



# 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 .....	VII
引言 .....	VIII
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 安全控制概述 .....	3
6 安全控制基线及其设计 .....	6
7 安全控制选择与规约 .....	7
7.1 选择与规约概述 .....	7
7.2 安全控制选择 .....	7
7.3 安全控制裁剪 .....	8
7.3.1 裁剪过程 .....	8
7.3.2 界定范围的指导 .....	8
7.3.3 安全控制补偿 .....	9
7.3.4 安全控制参数赋值 .....	9
7.4 安全控制补充 .....	10
7.5 建立安全控制决策文档 .....	11
8 安全控制选择过程应用 .....	12
附录 A (资料性附录) 工业控制系统面临的安全风险 .....	13
A.1 工业控制系统与传统信息系统对比 .....	13
A.2 信息系统安全威胁与防护措施对工业控制系统的影响 .....	14
A.3 工业控制系统面临的威胁 .....	15
A.4 工业控制系统脆弱性分析 .....	16
A.4.1 工业控制系统脆弱性概述 .....	16
A.4.2 策略和规程脆弱性 .....	16
A.4.3 网络脆弱性 .....	17
A.4.4 平台脆弱性 .....	19
附录 B (资料性附录) 工业控制系统安全控制列表 .....	22
B.1 规划(PL) .....	22
B.1.1 安全规划策略和规程(PL-1) .....	22
B.1.2 系统安全规划(PL-2) .....	22
B.1.3 行为规则(PL-3) .....	23
B.1.4 信息安全架构(PL-4) .....	23
B.1.5 安全活动规划(PL-5) .....	24
B.2 安全评估与授权(CA) .....	24

B.2.1	安全评估与授权策略和规程(CA-1)·····	24
B.2.2	安全评估(CA-2)·····	24
B.2.3	ICS连接管理(CA-3)·····	26
B.2.4	实施计划(CA-4)·····	26
B.2.5	安全授权(CA-5)·····	27
B.2.6	持续监控(CA-6)·····	27
B.2.7	渗透测试(CA-7)·····	28
B.2.8	内部连接(CA-8)·····	28
B.3	风险评估(RA)·····	28
B.3.1	风险评估策略和规程(RA-1)·····	28
B.3.2	安全分类(RA-2)·····	29
B.3.3	风险评估(RA-3)·····	29
B.3.4	脆弱性扫描(RA-4)·····	29
B.4	系统与服务获取(SA)·····	30
B.4.1	系统与服务获取策略和规程(SA-1)·····	30
B.4.2	资源分配(SA-2)·····	31
B.4.3	生存周期支持(SA-3)·····	31
B.4.4	服务获取(SA-4)·····	31
B.4.5	系统文档(SA-5)·····	32
B.4.6	软件使用限制(SA-6)·····	33
B.4.7	用户安装软件(SA-7)·····	33
B.4.8	安全工程原则(SA-8)·····	33
B.4.9	外部系统服务(SA-9)·····	34
B.4.10	开发人员的配置管理(SA-10)·····	34
B.4.11	开发人员的安全测试(SA-11)·····	35
B.4.12	供应链保护(SA-12)·····	35
B.4.13	可信性(SA-13)·····	36
B.4.14	关键系统部件(SA-14)·····	36
B.5	程序管理(PM)·····	36
B.5.1	程序管理计划(PM-1)·····	36
B.5.2	信息安全高管(PM-2)·····	37
B.5.3	信息安全资源(PM-3)·····	37
B.5.4	行动和里程碑计划(PM-4)·····	37
B.5.5	安全资产清单(PM-5)·····	37
B.5.6	安全性能度量(PM-6)·····	37
B.5.7	组织架构(PM-7)·····	37
B.5.8	关键基础设施计划(PM-8)·····	38
B.5.9	风险管理策略(PM-9)·····	38
B.5.10	安全授权过程(PM-10)·····	38
B.5.11	业务流程定义(PM-11)·····	39
B.6	人员安全(PS)·····	39
B.6.1	人员安全策略和规程(PS-1)·····	39
B.6.2	岗位分类(PS-2)·····	39

B.6.3	人员审查(PS-3)	40
B.6.4	人员离职(PS-4)	40
B.6.5	人员调离(PS-5)	40
B.6.6	访问协议(PS-6)	41
B.6.7	第三方人员安全(PS-7)	41
B.6.8	人员处罚(PS-8)	42
B.7	物理与环境安全(PE)	42
B.7.1	物理与环境安全策略和规程(PE-1)	42
B.7.2	物理访问授权(PE-2)	42
B.7.3	物理访问控制(PE-3)	42
B.7.4	传输介质的访问控制(PE-4)	43
B.7.5	输出设备的访问控制(PE-5)	43
B.7.6	物理访问监控(PE-6)	43
B.7.7	访问日志(PE-7)	44
B.7.8	电力设备与电缆(PE-8)	44
B.7.9	紧急停机(PE-9)	44
B.7.10	应急电源(PE-10)	45
B.7.11	应急照明(PE-11)	45
B.7.12	消防(PE-12)	45
B.7.13	温湿度控制(PE-13)	45
B.7.14	防水(PE-14)	46
B.7.15	交付和移除(PE-15)	46
B.7.16	备用工作场所(PE-16)	46
B.7.17	防雷(PE-17)	46
B.7.18	电磁防护(PE-18)	46
B.7.19	信息泄露(PE-19)	47
B.7.20	人员和设备追踪(PE-20)	47
B.8	应急计划(CP)	47
B.8.1	应急计划策略和规程(CP-1)	47
B.8.2	应急计划(CP-2)	47
B.8.3	应急计划培训(CP-3)	48
B.8.4	应急计划测试和演练(CP-4)	48
B.8.5	备用存储设备(CP-5)	49
B.8.6	备用处理设备(CP-6)	49
B.8.7	通信服务(CP-7)	50
B.8.8	系统备份(CP-8)	50
B.8.9	系统恢复与重建(CP-9)	50
B.9	配置管理(CM)	51
B.9.1	配置管理策略和规程(CM-1)	51
B.9.2	基线配置(CM-2)	51
B.9.3	配置变更(CM-3)	52
B.9.4	安全影响分析(CM-4)	53
B.9.5	变更的访问限制(CM-5)	53

B.9.6	配置设置(CM-6)	54
B.9.7	最小功能(CM-7)	54
B.9.8	系统组件清单(CM-8)	55
B.9.9	配置管理计划(CM-9)	55
B.10	维护(MA)	56
B.10.1	维护策略和规程(MA-1)	56
B.10.2	受控维护(MA-2)	56
B.10.3	维护工具(MA-3)	57
B.10.4	远程维护(MA-4)	57
B.10.5	维护人员(MA-5)	58
B.10.6	及时维护(MA-6)	58
B.11	系统与信息完整性(SI)	58
B.11.1	系统与信息完整性策略和规程(SI-1)	58
B.11.2	缺陷修复(SI-2)	59
B.11.3	恶意代码防护(SI-3)	59
B.11.4	系统监控(SI-4)	60
B.11.5	安全报警(SI-5)	61
B.11.6	安全功能验证(SI-6)	61
B.11.7	软件和信息完整性(SI-7)	62
B.11.8	输入验证(SI-8)	62
B.11.9	错误处理(SI-9)	62
B.11.10	信息处理和留存(SI-10)	63
B.11.11	可预见失效预防(SI-11)	63
B.11.12	输出信息过滤(SI-12)	63
B.11.13	内存防护(SI-13)	64
B.11.14	故障安全程序(SI-14)	64
B.11.15	入侵检测和防护(SI-15)	64
B.12	介质保护(MP)	64
B.12.1	介质保护策略和规程(MP-1)	64
B.12.2	介质访问(MP-2)	65
B.12.3	介质标记(MP-3)	65
B.12.4	介质存储(MP-4)	65
B.12.5	介质传输(MP-5)	65
B.12.6	介质销毁(MP-6)	66
B.12.7	介质使用(MP-7)	66
B.13	事件响应(IR)	67
B.13.1	事件响应策略和规程(IR-1)	67
B.13.2	事件响应培训(IR-2)	67
B.13.3	事件响应测试与演练(IR-3)	67
B.13.4	事件处理(IR-4)	68
B.13.5	事件监控(IR-5)	68
B.13.6	事件报告(IR-6)	69
B.13.7	事件响应支持(IR-7)	69

B.13.8	事件响应计划(IR-8)	69
B.14	教育培训(AT)	70
B.14.1	教育培训策略和规程(AT-1)	70
B.14.2	安全意识培训(AT-2)	70
B.14.3	基于角色的安全培训(AT-3)	70
B.14.4	安全培训记录(AT-4)	71
B.15	标识与鉴别(IA)	71
B.15.1	标识与鉴别策略和规程(IA-1)	71
B.15.2	组织内用户的标识与鉴别(IA-2)	71
B.15.3	设备标识与鉴别(IA-3)	72
B.15.4	标识符管理(IA-4)	73
B.15.5	鉴别符管理(IA-5)	73
B.15.6	鉴别反馈(IA-6)	74
B.15.7	密码模块鉴别(IA-7)	74
B.15.8	组织外用户的标识与鉴别(IA-8)	75
B.16	访问控制(AC)	75
B.16.1	访问控制策略和规程(AC-1)	75
B.16.2	账户管理(AC-2)	75
B.16.3	强制访问控制(AC-3)	76
B.16.4	信息流强制访问控制(AC-4)	77
B.16.5	职责分离(AC-5)	78
B.16.6	最小授权(AC-6)	78
B.16.7	失败登录控制(AC-7)	79
B.16.8	系统使用提示(AC-8)	80
B.16.9	以前访问提示(AC-9)	80
B.16.10	并发会话控制(AC-10)	80
B.16.11	会话锁定(AC-11)	80
B.16.12	会话终止(AC-12)	81
B.16.13	未标识鉴别的许可行为(AC-13)	81
B.16.14	远程访问(AC-14)	82
B.16.15	无线访问(AC-15)	83
B.16.16	移动设备的访问控制(AC-16)	83
B.16.17	外部系统的使用(AC-17)	84
B.16.18	信息共享(AC-18)	84
B.17	审计与问责(AU)	85
B.17.1	审计与问责策略和规程(AU-1)	85
B.17.2	审计事件(AU-2)	85
B.17.3	审计记录的内容(AU-3)	85
B.17.4	审计存储能力(AU-4)	86
B.17.5	审计失效响应(AU-5)	86
B.17.6	审计信息的监控、分析和报告(AU-6)	87
B.17.7	审计简化和报告生成(AU-7)	87
B.17.8	时间戳(AU-8)	87

B.17.9	审计信息保护(AU-9)	87
B.17.10	抗抵赖(AU-10)	88
B.17.11	审计信息保留(AU-11)	88
B.17.12	审计生成(AU-12)	88
B.18	系统与通信保护(SC)	89
B.18.1	系统与通信保护策略和规程(SC-1)	89
B.18.2	应用分区(SC-2)	89
B.18.3	安全功能隔离(SC-3)	90
B.18.4	共享资源中的信息(SC-4)	90
B.18.5	拒绝服务防护(SC-5)	90
B.18.6	资源优先级(SC-6)	91
B.18.7	边界保护(SC-7)	91
B.18.8	传输完整性(SC-8)	93
B.18.9	传输机密性(SC-9)	93
B.18.10	网络中断(SC-10)	94
B.18.11	密钥建立与管理(SC-11)	94
B.18.12	密码技术的使用(SC-12)	94
B.18.13	公共访问保护(SC-13)	95
B.18.14	安全属性的传输(SC-14)	95
B.18.15	证书管理(SC-15)	95
B.18.16	移动代码(SC-16)	95
B.18.17	会话鉴别(SC-17)	96
B.18.18	已知状态中的失效(SC-18)	96
B.18.19	剩余信息保护(SC-19)	97
B.18.20	执行程序隔离(SC-20)	97
附录 C (规范性附录)	工业控制系统安全控制基线	98
参考文献		105

## 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所有者、使用者、设计实现者以及信息安全管理部門,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