、中国电力科学研究院、中国核电工程有限公司、上海自动化仪表股份有限公司、北京交通大学、东土科技股份有限公司、清华大学、西门子(中国)有限公司、浙江大学、西南大学、重庆邮电大学、施耐德电气(中国)有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化(中国)有限公司、中国仪器仪表学会、北京和利时系统工程有限公司、工业和信息化部电子第五研究所、中国科学院沈阳自动化研究所、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、启明星辰、中国电子科技集团公司第三十研究所、深圳万讯自控股份有限公司、中标软件有限公司、横河电机(中国)有限公司北京研发中心。

本标准主要起草人:王玉敏、范科峰、梁潇、冯冬芹、王亦君、华镕、陈小淙、张建军、薛百华、许斌、高昆仑、王雪、刘枫、王浩、夏德海、周纯杰、张莉、王弢、刘杰、孙昕、徐皑冬、朱毅明、孙静、胡伯良、梅恪、刘安正、田雨聪、方亮、马欣欣、王勇、杜佳琳、陈日罡、李锐、刘利民、孔勇、刘文龙、李琳、黄敏、朱镜灵、张智、何佳、张建勋、孟雅辉、兰昆、成继勋、丁露、陈小枫、杨应良、杨磊。

引　言

0.1　概述

网络安全是一个在现代组织中日益重要的话题。多年来，许多涉及信息技术和业务的组织一直在关注网络安全，并且按照 ISO 和 IEC 标准已经建立了行之有效的网络安全管理系统（CSMS）（见 ISO/IEC 17799[23]1 和 ISO/IEC 27001 [24]），这些管理系统为组织机构提供了一种行之有效的方法来保护其资产免受网络攻击。

工业自动化控制系统（IACS）组织已经开始在日常流程中使用为业务系统开发的商用现成技术（COTS），这使得 IACS 设备受到网络攻击的可能性随之增加。由于多方面的原因，在对抗网络攻击方面这些系统通常不如专为 IACS 环境设计的系统那么健壮。这些弱点可能导致健康、安全和环境方面（HSE）的后果。

在没有理解这些后果的情况下，组织可能会试图使用已有的信息技术和业务安全方案来解决 IACS 的安全问题。尽管许多解决方案可以应用到 IACS，但是需要采取正确的方式以消除不良后果。

0.2　IACS 的网络安全管理系统

管理系统通常提供管理系统中应包括什么的指导，但不提供关于如何去开发管理体系的指导。本标准为阐述 IACS 的 CSMS 包含的元素，同时也提供如何为 IACS 开发 CSMS 的指导。

面对一个具有挑战性的问题时，一个非常常见的工程方法是将问题分解成更小的子问题，按照分治方式解决每个子问题。这是解决 IACS 网络安全风险的合理途径。然而，在解决网络安全方面常犯的错误是，试图用一套系统一次解决所有的网络安全问题。网络安全是一个更大的挑战，需要考虑整个 IACS 以及环绕和利用 IACS 的政策、规程、实践和人员。实施这样大范围的管理系统可能需要组织内部的文化变革。

在整个组织范围的基础上解决网络安全是一项艰巨的任务。但是对于安全来说，没有现成的解决方案。这很容易理解，因为没有适合所有情况的安全实践。理论上绝对的安全也许能实现，但是这很可能是不可取的，因为要达到这样近乎完美的状态必然要损失实用性。安全实际上是一个风险和成本的平衡。所有的情况有所不同。在某些情况下，风险可能与 HSE 因素有关而不是单纯的经济影响。风险可能带来不可恢复的后果而不是暂时性的财务挫折。因此一个强制性安全实践的解决方案集要么过于严格，费用昂贵无法遵循，要么不足以应对风险。

0.3　本标准与 ISO/IEC 17799 和 ISO/IEC 27001 的关系

ISO/IEC 17799[23]和 ISO/IEC 27001[24]是描述业务/信息技术系统的网络安全管理系统的优秀标准。这些标准中的内容大部分也适用于 IACS。该标准强调 IACS 网络安全实践的管理与业务/信息技术系统网络安全的管理之间需保持一致。这些程序的一致性可以节约开销。该标准鼓励用户阅读 ISO/IEC 17799 和 ISO/IEC 27001 获得额外的支持信息。本标准基于这些 ISO/IEC 标准制定，强调 IACS 和一般业务/信息技术系统的重要差异。本标准引入一个重要的概念，IACS 的网络安全风险可能带来 HSE 影响，应与其他现有风险管理实践结合来应对这些风险。

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

1　范围

本标准规定了如何在工业自动化和控制系统(IACS)中建立网络安全管理系统,并且提供了如何开发这些元素的指南。本标准与 IEC 62443-1-1 中描述的 IACS 相比,其定义和范围更广泛。

本标准中描述的 CSMS 中的元素主要是政策、过程、规程以及与人员相关的内容,描述了在组织范围内最终的 CSMS 将要包括或应当包括哪些内容。

注 1: IEC 62443 系列标准和参考文献中的其他文档讨论了有关安全的更细致的具体的技术和方案。

怎样开发 CSMS 的指导是一个例子,它代表了作者的观点:一个组织可以去开发元素,但它未必能在所有的情况下应用。为了给组织开发一套功能完整的 CSMS,本标准的用户必须仔细地阅读需求和适当地使用指导。本标准所讨论的策略和规程应该根据组织需要进行剪裁。

注 2: 可能有这种情况,如企业已经有自己的 CSMS 并增加了 IACS,或完全没有正式建立 CSMS。作者不能为 IACS 建立 CSMS 的组织预测所有情况,因此本标准不试图为所有情况提供解决方案。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 62443-1-1　工业通信网络　网络和系统网络安全　第 1-1 部分:术语、概念和模型(Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models)

3　术语、定义、缩略语和约定

3.1　术语和定义

IEC 62443-1-1 界定的以及下列术语和定义适用于本文件。

3.1.1

访问账户　access account

允许用户访问固定设备的特定数据或功能集的访问控制功能。

注:账户经常会和用户的身份(ID)和密码相关。这些用户 ID 和密码可以是个人的或者小组共用的,例如执行同样的工作任务的控制室工作小组。

3.1.2

行政管理实践　administrative practices

已定义好的和文档化的实践/规程,供员工能一直遵守。

注:通常用于企业内部的雇员。在 IACS 环境下,常与 HSE 有关。

3.1.3

资产　asset

组织所拥有或保管的物理或逻辑对象,该对象对组织具有潜在或实际的价值

[IEC 62443-1-1,3.2.6]