ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37980—2019

信息安全技术
工业控制系统安全检查指南

Information security technology—Guide for security inspection of industrial control systems

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
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:中国信息安全测评中心、中国电子技术标准化研究院、中国石油天然气集团公司、北京三零卫士信息安全技术有限公司,北京匡恩网络科技有限责任公司、青岛海天炜业过程控制技术股份有限公司、网神信息技术(北京)股份有限公司、浙江浙能台州第二发电有限责任公司、华能国际电力股份有限公司。

本标准主要起草人:戴忠华、彭勇、赵伟、韩雪峰、向憧、熊琦、邸丽清、高洋、范科锋、姚相振、李琳、周睿康、靖小伟、腾征岑、张建军、张大江、宿凤芹、李航、夏克晁、李辉。

引　言

随着工业化和信息化的深度融合，工业控制系统广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。工业控制系统指应用于工业领域的数据采集、监视与控制系统，是由计算机设备、工业过程控制组件和网络组成的控制系统，是工业领域的神经中枢。工业领域使用的控制系统包括监控与数据采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）系统等。近年来针对工业控制系统的攻击事件导出不穷，工业控制系统的安全性将直接关系到国家重要基础工业设施生产的正常运行和广大公众的利益。

本标准制定的目的是为了指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，进一步健全工业控制系统信息安全管理制度，完善工业控制系统信息安全技术措施，提高工业控制系统信息安全防护能力，为国家对重点行业工业控制系统信息安全检查等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

信息安全技术
工业控制系统安全检查指南

1 范围

本标准给出了工业控制系统信息安全检查的范围、方式、流程、方法和内容。

本标准适用于开展工业控制系统的信息安全监督检查、委托检查工作，同时也适用于各企业在本集团（系统）范围内开展相关系统的信息安全自检查。

注：本标准适用的检查范围是广泛应用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、钢铁、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关领域的工业控制系统。

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 25069—2010 信息安全技术 术语

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB/T 25069—2010 和 GB/T 32919—2016 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

由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。

注：工业控制系统的核心组件包括监控和数据采集系统、分布式控制系统、可编程逻辑控制器、主终端单元、远程终端单元、上位机，以及确保各组件通信的接口技术。

3.2

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

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。

注：SCADA 系统以计算机为基础，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、信息报警等。SCADA 系统一般由设在控制中心的主终端单元（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 distributed control system

以计算机为基础，在系统内部（单位内部）对生产过程进行分布控制、集中管理的系统。

注：DCS 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过程进行控制，控制管理级主要是对多个分散的子过程进行数据采集、统一调度和管理。

3.4

工业控制设备 industrial control device

对工业生产过程及装置进行检测与控制的设备。