ICS 25.040
N 10

中华人民共和国国家标准

GB/T 40211—2021/IEC/TS 62443-1-1:2009

工业通信网络　网络和系统安全 术语、概念和模型

Industrial communication networks—Network and system security—Terminology, concepts and models

(IEC/TS 62443-1-1:2009, Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models, IDT)

2021-05-21 发布　　2021-12-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC/TS 62443-1-1:2009《工业通信网络　网络和系统安全　第 1-1 部分:术语、概念和模型》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下:

——GB/T 18336.1—2015　信息技术　安全技术　信息技术安全评估准则　第 1 部分:简介和一般模型(ISO/IEC 15408-1:2009,IDT)

——GB/T 20720.1—2019　企业控制系统集成　第 1 部分:模型和术语(IEC 62264-1:2013,IDT)

本标准做了下列编辑性修改:

——修改了标准名称。

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)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、电力规划总院有限公司、中国核电工程有限公司、和利时科技集团有限公司、北京市自来水集团有限责任公司、浙江大学、华中科技大学、重庆邮电大学、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、西门子(中国)有限公司、施耐德电气(中国)有限公司、罗克韦尔自动化(中国)有限公司、中国科学院沈阳自动化研究所、北京启明星辰信息安全技术有限公司、北京国电智深控制技术有限公司、深圳万讯自控股份有限公司、中国电子科技集团公司第三十研究所、工业和信息化部电子第五研究所、西南大学、中国东方电气集团有限公司、北京四方继保自动化股份有限公司、国家工业信息安全发展研究中心、北京市轨道交通设计研究院有限公司、上海自动化仪表有限公司、重庆信安网络安全等级测评有限公司、公安部第三研究所、中国网络安全审查技术与认证中心、北京网御星云信息技术有限公司。

本标准主要起草人:王玉敏、梅恪、张晋宾、王彦君、华镕、孙静、张晨艳、冯冬芹、周纯杰、李锐、陈小淙、朱镜灵、魏旻、王浩、王弢、刘杰、成继勋、赵军凯、兰昆、尚文利、张为群、刘枫、刘志祥、袁晓舒、尚羽佳、郭永振、杜振华、张哲宇、肖衍、陆妹、丁长富、肖煦媛、高镜媚、闫韬、袁静、任卫红、甘杰夫、宋文刚。

引　言

本标准的主题是工业自动化和控制系统的安全。为了适用于不同的应用(如:行业类型),每条术语都进行宽泛的解读。

术语“工业自动化和控制系统”(IACS),包括了用于制造业和流程工业的控制系统、楼宇控制系统、地理上分散的操作诸如公共设施(例如:电力、天然气和供水)、管道和石油生产及分配设施、其他工业和应用如交通运输网络,那些使用自动化的或远程被控制或监视的资产。

本标准中的术语“安全”是指防止非法或有害的渗透,有意或无意的妨碍正常的和预期的运行、或不适宜的访问 IACS 的保密信息。本标准特别关注的计算机安全,包括计算机、网络、操作系统、应用和系统的其他可编程组件。

本标准的读者包括所有的 IACS 用户(包括设施运行、维护、施工和用户组织公司的一部分)、生产者、供应商、政府组织在内的、被影响的、控制系统计算机安全、控制系统实践者和安全实践者。因为信息技术(IT)和操作人员、工程人员以及制造商组织之间的互相理解和合作对于任何信息倡议取得全面成功都是非常重要的,本标准也是那些负责 IACS 和企业网络集成人员的参考资料。

本标准主要涉及以下几个典型的问题:

a) IACS 安全应用的范围是什么?

b) 如何使用统一术语定义安全系统的需要和要求?

c) 以什么基本概念为基础以便用于活动、系统属性和行动的进一步分析,这些对提供电子安全控制系统来说非常重要?

d) 如何对 IACS 构件进行分组或分类以用于定义和管理安全?

e) 控制系统应用中,不同的安全目标是什么?

f) 这些目标是如何建立和修改的?

每个问题都在本标准中详细介绍。

工业通信网络　网络和系统安全
术语、概念和模型

1　范围

1.1　概述

本标准是技术规范，定义了用于工业自动化和控制系统(IACS)安全的术语、概念和模型，是系列标准中其他标准的基础。

为了全面清晰地表达本标准的系统和组件，可以从几个方面定义和理解覆盖的范围，包括：

——所含功能性的范围；

——特定的系统和接口；

——选择所含活动的准则；

——选择所含资产的准则。

以下几节是对这些内容的介绍。

1.2　所含的功能性

本标准的范围能够描述为组织信息和自动化系统内的功能性范围。该功能性可以典型地以一个或更多的模型来描述。

本标准主要集中于工业自动化和控制，这在参考模型中有所描述(见第6章)。虽然考虑了业务系统和工业系统间进行数据完整性的交换，业务计划和物流系统并不在本标准的范围内。

工业自动化和控制包括了过程工业中典型常见的监视控制构件。也包括SCADA(监督和数据采集)，该系统常被组织用于操作关键基础设施。包括：

——输变电和配电；

——供气和供水管网；

——石油和燃气生产运营；

——燃气和液体传输管道。

除此之外，SCADA系统也可以应用在其他的关键和非关键基础设施中。

1.3　系统和接口

在所含的全部IACS中，该标准覆盖了系统中可能会改变或影响到工业过程的功能安全、安全和可靠运行。这些包括但不限于：

a) 工业控制系统及其相关通信网络，包括分布式控制系统(DCS)、可编程逻辑控制器(PLC)、远程终端单元(RTU)、智能电子设备、SCADA系统、网络化电子传感和控制、计量和管道传输系统以及监视和诊断系统[本标准中，工业控制系统包括基本过程控制系统和安全仪表系统(SIS)，不管它们是否物理上分离或整合]。

b) 与第6章描述的参考模型中第3层或更下层相关的系统。诸如先进或多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、生产执行系统、管道泄漏检测系统、工作管理、停电管理以及电能量管理系统。

c) 用于提供控制、功能安全、生产或远程操作功能以实现连续、批量、离散以及其他过程的相关内