ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32919—2016

信息安全技术　工业控制系统安全控制应用指南

Information security technology—Application guide to industrial control system security control

2016-08-29 发布　　2017-03-01 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 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息技术安全研究中心、中国电子技术标准化研究院、中国电监会信息中心、中国电力科学研究院、无锡市同威科技有限公司、深圳赛西信息技术有限公司。

本标准主要起草人:李京春、范科峰、李冰、王永忠、宫亚峰、刘贤刚、方进社、姚相振、周睿康、唐一鸿、徐金伟、魏方方、王宏、葛培勤、刘鸿运、胡红升、温红子、高昆仑、赵婷、陈雪鸿、詹雄、梁潇、宋斌、庞宁、彭恒斌。

引　言

工业控制系统(ICS)[包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)、可编程逻辑控制器(PLC)等产品]在核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域得到了广泛的应用。

随着信息技术的发展,特别是信息化与工业化深度融合以及物联网的快速发展,工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件,以各种方式与互联网等公共网络连接,传统信息系统所面临的病毒、木马等威胁正在向工业控制系统领域不断扩散,工业控制系统的信息安全问题日益突出。

工业控制系统安全控制应用指南是针对各行业使用的工业控制系统给出的安全控制应用基本方法,是指导选择、裁剪、补偿和补充工业控制系统安全控制,形成适合组织需要的安全控制基线,以满足组织对工业控制系统安全需求,实现对工业控制系统进行适度、有效的风险控制管理。

本标准适用于工业控制系统拥有者、使用者、设计实现者以及信息安全管理部门,为工业控制系统信息安全设计、实现、整改工作提供指导,也为工业控制系统信息安全运行、风险评估和安全检查工作提供参考。

信息安全技术　工业控制系统安全控制应用指南

1　范围

本标准提供了可用于工业控制系统的安全控制列表，规约了工业控制系统的安全控制选择过程，以便构造工业控制系统的安全程序——一种概念层面上的安全解决方案。

本标准适用于：

a）　方便规约工业控制系统的安全功能需求，为安全设计（包括安全体系结构设计）和安全实现奠定有力的基础。

b）　指导工业控制系统安全整改中安全能力的调整和提高，以便能使工业控制系统保持持续安全性。

本标准的适用对象是组织中负责工业控制系统建设的组织者、负责信息安全工作的实施者和其他从事信息安全工作的相关人员。

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。

GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统　industrial control system；ICS

工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

3.2

监控和数据采集系统　supervisory control and data acquisition system；SCADA

在工业生产控制过程中，对大规模远距离地理分布的资产和设备在广域网环境下进行集中式数据采集与监控管理的控制系统。它以计算机为基础、对远程分布运行设备进行监控调度，其主要功能包括数据采集、参数测量和调节、信号报警等。SCADA 系统一般由设在控制中心的主终端控制单元（MTU）、通信线路和设备、远程终端单元（RTU）等组成。

3.3

分布式控制系统　distribution control system；DCS

以计算机为基础，在系统内部（组织内部）对生产过程进行分布控制、集中管理的系统。DCS 系统一般包括现场控制级、控制管理级两个层次，现场控制级主要是对单个子过程进行控制，控制管理级主