ICS 25.040
N 10

中华人民共和国国家标准

GB/T 35673—2017/IEC 62443-3-3:2013

工业通信网络　网络和系统安全 系统安全要求和安全等级

Industrial communication networks—Network and system security—System security requirements and security levels

(IEC 62443-3-3:2013,Industrial communication networks—Network and system security—Part 3-3:System security requirements and security levels,IDT)

2017-12-29 发布　　2018-07-01 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

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 62443-3-3:2013《工业通信网络　网络和系统安全　第 3-3 部分：系统安全要求和安全等级》及其修正案 corrigendum1。

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 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)

为了使用方便,本标准做了下列编辑性修改：

——标准名称修改为“工业通信网络　网络和系统安全　系统安全要求和安全等级”；

——纳入了技术勘误 1 的内容,这些技术勘误涉及的条款已通过在其外侧页边空白位置的垂直双线(‖)进行了标示；

——对 5.7.1 中错误的序列号进行了修正。

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：北京匡恩网络科技有限责任公司、机械工业仪器仪表综合技术经济研究所、中国核电工程有限公司、北京和利时系统工程有限公司、西南电力设计院有限公司、东土科技股份有限公司、全球能源互联网研究院、北京市自来水集团有限责任公司、浙江大学、华中科技大学、西南大学、重庆邮电大学、中国软件测评中心、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、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、华北电力设计院工程有限公司、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、上海自动化仪表研究院、工业和信息化部电子第五研究所、横河电机(中国)有限公司北京研发中心。

本标准主要起草人：王春霞、张大江、王玉敏、梅恪、梁猛、芦宁、徐岩、王亦君、王弢、罗安、张晋宾、薛百华、梁潇、冯冬芹、刘枫、周纯杰、李锐、陈小淙、华镕、张晨艳、朱镜灵、刘安正、马欣欣、周峰、魏旻、刘杰、成继勋、赵军凯、兰昆、王英、张东旗、董黎芳、刘广庆、宋秀娟、杨泓彬、徐近升、刘畅、尚文利、潘东波、刘志祥、钱大涛。

引　言

0.1　概述

注：本标准是涉及工业自动化和控制系统(IACS)信息安全系列标准的一部分。是由 ISA99 委员会第四工作组的第 2 任务组与 IEC TC 65/WG 10 一起合作制定的。本标准描述了在 IEC 62443-1-1 中定义的与控制系统信息安全要求相关的七个基本要求，并对待评估系统(SuC)分配了系统安全等级。

工业自动化和控制系统(IACS)的组织越来越多地使用商用网络设备成品，因为价格低廉、性能高效和高度自动化。出于商业目的，控制系统也越来越多地与非 IACS 网络相互连接。这些设备采用开放的网络技术和持续增加的网络连接，为针对控制系统硬件和软件的网络攻击提供了机会。这个弱点可能导致所部署的系统产生健康、安全和环境(HSE)、财务或声誉问题。

部署商用信息网络安全解决方案来应对 IACS 安全的组织，可能无法完全理解采用这一措施的后果。尽管许多商业 IT 应用和安全解决方案可应用于 IACS，但是它们需要以合适的方式来应用，以避免因疏忽造成的后果。因此，需要结合功能要求和风险评估，通常也包括对运营问题的意识，来定义系统要求。

IACS 安全措施不宜具有引起基本服务和功能(包括应急程序)丢失的隐患。(经常部署的 IT 安全措施，确实有这种潜在弱点。)IACS 安全目标集中在控制系统的可用性、工厂保护、工厂运行(即使在降级模式)和时间关键(time-critical)的系统响应。IT 安全目标往往对这些因素有不同程度的重视；他们可能更关心的是保护信息，而非有形资产。无论工厂集成的实现程度如何，这些不同的目标需要明确地表述为安全目标。根据 IEC 62443-2-1 要求，风险评估中的关键一步是识别出哪些服务和功能对运行是必不可少的。(例如，在一些设施中，工程支持可能被判定为非基本的服务或功能。)在某些情况下，安全性的动作引起非基本的服务或功能的暂时丧失是可以接受的，但是基本服务或功能不宜受到不利影响。

本标准假定系统已经按照 IEC 62443-2-1 规定建立并运行了安全程序。进一步假定通过利用本标准描述的适当的控制系统要求及增强要求，实现了符合 IEC/TR 62443-2-3[5] 所建议的补丁管理。此外，IEC 62443-3-2[8] 描述了怎样对项目定义基于风险的安全等级(SL)，并用于选择符合本标准中详述的适当技术安全能力的产品。本标准的主要参考标准包括 ISO/IEC 27002[15] 和 NIST SP 800-53 第 3 版[24](见第 2 章和参考文献)。

IEC 62443 系列标准的主要目的是提供一种灵活的框架，以应对 IACS 当前和未来的脆弱性，并采用系统化的防御方式，实施必要的缓解方法。IEC 62443 系列标准的目的是扩展企业安全性，使之适应业务 IT 系统的要求，并与 IACS 独特的高可用性需求相结合。

0.2　目的和本标准的使用者

本标准在 IACS 领域的使用者包括资产所有者、系统集成商、产品供应商、服务供应商、合规性管理机构。合规性管理机构包括具有法定权力、根据法律法规进行合规性审计的政府机构和监管部门。

系统集成商、产品供应商和服务提供商将使用本标准来评价其产品和服务是否能够提供满足资产所有者目标安全等级(SL-T)要求的安全能力。对于 SL-T 的分配，单个控制系统的要求(SR)和增强要求(RE)的适用性将基于资产所有者的安全策略、规程和基于具体场所的风险评估。值得注意的是，某些 SR 存在允许例外的特定条件，例如当满足 SR 将违反控制系统的基本操作要求时(这可能需要增加补偿对抗措施)。

当设计控制系统为满足特定 SL-T 相关的一系列 SR 时，不必要求该控制系统的每个组件都满足本标准强制级别的每项系统要求。补偿对抗措施可以用来提供其他子系统所需的功能，在控制系统级，全部的 SL-T 要求都得到满足。在设计阶段宜考虑包括补偿措施，并附有详尽的文档，这样所达到的控制系统 SL、SL-A(控制系统)，充分体现了安全能力的设计预期。同样，为满足整个控制系统的 SL，在认证测试和/或安装后的审计时，可以应用补偿措施并做文件记录。

本标准未提供设计和建立集成安全架构的详细内容。这需要额外的系统级分析和 IEC 62443 系列的其他标准(见 0)衍生的要求。需要注意的是，本标准的目标不是提供详细的规范来建立一个安全架构。本标准的目标是定义一个通用的最低限度要求，逐步达到更严格的信息安全等级。符合这些要求的架构实际设计是系统集成商和产品供应商的工作。在此工作中，他们可以自由选择，从而支持竞争和创新。因此，本标准仅严格地明确功能要求，并不涉及这些功能要求应如何满足。

0.3 本标准在 IEC 62443 系列标准的应用

图 1 给出了本标准撰写时 IEC 62443 系列标准的构成。

IEC 62443-3-2 使用 SR 和 RE 作为一个检查清单。在待评估系统(SuC)使用区域和管道术语进行描述，以及相应的目标 SL 分配给这些区域和管道之后，本标准定义的 SR 和 RE，以及它们与安全能力等级 SL(SL-C)的映射关系，汇集成控制系统设计需要满足的要求列表。一个给定的控制系统设计就可以 SL-A 为条件，进行完整性检查。

图 1 IEC 62443 系列标准的结构

IEC/TS 62443-1-3[2]将基本要求(FR)，SR，RE 和 SL-C 的映射作为检查表来测试量化指标规范的完整性。量化的安全符合性指标基于特定的上下文。结合 IEC 62443-3-2，资产所有者的 SL-T 的任务要求转换成量化指标，用来支持系统的分析和设计权衡研究，以及开发安全体系结构。

IEC 62443-4-1[9]提出产品开发过程中的总体要求。例如，IEC 62443-4-1 的规定内容都是围绕产品

供应商。产品安全性的要求都源于本标准中规定的基线要求列表和 RE。开发这些产品的功能时，将使用 IEC 62443-4-1 质量规范。

IEC 62443-4-2[10]包含一系列派生要求，提供了详细的本标准 SR 到子系统和 SuC 组件的映射。在本标准撰写的时候，IEC 62443-4-2 涉及的组件类别分别为：嵌入式设备、主机设备、网络设备和应用程序。同样，IEC 62443-4-2 主要以供应商（产品供应商和服务供应商）为中心。产品安全性的要求，首先来自本标准中规定的基本要求和 RE 列表。IEC 62443-3-2 和 IEC/TS 62443-1-3 的安全要求和度量被用来完善这些规范性派生需求。

工业通信网络　网络和系统安全
系统安全要求和安全等级

1　范围

本标准规定了与 IEC 62443-1-1 中所描述的 7 个基本要求(FR)相关的详细的技术类控制系统要求(SR),包括定义了控制系统安全能力等级(SL-C)要求。当为特定资产开发适用的控制系统目标 SL,即 SL-T(控制系统)时,对于待评估系统(SuC),工业自动化和控制系统(IACS)的各方可以将这些要求和明确的安全区域及管道一同采用。

根据 IEC 62443-1-1 定义,7 个基本要求(FR)如下:

a)　标识和鉴别控制(IAC);

b)　使用控制(UC);

c)　系统完整性(SI);

d)　数据保密性(DC);

e)　受限的数据流(RDF);

f)　对事件的及时响应(TRE);

g)　资源可用性(RA)。

这 7 项要求是控制系统能力 SL(SL-C)的基础。本标准的目标及目的在于确定控制系统级的安全能力等级。目标 SL(SL-T)或如何实现 SL(SL-A),不在本标准规定的范围。

全面实现控制系统的 SL 目标,还需参见 IEC 62443-2-1 规定的一系列非技术性、程序相关的 SR 能力要求。

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

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

3　术语、定义、缩略语和约定

3.1　术语和定义

IEC 62443-1-1 和 IEC 62443-2-1 界定的以及下列术语和定义适用于本文件。

注:下列术语和定义多数是基于国际标准化组织(ISO)、国际电工委员会(IEC)或美国标准技术研究院(NIST)的标准,为适用于控制系统信息安全要求,有时会做少量修正以增强实用性。