ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36323—2018

信息安全技术
工业控制系统安全管理基本要求

Information security technology—
Security management fundamental requirements for industrial control systems

2018-06-07 发布　　2019-01-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　ICS 安全管理基本框架及关键活动 …… 2
5.1　ICS 安全管理基本框架 …… 2
5.2　顶层承诺 …… 3
5.3　规划评估 …… 4
5.4　资源支持 …… 4
5.5　策略实施 …… 4
5.6　绩效评价 …… 5
5.7　持续改进 …… 5
6　ICS 安全管理基本控制措施 …… 5
6.1　安全控制措施分类 …… 5
6.2　安全评估和授权(CA) …… 6
6.3　系统和服务获取(SA) …… 8
6.4　人员安全(PS) …… 11
6.5　规划(PL) …… 12
6.6　风险评估(RA) …… 13
6.7　应急规划(CP) …… 14
6.8　物理和环境安全(PE) …… 17
6.9　配置管理(CM) …… 20
6.10　系统和信息完整性(SI) …… 22
6.11　介质保护(MP) …… 25
6.12　事件响应(IR) …… 26
6.13　意识和培训(AT) …… 28
6.14　访问控制(AC) …… 29
6.15　维护(MA) …… 33
6.16　审计和可核查性(AU) …… 34
6.17　标识和鉴别(IA) …… 37
附录 A（资料性附录）　不同安全级别的 ICS 安全管理基本要求对应表 …… 40
参考文献 …… 45

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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:中国电子技术标准化研究院、国家信息技术安全研究中心、公安部第三研究所、华东师范大学、中国电子科技集团公司第三十研究所、中国信息安全研究院有限公司、上海三零卫士信息安全有限公司、北京神州绿盟信息安全科技股份有限公司、启明星辰信息技术有限公司、烽台科技(北京)有限公司、浙江浙能台州第二发电有限责任公司、北京工业大学、国网浙江省电力公司电力科学研究院、华能国际电力股份有限公司长兴电厂、桂林电子科技大学、西安电子科技大学、浙江大学、中国科学院沈阳自动化研究所、和利时集团、全球能源互联网研究院有限公司、沈机(上海)智能系统研发设计有限公司、深圳赛西信息技术有限公司、广州数控设备有限公司、北京江南天安科技有限公司、中京天裕科技(北京)有限公司、北京匡恩网络科技有限责任公司。

本标准主要起草人:范科峰、刘贤刚、李琳、姚相振、周睿康、李冰、顾健、上官晓丽、许东阳、龚洁中、王惠莅、刘鸿运、何道敬、龚亮华、尚文利、杨晨、蔡磊、仵大奎、刘硕、张建军、王晓鹏、徐克超、周慎学、尹峰、陈胜军、阮伟、杨震、高昆仑、赖英旭、沈玉龙、裴庆祺、许川佩、陈冠直、梁潇、王勇、黄云鹰、杨堂勇、晏培。

引　言

随着计算机和网络技术的发展，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，包括分布式控制系统（DCS）、监控与数据采集（SCADA）系统和可编程逻辑控制器（PLC）等产品广泛应用于核设施、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、城市设施等国家重要领域。工业控制系统（ICS）由单机走向互联、从封闭走向开放、从自动化走向智能化进程的加快，使得工业控制系统的信息安全问题日益突出，工业控制系统一旦遭受攻击，将严重威胁人民生命财产安全和国家政权稳定。对此，全国信息安全标准化技术委员会（SAC/TC 260）立项研制了工业控制系统信息安全分级、管理要求、控制应用指南等多项标准。

本标准针对各行业工业控制系统的安全管理活动的共性特点，提出了工业控制系统安全管理基本框架，从领导、规划、支持、运行、绩效评价和持续改进等方面为工业控制系统安全管理活动提出了规范性要求，并给出了为实现该安全管理基本框架所需的安全管理基本控制措施和各级工业控制系统安全管理基本控制措施对应表，以满足组织对各级工业控制系统的安全管理需求，为实现对工业控制系统适度、有效的安全管理控制提供参考。

信息安全技术
工业控制系统安全管理基本要求

1 范围

本标准规定了工业控制系统安全管理基本框架及该框架包含的各关键活动，并提出为实现该安全管理基本框架所需的工业控制系统安全管理基本控制措施，在此基础上，给出了各级工业控制系统安全管理基本控制措施对应表（参见附录 A），用于对各级工业控制系统安全管理提出安全管理基本控制要求。

本标准适用于非涉及国家秘密的工业控制系统建设、运行、使用、管理等相关方进行工业控制系统安全管理的规划和落实，也可供工业控制系统安全测评与安全检查工作作为参考依据。

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 22080—2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

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 22080—2016、GB/T 22081—2016、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）等。

3.2

分布式控制系统 distributed control system；DCS

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

3.3

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

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：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、远程终端单位（RTU）等组成。