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 …… 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 可信赖性(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

要是对多个分散的子过程进行调度管理、数据采集和集中显示。

3.4

可编程逻辑控制器　programmable logic controller;PLC

采用可编程存储器,通过数字运算操作对工业生产装备进行控制的电子设备。PLC 主要执行各类运算、顺序控制、定时执行等指令,用于控制工业生产装备的动作,是工业控制系统的主要基础单元。

3.5

安全控制　security control

应用于工业控制系统的管理、运行和技术上的防护措施和对策,以保护工业控制系统及其信息的保密性、完整性和可用性等。

3.6

安全程序　security program

在工业控制系统的安全建设中,为满足组织安全需求和安全目的,适当采选的一组有序的安全控制集。

3.7

安全控制族　security control family

本标准将相关主题的安全控制作为一个安全控制族,所有的安全控制分成 18 个安全控制族,即:规划(PL)、安全评估与授权(CA)、风险评估(RA)、系统与服务获取(SA)、程序管理(PM)、人员安全(PS)、物理与环境安全(PE)、应急计划(CP)、配置管理(CM)、维护(MA)、系统与信息完整性(SI)、介质保护(MP)、事件响应(IR)、教育培训(AT)、标识与鉴别(IA)、访问控制(AC)、审计与问责(AU)、系统与通信保护(SC)。

3.8

安全控制基线　security control baseline

安全控制基线是安全控制选择过程的起始点,是为帮助组织选择满足安全需求的、最具成本效益的、适当的安全控制集而制定的最低安全基准线。

4　缩略语

下列缩略语适用于本文件。

ICS 工业控制系统(Industrial Control System)

SCADA 监控和数据采集系统(Supervisory Control and Data Acquisition)

DCS 分布式控制系统(Distributed Control System)

PCS 过程控制系统(Process Control System)

PLC 可编程逻辑控制器(Programmable Logic Controller)

RTU 远程终端单元(Remote Terminal Unit)

IED 智能电子设备(Intelligent Electronic Device)

DRP 灾难恢复计划(Disaster Recovery Planning)

ACL 访问控制列表(Access Control List)

DNS 域名系统(Domain Name System)

DHCP 动态主机配置协议(Dynamic Host Configuration Protocol)

DNP 分布式网络协议(Distributed Network Protocol)

RPC 远程过程调用协议(Remote Procedure Call Protocol)

DCOM 分布式组件对象模式(Microsoft Distributed Component Object Model)

OPC 用于过程控制的对象连接与嵌入(Object Linking and Embedding for Process Control)

PAD 个人数字助手，又称掌上电脑(Personal Digital Assistant)
DoS 拒绝服务(Denial of Service)
CVE 通用漏洞列表(Common Vulnerabilities and Exposures)
OVAL 脆弱性评估语言(Open Vulnerability Assessment Language)
EAL 评估保证级(Evaluation Assurance Level)
PKI 公钥基础设施(Public Key Infrastructure)
AC 访问控制(Access Control)
AT 教育培训(Awareness and Training)
AU 审计与问责(Audit and Accountability)
CA 安全评估与授权(Security Assessment and Authorization)
CM 配置管理(Configuration Management)
CP 应急计划(Contingency Planning)
IA 标识与鉴别(Identification and Authentication)
IR 事件响应(Incident Response)
MP 介质保护(Media Protection)
PE 物理与环境安全(Physical and Environmental Protection)
PL 规划(Planning)
PM 程序管理(Program Management)
PS 人员安全(Personnel Security)
RA 风险评估(Risk Assessment)
SA 系统与服务获取(System and Services Acquisition)
SC 系统与通信保护(System and Communications Protection)
SI 系统与信息完整性(System and Information Integrity)

5 安全控制概述

从概念上来说，工业控制系统的安全与其他领域的安全是一样的，如图 1 所示：

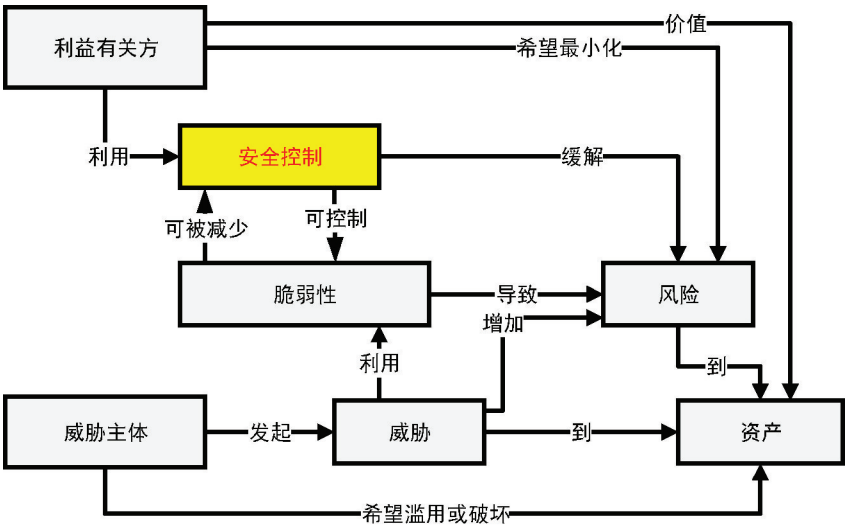

图 1 安全(SECURITY)及其相关概念

图 1 表明了安全(security)及其相关概念间的关系。其中的控制是指:应用于工业控制系统中管理、运行和技术上的保护措施和对策,以保护工业控制系统及其信息的保密性、完整性和可用性等。应用这些控制的目的是,减少脆弱性或影响,抵御工业控制系统所面临的安全威胁,从而缓解工业控制系统的安全风险,以满足利益相关者的安全需要。

本标准附录 B 中给出了可用于工业控制系统的安全控制列表。

为了有效地表达工业控制系统中管理、运行和技术上的措施和对策,应给出该措施对应的动作、输入/输出及其对应的前置条件和后置条件,特别是给出该控制的效果。例如:关于审计处理失效响应的控制:

控制:

工业控制系统:

a) 对于审计处理失效的事件,向【赋值:组织定义的人员】报警;

b) 采取【选择:组织定义的动作,例如:停止系统的运行,重写原有的审计记录,停止生成新的审计记录等】。

其中的“报警”和“采取组织定义的动作”,就是该控制对应的动作;而“审计处理失效的事件”就是该控制的一个输入;“向组织定义的人员(报警)”就是该控制的一个后置条件。并且,通过补充指导,强调了该措施和对策的其他要素,例如:

补充指导:

a) 审计处理失效包括软硬件错误、审计获取机制失败、审计存储空间达到或超出极限等;

b) 组织可针对不同审计处理失效(例如,由于类型、位置、严重程度或这些因素的组合),选择定义附加的措施;

c) 该控制应用于每个审计数据存储库(即存储审计记录的 ICS 部件),应用于组织的整个审计存储能力(即组合了所有审计数据存储库);

d) 在 ICS 不支持审计的情况下,包括对审计失效的响应,组织应按裁剪指导,使用合适的补偿控制(例如,在隔离的信息系统上提供审计能力)。

e) 相关安全控制:AU-4、SI-12。

如果有必要强调一个控制在深度上的能力,以支持更可靠的保护,可通过控制增强来表达,例如:就上述的控制而言,其控制增强可表达为:

控制增强:

a) 对审计处理失效|审计存储能力的响应

在【赋值:组织定义的时间段】内,当分配给审计记录的存储量达到【赋值:组织定义的最大审计记录存储容量】的某一百分比时,ICS 向【赋值:组织定义的人员、角色或岗位】提供一个警示。

b) 对审计处理失效|实时报警的响应

当【赋值:组织定义的、要求实时报警的审计失效事件】发生时,ICS 在【赋值:组织定义的实时报警时间段】内,向【赋值:组织定义的人员,角色和岗位】发出报警。

c) 对审计处理失效|可配置的流量阈值的响应

ICS 执行可配置的流量阈值,反映对审计能力的限制,并【选择:拒绝、延迟】网络流量超出这些阈值。

d) 对审计处理失效|失效宕机的响应

当【赋值:组织定义的审计事件】发生时,ICS 调用【选择:完全宕掉系统,部分宕掉系统;降低运行模式,仅具有有限可用的业务处理能力】,除非存在一种可选的审计能力。

因此，为了更方便地使用控制选择和规约过程，把控制概括为十八个族。每个族包含一些与该族的安全功能相关的安全控制。为每个控制族赋予了唯一的由两个字符组成的标识符，并对族中的每个安全控制，采用了如下基本的描述结构：

族标识符-编号（XX-NN）：
控制节
补充指导节
控制增强节

其中：

控制节为保护组织或工业控制系统的某个特殊方面，提供了所需要的特定安全能力的简洁陈述，描述了要由组织或工业控制系统进行的与安全相关的活动或动作。对于某些控制，通过允许组织选择性地定义与该控制相关参数的输入值，如使用控制中的“赋值”和“选择”操作，实现一定程度的灵活性。

补充指导节提供了一些与特定安全控制相关的信息，指导组织在定义、开发和实现安全控制时适当地使用。在一些情况中，补充指导提供了在组织运行环境、特定业务需求或风险评估中关切的安全需求，或一些重要的注意事项，以及实现安全控制所需要的灵活性等细节。

控制增强节为：

a） 对基本的控制构造附加的、相关的安全能力；

b） 增强基本控制的安全能力。

提供了相应的陈述。控制增强用于需要更大保护的工业控制系统。

通过控制节、补充指导节和控制增强节所描述的控制，使给出的每一控制可有效地表达工业控制系统的安全需求。

本标准给出的三大安全控制类（管理类、运行类和技术类），十八个安全控制族和族标识符的对照关系如表1所示：

表1 安全控制族

族标识符	安全控制族	安全控制类
AC	访问控制（Access Control）	技术
AT	教育培训（Awareness and Training）	运行
AU	审计与问责（Audit and Accountability）	技术
CA	安全评估与授权（Security Assessment and Authorization）	管理
CM	配置管理（Configuration Management）	运行
MA	维护（Maintenance）	运行
CP	应急计划（Contingency Planning）	运行
IA	标识与鉴别（Identification and Authentication）	技术
IR	事件响应（Incident Response）	运行
MP	介质保护（Media Protection）	运行
PE	物理与环境安全（Physical and Environmental Protection）	运行
PL	规划（Planning）	管理
PM	程序管理（Program Management）	管理
PS	人员安全（Personnel Security）	运行

表 1（续）

族标识符	安全控制族	安全控制类
RA	风险评估(Risk Assessment)	管理
SA	系统与服务获取(System and Services Acquisition)	管理
SC	系统与通信保护(System and Communications Protection)	技术
SI	系统与信息完整性(System and Information Integrity)	运行

6 安全控制基线及其设计

为了给出工业控制系统概念层面上的一种安全解决方案，即构造工业控制系统的安全程序，本标准结合工业控制系统基本特征(参见附录 A)，结合以往诸多工业控制系统的安全实践，将附录 B 中工业控制系统的安全控制集分为三个级别，统称为安全控制基线，即基于工业控制系统安全风险的影响程度对安全控制的一个分级，可作为规划工业控制系统中选择安全控制的一个起始点。

在设计安全控制基线中，基于了以下基本假设：

a) 工业控制系统处于物理设施内；

b) 工业控制系统中的用户数据和信息是相对长久的；

c) 工业控制系统是多用户运行的；

d) 工业控制系统中的用户数据和信息必须限制已授权用户的共享；

e) 工业控制系统处于网络化环境中；

f) 工业控制系统自然具有一些特殊目的；

g) 组织具有必要的架构、资源和基础设施，来实现所选基线中的控制。

基线设计的这些基本假设，影响着工业控制系统安全控制的选择，还影响着工业控制系统安全控制的评估、监视和改进。如果一个或多个前提假设是无效的，那么附录 C 中所分配给该基线的一些安全控制就可能是不适用的，针对这种情况可通过应用后续章节所述的裁剪过程以及风险评估予以处理。

相应地，一些可能的情况未包含在假设内，例如：

a) 组织内存在的内部人员攻击；

b) 工业控制系统处理、存储或传输的保密数据和信息；

c) 组织内存在高级持续性攻击(APT)；

d) 基于法律、法规、规章、制度等特殊要求的特殊保护；

e) 工业控制系统需要与其他系统进行跨安全域间通信。

如果任何以上情况出现，就可能需要在附录 B 中选择一些附加的安全控制和控制增强，以确保准确的保护；以上情况也可通过应用后续章节所述的裁剪过程(特别是安全控制补充)和风险评估的结果，予以有效地处理。

本标准设计的安全控制基线(具体见附录 C)，可应用于以下两种情况：

第一种情况，基于工业控制系统的安全风险评估，按风险影响程度将工业控制系统划分为低影响系统、中影响系统和高影响系统。在这种情况下，低影响系统选择第一级安全控制基线；中影响系统选择第二级安全控制基线；高影响系统选择第三级安全控制基线。

第二种情况，通过定级划分准则，见 GB/T 22240—2008，已将工业控制系统划分为相应的安全等级。在这种情况下，1 级、2 级系统选择第一级安全控制基线；3 级系统选择第二级安全控制基线；4 级、5 级系统选择第三级安全控制基线。

7 安全控制选择与规约

7.1 选择与规约概述

工业控制系统安全是一项系统工程，单一的产品和技术不能有效地保护工业控制系统安全，组织应在充分挖掘工业控制系统安全需求的基础上，制定满足组织使命和业务功能需求的工业控制系统安全战略。有效的工业控制系统安全战略，应采用深度防御及层次化的安全机制，使任一安全机制失效的影响最小化。工业控制系统安全应在组织工业控制系统安全战略指导下，通过适当组合配置的安全控制予以实现。

组织在充分考虑工业控制系统的特殊性、安全需求和工业控制系统与传统信息系统间的差异性（参考附录 A，或参阅其他相关文献资料）的基础上，通过风险评估梳理工业控制系统及相关资产，针对工业控制系统存在的脆弱性，分析工业控制系统面临的威胁和风险，评估风险发生的可能性以及风险发生可能造成的影响和危害，制定风险处置原则和处置计划，将工业控制系统安全风险控制在可接受的水平。

本标准附录 C 中给出的安全控制基线，仅是为了工业控制系统的安全需求规约，作为进行安全控制选择与规约的起始点。因此，为了使组织的工业控制系统是安全的，就必须实施选择并规约安全控制和控制增强的过程，该过程包括以下三个子过程：

a） 选择初始安全控制基线；

b） 裁剪所选择的初始安全控制基线；

c） 补充经裁剪的安全控制基线。

安全控制选择与规约过程可概括为图 2 所示：

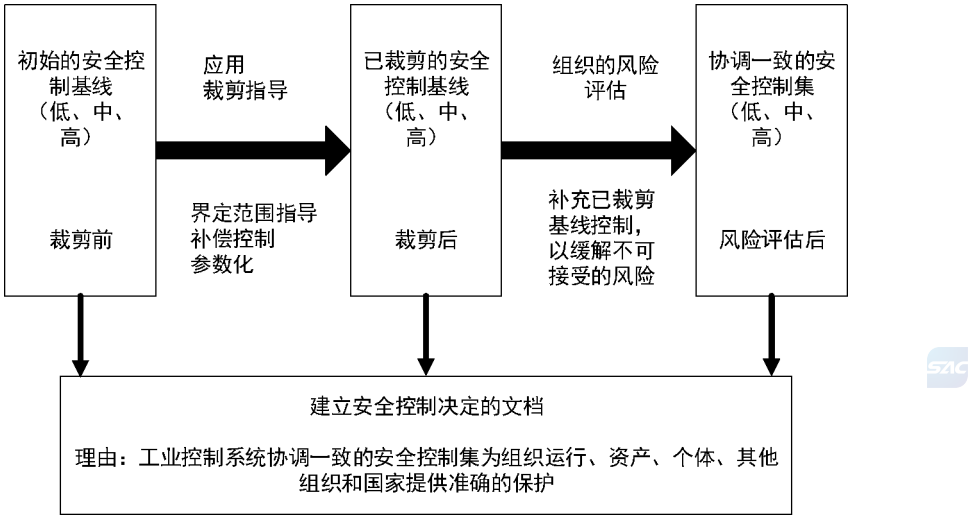

图 2 安全控制选择与规约过程

7.2 安全控制选择

选择基线安全控制是选择并规约安全控制的第一步，组织依据工业控制系统信息安全定级或工业控制系统风险评估结果，根据安全控制基线的应用指导（参见第 6 章），从附录 C 中三个安全控制基线中选择一个合适的基线控制集。选择基线安全控制集时应注意第 6 章所描述的前提假设。

7.3 安全控制裁剪

7.3.1 裁剪过程

在从附录C中选择基线安全控制的初始集后，组织开始基线安全控制的裁剪过程。裁剪过程包括以下3个活动：

a) 依据所选择的基线安全控制，应用界定范围的指导，获得初步可用的控制集；

b) 需要时选择补偿安全控制，以调整初步可用的控制集，获得更可实现的控制集；

c) 通过显式的赋值陈述和选择陈述，规约安全控制中的参数，完成所选基线的定义。

7.3.2 界定范围的指导

界定范围的指导，就所选安全控制基线中每个安全控制的适用性和实现，为组织提供了特定的条款和条件。

应用界定范围的指导，是基于工业控制系统所支持的业务功能和系统运行环境，从初始安全控制基线中删除一些不必要或不适用的安全控制，有助于确保组织仅选择那些可为工业控制系统提供合适程度保护所需要的控制。下面给出一些界定范围的考量，它们可潜在地影响如何应用所选的安全控制基线以及如何实现安全控制。

a) 与控制和应用范围有关的考量

工业控制系统概念是个多层次抽象概念，既包括多个系统组成的复杂系统，又包括单个板卡组成的简单系统。越来越复杂的工业控制系统需要仔细分析在风险管理不同等级(组织级、业务流程级和系统级)中的安全控制的分配和应用。初始安全控制基线中的控制适用于工业控制系统层面，但未必适用于系统组件层面。基线中的一些控制，对工业控制系统范围内的每个系统部件，给出了并非必要的一些控制。一些安全控制仅适用于工业控制系统部件，提供或支持由该控制所强调的安全能力，并缓解潜在的风险。例如，通常把审计控制作为工业控制系统的一个部件，以提供审计能力，并不适用于组织内每个用户层的工作站；或当工业控制系统的部件是单一用户的、无网络连接或是物理隔离网络的一部分时，这些特征可为不把所选择的控制应用到那些部件中提供合适的理由。组织应评估工业控制系统部件清单，以确定安全控制是否适用于各种不同的部件，而后就如何应用控制做出明确的决策，以满足组织的安全需求。

b) 与安全目的有关的考量

基线中的一些控制仅独特地支持保密性、完整性或可用性的安全目的，对此可把它们降级为低基线中对应的控制(或如果在低基线中没有给出定义的话，予以删除或修改)。该降级、修改或删除的动作当且仅当以下情况成立才进行：

1) 安全控制所完成的安全目的可以由组织风险评估所支持；

2) 不会对工业控制系统相关安全保护水平造成不利影响。

例如，一个工业控制系统被评估为中等影响，其可用性和完整性为中等影响，其保密性为低等影响，那些仅与保密性相关的安全控制在不影响安全性目标的前提下可以降低到低级别的基线要求。以下安全控制可作为降级的候选控制：

1) 与保密性相关的安全控制包括：AC-18、MA-3c)、MP-3、MP-4、MP-5、MP-5d)、MP-6、PE-4、PE-5、SC-4、SC-9、SC-9a)等；

2) 与完整性相关的安全控制包括：CM-5、CM-5a)、CP-8a)、SC-8、SC-8a)、SI-7、SI-7a)、SI-7d)、SI-8等；

3) 与可用性相关的安全控制包括：CP-2a)、CP-2b)、CP-2c)、CP-2d)、CP-2e)、CP-2f)、CP-3a)、CP-4a)、CP-4b)、CP-6、CP-6a)、CP-6b)、CP-6c)、CP-7、CP-7a)、CP-7b)、CP-7c)、CP-8、CP-8b)、CP-

8c)、CP-8d)、CP-8e)、CP-8f)、CP-9a)、CP-9b)、CP-9c)、CP-9d)、MA-6、PE-9、PE-10、PE-11、PE-12、PE-13、PE-14、PE-16 等。

c) 与技术有关的考量

安全控制涉及了一些特定的技术(如:无线、加密、PKI 等),这样的控制仅当在工业控制系统内使用时或需要时,它们才是适用的。一些控制可通过自动化机制予以支持,如果这样的机制不存在,或市场上或政府采购产品目录中现在没有或还不能应用时,并不要求开发这样的机制。例如,为了维护最新的、完备的、精确的、现时可用的工业控制系统基线配置,可能使用一些自动化机制。如果自动化机制不是现时可用的、合算的或技术上不是可行的,就需要使用一些补偿的安全控制,通过非自动化机制或规程予以实现的,以便满足所规约的安全控制的需求(参见补偿安全控制相关章节)。

d) 与物理基础设施有关的考量

基线中的一些控制涉及了组织物理基础设施(例如,物理控制,诸如上锁和门禁;有关温度、湿度、照明、防火以及电力等),仅适用于那些存放设施的地方,直接为工业控制系统(包括诸如场站等信息技术资产)提供保护和支持,或直接与工业控制系统有关。

e) 与策略和规章有关的考量

基线中的一些控制强调了某些法律、法规、方针、政策、标准等要求,仅当这些控制的应用环境与相关法律、法规、方针、政策、标准一致时才需要。

f) 与运行环境有关的考量

基线中的一些安全控制依赖于运行环境,仅当在环境中使用该工业控制系统时才适用。例如,一些物理安全控制不适用于那些基于空间的系统,一些温度和湿度的控制不适用于室内设施之外的远程传感器。

g) 与共用控制相关的考量

共用控制是指那些可以被组织内多个工业控制系统继承使用的安全控制。如果一个工业控制系统继承了共用控制,那么其安全性能是由另一个实体提供的,该系统就不需要显式地实现该控制。共用安全控制的标识与定义会影响组织的整体资源支出。将安全控制指定为共用安全控制的决策可能会极大地影响单个工业控制系统安全控制基线的组成。

7.3.3 安全控制补偿

补偿安全控制是由组织选择使用的、用于替代所选安全控制基线中一些特定的安全控制,为工业控制系统所处理、存储或传输的信息提供等价的或可比的保护。

当组织无法有效地实现初始安全控制基线中具体的安全控制时,或者当组织工业控制系统和运行环境存在特殊性时,或者当初始安全控制基线中具体的安全控制不能高效地实现风险减少或缓解时,也就是基线中的控制不是一种合算的措施或对策时,组织可以选取补偿安全控制。并为每个补偿安全控制在工业控制系统安全计划中详细描述选取的原因,以及补偿安全控制如何提供等价保护的说明。

通常,在应用界定范围的考量后,组织就可能发现有必要选择并使用补偿安全控制。组织应如此使用补偿安全控制:

首先,要从附录 B 中来选择补偿控制,其中如果没有合适可用的补偿控制,组织才可采用其他源中合适的补偿控制;

其次,组织为补偿控制如何为工业控制系统提供等价的安全能力以及为什么不能使用该基线安全控制,给出支持理由;

最后,组织评价并接受在工业控制系统中使用补偿安全控制所带来的相关风险。

7.3.4 安全控制参数赋值

安全控制基线中的部分安全控制和控制增强包含嵌入参数(例如:赋值和选择陈述),例如,审计失

效响应(AU-5)：

审计失效响应(AU-5) **控制：** 工业控制系统： a) 对于审计处理失效的事件，向【赋值：组织定义的人员】报警； b) 采取【赋值：组织定义的动作，例如：停止系统的运行，重写原有的审计记录，停止生成新的审计记录等】。

安全控制参数为组织定义控制和控制增强的一定部分提供了灵活性，以便支持特定组织的需求。

在应用界定范围考量后，组织应评审带有赋值和选择陈述的安全控制和控制增强，并为所标识的参数确定组织定义的值。参数值可根据相关法律、法规、规章、制度、政策或标准予以规定。

一旦组织为安全控制和控制增强定义了参数值，那么这些定义的赋值和选择就成为安全控制和控制增强的有机部分。

通常，组织应在选择补偿控制前，规约安全控制参数值，因为安全控制参数的规约完成了安全控制的定义，可能会影响补偿控制的需求。

对于以上章节所述裁剪过程的实施，应当注意以下事项：

a) 在实施初始安全控制基线的裁剪过程前，应与组织相关领导协商裁剪活动，并得到批准。

b) 组织不能随意为运行方便而移出安全控制。安全控制的裁剪决策应基于业务需要，是可论证的，并是伴同明确的、基于风险的评估决定。

c) 裁剪决策，包括决策理由，以及裁剪出的安全控制及其理由，均要记录在组织工业控制系统安全计划中，并作为安全计划批准过程的一部分，得到负责领导的审批。

综上，有关安全控制裁剪过程的应用，如图 3 中突出部分：

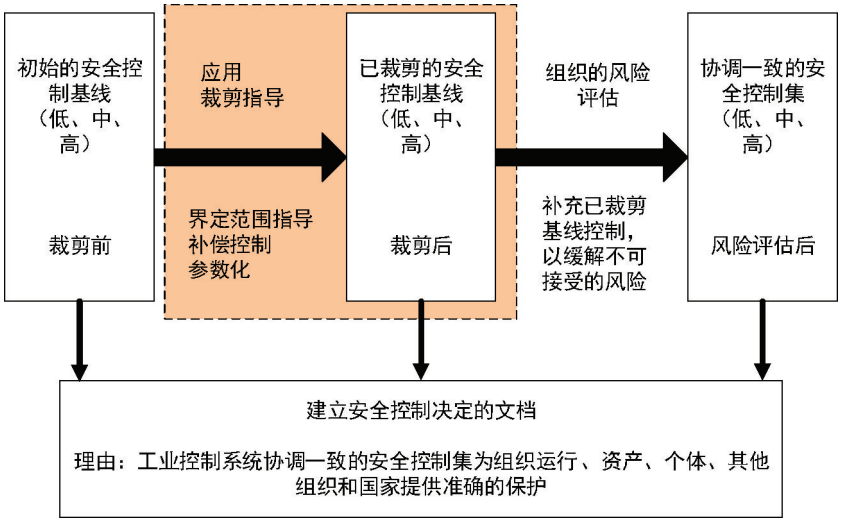

图 3 安全控制裁剪过程

7.4 安全控制补充

裁剪后的安全控制基线，仅确定一个工业控制系统所需要的安全控制集的基础或起始点。只有在组织风险评估的指导下才能最后确定合适的安全控制集。在控制选择过程中的风险评估，为确定裁剪后的基线安全控制的充分性，提供了重要的输入。在许多情况中，为强调特定的威胁和脆弱性，为满足法律、法规、方针、政策、标准和规章制度等要求，需要补充一些附加的安全控制和控制增强。组织应最

大化地使用附录 B 中所给出的安全控制，以支持补充和增强安全控制过程，向经裁剪的安全控制基线中增加安全控制和控制增强。

为了补充已裁剪的安全控制基线，组织可使用需求定义法或空隙分析法选择安全控制和控制增强。在需求定义法中，组织获得有关敌对方活动的特定、可靠的威胁信息（或做出一种有根据的假设），以及一定能力或攻击的潜能（例如技能水平、经验、可用的资源等）。为了有效地抵御具有所陈述能力和潜能敌对方的攻击，组织应从附录 B 选择一些附加的安全控制和控制增强，以获得这样的安全能力。

相对于需求定义法，空隙分析法以组织当前安全能力的评估开始，基于初始的安全能力评估，组织确定可预见的威胁类型。如果组织当前的安全能力是不充分的，那么通过空隙分析就可确定所需要的安全能力。然后，组织从附录 B 中选择一些所需要的安全控制和控制增强，以达到期望的安全能力。

存在一些情况，为了充分保护组织使命和业务功能，组织使用了一些超出其能力的信息技术，即组织在工业控制系统中不能应用充分的安全控制来精确地减少或缓解风险。在这些情况中，就需要一种可选的安全战略，来预防组织使命和业务功能遭受负面影响。当安全控制在技术、资源约束下不能实现时或当控制缺乏期望的有效性来抵御已标识的风险时，应限制技术应用或限制工业控制系统的使用，来减少或缓解风险。可使用的限制包括：

a） 限制工业控制系统可处理、存储或转送的信息；

b） 限制组织使命和业务功能的自动化方式；

c） 禁止移动工业控制系统或系统部件；

d） 禁止外部网络访问组织工业控制系统；

e） 禁止工业控制系统部件里中、高影响的访问。

综上，对经裁剪的安全控制基线的补充，如图 4 中突出部分：

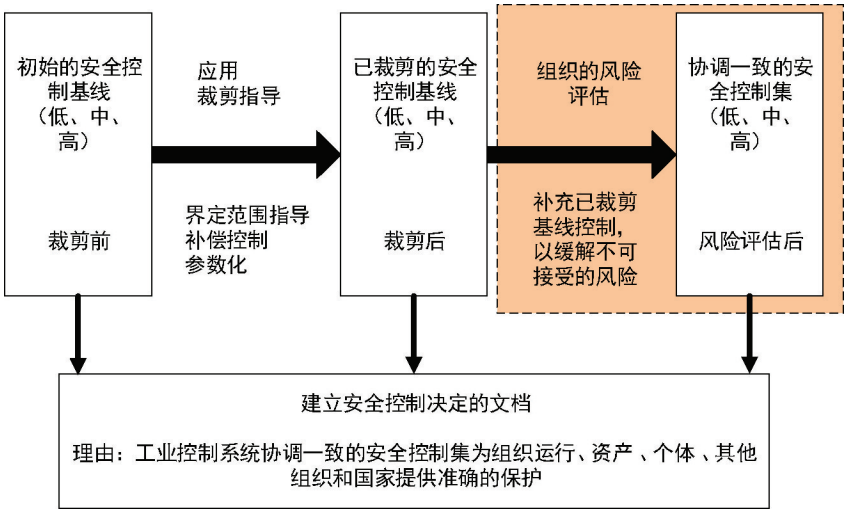

图 4 安全控制补充过程

7.5 建立安全控制决策文档

由于安全控制的描述相对精炼、抽象，可能缺乏实现安全控制的足够信息。组织应在工业控制系统安全计划中详细描述安全控制的实现目的、实现细节、适用范围以及安全控制与安全需求间的切合度等安全控制实现相关的规范信息。但在描述安全控制的规范信息时，不能更改安全控制的原始意图。

在安全控制选择过程期间，组织应建立所有安全控制的决策文档，为这些决策提供有力的理由。当存在对组织使命和业务功能的潜在影响，或在检查工业控制系统整个安全考量时，或当工业控制系统进行重大变更时，或当定期审核工业控制系统安全时，该文档均是基本的支撑资料。最终选择安全控制集

及其选择过程的支持理由，以及任何工业控制系统的使用限制，均应记录在该工业控制系统安全计划中。该过程如图 5 中突出部分：

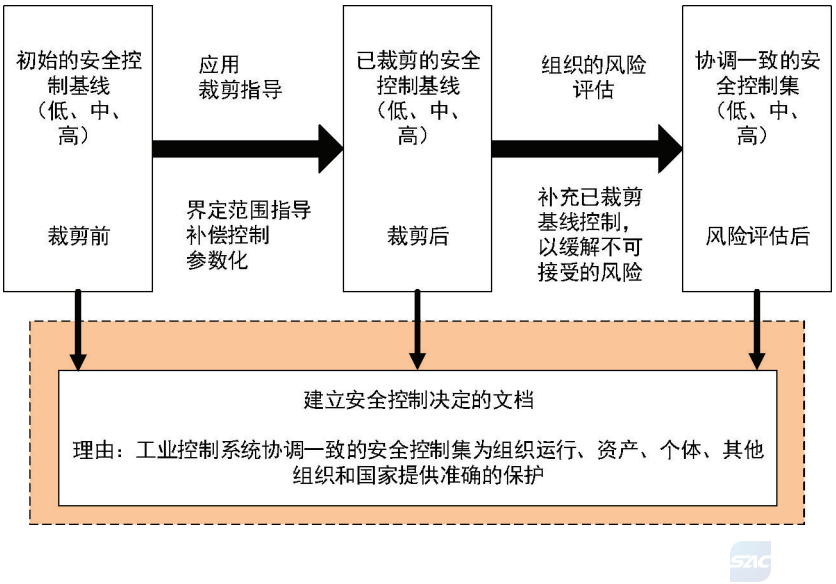

图 5　建立安全控制决策文档

8　安全控制选择过程应用

安全控制选择过程可从两个不同的角度，应用于组织的工业控制系统。一个角度是新系统的开发，另一个角度是在运行系统。对于新开发系统，由于系统并不存在，并且组织没有进行初始的安全定级，因此要从需求定义的视角来应用安全控制选择过程。包含在工业控制系统安全计划中的安全控制，作为组织的安全规格说明，应用在设计、开发、实现、运行等系统生命周期各阶段。

对于在运行系统，当系统发生重大变更时，要用空隙分析法来应用安全控制选择过程。由于系统已经存在，组织已完成了安全定级和安全控制选择过程，其结果已在系统安全计划中，并在系统中予以实现。因此，可以用以下方式应用空隙分析：

首先，基于当前系统处理、存储和传输的不同业务类型，重新评估、确认系统安全级别，必要时调整系统安全级别。

其次，重新评审现有安全计划，以确保系统风险保持在可接受的水平，分析当前使用的、相关联的安全控制与安全需求间的切合程度，记录需增加的安全控制，整理并调整到安全计划中。必要时重新实施风险评估，重新制定安全计划。

最后，实现经调整的或重新制定的安全计划中的安全控制，在措施和里程碑计划中记录任何没有实现的安全控制，并与新开发系统相同的方式继续其余步骤。

附 录 A
（资料性附录）
工业控制系统面临的安全风险

A.1 工业控制系统与传统信息系统对比

大多数的工业控制系统均在网络、个人计算机和互联网普及以前开发并使用，设计之初主要用于解决高效、稳定、可靠、安全等需求。通常情况下，它们与外部网络物理隔离，并且运行在专有的、具有基本错误检测和处理能力的软、硬件平台和通信协议上，缺乏面对当前互联网时代所需要的安全通信能力。虽然这些系统设计时关注了可靠性、可用性和可维护性，但没有预料到在解决性能和故障统计等需求时需要面对的信息安全问题。在当时，工业控制系统安全仅意味着物理上专有网络访问和系统控制台功能。

工业控制系统在20世纪80年代和90年代与微处理器、个人计算机和网络技术同步发展，在90年代后期，互联网技术开始融入到工业控制系统的设计中。这些新技术带来的变化使工业控制系统面临的新威胁，并增加了工业控制系统受到损害的可能性。

最初，工业控制系统使用专门的硬件和软件系统，类似于独立运行的专用控制协议。随着低成本的互联网协议设备正在取代专有设备的解决方案产生，网络安全漏洞和安全事件发生的可能性不断增加。随着工业控制系统开始采用IT解决方案来促进企业连接和远程访问等功能，设计并使用标准计算机、操作系统和网络协议，工业控制系统越来越像IT系统。这些支持新的IT功能技术的集成，工业控制系统与之前相比减少了封闭性，也产生了新的安全需求。虽然传统IT系统已具备解决这些安全问题的解决方案，但在工业控制系统中引入这些解决方案必须考虑工业控制系统的特殊性。在某些情况下需要针对工业控制系统的特殊性裁剪这些安全解决方案。

工业控制系统与传统IT系统相比存在许多特殊性，包括不同的风险和优先级，不同的性能和可靠性要求等。下面列出了解决工业控制系统安全需要考虑的特殊性：

a） 性能需求

工业控制系统通常是严格按照时序要求的，可接受的延时和抖动标准与具体系统相关，系统需要确定的响应，高处理能力通常不是必须的。而传统IT系统需要高处理能力，而能够接受一定的延时和抖动。

b） 可用性需求

很多工业控制系统具有工作连续性，意外的中断往往是不可接受的。中断是按计划进行的，并提前数日或数周完成规划安排。详尽的部署测试是必不可少的，以确保高工业控制系统的高可用性。在某些情况下，工业控制系统所生产的产品或所使用的设备比系统处理或传递的信息更重要。因此，工业控制系统对高可用性、可靠性和可维护性要求，使用典型的IT策略，如重新启动组件，通常是不可接受的解决方案。部分工业控制系统采用冗余组件，并保持并联运行，以保证在主组件异常或不可用时保证系统运行的连续性。

c） 风险管理需求

在典型的IT系统中，数据机密性和完整性通常是首要关注问题。而工业控制系统首要关注问题是防止危害生命、公众健康或信心，监管合规，防止设备、产品或知识产权的损失等。

d） 安全焦点

在典型的IT系统中，安全焦点是保障IT资产的正常运行，并保护这些资产中处理、存储或传输的信息。在某些体系架构中，存储和处理的信息更为关键，并得到更多的保护。对于工业控制系统，边缘

设备(如 PLC、操作员站、DCS 等)直接负责控制过程而需要仔细保护。由于可能对每个边缘设备产生不利影响,对工业控制系统中央服务器的保护也非常重要。

e) 物理交互

典型的 IT 系统往往与环境没有物理上的相互作用。而工业控制系统可能与物理环境间有非常复杂的相互作用。因此,集成到工业控制系统中任何安全功能必须进行严格测试,以确保安全功能不会影响工业控制系统的正常功能。

f) 时间确定性响应

在典型的 IT 系统中,实现访问控制时不必过多关心数据流的情况。而在工业控制系统中,系统自动响应时间或者系统对人类交互的响应是非常关键的,如:在 HMI 中的身份验证和授权不得妨碍或干扰工业控制系统的紧急措施,信息流不能中断。因此,工业控制系统安全控制的运用应受到严格的的限制。

g) 系统运行

工业控制系统的操作系统和应用程序可能无法容忍典型 IT 系统的安全实践。控制网络往往比较复杂,需要不同的专业知识(例如,控制网络通常由控制工程师管理,而非 IT 人员)。在运行的控制网络中,软件和硬件的升级更困难。许多系统可能不具有必要的功能,包括加密功能、错误日志记录和密码保护等 IT 系统中最基本的功能。

h) 资源约束

工业控制系统和它们的实时操作系统往往是资源受限的系统,通常不包括典型 IT 系统的安全能力。在工业控制系统组件上可能没有可用的计算资源来改造现有的安全功能。此外,在某些情况下,因为工业控制系统供应商许可证和服务协议,第三方安全解决方案是不允许的。

i) 通信

用于工业控制系统现场控制和处理器间通信的通信协议是专有的,与典型的 IT 系统通信协议完全不同。

j) 变更管理

无论是 IT 系统还是工业控制系统,变更管理都是保证完整性的重要措施。未安装补丁的软件是一个巨大的安全漏洞。通常采用适当的安全策略和程序及时进行 IT 系统软件的更新,包括安全补丁更新。此外,这些更新通常使用基于服务器的工具来自动实现。因为更新需要进行全面的测试和计划,工业控制系统的更新往往不及时。另外,由于工业控制系统通常使用旧版的操作系统,供应商已停止技术支持,因此,更新程序往往不适用于工业控制系统。因此,工业控制系统的变更(包括硬件、固件和软件的变更)过程需要经过工业控制系统专家、信息安全专家和信息系统专家的仔细评估。

k) 服务支持

典型的 IT 系统允许多样化的支持方式。而对于工业控制系统,服务支持通常来自于单一供应商,可能不存在多样化的支持方式。

l) 组件生命周期

由于技术的快速演变,典型的 IT 组件只有 3 年～5 年的生命周期。而工业控制系统组件的生命周期往往有 15 年～20 年,甚至更长。

m) 组件访问

典型的 IT 系统组件通常是本地的和易于访问的,而工业控制系统组件可能是分离的、远程的,对它们的访问需要大量的外部尝试。

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

工业控制系统运行引发出许多与大多数 IT 系统不同的安全挑战。例如大多数安全措施是为对付因特网上黑客制定的。因特网环境与工业控制系统运行环境是极其不同的。所以在安全行业中对安全

需求以及安全措施可能影响工业控制系统运行的特殊要求，通常是缺乏认识的。

a） 拒绝服务的影响

已经制定的安全服务和技术主要是为了并不具有许多严格性能和可靠性要求的行业，而这些恰恰是工业控制系统运行所需要的。例如：与授权客户不能访问其银行账户相比，使授权调度员无法访问工业控制系统远端站场控制有可能造成更为严重的后果。所以拒绝服务的威胁远比许多典型因特网交易更为巨大。

b） 加密传输

使用工业控制系统的行业中使用的许多通信信道是窄带的而且端设备经常受到内存和计算机能力的限制，从而由于某些安全措施所需的开销而不允许采用，如加密和密钥交换。

c） 密钥管理

大多数系统和设备是位于地域广大而分散、无人的远方场所，且根本没接入到因特网。这使得密钥管理、证书撤消和其他一些安全措施难于实现。

d） 公网联接

许多系统都由公共线路通信通道连接（条件所限无专网），由于协议不兼容，所以工业通用的网络安全措施（协议）不能工作。

e） 无线通信的影响

虽然无线通信正广泛为许多应用所使用，但工业控制系统使用这些无线技术的场所和所实现的功能，有较多限制；部分是因为远端站场恶劣的电磁环境对可用性的潜在影响（如变电站的高电噪声环境）；部分是因为一些应用要求非常快速且极其可靠的响应（吞吐量），即使许多无线技术具有相应的安全措施，也可能因为增加系统开销而未实现。

A.3 工业控制系统面临的威胁

随着工业控制系统网络化、系统化、自动化、集成化的不断提高，其面临的安全威胁日益增长。从发生的典型事件看，针对工业控制系统的安全威胁主要来自五个方面：

a） 自然环境因素；

b） 人为错误或疏忽大意；

c） 设备故障；

d） 病毒等恶意软件；

e） 敌对威胁，如黑客、僵尸网络的操控者、犯罪组织、国外情报机构、恶意软件的作者、恐怖分子、工业间谍、内部攻击者等。

表 A.1 详细列出了工业控制系统可能面临的威胁。

表 A.1 工业控制系统可能面临的威胁

威胁源	描述
内部攻击者	具有攻击性的内部员工是计算机犯罪的主要来源之一。内部攻击者了解目标系统，往往被允许不受限制的访问系统，所以并不需要掌握太多关于计算机入侵的知识，就可以破坏系统或窃取系统数据。内部人员威胁也包括外购产品的供应商
黑客	黑客入侵往往是为了获得刺激和成就感。大多数这类攻击者本来不具备专业攻击技术，现在却可以从互联网上下载攻击脚本和程序，向目标发起攻击；而且攻击工具越来越高级和更容易使用。并且黑客的数量庞大，分布在全球，即使是独立或短暂的攻击破坏，也会导致严重的后果，总体上形成了相对较高的安全威胁

表 A.1（续）

威胁源	描述
僵尸网络的操控者	僵尸网络的操控者通过操纵大量系统进行协同攻击、散布钓鱼网、垃圾邮件和恶意软件。有时候他们利用这些受控制的系统和网络，在黑市上将拒绝服务攻击、垃圾邮件攻击或者网络钓鱼攻击等进行买卖交易
恶意软件的作者	居心不良的个人或组织通过制造并传播恶意软件对用户实施攻击。一些破坏性的恶意软件会损害系统文件或硬件驱动器、控制关键过程、开启执行程序以及控制系统所控制的设备等
恐怖分子	恐怖分子试图破坏、致瘫或利用关键基础设施来威胁国家安全，引起大规模人员伤亡，削弱国家经济，降低民众的士气与信心。恐怖分子可能利用钓鱼网站和恶意软件来获取资金或搜集敏感信息，也可能会伴攻一个目标以转移对其他目标的关注程度和保护力度
工业间谍	工业间谍通过暗中活动的方式企图获取有情报价值的资产和技术秘密
犯罪组织	犯罪组织一般为了获取钱财攻击系统，他们往往利用垃圾邮件、网络钓鱼、恶意软件来实施身份盗窃和网上欺诈行为。国际间谍组织和犯罪组织也会进行工业间谍活动，大规模的盗窃金钱，雇用或培养黑客人才，从而对国家安全造成威胁
境外国家力量	国外情报机构等国家力量利用计算机作为信息收集和间谍活动的一部分，个别国家致力于发展信息战，通过破坏供给、通信和经济基础设施，对目标国人民的日常生活造成非常重大的影响

A.4 工业控制系统脆弱性分析

A.4.1 工业控制系统脆弱性概述

本章列出的脆弱性是典型工业控制系统可能存在的，这些脆弱性的列出顺序不反映脆弱性发生的优先性以及脆弱性发生后造成影响的严重性。本章主要从策略和规程、网络和系统平台三方面陈述工业控制系统中可能存在的脆弱性。实际应用的工业控制系统都会遇到所述脆弱性中的一部分，但也可能包含下文没有提到的系统独有的脆弱性。

A.4.2 策略和规程脆弱性

表 A.2 描述了工业控制系统策略和规程存在的脆弱性。

表 A.2 工业控制系统策略和规程脆弱性

脆弱性	描述
不精确的工业控制系统安全策略	不精确的策略经常会把脆弱性引入到工业控制系统中
没有依据工业控制系统的安全策略，编制明确、具体、书面的安全规程文档	建立有效安全程序的一个根本措施是：编制明确、具体的安全规程文档，并据此对有关人员进行培训
没有对工业控制系统进行正式的安全培训	设计一种文档化的正式安全培训和学习程序，可以使有关人员掌握当时组织上的安全策略和规程，掌握工业上信息安全标准和建议的实践。如果没有针对特定工业控制系统策略和规程进行培训，就不能期望有关人员来维护一个安全的工业控制系统环境

表 A.2（续）

脆弱性	描述
不合理的安全体系架构设计	控制工程人员缺乏安全方面的基本培训，设备和系统供应商的产品中没有必要的安全特性
没有工业控制系统设备安装使用指导文件或工业控制系统设备安装使用指导文件有缺陷	设备安装使用指导文件应及时更新、随时备用。这些指导文件是解决工业控制系统故障的恢复程序中所必不可少的
缺少安全实施的管理机制	安全方面的实施负责人员应对文档化安全策略和规程承担相应责任
没有工业控制系统特定的持续运行或灾难恢复计划(DRP)	编制、测试 DRP，确保在主要硬件、软件失效中或在服务设施毁坏中是可用的。如果工业控制系统缺少 DRP，就可能导致宕机次数增加，导致生产力的丧失
未对工业控制系统进行审计	独立的安全审计应评审和检查系统的记录和活动，确定系统控制的准确性，并确保符合已建立的工业控制系统安全策略和规程。审计人员还应当经常检查工业控制系统安全服务是否缺失，并提出改进建议，这样能够使安全控制措施更有效
没有明确具体的配置变更管理程序	应当制定并严格执行工业控制系统硬件、固件、软件的变更控制程序和相关程序文件，以保证工业控制系统得到实时保护，配置变更管理程序的缺失将导致安全监管疏忽、信息暴露和安全风险

A.4.3 网络脆弱性

表 A.3、表 A.4、表 A.5、表 A.6、表 A.7 分别描述了工业控制系统网络硬件、网络结构、网络边界、通信和无线连接及网络设备配置五个方面的脆弱性。

表 A.3 工业控制系统网络硬件脆弱性

脆弱性	描述
网络设备物理保护不足	应该对网络设备的物理访问进行控制，以防止破坏网络设备
缺少环境控制	缺少环境控制会导致处理器失常。例如，一些处理器在过热情况下会自动关闭实现自我保护，一些处理器则会烧毁
不安全的物理端口	不安全的通用接口如 USB、PS/2 等外部接口可能会导致未授权的设备接入
无关人员可以物理访问网络设备	不合适的对网络设备的物理访问会导致：数据和硬件窃取、数据和硬件的物理损伤破坏、对安全环境的篡改、未授权的阻止或控制网络行为以及关闭物理数据链路等

表 A.4 工业控制系统网络结构脆弱性

脆弱性	描述
薄弱的网络安全架构	因业务和操作需要对工业控制系统网络架构的开发和修改，可能在不经意间将安全漏洞引入网络架构的某一部分中
在控制网中传输非控制数据	控制数据与非控制数据有着不同的要求，比如可靠性程度不同。因此，在同一个网络中传输两种流量会存在难以对网络进行配置的问题。例如，非控制流量可能会大量损耗控制流量传输所需要的资源，导致工业控制系统功能中断

表 A.4（续）

脆弱性	描述
IT 网络服务应用在控制网络中	IT 网络中实施的服务，如 DNS、DHCP 等，在控制网络中被使用时，可能引入额外的严重安全漏洞
重要网络链路或设备没有冗余配置	在重要的网络中没有链路或设备冗余备份可能遭遇单点故障

表 A.5　工业控制系统网络边界脆弱性

脆弱性	描述
安全边界定义不清晰	控制网络边界定义不清晰，将难以保证必要的安全措施被合适的实施或配置，会导致对系统和数据的未授权的访问和其他问题
网络边界访问控制措施不当	缺少或未配置合适的边界访问控制措施会导致无用数据在网络间传递。这会引起多种问题，如攻击和病毒在网络中扩散，可以在其他网络中对控制网中敏感数据进行监控和窃听及对系统进行非法访问等

表 A.6　通信和无线连接脆弱性

脆弱性	描述
使用标准的、有文档记载的明文通信协议	攻击者可以使用协议分析器或者其他设备解码 ProfiBus、DNP、Modbus 等协议传输的数据，实现对工业控制系统的网络监控。使用这些协议也可以使攻击者更容易攻击工业控制系统或控制工业控制系统网络行为
缺少用户、数据或设备的认证	许多工业控制系统协议不具备认证机制。没有认证，就会存在重放或篡改数据的可能性
缺少通信完整性保护	大部分的工业协议不具备完整性检查机制。攻击者可以操纵这种没有完整性检查的通信
无线连接客户端与接入点间认证不足	无线客户端与接入点之间需要完整的相互认证，保证客户端访问的不是攻击者伪造的接入点，同时也保证非法入侵者无法访问工业控制系统无线网络
无线连接客户端与接入点间数据保护不力	无线客户端与接入点间传递的敏感数据未采用加密保护，攻击者监听明文信息造成信息泄露

表 A.7　工业控制系统网络设备配置脆弱性

脆弱性	描述
没有使用数据流控制	未采用数据流控制机制，如利用访问控制列表（ACL），限制系统或人对网络设备的直接访问
IT 安全设备配置不当	使用缺省配置往往导致主机上运行了不必要的开放端口和可能被威胁所利用的网络服务。不当的防火墙配置规则和路由器访问控制列表将允许不必要的流量通过
没有备份网络设备配置	没有制定和实施网络设备配置备份和恢复规程，对网络设备的配置偶然或者恶意的修改可能造成系统通信中断并无法及时恢复

表 A.7（续）

脆弱性	描述
传输中没有对口令进行加密	以明文传输的口令很容易被攻击者窃听，攻击者会利用这些口令对网络设备进行非法访问。通过这种访问，攻击者可以破坏工业控制系统操作或者监视工业控制系统网络行为
网络设备口令未及时更新	密码应定期更换，这样，即使未授权用户获得密码，也只有很短的时间段内可以访问网络设备。未定期更换密码可能使黑客破坏工业控制系统的操作或监视器工业控制系统的网络活动
采用的访问控制不足	通过非法访问网络设备，攻击者可以破坏工业控制系统操作或者监视工业控制系统网络行为

A.4.4 平台脆弱性

表 A.8、表 A.9、表 A.10、表 A.11 分别描述了工业控制系统平台硬件、平台软件、平台配置及平台病毒防护四个方面的脆弱性。

表 A.8 工业控制系统平台硬件脆弱性

脆弱性	描述
重要系统安全保护不足	许多远程设备没有配备专门的运行维护工作人员，也没有物理监视技术手段
缺少环境控制	缺少适当的环境控制措施会导致处理器不能正常工作。例如温度过高时，一些处理器会自动关闭，一些会烧熔
未授权人员对设备的物理访问	考虑到有紧急关闭或重启之类的安全要求，应保证只有必要的人员可以物理访问工业控制系统设备。对工业控制系统设备访问不当会导致：数据和硬件窃取、数据和硬件的物理损伤和破坏、对功能环境（例如：数据连接，可移动介质的未授权使用，增加/移除设备）的非法篡改、物理数据链路关闭、检测不到的数据拦截或窃听（键盘输入或其他录入方式）
无线频率和电磁脉冲	无线电磁波会损害控制系统中的硬件。造成的影响轻则扰乱命令和控制，重则对电路板造成永久损坏
缺少备份电源	重要资产缺少备份电源，一旦停电工业控制系统就会关闭，导致不安全事件发生
重要组件没有冗余配置	重要的组件没有备份会导致单点故障

表 A.9 工业控制系统平台软件脆弱性

脆弱性	描述
缓冲溢出	工业控制系统软件可能存在缓存溢出的问题。攻击者可以利用这一点实施攻击
缺省配置为关闭的安全功能	如果关闭或者不使用产品自带的安全功能，那么这样的安全功能将不能起到作用
拒绝服务攻击	工业控制系统软件可能遭受 DoS 攻击，导致系统不能被合法用户访问，或者系统操作和功能延迟
对未定义、定义不明或“非法”情况的错误处理	一些工业控制系统实施可能遭受格式错误或者包含非法域值的包的攻击

表 A.9（续）

脆弱性	描述
依赖 RPC 和 DCOM 的 OPC	不升级系统补丁，RPC/DCOM 的脆弱性可能被利用来攻击 OPC
使用不安全的工业控制系统协议	DNP3.0、Modbus、IEC 60870-5-101、IEC 60870-5-104 和其他一些协议在工业中被普遍使用，而且协议的相关信息随处可得。这些协议只有很少或根本不包含安全功能
使用明文	许多工业控制系统协议以明文方式传递信息，导致消息很容易被攻击者窃听
配置和程序软件的认证和访问控制不足	攻击者可以通过非法访问配置和程序软件破坏设备或系统
没有安装入侵检测和防御软件	入侵行为会导致系统不可用，数据被截获、修改和删除，控制命令的错误执行
工业控制系统安全后门	不法供应商为了各种目的，给系统设置的后门，这些后门的危害特别大
通信协议脆弱性	工业控制系统采用的部分通信协议，由于设计原因存在安全脆弱性，这些协议脆弱性可能被攻击者利用，造成系统的不可用，数据被截获、修改和删除，控制系统执行错误的动作等等

表 A.10　工业控制系统平台配置脆弱性

脆弱性	描述
没有及时安装操作系统和应用安全补丁	未及时补丁的操作系统和应用可能包含新发现的脆弱性，这些脆弱性可能会被攻击所利用
没有经过彻底的测试就安装了操作系统和应用安全补丁	操作系统和应用的安全补丁不经测试就安装可能会对工业控制系统的正常操作产生影响
使用缺省配置	缺省配置中往往会开放不安全或者不必要的端口、服务和应用
重要的配置没有被存储或备份	没有制定和实施工业控制系统软硬件配置备份和恢复规程，对系统参数意外或者恶意的修改可能造成系统故障或数据丢失
便携设备上数据未受保护	假如敏感数据（密码，拨号号码）以明文方式存储在了移动设备上，比如笔记本、PDA，那么一旦这些设备丢失了或者被偷了，系统安全就会遭受极大威胁
缺少恰当的口令策略	没有口令策略，系统就没有了合适的口令控制，使得对系统的非法访问更容易。口令策略是整个工业控制系统安全策略的一部分，口令策略的制定应考虑到工业控制系统处理复杂口令的能力
未使用口令	应该在工业控制系统组件上使用口令以阻止非法访问。口令相关的脆弱性包括：系统登录无口令（如果系统有用户账户）；系统启动无口令（如果系统没有用户账户）；系统待机无口令（如果工业控制系统组件一段时间内没被使用）
口令使用不当	应该保证口令的安全，防止非法访问。包括：以明文方式将口令记录在本地系统；和同事的个人账户使用同一的口令；在收受贿赂后，将口令交给潜在攻击者；在未受保护的通信中以明文方式传输口令
访问控制不当	访问控制方法不当，可能使工业控制系统用户具有过多或过少的权限。如采用缺省的访问控制设置使得操作员具备了管理员特权

表 A.10（续）

脆弱性	描述
没有安装入侵检测和防御软件	入侵行为会导致系统不可用，数据被截获、修改和删除，控制命令的错误执行
不安全的工业控制系统组件远程访问	系统工程师或厂商在无安全控制措施的情况下，实施对工业控制系统的远程访问，可能致工业控制系统访问权限被非法用户获取

表 A.11　工业控制系统平台病毒防护脆弱性

脆弱性	描述
没有安装病毒防护软件	恶意软件会导致系统性能低下、系统不可用和数据被截获、修改和删除。因此需要安装病毒防护软件，比如杀毒软件，防止系统感染病毒
病毒防护软件病毒库过期	病毒防护软件病毒库过期导致系统容易被新的病毒攻击
没经过仔细的测试就安装病毒防护软件及其病毒库升级包	未经测试就安装病毒防护软件及其病毒库升级包可能会影响工业控制系统的正常运行

附 录 B
（资料性附录）
工业控制系统安全控制列表

B.1 规划（PL）

B.1.1 安全规划策略和规程（PL-1）

控制要求：

组织应：

a） 制定并发布安全规划的策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门间的协调和合规性；

b） 制定并发布安全规划规程，以推动安全规划的策略及与相关安全控制的实施；

c） 按【赋值：组织定义的时间间隔】，对安全规划的策略及规程进行评审和更新。

补充指导：

a） 通过该控制来产生一些能有效实现安全规划族中安全控制和控制增强的策略与规程；

b） 该策略和规程应与相关法律、法规、规章、制度、政策、标准和指南是一致的；

c） 安全规划策略可作为组织信息安全策略的一部分；

d） 安全规划规程可针对一般性的安全程序予以开发，当需要时，可针对特殊 ICS 予以开发。

控制增强：无

B.1.2 系统安全规划（PL-2）

控制：

组织应：

a） 开发与组织使命和业务功能相一致的 ICS 安全计划，该计划应包括：

1） 显式地定义了系统的授权边界；

2） 通过组织使命和业务过程，描述了 ICS 的运行环境；

3） 提供了 ICS 的安全定级及定级理由；

4） 描述了与其他 ICS 的关系或连接；

5） 提供了该系统的安全需求概要；

6） 描述了满足安全需求的已有的或规划的安全控制，以及剪裁和补充决策的理由；

7） 在计划实现前，是否得到评审和批准；

b） 按【赋值：组织定义的时间间隔】，评审 ICS 安全计划；

c） 为了强调 ICS 和运行环境的变更，根据安全计划实现期间或安全控制评估期间所标识的问题，对该计划进行调整。

补充指导：

a） 关于“控制”实例化要求

安全计划内含一些有意义的信息，包括对安全控制中“赋值”和“选择”陈述的参数规约，包括通过参考文献有关参数的规约，以便能无歧义地实现安全控制，符合该安全计划的意图，并能使以后作出如下判断：如果该计划按预期实现，还存在哪些对组织运行和资产以及对个体、其他组织和国家的风险。

b） 关于计划实现基本要求

安全计划实现前，应得到授权官员或其代表的评审和批准，并作为组织风险管理战略的一部分。

c) 相关安全控制：AC-2、AC-6、AC-14、AC-17、AC-20、CA-2、CA-3、CA-7、CM-9、CP-2、IR-8、MA-4、MA-5、MP-2、MP-4、MP-5、PL-7、PM-1、PM-7、PM-8、PM-9、SA-5、SA-17。

控制增强：

a) 组织为 ICS 开发安全操作概念，至少包括：系统意图、系统体系架构描述、安全授权安排、安全定级以及定级决策中所考虑的相关因素；

b) 按【赋值：组织定义的时间间隔】，评审并调整安全操作概念；

增强补充指导：

1) 安全操作概念可以包含在 ICS 安全计划中；

c) 组织为 ICS 开发功能体系结构，该结构标识并维护所有外部接口，通过接口交换的信息以及与每一接口相关联的保护机制；

d) 应定义用户角色，以及为每一角色所赋予的访问权限；

e) 唯一独特的安全需求，例如，对暂时闲置的关键数据元素进行加密；

f) 按可用相关法律、法规、方针、政策、标准和指南，ICS 的安全定级，以及任意特殊的保护要求；

g) 信息恢复优先级或 ICS 服务的优先级。

B.1.3 行为规则（PL-3）

控制：

组织应：

a) 针对 ICS 的用法，建立并制定所有 ICS 用户的行为规则，描述他们的责任和期望的行为；

b) 在授权访问 ICS 前，接受来自用户签署的有关他们已经阅读的、理解的和同意遵守该行为规则方面的意见。

补充指导：

a) 组织应基于用户的角色和责任，考虑一些不同的规则集，例如，适用于特权用户的规则和适用于一般角色的规则之间的区分；

b) 可使用电子签名，作为认可的行为规则。

c) 相关安全控制：AC-2、AC-6，AC-8、AC-9、AC-17、AC-18、AC-19、AC-20、AT-2、AT-3、CM-11、IA-2、IA-4、IA-5、MP-7、PS-6、PS-8、SA-5。

控制增强：

a) 在行为规则中，组织应显式地限制对外部网站的使用，限制共享系统的账户信息。

B.1.4 信息安全架构（PL-4）

控制：

组织应：

a) 基于纵深防御的思想制订工业控制系统的信息安全架构，描述信息安全保护的需求、方法及有关外部服务的安全假设或依赖关系；

b) 按【赋值：组织定义的时间间隔】审核并更新信息安全架构；

c) 考虑信息安全体系的变更对安全规划、系统采购过程的影响。

补充指导：

a) 该控制专注于组织设计开发 ICS 需关注的行为；

b) 信息安全结构包括架构描述、安全功能配置和分配、外部接口的安全相关信息、信息交换的接口以及与每个接口相关联的保护机制等；

c) 信息安全架构可以包括其他重要的安全相关信息，如：用户角色和访问权限分配、独特的安全

要求、信息处理类型、存储和传输的系统、系统服务恢复优先级以及任何其他特定的保护需求；

d) 相关安全控制：CM-2、CM-6、PL-2、PM-7、SA-5。

控制增强：

a) 应基于纵深防御的思想设计信息安全架构；

b) 应在预定义的位置和架构层部署特定的安全防护以获得全面的安全保障。

B.1.5 安全活动规划（PL-5）

控制：

a) 在可影响 ICS 的安全活动进行前，组织应规划并协调，以便减少对组织运行、组织资产和个体的影响。

补充指导：

a) 与安全有关的活动，例如包括：安全评估、安全审计、硬件和软件的维护以及持续性计划的测试和演练；

b) 组织事先所进行的规划和协调，包括两个方面：应急情况和非应急情况；

c) 相关安全控制：PL-2。

控制增强：无

B.2 安全评估与授权（CA）

B.2.1 安全评估与授权策略和规程（CA-1）

控制：

组织应：

a) 制定并发布安全评估与授权策略及规程方针策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门间的协调和合规性；

b) 制定并发布安全评估与授权方针策略及规程，以推动安全评估与授权策略及与相关安全控制的实现；

c) 按【赋值：组织定义的时间间隔】，对安全评估与授权策略和规程进行评审和更新。

补充指导：

a) 通过该控制来有效实现安全评估与授权族中安全控制和安全增强的策略和规程；

b) 这些策略和规程要与相关法律、法规、政策和标准保持一致；

c) 安全评估与授权策略可作为组织信息安全策略的一部分；

d) 安全评估与授权规程一般可针对安全程序予以开发，当需要时也可针对特殊的 ICS 予以开发；

e) 在开发安全评估与授权策略中，组织风险管理战略是一个重要的因素。

控制增强：无

B.2.2 安全评估（CA-2）

控制：

组织应：

a) 按【赋值：组织定义的时间间隔】评估 ICS 安全控制，以确定这些控制正确实现程度，按预期运行的程度，产生期望结果的程度，是否满足系统的安全需求；

b) 产生评估报告，记录评估结果。

补充指导：

a) 组织应评估ICS安全控制，作为满足安全需求年度评估的一部分，作为持续监视的一部分，作为ICS开发生存周期中系统测试和评估的一部分；

b) 评估报告按【赋值：组织要求的详细程度】来记录评估结果，以便确定该报告的准确性和完备性；

c) 按安全需求，在【赋值：组织定义的时间间隔】内进行一次安全评估，最少一年进行一次安全评估；

d) 为了满足年度评估要求，组织可持续监视或作为系统开发生存周期过程一部分的ICS测试和评估，勾画出信息安全评估结果；

e) 现有的安全评估结果，只要仍然有效，可在一定程度上予以复用，并在需要时与附加的评估互补；

f) 安全评估活动绝对不能影响ICS正常运行；

g) 如果必须离线评估ICS，应将评估活动安排在计划好的ICS停机阶段；

h) 某些情况下，组织认为ICS在线测试不可取或不适用或可能产生负面影响，应按裁剪指导，使用合适的补偿控制（例如，提供一个替代的系统进行评估），并在安全计划中记录原因；

i) 相关安全控制：CA-4、CA-6、CA-7。

控制增强：

a) 组织应使用独立的评估人员和评估组织，进行ICS中的安全评估；

b) 作为安全评估的一部分，组织应【赋值：组织定义的时间间隔】开展【选择：深度监视、恶意用户测试、渗透测试或组织定义的其他形式的安全测试】。

增强补充指导：

1) 渗透测试演练物理方面和技术方面的安全控制。渗透测试的标准方法包括：测试前分析，基于目标系统的整个了解；测试前潜在脆弱性的标识，基于测试前分析；对于所标识脆弱性，确定其可利用性所设计的测试；

2) 在任一渗透测试场景开始前，各方应就详细的测试规则达成一致意见；这些规则与实施攻击中的威胁源所使用的工具、技术和规程是相互联系的；

3) 进行渗透测试的渗透代理或渗透小组，其独立程度可由组织的风险评估予以指导，做出相应的决策；

4) 进行红色小组演练，作为模拟的敌对方，尝试破坏组织使命和业务过程，以便提供一个综合详细的ICS和组织的安全能力评估；

5) 渗透测试可以是以实验室为基础的测试，但一般期望是更综合性的，并反映实际条件的测试；

6) 进行ICS监视、恶意用户测试、渗透测试、红色小组演练以及其他形式的安全测试，其目的是为了通过演练，来改善组织的实际现状，作为关注组织改进系统和组织安全状态的行为的一种手段；

7) 依据相关法律、法规、政策、制度和标准的要求进行测试；

8) 测试方法要得到授权官员的批准，其中应与组织风险管治功能部门协调；

9) 在红色小组演练期间，覆盖的脆弱性应编入到脆弱性修补过程中；

c) 组织应开发并使用安全评估计划，描述ICS要予评估的可用的安全控制和控制增强，描述评估环境，评估范围，评估组以及评估角色和责任；

d) 组织应开发并使用评估规程文档，其中包含实现的安全控制和控制增强的详细描述，以及该实现如何在评估期间得以验证；

e) 组织应向相关主管部门汇报书面形式的安全评估结果。

B.2.3 ICS 连接管理(CA-3)

控制:

组织应:

a) 制定 ICS 与其他 ICS 互联安全规定,授权 ICS 与外部其他系统进行连接;

b) 对 ICS 与外部其他工业控制系统连接的接口特征、安全要求、通信信息特性等内容进行记录;

c) 在【赋值:组织定义的时间间隔】评审 ICS 与外部的连接情况,以验证 ICS 连接是否符合规定要求。

补充指导:

a) 组织应评估 ICS 中的安全控制,作为满足安全需求年度评估的一部分,作为持续监视的一部分,作为 ICS 开发生存周期过程中系统测试与评估一部分;

b) 评估报告应按组织要求的详细程度来记录评估结果,以便确定该报告的准确性和完备性;

c) 按安全需求,按【赋值:组织定义的时间间隔】进行安全控制评估;

d) 为了满足年度评估需求,组织可持续监视或作为系统开发生存周期过程一部分的 ICS 测试和评估,勾画出信息安全评估结果;

e) 现有的安全评估结果,只要仍然有效,可在一定程度上予以复用,并当需要时与附加的评估互补;

f) 相关安全控制:AC-2、AC-4。

控制增强:

a) 组织应阻止把未分保密等级的国家安全系统直接连接到外部网络。

增强补充指导:

1) 不直接连接,意指在没有使用得到批准的边界保护设备(例如防火墙)的情况下,不能连接到外部网络。

b) 组织应阻止把具有保密等级的国家安全系统直接连接到外部网络。

增强补充指导:

1) 不直接连接,意指在没有使用得到批准的边界保护设备(例如防火墙)的情况下,不能连接到外部网络;

2) 得到批准的边界保护设备(一般是予以管理的接口/跨域系统),提供从该工业控制系统到外部与 AC-4 一致的网络之信息流执行。

B.2.4 实施计划(CA-4)

控制:

组织应:

a) 制定行动计划,在其中记录下拟采取的整改行动,以改正在安全控制评估中发现的弱点和不足,减少或消除系统中的已知漏洞;

b) 根据安全评估、后果分析和持续监控的情况,按【赋值:组织定义的时间间隔】更新现有的行动计划。

补充指导:

a) 该计划记录了组织为纠正在安全评估期间所发现的弱点或不足所规划的修补动作,目的是减少或消除系统中已知的脆弱性;

b) 行动计划是安全授权包中的一个关键文档;

c) 该计划的调整是基于安全评估中、安全影响中的发现,并继续进行监视活动;

d) 相关安全控制:CA-2、CA-7、CM-4。

控制增强：

a） 组织应使用有助于实施计划准确、适时和到时可用的自动化机制。

B.2.5 安全授权（CA-5）

控制：

组织应：

a） 指定【赋值：高层管理人员】作为 ICS 的授权责任人；

b） 未经授权责任人正式授权，ICS 不得投入运行；

c） 在【赋值：组织定义的时间间隔】或发生重大变更时，对 ICS 重新进行安全授权。

补充指导：

a） 授权责任人应具有 ICS 的预算能力，或负责系统所支持的组织使命或业务运行；

b） 通过安全授权过程，授权责任人应考虑与 ICS 运行相关联的安全风险，相对应的，授权责任人应在与理解和接受 ICS 相关安全风险相称的管理岗位；

c） 通过使用综合持续的监视过程，持续地调整授权（如包含风险评估的安全计划）中所包含的关键信息、安全评估报告以及行动计划，向授权责任人和 ICS 拥有者提供及时的 ICS 安全状态；

d） 为了减少管理安全再授权的成本，授权责任人应使用持续监视过程的结果，尽可能按那个基础，做出再授权的决定；

e） 相关安全控制：CA-2、CA-7、PM-9。

控制增强： 无

B.2.6 持续监控（CA-6）

控制：

a） 组织应持续监视 ICS 中的安全控制。

补充指导：

a） 持续监视程序允许组织依据变化的威胁、脆弱性、技术、使命和业务过程，在高动态运行环境中及时维护 ICS 的安全授权；

b） 使用自动化支持工具来持续监视安全控制，进行实时的 ICS 风险管理；

c） 有效的持续监视程序包括：ICS 构件的配置管理和控制、系统变更或其运行环境的变更的安全影响分析、持续评估安全控制和 ICS 状态报告；

d） 该控制与监视配置变更中所需要的活动紧密相关并相互支持。有效的持续监视程序，导致不断地调整安全计划、安全评估报告、动作和里程碑计划；

e） 严格和良好地执行持续监视程序，可充分地减少重新授权 ICS 所需要的工作量；

f） 组织应确保评估不干扰 ICS 的功能；

g） 相关安全控制：CA-2、CA-4、CA-5、CM-3、CM-4。

控制增强：

a） 组织应使用独立评估人员或评估组织，在持续的基础上来监视工业控制系统的安全控制。

增强补充指导：

1） 组织在持续监视期间，通过要求独立评估人员或小组评估工业控制系统授权周期期间所有安全控制，可以扩大并最大化安全控制持续评估的价值。

b） 组织应【赋值：组织定义的时间间隔】规划、安排并进行评估，宣布或不宣布【选择：深度监视、恶意用户测试、渗透测试、红色小组演练或组织定义的其他形式的安全评估】，以便确保符合所有脆弱性缓解过程。

增强补充指导：

1） 脆弱性缓解规程的例子包含在信息保障脆弱性警告中，期望通过测试来确保工业控制系统的安全能力，持续提供准确的保障，以免不断演化威胁和脆弱性。
2） 符合性测试还提供了独立的确认。
3） 参见 CA-2 的补充指导，增强 b)给出了恶意用户测试、渗透测试、红色小组演练以及其他形式的安全测试的进一步信息。

B.2.7 渗透测试（CA-7）

控制：

a） 组织应按【赋值：组织定义的时间间隔】对 ICS 及组件执行渗透测试，以保障 ICS 能够抵抗一定强度的攻击。

补充指导：

a） 渗透测试通过模仿攻击者攻击的方式，来分析 ICS 系统或组件可能存在的脆弱性和漏洞；
b） 渗透测试是一种特殊的 ICS 系统或组件进行评估方式，以发现可能被攻击者利用的漏洞；
c） 渗透测试用来验证的漏洞被利用程度，以及可能遭受的损坏；
d） 渗透测试可以针对 ICS 硬件、软件或固件组件进行；
e） 相关安全控制：CA-2。

控制增强：

a） 组织应聘请专业的第三方渗透组织或团队对 ICS 开展渗透测试。

B.2.8 内部连接（CA-8）

控制：

a） 组织应对连接 ICS 及组件的内部系统进行授权；
b） 应对每个内部连接的系统特性、安全性要求、通信方式、交互内容等进行归档登记。

补充指导：

a） 该控制适用于组织内与 ICS 连接的所有系统，包括移动设备、笔记本/台式电脑、打印机、复印机、传真机、扫描仪、传感器和服务器等。
b） 相关安全控制：CA-3、CA-4。

控制增强：

a） 在建立内部连接前，在 ICS 系统或组件上执行安全合规性检查。

B.3 风险评估（RA）

B.3.1 风险评估策略和规程（RA-1）

控制：

组织应：

a） 制定并发布正式的风险评估策略，其中应包含目的、范围、角色、责任、管理承诺、组织各部门间的协调以及合规性；
b） 制定并发布正式的风险评估规程，以推动风险评估策略及与相关安全控制的实施；
c） 按【赋值：组织定义的时间间隔】，对风险评估策略和规程进行评审和更新。

补充指导：

a） 期望通过该控制来有效实现风险评估族中安全控制以及安全增强的策略和规程；
b） 该策略和规程应与相关法律、法规、政策、规章、制度、标准和指南保持一致；
c） 风险评估策略可作为组织信息安全策略的一部分；

d) 风险评估规程可针对一般性的安全程序予以开发，也可针对特殊 ICS 予以开发；

e) 在开发配置管理策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.3.2 安全分类（RA-2）

控制：

组织应：

a) 按国家法律、法规、政策和标准，对 ICS 进行分类；

b) 在该 ICS 的安全计划中，记录安全分类结果（包括这样分类的理由）；

c) 确保对该安全分类决定进行了评审，并得到授权官员的批准。

补充指导：

a) 安全分类描述了信息和 ICS 受到破坏后，丧失保密性、完整性或可用性对组织运行、组织资产和人员潜在的负面影响；

b) 组织进行安全分类过程，作为大量组织的一项活动，涉及到首席信息官、高层信息安全官、ICS 拥有者、关键使命拥有者等；

c) 组织还要考虑对其他组织的负面影响；

d) 安全分类过程支持信息资产目录的创建，与 PM-8（配置管理族：ICS 构件目录）一起，把目录中信息资产映射到处理、存储和传输信息的系统部件；

e) 相关安全控制：CM-8、MP-4、RA-3、SC-7。

控制增强：无

B.3.3 风险评估（RA-3）

控制：

组织应：

a) 进行风险评估，包括对支持组织运行的信息和 ICS 的未授权访问、使用、泄露、破坏、修改、毁坏，所造成损害的可能性和严重程度；

b) 按【赋值：组织定义的时间间隔】，评审风险评估的结果；

c) 按【赋值：组织定义的时间间隔】，或当标识了新的威胁和脆弱性，或出现了可能影响系统安全状态的其他条件时，或当 ICS 或运行环境进行重大改变时，调整风险评估。

补充指导：

a) 风险评估中应主要考虑：脆弱性、威胁源，以及所规划的或已有的安全控制，目的是为了确定在该 ICS 运行中，组织运行和资产、个体、其他组织和国家所具有的残余风险程度；

b) 风险评估中还要考虑组织运行和资产或来自外部组织的个体（例如：服务提供者，评估组织 ICS 的个体，外部实体）所带来的风险；

c) 风险评估中应遵循相关法律、法规和政策要求；

d) 相关安全控制：RA-2、PM-9。

控制增强：无

B.3.4 脆弱性扫描（RA-4）

控制：

组织应：

a) 按【赋值：组织定义的时间间隔】或按【赋值：组织定义的过程】，或当标识并报告了新的可能影响系统的脆弱性时，对系统和主机应用进行扫描；

b) 依据采用的标准，使用脆弱性扫描工具和技术来：
   1) 列举平台、软件缺陷和不合适的配置；
   2) 格式化和使之透明，并产生检测列表以及相应的测试规程；
   3) 度量脆弱性影响；
c) 分析由安全控制评估所产生的脆弱性扫描报告和结果；
d) 依据组织的风险评估，按【赋值：组织定义的响应时间】，修补脆弱性；
e) 与【赋值：指定的组织内人员】，共享脆弱性扫描过程和安全控制评估中的信息，以助于消除在其他 ICS 中类似的脆弱性。

补充指导：

a) 关于该控制的输入：ICS 的安全分类，可指导脆弱性扫描频率和详细程度。
b) 关于实施该控制的方法：对于定制软件和应用的脆弱性分析，可能需要一些附加的、更详细的特殊技术和途径（例如：源代码评审，源代码分析等）。
c) 关于扫描对象：脆弱性扫描包括对用户或设备是不可访问的特定功能、端口、协议和服务，以及对不合适的配置或不正确操纵信息流的机制。
d) 关于实施该控制所使用的工具：组织可考虑使用兼容国家漏洞数据库命名规则中脆弱性并使用开放的脆弱性评估语言的工具，来测试存在的脆弱性。
e) 在 ICS 网络上进行脆弱性扫描和渗透测试要确保 ICS 功能不受到扫描过程的负面影响。
f) 在非 ICS 网络上使用脆弱性扫描工具，也应特别小心，以确保它们没有扫描 ICS 网络。
g) 在组织基于其特定的理由不在生产的 ICS 上进行脆弱性扫描的情况下，组织应按裁剪指导，使用补偿控制。
h) 相关安全控制：CA-2、CA-7、CM-4、CM-6、RA-2、RA-3、SA-11、SI-2。

控制增强：

a) 组织使用的脆弱性扫描工具，应具有容易调整扫描配置能力；
b) 组织按【赋值：组织定义的时间间隔】，或当标识和报告新的脆弱性时，调整已扫描的 ICS 脆弱性；
c) 组织使用可证实具有一定深度和广度覆盖的脆弱性扫描系统；
d) 组织应明确 ICS 中的什么信息不应被泄露；
e) 为支持更全面的扫描活动，对组织标识的 ICS 组件，应被赋予特定的访问授权；
f) 组织应使用自动化机制及时比较脆弱性扫描结果，以便确定 ICS 脆弱性的趋势；
g) 按【赋值：组织定义的时间间隔】，组织使用自动化机制来发现当前 ICS 中存在的未授权软件；
h) 组织评审历史审计日志，确定所标识的脆弱性是否以前得以利用；
i) 组织应进行 ICS 的脆弱性分析，基于脆弱性分析，执行 ICS 上的渗透测试，以便确定所标识的脆弱性的可利用性。

   增强补充指导：

   渗透测试的标准方法包括：
   1) 基于对该 ICS 的完整了解，所进行的测试前分析；
   2) 基于测试前分析，标识测试前潜在的脆弱性；
   3) 进行设计的测试，确定所标识脆弱性的可利用性。

B.4 系统与服务获取（SA）

B.4.1 系统与服务获取策略和规程（SA-1）

控制：

组织应：

a） 制定并发布正式的系统和服务获取策略，其中应包含目的、范围、角色、责任、管理承诺、组织各部门之间的协调以及合规性；

b） 制定并发布正式的系统和服务获取规程，以推动风险评估策略及与相关安全控制的实施；

c） 应按【赋值：组织定义的时间间隔】，对系统和服务获取策略和规程进行评审和更新。

补充指导：

a） 期望通过该控制来有效实现系统和服务获取族中安全控制和安全增强的策略和规程；

b） 这些策略和规程要与相关法律、法规、政策以及相关的标准保持一致；

c） 系统和服务获取策略可作为组织信息安全策略的一部分；

d） 系统和服务获取规程一般可针对安全程序予以开发，当需要时也可针对特殊的 ICS 予以开发；

e） 在开发系统和服务获取策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.4.2 资源分配（SA-2）

控制：

组织应：

a） 在组织使命和业务过程规划中，确定 ICS 的信息安全需求；

b） 确定并分配保护 ICS 所需要的资源，作为 ICS 主规划一部分，作为投资控制过程的一部分；

c） 在组织的活动程序和预算文档中，建立信息安全的相应条目。

补充指导：

相关安全控制：PM-3、PM-11。

控制增强：无

B.4.3 生存周期支持（SA-3）

控制：

组织应：

a） 采用系统生存周期管理方法来管理 ICS；

b） 在整个系统生存周期中，定义 ICS 安全角色和责任，并建立相应的文档；

c） 标识具有 ICS 安全角色和责任的个体。

补充指导：

相关安全控制：AT-3、PM-7、SA-8。

控制增强：无

B.4.4 服务获取（SA-4）

控制：

a） 在 ICS 获取合同中，组织应基于风险评估，按相关法律、法规、政策、标准和指南的要求，显式地给出如下需求和规约：安全功能需求和规约、与安全有关的文档需求、与开发和演化有关的保障需求。

补充指导：

a） 应制定 ICS 及其部件和服务的获取文档，包括描述以下内容的需求：安全需要、需要的设计和开发过程、需要的测试和评估规程、需要的文档；

b） 对于获取文档中的需求，当标识了新的威胁和脆弱性时，或当采用新的实现技术时，允许调整

其中的安全控制；

c) 获取文档还包括有关 ICS 文档方面的需求；这些文档强调用户和系统管理员的指南，以及有关安全控制实现方面的信息；文档的详细程度将基于该 ICS 的安全分类；

d) 所需要的文档包括安全配置设置和安全实现指南；

e) 相关安全控制：CM-6、PL-2、PS-7、SA-3、SA-5、SA-8。

控制增强：

a) 组织应要求供应商或合同方在文档中提供描述该 ICS 及其部件和服务所使用的安全控制的详细功能特性信息，可对安全控制进行分析和测试；

b) 组织应要求供应商或合同方在文档中提供描述该 ICS 及其部件和服务所使用的安全控制的设计和实现的详细信息，可对安全控制进行分析和测试；

c) 组织应限制获取市场上具有安全能力的信息技术产品，在使用前应进行评估和确认；

增强补充指导：

1) 健壮性需求，组织使命和业务过程，以及整个客户需要，能使有经验的 ICS 安全工程人员，针对正提交评估的产品，提出使用什么样保障等级（EAL）的信息技术产品的建议。

d) 组织应要求软件供应商或制造方证实他们的软件开发过程使用了安全的工程方法、质量控制过程和确认技术，使软件弱点和恶意最小化；

e) 组织应确保所获取的每一个部件显式地分配给 ICS，并且系统拥有者承认该分配；

f) 组织应限制在市场上获取的现成信息技术产品，是那些已通过国家安全相关部门评估的产品，具有信息保障和能使达到保障管治的现成信息技术；

g) 为了保护公共发布的信息，免遭恶意的干扰或破坏，并确保它的可用性，组织应确保使用了市场上具有基本的信息保障能力的信息技术产品；

h) 当信息对那些未被授权访问 ICS 中所有信息的个体访问的时候，为了保护受控的非机密信息，组织应确保使用市场上基本信息保障能力的信息技术产品；

i) 为了保护国家机密的安全信息，仅使用市场上高信息安全保障能力的信息技术产品，确保信息技术产品已通过国家安全相关部门的评估和确认；

j) 组织应要求获取文档中的 ICS 部件，以安全和规定的配置方式予以交付，并且该安全配置对任何软件重新安装或调整均是默认的配置。

B.4.5 系统文档（SA-5）

控制：

a) 组织应编制可用于授权人员和管理员的 ICS 文档。该文档应描述如下内容：

1) ICS 的安全配置、安装和运行；

2) 安全特征和功能的有效使用和维护；

3) 有关配置和行政管理功能用中已知的脆弱性；

4) 并按要求对这样的文档予以保护。

b) 组织应编制可用于授权用户的 ICS 文档。该文档应描述如下内容：

1) 用户可访问的安全特征和功能，以及如何有效使用这些安全特征和功能；

2) 用户与系统交互的方法，以便使个体能以安全的模式来使用系统；

3) 在维护信息安全和 ICS 安全中的用户责任；

4) 并按要求对这样的文档予以保护。

c) 当文档或是不可用时或不存在时，记录要编制的 ICS 文档。

补充指导：

相关安全控制：CM-6、CM-8、PL-2、PL-4、PS-2、SA-3、SA-4。

控制增强：

a） 需要时，获取并保护描述 ICS 中所使用的安全控制的功能特性的具有充分的详细的文档，允许对其中功能特性进行分析和测试，从而使文档对授权人员、供应商、制造者是可用的；

b） 需要时，获取并保护描述了 ICS 与安全有关的外部接口的具有充分的详细程度的文档，允许对其中外部接口进行分析和测试，从而使文档对授权人员、供应商、制造者是可用的；

c） 需要时，获取并保护以子系统以及安全控制的实现细节来描述 ICS 高层设计的具有充分的详细程度的文档，允许对其中的子系统和实现细节进行分析和测试，从而使文档对授权人员、供应商、制造者是可用的；

d） 需要时，获取并保护描述了 ICS 与安全有关外部接口的具有充分的详细程度的文档，允许对其中外部接口进行分析和测试，从而使文档对授权人员、供应商、制造者是可用的；

e） 需要时，获取和保护 ICS 的源码，并对授权人员是可用的，允许进行分析和测试。

B.4.6 软件使用限制（SA-6）

控制：

组织应：

a） 按照采购合同、协议等合法手段来使用软件及其相关文档；

b） 对于由授权许可所保护的软件及相关文档，控制其拷贝和分布；

c） 控制并记录文件共享技术的使用，确保共享技术未被用于未授权发布、执行或拷贝等。

补充指导：

a） 依赖于组织的需要，跟踪系统可以涉及简单的复印或完全自动化的特定应用。

b） 相关安全控制：CM-6、CM-8、PL-2、PL-4、PS-2、SA-3、SA-4。

控制增强：

a） 防止在 ICS 中使用来自开源、受限制的或无认证源代码源的可执行代码；

b） 仅当没有可选的解决方案时，才允许使用那样的源代码，但要提出相应的期望，并得到授权责任人的授权同意。

B.4.7 用户安装软件（SA-7）

控制：

a） 组织应实施显式的规则，管制用户安装的软件。

补充指导：

a） 如果提供了必要的特权，用户才可以安装软件；

b） 组织应【赋值：标识允许安装什么类型的软件（例如对现有软件的调整和打补丁），阻止什么类型软件的安装】；

c） 相关安全控制：PM-7、SA-3、SA-4、SC-2、SC-3。

控制增强：无

B.4.8 安全工程原则（SA-8）

控制：

a） 组织应将 ICS 安全工程原则应用于 ICS 的需求规约、设计、开发、实现和变更中。

补充指导：

a） 应用安全工程原则主要是针对新开发的 ICS 或针对正在进行升级的系统，并把这样的工程原则集成到该系统的开发生存周期中；

b） 对于在运行系统，组织把安全工程原则应用于系统的调整和修改，使之能够灵活性地给出系

统中硬件、软件和固件的当前状态；

c) ICS 的安全工程原则，包括但不限于：

1) 开发层次化的保护；

2) 建立有效的安全策略、体系结构、控制，作为设计的基础；

3) 把安全编入到该系统的生存周期中；

4) 描绘物理和逻辑边界；

5) 确保开发人员和集成人员得到有关如何开发 ICS 安全软件的适当培训；

6) 剪裁安全控制，以便满足组织和运行需要，减少或缓解风险到可接受程度；

d) 相关安全控制：PM-7、SA-3、SA-4、SA-17、SC-2、SC-3。

控制增强：无

B.4.9 外部系统服务(SA-9)

控制：

组织应：

a) 要求 ICS 服务的外部提供者遵从组织的信息安全需求，并按相关法律、法规、方针、政策、规章、制度、标准和指南的要求，使用合适的安全控制；

b) 针对外部 ICS 服务，定义用户角色、责任，并建立相应的文档；

c) 监视外部服务提供者是否符合安全控制。

补充指导：无

相关安全控制：CA-3、IR-7、PS-7。

控制增强：

a) 在获取指定的 ICS 安全服务前，进行组织层面上的风险评估；

b) 确保获取的指定 ICS 安全服务，得到【赋值：组织定义的高层领导批准】。

增强补充指导：

1) 指定的 ICS 安全服务，包括：不良事件监视、分析和响应，与信息安全相关设备的运行。

B.4.10 开发人员的配置管理(SA-10)

控制：

组织应要求 ICS 开发人员和集成人员：

a) 在 ICS 设计、开发、实现和运行期间执行配置管理；

b) 管理并控制对 ICS 的变更；

c) 仅实现那些得到组织批准的变更；

d) 建立得到批准的 ICS 变更文档；

e) 跟踪安全缺陷和缺陷解决方案。

补充指导：

相关安全控制：CM-3、CM-4、CM-9。

控制增强：

a) 组织要求 ICS 开发人员和集成人员提供软件的完整性检测，以便在软件交付后，支持组织进行软件完整性验证；

b) 在开发人员和集成人员指定的配置管理项缺少的情况下，组织为相关人员提供可选的配置管理过程。

增强补充指导：

1) 配置管理过程涉及关键的组织人员，该人员负责评审并批准对 ICS 提出的变更建议，还

涉及在实现任一变更之前进行影响分析的组织人员。

B.4.11 开发人员的安全测试(SA-11)

控制：

组织应要求 ICS 开发人员、集成人员与相关的安全人员商讨：

a) 建立并实现安全测试和评估计划；

b) 实现可验证缺陷修补的过程，纠正安全测试和评估期间发现的弱点和不足；

c) 建立安全测试和评估的文档和缺陷修补过程文档。

补充指导：

a) 开发的安全测试结果，在得到验证后，应最大灵活性地使用，并了解这些结果所受到的影响；

b) 测试结果可用于支持交付的 ICS 的安全授权过程；

c) 相关安全控制：CA-2、CM-4、SA-3、SA-4、SA-5、SI-2。

控制增强：

a) 组织应要求 ICS 开发人员和集成人员使用代码分析工具检查软件中的公共缺陷，并建立分析结果文档；

b) 组织应要求 ICS 开发人员和集成人员执行脆弱性分析，建立脆弱性、利用可能性以及风险缓解文档；

c) 组织应要求 ICS 开发人员和集成人员依据独立验证和确认代理的证据，创建并实现一个安全测试和评估计划。

B.4.12 供应链保护(SA-12)

控制：

a) 组织应使用【赋值：组织定义的防止供应链威胁的度量列表】，防止供应链威胁，作为 ICS 综合防御安全战略的一部分。

补充指导：

a) 防御途径有助于 ICS 整个生命周期内的保护，即设计、开发、安装、系统集成、运行、维护和退役期间的保护；

b) 这样的保护是通过标识、管理、消除生存周期每一阶段上的脆弱性，并使用互补的缓解风险的支持战略而实现的；

c) 相关安全控制：AT-3、CM-8、IR-4、PE-16、PL-8、SA-3、SA-4、SA-8、SA-10、SA-14、SA-15。

控制增强：

a) 组织应使用匿名的获取过程；

b) 组织应购置初始获取中所有 ICS 部件以及相关附件；

增强补充指导：

1) 购买 ICS 所有系统和组件，可避免在未来几年中使用不大可信赖的次级产品或重新在市场上购买产品。

c) 对要获取的硬件、软件、固件或服务，在编入合同协议前，组织应对供应方进行认真的评审；

增强补充指导：

1) 组织评审供应者链，看他们在 ICS 部件或产品的开发和制造中是否使用合适的安全过程。

d) 有关 ICS、ICS 部件以及信息技术产品，组织应使用可信的运输途径；

e) 组织应使用多种多样的 ICS、ICS 部件、信息技术产品和 ICS 服务的供应方；

f) 组织应使用标准配置的 ICS、ICS 部件、信息技术产品；

g) 组织应使 ICS、ICS 部件、信息技术产品的购置决策和交付之间的时间最短；

h） 组织对交付的ICS、ICS构件、信息技术产品进行独立分析和渗透测试。

B.4.13 可信赖性（SA-13）

控制：

a） 组织应要求ICS满足【赋值：组织定义的可信等级】。

补充指导：

a） 该控制的目的是确保组织了解可信赖性的重要，并在ICS设计、开发和实现时，做出显式的可信赖性决策；

b） 可信赖性是ICS的一个特性，表达了系统防护信息在被系统处理、存储和传输中保密性、完整性和可用性所期望的程度；

c） 相关安全控制：RA-2、SA-4、SA-8、SA-14、SC-3。

控制增强：无

B.4.14 关键系统部件（SA-14）

控制：

组织应：

a） 确定【赋值：需要重新实现的关键工业控制系统部件列表】；

b） 重新实现或定制开发这样的ICS部件。

补充指导：

a） 基本假定是，由于来自供应链的威胁，【赋值：组织定义的信息技术产品】不是可信的；

b） 组织应重新实现或定制开发这样的ICS部件，以满足高保障需求。

控制增强：

a） 标识还没有见到可选源的ICS部件；

b） 使用【赋值：组织定义的保障策略】，确保ICS部件的关键安全控制没有受到破坏。

增强补充指导：

1） 组织考虑实施的措施，包括：增强审计、限制源代码和系统功能的访问等。

B.5 程序管理（PM）

B.5.1 程序管理计划（PM-1）

控制：

a） 组织应开发并宣贯一套组织层面的ICS信息安全程序管理计划，包括：

1） 提供安全程序要求概述，以及满足这些要求的安全程序管理控制的说明；

2） 提供有关程序管理控制的充分信息，以便能够实现该计划的意图，并确定该计划是否能够按计划实施；

3） 应包括角色、责任、管理承诺、组织机构之间的协调和合规性；

4） 获得组织内【赋值：相关责任人】的批准；

b） 应按【赋值：组织定义的时间间隔】，修订完善该信息安全程序管理计划；

c） 应修改计划来满足组织变更的需求，或满足计划实施和安全评估过程中发现问题的需求。

补充指导：

a） 信息安全程序管理计划可作为独立文件，或大型文件的一部分；

b） 信息安全程序管理计划控制是组织范围内的通用控制；

c） 程序管理策略可作为组织信息安全策略的一部分。

控制增强：无

B.5.2 信息安全高管（PM-2）

控制：

组织应任命高级信息安全官，负责资源协调、开发、实现和维护组织范围的 ICS 信息安全。

补充指导：无

控制增强：无

B.5.3 信息安全资源（PM-3）

控制：

组织应：

a） 确保实现信息安全程序和文档所有例外要求所需的资源；

b） 雇佣一个能够实现 ICS 信息安全需求所需资源的合作伙伴；

c） 确保信息安全资源可按照计划提供。

补充指导：

a） 组织可指定并授权投资审查委员会来管理和监督的信息安全相关资本规划和投资支出过程。

控制增强：无

B.5.4 行动和里程碑计划（PM-4）

控制：

组织应实现一个确保 ICS 信息安全行动计划，以减轻风险发生时对组织使命、业务运行和资产造成的影响。

补充指导：

a） 该计划是信息安全程序的重要关键文档；

b） 该计划的更新是基于安全控制的结果评估、安全影响分析，是持续的监控活动；

c） 相关的控制：CA-5。

控制增强：无

B.5.5 安全资产清单（PM-5）

控制：

a） 组织应开发并维护一套 ICS 的安全资产清单。

补充指导：

a） 该控制应满足相关标准对资产清单的要求。

控制增强：无

B.5.6 安全性能度量（PM-6）

控制：

a） 组织应开发、监控并报告 ICS 信息安全性能度量结果。

补充指导：

a） 安全性能度量是组织 ICS 信息安全程序和安全控制设施效果的基础指标。

控制增强：无

B.5.7 组织架构（PM-7）

控制：

a) 设计组织架构时应充分考虑 ICS 信息安全风险对组织使命、业务运行、资产、个人、国家等的影响。

补充指导：

a) 组织架构设计应考虑国家对组织架构的相关要求；

b) 将安全需求和安全控制整合到组织架构中，有助于确保早期 ICS 生命周期中的安全考虑得以满足，并符合组织业务流程需要；

c) 完整的安全体系与组织风险管理应和安全策略相一致；

d) 通过实施风险管理、安全标准和指南，能有效地实现了安全要求和安全控制的集成；

e) 相关控制：PM-11、RA-2。

控制增强：无

B.5.8 关键基础设施计划（PM-8）

控制：

a) 组织应开发、发布并按【赋值：组织定义的时间间隔】更新一套满足相关要求的关键基础设施和关键资源保护计划。

补充指导：

a) 定义关键基础设施和关键资源保护计划应满足相关法律、法规、规章、制定、标准和指南的要求；

b) 相关控制：PM-1、PM-9、PM-11、RA-3。

控制增强：无

B.5.9 风险管理策略（PM-9）

控制：

组织应：

a) 开发一套全面的风险管理策略来保护组织业务和资产；

b) 风险管理策略应与组织战略相一致。

补充指导：

a) 组织层面的风险管理策略应包括：明确表达组织风险承受能力、可接受的风险评估方法、风险缓解策略、随着时间的推移持续的评估和监控风险的方法；

b) 风险执行功能可促进组织范围内风险管理策略的一致性；

c) 组织范围内的风险管理策略应是广泛和全面的；

d) 相关控制：RA-3。

控制增强：无

B.5.10 安全授权过程（PM-10）

控制：

组织应：

a) 通过安全授权过程管理组织信息安全状态；

b) 指定专人负责风险管理过程中安全授权的角色和职责；

c) 将安全授权过程集成到组织范围内的风险管理流程中。

补充指导：

a) 安全授权过程是实施风险管理和满足相关标准规范的必要组成部分；

b) 为每个 ICS 指定安全授权负责人。

c) 相关控制：CA-6。

控制增强：无

B.5.11 业务流程定义（PM-11）

控制：

组织应：

a) 在考虑信息安全及安全风险对组织运营、组织资产、个人、其他组织和国家等影响的基础上定义业务流程；

b) 根据信息安全需要定义业务流程和修改业务流程，直到满足信息安全保护需要。

补充指导：

a) 信息安全保护需求是技术无关的，应对抗来自组织、个人或国家等层面对机密性、完整性和可用性的威胁；

b) 信息安全保护需求来自于组织业务需求，选择符合【赋值：组织定义的业务流程和风险管理策略】；

c) 信息安全保护需求确定组织所需的安全控制和支撑业务流程的 ICS；

d) 固有的组织信息安全保护需求定义存在明显不足，可能无法有效保护 ICS 信息安全；

e) 业务流程定义和关联信息安全保护需求应按组织政策和程序进行归档；

f) 相关控制：PM-7、PM-8、RA-2。

控制增强：无

B.6 人员安全（PS）

B.6.1 人员安全策略和规程（PS-1）

控制：

组织应：

a) 制定并发布正式的人员安全策略，内容至少应包含：目的、范围、角色、责任、管理承诺、相关部门间的协调以及合规性；

b) 制定并发布正式的人员安全规程，以推动人员安全策略和相关人员安全控制的实施；

c) 按【赋值：组织定义的时间间隔】，对人员安全策略和规程进行评审和更新。

补充指导：

a) 该控制有效实现该族中的安全控制和控制增强，编制所需要的策略和规程。

b) 该策略和规程应与国家相关法律、法规、政策、标准和指南保持一致。

c) 人员安全策略可作为组织信息安全策略的一部分。

d) 人员安全规程可针对一般性的安全程序予以开发；需要时，可针对特殊 ICS 予以开发。

e) 在开发人员安全策略时，组织风险管理策略是重要因素。

控制增强：无

B.6.2 岗位分类（PS-2）

控制：

组织应：

a) 建立 ICS 岗位分类机制；

b) 评估 ICS 所有岗位的风险；

c) 建立人员审查制度，尤其对控制和管理 ICS 关键岗位的人员进行审查；

d) 按【赋值:组织定义的时间间隔】对岗位风险进行评审和更新。

补充指导:

a) 岗位风险命名与实施的人员管理策略和指导是一致的;

b) 筛选准则涉及显式的信息安全角色委派需求(例如:培训,安全清理);

c) 相关安全控制:AT-3、PL-2、PS-3。

控制增强:无

B.6.3 人员审查(PS-3)

控制:

组织应:

a) 在授权访问 ICS 及相关信息前进行人员审查;

b) 在人员离职或岗位调整时对其进行审查。

补充指导:

a) 人员审查应符合国家相关法律、法规、政策、标准和指南;

b) 组织可基于 ICS 的安全定级,为访问 ICS 的人员【赋值:定义不同的审查条件和审查频率】;

c) 相关安全控制:AC-2、IA-4、PE-2、PS-5、PS-6。

控制增强:

a) 组织应确保每个访问涉及国家秘密信息处理、存储或传输 ICS 的用户,按该 ICS 最高信息秘密等级进行人员审查,并对访问人员进行了相应的保密教育;

b) 组织确保每个访问涉及敏感信息处理、存储或传输 ICS 的用户,按该系统敏感信息的最高秘密等级进行人员审查,并对访问人员进行了相应的保密教育。

B.6.4 人员离职(PS-4)

控制:

组织应:

a) 终止离职人员对 ICS 的访问权限;

b) 删除与离职人员相关的任何身份鉴别信息;

c) 与离职人员签订安全保密协议;

d) 收回离职人员所有与安全相关系统的所有权;

e) 确保离职人员移交与 ICS 相关资产和工具。

补充指导:

a) 与 ICS 相关资产和工具,包括:系统管理技术手册,密钥,身份标识卡;

b) 离职谈话,确保个体理解由前任雇佣人员所强加的任意安全约束,并对所有与 ICS 有关的特性,实现合理的可核查性;

c) 在一些情况中,例如:在任务遗弃的情况,某些有病情况,以及没有可用的监管人员情况,对人员的离职谈话有可能是不能进行的;

d) 离职谈话对个体的安全清理是重要的,特别对由于某种原因所终止的雇员或合同方,该控制的及时执行是基本的控制;

e) 相关安全控制:AC-2、IA-4、PE-2、PS-5、PS-6。

控制增强:无

B.6.5 人员调离(PS-5)

控制:

a) 当人员调离到组织内其他工作岗位时，组织应【赋值：在规定的时间】内，评审其对 ICS 的逻辑和物理访问，并根据评审结果调整其访问权限。

补充指导：

人员调离到组织内其他工作岗位，无论是永久还是临时的，均应：

a) 收回老的，并换发新的钥匙、通行证等相关证件；

b) 关闭 ICS 原账户，并根据新职位的需要开新账号；

c) 改变 ICS 的访问权限；

d) 提供个人以前的工作地点和 ICS 账户访问官方记录；

e) 相关安全控制：AC-2、IA-4、PE-2、PE-2、PS-4。

控制增强：无

B.6.6 访问协议（PS-6）

控制：

组织应：

a) 制定 ICS 的访问协议并形成文件；

b) 按【赋值：组织定义的时间间隔】评审并更新访问协议；

c) 确保在授权人员访问 ICS 前与其签订访问协议，并在访问协议更新或到期后重新签订。

补充指导：

a) 访问协议，包括：保密协议、可接受的使用协议、行为规则等相关协议；

b) 所签订的访问协议包括承诺，即个人已阅读、理解对 ICS 有关的授权访问约束，并同意遵循；

c) 在承诺的访问协议中，可使用电子签名，除非组织策略明文规定不能使用；

d) 相关安全控制：PL-4、PS-2、PS-3、PS-4、PS-8。

控制增强：

a) 组织应确保特殊保护措施 ICS 的访问，仅授权给：

1) 具有有效访问授权的人；

2) 满足相关人员安全准则的人。

b) 组织应确保特殊保护措施的秘密信息的访问，仅授权给：

1) 具有有效访问授权的人；

2) 满足相关的、符合可用的法律的人员安全准则的人；

3) 已阅读、理解已签署保密协议的人。

B.6.7 第三方人员安全（PS-7）

控制：

组织应：

a) 为第三方供应商建立包含安全角色和责任的人员安全要求，并形成文件；

b) 要求第三方供应商遵守已制定的人员安全策略和规程；

c) 第三方供应商在人员调动或离职时予以告知；

d) 监视第三方供应商的合规性。

补充指导：

a) 第三方供应商包括：服务单位，合同方以及提供 ICS 开发、ICS 技术服务、外源应用以及网络安全管理等；

b) 在与获取有关的文档中，组织一般会明确人员安全需求；

c) 相关安全控制：PS-2、PS-3、PS-4、PS-5、PS-6、SA-9。

控制增强：无

B.6.8 人员处罚（PS-8）

控制：

a） 组织应对违反安全策略和规程的人员建立违规处罚制度。

补充指导：

a） 该制度应与相关法律、法规、制度相一致；

b） 该制度应在访问协议中描述，并可包含在一般性的人员策略和规程中；

c） 相关安全控制：PL-4、PS-6。

控制增强：无

B.7 物理与环境安全（PE）

B.7.1 物理与环境安全策略和规程（PE-1）

控制：

组织应：

a） 制定并发布正式的物理和环境安全策略，内容至少应包含：目的、范围、角色、责任、管理承诺、相关部门间的协调和合规性；

b） 制定并发布正式的物理和环境安全章程，以推动物理和环境保护策略和相关安全控制的实施；

c） 按【赋值：组织定义的时间间隔】，对物理和环境保护策略及规程进行评审和更新。

补充指导：

a） 物理和环境保护策略和章程应与适用的法律、法规、政策及标准等相一致。物理和环境保护策略可以包含在组织的通用信息安全策略中，需要时，可针对特殊 ICS 予以开发。

控制增强：无

B.7.2 物理访问授权（PE-2）

控制：

组织应：

a） 制定并维护对 ICS 具有访问权限的人员名单；

b） 按【赋值：组织定义的时间间隔】对授权人员进行评审和批准；

c） 根据职位、角色对 ICS 实施进行物理访问授权。

补充指导：

a） 授权证书包括标记卡和智能卡等；

b） 组织应及时从访问列表中清除那些不再访问 ICS 的人员。

控制增强：无

B.7.3 物理访问控制（PE-3）

控制：

组织应：

a） 加强对 ICS 实施所在出入口的物理访问控制；

b） 在指定出入口采用围墙、门禁、门卫等物理访问控制措施，具有物理访问授权不代表对该区域 ICS 组件有逻辑访问权；

c) 在访问 ICS 设施前对人员的访问权限进行验证；
d) 维护物理访问记录；
e) 制定公共访问区访问控制策略；
f) 在需要对访客进行陪同和监视的环境下对访问者的行为进行陪同和监视。

补充指导：

a) 组织应使用物理访问设备(如，密码锁、读卡机)或配备门卫等方式控制人员访问 ICS 设施；
b) 组织应使用规则保护密码锁和其他访问控制设施；
c) 组织应按【赋值：组织定义的时间间隔】更换访问控制设备的口令，在密码泄露和人员调动或离职时更换访问控制设备的口令；
d) 置于公共区域内的 ICS 外围设备应控制该区域的访问；
e) 相关安全控制：PE-2、PE-4、PS-3。

控制增强：

a) 组织应控制对 ICS 的物理访问，这些控制应独立于对设施的物理访问控制；
b) 应对较容易进入且拥有可移动介质驱动器的计算机采取带锁、卸载或禁用等手段提高安全性；
c) 应将服务器放置在带锁的区域并采用认证保护机制；
d) 应将 ICS 网络设备放置在只能由授权人员访问的符合环境要求的安全区域中。

B.7.4 传输介质的访问控制(PE-4)

控制：

a) 组织应采用安全防护措施对 ICS 设施内的传输线路进行物理访问控制。

补充指导：

a) 对 ICS 实施传输线路的保护有助于防止对意外损坏、中断和物理篡改；
b) 物理安全措施有助于防止未加密的传输信息的窃听和篡改；
c) 相关安全控制：MP-2、MP-4、PE-2、PE-3。

控制增强：无

B.7.5 输出设备的访问控制(PE-5)

控制：

a) 组织应控制对 ICS 输出设备的物理访问，防止未授权人员获取输出信息。

补充指导：

a) ICS 输出设备，包括：监视器、打印机以及其他视听设备等；
b) 输出设备的访问控制包括，放置在锁定的房间内、放置在安全领域，对输出设备进行授权访问，监控人员使用；
c) 相关安全控制：PE-2、PE-3、PE-4。

控制增强：

a) 控制对输出设备的物理访问；
b) 确保只有授权人员收到来自设备的输出；
c) 组织应对输出设备进行标记，标明哪些信息可以标记的输出设备输出。

B.7.6 物理访问监控(PE-6)

控制：

a) 组织应监控对 ICS 的物理访问，以监测并响应物理安全事件。

补充指导：

a） 组织应按【赋值：组织定义的时间间隔】审查物理访问日志，调查明显的安全侵害或可疑的物理访问行为；

b） 组织应对检测出的物理安全事件做出响应；

c） 相关安全控制：CA-7、IR-4。

控制增强：

a） 组织应设置防盗报警系统，识别潜在入侵、实时入侵报警并发起适当的响应行为；

b） 组织应采用自动化设备识别入侵，并实施自动响应动作；

c） 组织应采用视频监控，并保留视频记录。

B.7.7 访问日志（PE-7）

控制：

a） 组织应保存 ICS 访问日志；

b） 组织应指派人员按【赋值：组织定义的时间间隔】期审查访问日志。

补充指导：

a） 访问日志应包括：来访人员的名字、所属组织、访客签名、访问目的、鉴别形式、访问的 ICS 及部件、进入和离开的时间、陪同监视人名字；

b） 公共区域的访问不记录在 ICS 访问日志内。

控制增强：

a） 组织使用自动化的机制促进访问日志的维护和回顾；

b） 组织维护所有物理访问的记录，包括访客和授权用户。

B.7.8 电力设备与电缆（PE-8）

控制：

a） 组织应保护 ICS 的电力设备和电缆，免遭破坏和损坏；

b） 组织应依据安全需求和风险，采用禁用或对电源进行物理保护的手段来防止系统的非授权的使用。

补充指导：无

a） 组织应确定在不同地点的电力设备和电缆的保护需求。

b） 相关安全控制：PE-4。

控制增强：

a） 组织使用冗余的电力设备和电缆；

b） 组织应对【赋值：组织定义的关键工业控制系统部件列表】，使用自动化灾难备份等安全控制措施。

B.7.9 紧急停机（PE-9）

控制：

组织应：

a） 确保在紧急情况下能够切断 ICS 电源或个别组件电源；

b） 在【赋值：组织定义的工业控制系统或系统部件位置】设置安全易用的紧急断电开关或设备；

c） 保护紧急断电能力以防止非授权操作。

补充指导：无

控制增强：无

B.7.10 应急电源(PE-10)

控制：

组织应：

a) 为 ICS 配备应急 UPS 电源，并计算其续航时间；

b) 提供短期不间断电源，以便在主电源失效的情况下正常关闭 ICS；

c) 提供长期备份电源，以便主电源失效时在规定时间内保持 ICS 功能。

补充指导：

a) 相关安全控制：AT-3、CP-2。

控制增强：

a) 组织应为 ICS 提供备用电力供应系统，ICS 能够在主电源长期丧失的事故中有能力维持 ICS 所必须的最小的运行能力。

b) 组织应提供 ICS 长期的备用电力供应系统，该系统是独立运行而不依赖外部电源的。

B.7.11 应急照明(PE-11)

控制：

组织应：

a) 为 ICS 部署应急照明并进行维护，并确保其在断电情况下的可用性；

b) 在急照明设施中包含紧急通道和疏散通道指示牌。

补充指导：无

a) 相关安全控制：CP-2、CP-7。

控制增强：无

B.7.12 消防(PE-12)

控制：

组织应：

a) 为 ICS 部署火灾检测和消防系统或设备，并维护该设备；

b) 为消防系统或设备配备独立电源。

补充指导：

a) 防火灭火设备或系统包括但不限于洒水系统、手动灭火器、固定灭火水龙带和冒烟检测设备。

控制增强：

a) 使用防火设备或系统，该设备或系统在火灾事故中会自动激活并通知组织和紧急事件处理人员；

b) 使用灭火设备或系统，该设备或系统为组织和紧急事件处理人员提供任何激活操作的自动通知；

c) 使用自动灭火系统；

d) ICS 组件集中部署的区域，如主机房、通信设备机房等应采用具有耐火等级的建筑材料，采取区域隔离防火措施，将重要设备与其他设备隔离。

B.7.13 温湿度控制(PE-13)

控制：

组织应：

a) 维护 ICS 所在设施的温湿度，使其处于可接受的范围；

b） 按【赋值：组织定义的时间间隔】监视温湿度。

补充指导：无

控制增强：

a） ICS 组件集中部署的区域，如主机房、通信设备机房等应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

B.7.14 防水（PE-14）

控制：

a） 组织应提供易用、工作正常的、关键人员知晓的总阀门或隔离阀门以保护 ICS 免受漏水事故的损害。

b） ICS 组件集中部署的区域，如主机房、通信设备机房等水管安装不得穿过机房屋顶和活动地板下，防止雨水通过机房窗户、屋顶和墙壁渗透。

补充指导：无

控制增强：

a） 组织应使用自动化机制，在重大漏水事故时能保护 ICS 免受水灾。

B.7.15 交付和移除（PE-15）

控制：

a） 组织应对【赋值：组织定义的工业控制系统部件类型】进行授权、监视、控制，并维护相关记录。

补充指导：

a） 组织应控制交付和移除区域，如果可能，设置独立区域，以防止未授权访问。

b） 相关安全控制：CM-3、MA-2。

控制增强：无

B.7.16 备用工作场所（PE-16）

控制：

组织应：

a） 在备用工作场所，使用【赋值：组织定义的管理、运行和技术上的工业控制系统安全控制】；

b） 评估备用工作场所安全控制措施的可行性和有效性；

c） 提供安全事件发生时与信息安全人员沟通的渠道。

补充指导：无

控制增强：无

B.7.17 防雷（PE-17）

控制：

a） 组织应在放置 ICS 的设施内设置避雷装置，系统和组件集中部署区域，如主机房、通信设备机房等应满足机房相关安全标准。

补充指导：无

控制增强：无

B.7.18 电磁防护（PE-18）

控制：

a） ICS 应满足电磁防护要求，防止外界电磁干扰和设备寄生耦合干扰；电源线和通信线缆应隔

离，避免互相干扰。

补充指导：无

控制增强：无

B.7.19 信息泄露（PE-19）

控制：

a） 组织应保护 ICS 使其免遭电磁信号辐射造成的信息泄露。

补充指导：无

控制增强：无

B.7.20 人员和设备追踪（PE-20）

控制：

a） 组织应采用资产定位技术来追踪并监视控制区域内的人员活动和设备位置，以确保它们处于被允许的区域，识别需要辅助的人员，并支持应急响应。

补充指导：无

控制增强：

a） 当有违授权的访问或紧急事件发生时，电子监控机制告警。

B.8 应急计划（CP）

B.8.1 应急计划策略和规程（CP-1）

控制：

组织应：

a） 制定并发布正式的应急计划策略，内容包括目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及依从关系等；

b） 制定并发布正式的应急计划章程，以推进应急计划策略及相关安全控制的实施；

c） 按【赋值：组织定义的时间间隔】，对应急计划策略及规程进行评审和更新。

补充指导：

a） 应急计划策略和章程应与相关的法律、法规、政策、制度及标准相一致。

b） 应急计划策略可以包含在组织的通用信息安全策略中，需要时，可以为一般的安全程序或特殊 ICS 制定应急计划章程。

控制增强：无

B.8.2 应急计划（CP-2）

控制：

组织应：

a） 制定 ICS 应急计划并获得管理层批准。计划中应识别 ICS 业务应急需求、规定系统恢复优先级与目标、明确责任人；

b） 制定 ICS 灾难恢复计划并获得管理层批准。灾难恢复计划应包含：启动灾难恢复计划的事件；由自动运行变更手动运行规程；由远程控制变更为就地控制规程；响应者的角色和职责；备份及存储的规程；逻辑网络图；授权对 ICS 进行物理和逻辑访问的人员清单；联系信息（包括 ICS 厂商、网络管理员、ICS 支持人员等）；当前配置信息；部件更换要求；

c） 把计划发布到【赋值：组织定义的、由名字和角色所标识的关键持续性人员和组织单位】；

d) 按【赋值:组织定义的时间间隔】,组织评审计划。

补充指导:

a) 在系统内部或与操作设备通信过程中发生处理失败时,应执行某些预置措施,如:
   1) 向操作者发出失败警告,不采取措施;
   2) 向操作者发出失败警告,并安全关闭处理进程;
   3) 保留失败前最后的操作设置。

b) 组织应为各类系统或设施,定义连续性计划,在 ICS 内或运行设施的通信内丧失处理的事件中,ICS 执行预先确定的规程(例如,警示设施的操作员,然后空运行;警示设施的操作员,然后安全地停止工业过程;警示设施的操作员,然后在失效之前维护最后的运行设置)。

c) 考虑恢复系统状态变量,作为恢复的一部分(例如,在破坏之前,把机阀恢复到它们原始的设置)。

d) 相关安全控制:CP-6、CP-7、CP-8、CP-9。

控制增强:

a) 组织应协调应急计划与其他计划间的一致性;

b) 组织应规划应急处理时的信息处理、通信和环境等支撑能力;

c) 组织应维护应急计划,保障基本业务功能在规定的时间内保持正常运行;

d) 组织应维护应急计划,保障全部业务功能在规定的时间内保持正常运行;

e) 组织应维护硬件计划,保障基本业务功能不受影响或很少影响地异地运行;

f) 组织应维护硬件计划,保障全部业务功能不受影响或很少影响地异地运行。

B.8.3 应急计划培训(CP-3)

控制:

组织应:

a) 制定应急培训计划,并向具有相应角色和职责的工业控制系统用户提供应急培训;

b) 按【赋值:组织定义的时间间隔】或在工业控制系统变更时,对相应人员进行应急培训。

补充指导:

a) 相关安全控制:AT-2、AT-3、CP-2。

控制增强:

a) 模拟事件以配合应急培训,使得人员在危难时刻具备高效的应对能力。

b) 使用自动化机制提供更加全面、真实的培训环境。

B.8.4 应急计划测试和演练(CP-4)

控制:

组织应:

a) 测试和演练工业控制系统的应急计划;有备用处理场所的应在备用处理场所进行测试和演练;尽量采用自动机制进行。

b) 测试和演练时,应与负责相关计划的组织内各部门之间协调。

c) 测试和演练后,应将工业控制系统完整恢复和重建到已知状态。

d) 评审应急计划的测试结果;如有不合格项应启动纠正措施。

e) 按【赋值:组织定义的时间间隔】或应急计划变更时,进行【赋值:组织定义的测试和演练】。

补充指导:

a) 以多种方式测试、演练应急计划并确定潜在的不足;

b) 应急计划测试、演练的深度和精细度随着 ICS 影响等级的增加而提高;

c) 应急计划测试、演练中应对按照计划所执行的紧急操作对系统运行、财产和人员的影响程度作出判断；

d) 由于对性能、安全(safety)或可靠性具有重大影响而没有在 ICS 上测试或演练该连续性计划的情况下，组织应按裁减指导，使用合适的补偿控制(例如，使用安排的或非安排的系统维护活动，包括对 ICS 部件和系统设施的响应，作为测试或演练连续性计划的机会)。

e) 相关安全控制：CP-2、CP-3、IR-3。

控制增强：

a) 组织协调应急计划与其他相关计划相一致的测试和演练；

b) 组织可在备用系统上测试、演练应急计划，并评估备用系统的应急处理能力；

c) 组织应采用自动化机制，更彻底、有效地测试和演练应急计划；

d) 组织应设计一套完整的工业控制系统的恢复和再构造，以便了解持续性计划测试部分的【选择：安全(secure)/可靠(safe)】状态。

增强补充指导：

1) 重新设立该 ICS，涉及系统状态变量的恢复(例如，恢复阀门应具有合适的设置)。

B.8.5 备用存储设备(CP-5)

控制：

组织应：

a) 建立备用存储设备，包括可存储和恢复 ICS 备份信息的必要协议；

b) 确保备用存储设备的信息安全防护措施与主存储场所相同。

补充指导：

a) 备份的频率和将备份数据传输至备用存储设备的速率要与恢复时间目标和恢复点目标相一致。

控制增强：

a) 备用存储设备与主存储设备实施物理隔离，以防止受到同样灾难的破坏；

b) 对备用存储设备进行配置，保证其进行及时有效的恢复操作；

c) 明确当发生区域性破坏或灾难时，备用存储设备潜在的问题，并明确补救措施。

B.8.6 备用处理设备(CP-6)

控制：

组织应：

a) 建立备用处理设备，并规定 ICS 迁移至备用处理设备并重启运行的时间要求；

b) 确保迁移和恢复运行所需要的设备和供给在备用设备可用；

c) 确保备用处理设备的信息安全防护措施与主处理设备相同。

补充指导：

a) 在规定的时间内恢复操作所需的设备和供给在备用设备上可用，或者可以通过规定途径传输到备用设备上；

b) 恢复 ICS 操作的时间表要与系统建立的恢复时间目标相一致。

控制增强：

a) 备用处理设备应与主处理设备实施物理隔离，以防止受到同样灾难的破坏；

b) 组织应明确灾难发生时的迁移行动，并保障灾难发生时备用处理设备可用；

c) 组织应按业务可用性需求，开发备用设备的替代服务优先级；

d) 组织应配置备用设备为就绪状态，准备支持基本的业务功能；

e) 组织应确认备用设备提供的安全功能与主设备一致。

B.8.7 通信服务(CP-7)

控制:

a) 组织应建立备用通信服务,当主通信服务中断时,在【赋值:组织定义时间】内恢复组织基本业务运行。

补充指导:

相关控制:CP-2、CP-3、CP-6。

控制增强:

a) 组织应根据本组织的可用性要求,开发包含优先服务条款的主、备用电信服务协议;

b) 组织在选择备用电信服务时,应考虑降低单点故障,尽可能选择不同的服务商;

c) 组织应要求主、备电信服务商均提供应急响应计划。

B.8.8 系统备份(CP-8)

控制:

组织应:

a) 制定 ICS 备份策略,备份策略应当包括:备份方式、备份频率、备份内容、备份介质等;

b) 按照已制定的备份策略对用户信息、系统信息及系统文档进行备份;

c) 采取安全防护措施,保护备份信息的保密性、完整性和可用性。

补充指导:

a) 备份的频率和将备份数据传输至备用存储设备的速率要与恢复时间目标和恢复点目标相一致。

b) 完整性和可用性是系统备份信息主要关注的特性,保护备份信息以免非法泄露也非常重要。应根据存储在备份介质上的信息的类型和重要程度,确定在完整性、可用性、机密性方面需要采取的安全保护措施。

c) 系统关键数据如业务数据、设备配置数据、性能数据、告警数据等应有本地数据备份,按【赋值:组织定义的周期】进行全备。

d) 相关安全控制:CP-2、CP-6、MP-4、SC-13。

控制增强:

a) 采用合适的机制(如数字签名、加密散列)对 ICS 备份信息进行完整性保护;

b) 按预定的频率对备份信息进行测试以确保介质的可靠性和信息的完整性,保证备份信息的可用性;

c) 作为应急计划测试和演练的一部分,在恢复 ICS 功能时有选择地使用备份信息;

d) 将操作系统和其他重要 ICS 软件的备份副本存储在隔离设备上或者没有配置操作软件的存储器中;

e) 建立异地灾备中心,利用通信网络将信息实时备份到异地灾备中心;

f) 建设备份系统,实现 ICS 数据的自动备份。

B.8.9 系统恢复与重建(CP-9)

控制:

组织应:

a) 支持 ICS 的恢复与重建,在破坏或故障后能够恢复到系统原有状态;

b) 按【赋值:组织定义的、与恢复时间和恢复点的目标一致的时间间隔】,进行 ICS 中用户层信息

的恢复；

c) 按【赋值：组织定义的、与恢复时间和恢复点的目标一致的时间间隔】，进行 ICS 中系统层信息的恢复。

补充指导：

a) 安全地将 ICS 恢复与重建到原有的状态意味着所有系统参数（包括默认值或自定义值）都将被重新设置为安全值，补丁要重新安装，安全相关的配置要重新设置，应用软件和系统软件要重装，加载最近一次安全备份上的信息，系统需要进行全面测试。

b) 在某些情况下，ICS 可能不合适或不适用该控制，组织应在安全计划中记录不采用该控制的原因，必要时选取合适的补偿控制。

c) 重建 ICS，涉及系统状态变量的恢复（例如，恢复阀门应具有合适的设置）。

d) 相关安全控制：CA-2、CA-6、CA-7、CP-2、CP-6。

控制增强：

a) 应按【赋值：组织定义的时间间隔】，测试恢复信息，以验证可靠性和信息完整性；

b) 组织提供一套补偿的安全控制，在【赋值：组织定义的时间间隔】内，将系统恢复到确定的状态；

c) 组织提供一套在【赋值：组织定义的时间间隔】内，将 ICS 组件恢复到安全和运行状态；

d) 按【赋值：组织定义实时度】，配置实时或准实时的失败恢复能力；

e) 组织应对备份/恢复所用的硬件、软件和固件实施保护。

B.9 配置管理（CM）

B.9.1 配置管理策略和规程（CM-1）

控制：

组织应：

a) 制定并发布正式的配置管理策略，其中应包含目的、范围、角色、责任、管理承诺、部门间的协调以及合规性；

b) 制定并发布正式的配置管理规程，以推动配置管理策略及与相关安全控制的实施；

c) 按【赋值：组织定义的时间间隔】，对配置管理方针策略及规程进行评审和更新。

补充指导：

a) 通过该控制，为有效实现该族中的安全控制和控制增强，编制所需要的策略和规程；

b) 该策略和规程应与相关法律、制度、政策、规章、标准和指南保持一致；

c) 配置管理策略可作为组织信息安全策略的一部分；

d) 配置管理规程可针对一般性的安全程序予以开发，当需要时，可针对特殊 ICS 予以开发；

e) 在开发配置管理策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.9.2 基线配置（CM-2）

控制：

组织应：

a) 制定并维护 ICS 当前的配置基线；

b) 按【赋值：组织定义的时间间隔】或在系统发生重大变更后，对基线配置进行评审和更新；

c) 保留旧版本 ICS 基线配置，以便必要时恢复配置。

补充指导：

a) 组织应为 ICS 及与 ICS 通信和连接的部件，建立了一个基线配置；
b) 该基线配置提供了有关 ICS 的信息，如：为工作台、服务器、网络部件或移动设备所装载的标准软件；提供了有关网络拓扑以及系统体系结构中的逻辑地点等信息；
c) 该基线配置是对所构造 ICS 的最近的规格说明；
d) 维护该基线配置，涉及当该 ICS 改变时，及时创建新的基线；
e) ICS 的基线配置与组织的业务体系结构是一致的；
f) 相关安全控制：CM-3、CM-6、CM-8。

控制增强：

a) 组织应按【赋值：组织定义的时间间隔】、【赋值：组织定义的情况】所要求，在系统部件整体安装和升级等情况下评审并调整 ICS 的基线配置；
b) 组织应使用自动化机制，及时维护 ICS 配置，确保保持完整、准确、就绪可用的基线；
c) 组织应为开发和测试环境，维护一个基线配置；
d) 组织应开发并维护已授权可在组织 ICS 予以执行的【赋值：组织定义的软件程序列表】，使用拒绝授权、除此之外的允许授权策略，标识在组织 ICS 上所有被允许执行的软件；
e) 组织应开发并维护没有被授权可在组织 ICS 上执行的【赋值：组织定义的软件程序列表】，使用显式的拒绝授权策略，标识在组织 ICS 上所有被允许执行的软件；
f) 组织应保留被认为可支持回滚的、老的基线配置版本。

B.9.3 配置变更（CM-3）

控制：

组织应：

a) 批准对 ICS 的变更，并显式给出有关对安全影响的考虑；
b) 建立得到批准的、对系统的受控配置变更；
c) 保留并评审对系统的受控配置变更记录；
d) 审计与受控配置变更相关联的活动；
e) 通过【赋值：组织定义的配置变更控制元素】，按【赋值：组织定义的时间间隔】，召开会议，协调配置变更控制活动。

补充指导：

a) 组织应确定 ICS 配置变更类型；
b) 配置变更涉及到系统性的建议、理由、实施、测试、评估、审查和配置；
c) 更改配置包括组件改变、技术产品的配置修改、紧急修改和缺陷修复等；
d) 变更审计是指变更前后实施变更所需的活动；
e) 相关安全控制：CM-2、CM-4、CM-5、CM-6。

控制增强：

a) 组织应使用自动化机制，来建立对 ICS 所提议的变更之文档，通知指定的批准机构，强调【赋值：组织定义的时间周期】没有接受到的批准，禁止变更，直到接受到指定的批准，建立对 ICS 完成变更的文档；

增强补充指导：

1) 在 ICS 不支持使用自动化机制来实现配置变更控制的情况下，组织应按裁剪指导，使用非自动化的机制或规程作为一个补偿控制。

b) 在实现 ICS 变更前，组织应测试、确认这些对 ICS 的变更，并建立相应的文档；
c) 组织使用自动化机制，实现对当前 ICS 基线的变更，并通过所安装的配置库，开发调整的基线；
d) 组织要求信息安全代表，成为【赋值：组织定义的配置变更控制元素】的成员。

B.9.4 安全影响分析(CM-4)

控制:

a) 组织包括【赋值:组织定义的人员列表以及信息安全代表】应在实施变更前,应对 ICS 配置变更进行分析,并判断该变更可能带来的潜在安全影响。

补充指导:

a) 组织人员以及信息安全代表,如 ICS 安全官员;

b) 为了分析对 ICS 的变更和相关的安全细节,安全影响分析的人员应具有合适的技能和专业技术;

c) 安全影响分析还可以包括风险评估,以便确定变更的影响,确定是否需要附加的安全控制;

d) 安全影响分析是继续监视 ICS 中安全控制的一项重要活动;

e) 组织应考虑 ICS 的安全(safety)和信息安全的相互依赖性;

f) 相关安全控制:CA-2、CA-7、CM-3、CM-9。

控制增强:

a) 在新组件被安装到运行环境前,在不同的测试环境中进行测试、分析,寻找由于弱点、不足、不相容或恶意所产生的安全影响;

b) 在实施 ICS 变更后,应检测安全功能,以验证变更已被正确地实现,且满足相应系统的安全需求。

B.9.5 变更的访问限制(CM-5)

控制:

组织应:

a) 定义、记录、批准和实施与 ICS 变更相关的物理和逻辑访问限制。

b) 限制工业控制系统开发方和集成方对生产环境中的 ICS 及其硬件、软件和固件的直接变更。

补充指导:

a) 对系统硬件、软件和固件的任何变更,均可能潜在地对系统的整体安全产生重大影响;

b) 只有以启动变更为目的的、被授权的个体才允许获得对 ICS 组件的访问;

c) 为确保变更的顺利实现,应保存并维护访问记录;

d) 变更的访问限制还应包括软件库、物理和逻辑访问控制、自动化工作流、媒介库,抽象层等;

e) 在其他控制中包含了对实现该安全控制所必要的机制和过程;

f) 相关安全控制:AC-3、AC-6、CM-3、CM-6、PE-3。

控制增强:

a) 组织应使用自动化机制执行访问限制,支持执行动作的审计;

增强补充指导:

1) 在 ICS 不支持使用自动化机制来执行变更的访问限制的情况下,组织应按裁剪指导,使用非自动化的机制或规程作为补偿控制。

b) 组织应按【赋值:组织定义的时间间隔】,进行 ICS 变更的审计,分析未经授权的变更;

c) ICS 应禁止安装没有得到组织认可和批准的软件程序;

增强补充指导:

1) 在 ICS 不支持预防没有通过组织认可和批准的证书而安装软件程序的情况下,组织应按裁剪指导,使用可替代的机制或规程作为一个补偿控制(例如,审计软件安装)。

d) 对【赋值:组织定义的 ICS 部件和系统层信息】的变动,执行双人规则;

e) 组织应限制系统开发人员和集成人员,在生产环境中只有授权才能更改硬件、软件和固件以及

系统配置信息；按【赋值：组织定义的时间周期】，评审并重新评估 ICS 开发人员/集成人员的权利；

f) 组织应保护软件库，以免引入未授权的代码或恶意代码；

g) ICS 实现自动功能或机制，以发现不恰当的系统变更。

B.9.6 配置设置（CM-6）

控制：

组织应：

a) 依据安全配置检查清单，实施工业控制系统中所使用产品的配置，并实现与运行需求一致的模式；

b) 基于 ICS 的运行需求，评估 ICS 组件与已设配置存在的偏差，并对其进行标识和记录；

c) 根据相关策略和规程，监控配置设置项的变更；

d) 使用自动机制，对配置设置进行集中管理、应用和验证。不支持自动化机制的 ICS，采用其他方式进行集中管理，应用，并验证配置设置；

e) 将检测到的未授权的、与安全相关的配置变更纳入到事件响应中，以确保对被检测事件的追踪、监视、纠正，并形成可用的历史记录。

补充指导：

a) 配置设置是 ICS 中与安全相关的可配置参数；

b) 安全相关参数是那些可能影响 ICS 安全状态，或支撑其他安全控制需求的参数；

c) 组织可从 ICS 中导出组织层面的强制性配置参数；

d) 安全配置列表是一系列指令、过程或参数，用于配置 ICS 以满足组织业务需求；

e) 相关安全控制：CM-2、CM-3。

控制增强：

a) 组织应使用自动化机制，集中管理、应用并验证配置设置；

增强补充指导：

1) 在 ICS 不支持使用自动化机制来集中管理、应用和验证配置设置的情况下，组织应按裁剪指导，使用非自动化的机制或规程作为补偿控制。

b) 组织应使用自动化机制，对未授权改变【赋值：组织定义的配置设置】做出响应；

c) 组织应将发现的未授权、与安全有关的配置改变，结合到组织的安全事件响应能力，以确保每一个所发现的事件予以跟踪、纠正；

d) ICS 在引入到生产环境前，应证实其符合安全配置指南。

B.9.7 最小功能（CM-7）

控制：

组织应：

a) 对 ICS 按照仅提供最小功能进行配置，并按照【赋值：组织定义的列表】，对非必要功能、端口、协议和服务的使用进行禁止或限制；

b) 按【赋值：组织定义的时间间隔】对 ICS 进行评审，以标识和排除不必要的功能、端口、协议和服务。

补充指导：

a) ICS 往往提供额外的功能和服务；

b) 默认提供的部分功能和服务可能不是组织需要的；

c) 有时个别组件提供多个功能和服务，限制某个功能和服务可能会影响其他功能的正常运行，限

制某个功能时应仔细审查；

d) 组织应禁止无用的、未使用的物理和逻辑端口和协议，以防止未授权的连接或访问；

e) 组织可以利用网络扫描工具、IDS/IPS、防火墙等系统或工具来识别和阻止禁用功能、端口、协议和服务；

f) 相关安全控制：AC-6、CM-2、RA-5。

控制增强：

a) 为标识并消除不必要的功能、端口、协议和服务，应按【赋值：组织定义的时间间隔】对 ICS 进行风险评估；

b) 组织应使用自动化机制，应对授权软件程序、未授权软件程序的执行；

增强补充指导：

1) 在该 ICS 不使用自动化机制来预防程序执行的情况下，组织按一般的裁剪指导，使用补偿控制（例如，外部的自动化机制，规程）。

c) 组织应确保提供了满足组织需求的功能、端口、协议和服务。

B.9.8 系统组件清单（CM-8）

控制：

组织应开发并维护 ICS 组件清单，并建立相应的文档。该清单应：

a) 准确地反映当前 ICS；

b) 与 ICS 的授权边界是一致的；

c) 其粒度应满足跟踪和报告需要；

d) 包含【赋值：组织定义的、达到有效性的和可核查性信息】；

e) 对指定的组织官员的评审和审计是可用的。

补充指导：

a) 对达到有效特性的可核查性被认为是必要的信息，例如：硬件清单规格说明（制造方，类型，系列号，物理位置），软件许可信息，ICS 和部件拥有者以及网络化部件或设备，机器名和网络地址。

b) 相关安全控制：CM-2、CM-6、PM-5。

控制增强：

a) 当新组件安装、组件拆除或 ICS 调整时，调整 ICS 组件清单；

b) 组织应使用自动化机制，帮助及时、完整和准确地维护 ICS 组件清单；

c) 组织应使用自动化机制，按【赋值：组织定义的时间间隔】，检测 ICS 增加的未授权组件或设备；

d) 组织应通过名字、位置和角色等标识 ICS 组件的可核查性；

e) 组织应验证 ICS 物理边界内的所有组件或已被列入清单，作为系统的一部分，或被其他系统所知道，作为那个系统中的一部分；

f) 组织应关注在 ICS 组件清单中所有配置。

B.9.9 配置管理计划（CM-9）

控制：

组织应开发 ICS 的配置管理计划，建立相应的文档并实现该计划。该计划包括：

a) 强调角色、责任和配置管理过程和规程；

b) 应按【赋值：组织定义 ICS 配置项】，并在系统开发生存周期内，把这些配置项放入配置管理中；

c) 为标识和管理系统生存周期中的配置项，建立相应的手段。

补充指导：

a） 配置项是 ICS 中可被配置管理的项，包括硬件、软件、固件和文档；

b） 配置管理计划应满足组织配置管理策略需要，可经裁剪用于特定的 ICS；

c） 配置管理计划定义了 ICS 生命周期中配置管理的详细过程和程序；

d） 配置管理审批过程包括指派对配置变更审批负责人、配置变更影响分析者和配置变更执行者；

e） 相关安全控制：CM-2、CM-3、CM-4、CM-5、CM-8。

控制增强：

a） 组织把开发配置管理过程的责任，赋予不直接参与系统开发的组织人员。

B.10 维护（MA）

B.10.1 维护策略和规程（MA-1）

控制：

组织应：

a） 制定并发布正式的 ICS 维护策略，其中应包含目的、范围、角色、责任、管理承诺、各部门间的协调以及合规性；

b） 制定并发布正式的 ICS 维护规程，以推动系统维护策略及相关安全控制的实施；

c） 按【赋值：组织定义的时间间隔】，对维护策略和规程进行评审和调整。

补充指导：

a） 期望通过该控制，为有效实现该族中的安全控制和控制增强，编制所需要的策略和规程；

b） 该策略和规程应与相关法律、法规、制度、政策、标准和指南保持一致；

c） 维护策略可作为组织信息安全策略的一部分；

d） 维护规程可针对一般性的安全程序予以开发，当需要时，可针对特殊 ICS 予以开发；

e） 在开发配置管理策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.10.2 受控维护（MA-2）

控制：

组织应：

a） 根据产品供应商的规格说明以及组织的要求，对 ICS 系统组件的维护和修理进行规划、实施、记录，并对维护和修理记录进行评审；

b） 审批和监督所有的运维活动，无论是现场还是远程维护，无论设备是工作状态还是非工作状态；

c） 按照【赋值：组织定义的角色或人员要求】，明确批准对 ICS 或组件等设施的异地维护或维修；

d） 按照组织要求，删除异地维护或维修设施的存储资料；

e） 检查确认所有的安全控制在 ICS 或组件维护维修期间能够正常工作；

f） 产品供应方或维护方应承诺未经用户同意不得采集用户相关信息、不得远程控制用户产品；

g） 如果采用远程维护的方式，组织应根据产品的运维需求，为远程控制端口设置控制权限和控制时间窗；

h） 按【赋值：组织定义的要求】登记记录维护维修。

补充指导：

a） 创建有效的维护记录所必要的信息，包括：维护日期和时间、维护人员或组织信息、维护描述、涉及的 ICS 或组件的拆除或替换。

b） 相关安全控制：CM-3、CM-4、MA-4、SI-2。

控制增强：

a） 采用自动化的机制按【赋值：组织定义的时间间隔】来组织、规划、实施和记录维护或维修；

b） 准确、完整地记录所有的维护或维修的行动计划、要求、过程和完成；

c） 在远程维护完成后，组织应安排专人立即关闭为远程维护需求开放的权限设置。

B.10.3 维护工具（MA-3）

控制：

a） 组织应批准、控制、监测 ICS 维护工具及其使用。

补充指导：

a） 维护工具通常包含硬件、软件形式的诊断测试设备或固件程序；

b） 维护工具是恶意代码的潜在传播工具；

c） 相关安全控制：MA-2、MA-5。

控制增强：

a） 组织应检查、监督维护人员可能的对 ICS 设备维护工具的不当使用或擅自修改；

b） 组织应检查用于 ICS 设备维护的工具、诊断测试程序是否包含恶意代码；

c） 组织应防止含组织信息的 ICS 设备或组件在维护或维修时的擅自拆除，确保替换下的设备或组件包含的信息被消除，从 ICS 拆除设备或组件应获得【赋值：组织定义的个人或角色】的授权；

d） 维护工具应限制在授权人员内部使用；

e） ICS 维护工具不能收集用户信息。

B.10.4 远程维护（MA-4）

控制：

组织应：

a） 批准、监督 ICS 的远程维护或诊断行为；

b） 仅允许与组织安全策略和安全计划一致的远程维护诊断工具；

c） 在建立远程维护诊断会话时应采用强认证方式；

d） 维护远程维护诊断行为的记录；

e） 远程维护诊断行为结束时应关闭会话和网络连接。

补充指导：

a） 远程维护通常是通过外部网络或内部网络进行的维护诊断行为；

b） 为远程维护诊断行为开放的会话，往往会影响安全设置；

c） 相关安全控制：AC-2、AC-3、MA-2、MA-5、PL-2、SC-7。

控制增强：

a） 组织应根据【赋值：组织定义的审计策略】对远程维护诊断行为进行审计，并审查远程维护诊断期间所有的行为；

b） 组织应在安全策略或安全计划等文件中规范远程维护诊断行为；

c） 组织应仅在远程维护诊断期间开放 ICS 或设备的远程维护服务功能；产品或系统供应商应在交付时告知组织如何关闭/开放远程维护服务功能；

增强补充指导：

1） 在危机或紧急情况下，组织可能需要即可访问非本地维护和诊断服务，以便恢复基本的 ICS 运行或服务；

2） 在组织不必访问所需安全层上非本地维护和诊断服务的情况下，组织应按裁剪指导，使用合适的补偿控制（例如，把该维护和诊断服务的范围限制到最小的基本活动，认真监视并审计非本地维护和诊断服务）。

d） 组织应采用【赋值：组织定义的强认证机制】保护远程维护会话，并将该类会话与系统其他会话通过物理或逻辑的方式进行隔离；

e） 组织应根据【赋值：组织定义的人员或角色】对每个远程维护会话进行授权和确认；

f） 组织应采用一定的安全机制实现远程维护会话的机密性和完整性保护；

g） 在远程维护会话终止时，ICS 应进行终止确认。

B.10.5 维护人员（MA-5）

控制：

组织应：

a） 建立了维修人员授权过程，并维护授权人员或组织列表；

b） 确信维护人员具有访问授权；

c） 指派具有访问权限和技术能力的组织内部人员监督管理不具有访问权限的维护人员。

补充指导：

a） 监督人员应具有访问所维护的 ICS 的权限；

b） 监督人员应具有一定的专业技术能力，以保障对维护人员的监督需要；

c） 以前没有授权的维修人员，如制造商、供应商、系统集成商、顾问，在进行维护诊断时，可能需要访问 ICS 的授权，基于组织的风险评估策略，可以发放临时授权凭据。

d） 相关安全控制：AC-2、IA-8、MP-2、PE-2。

控制增强：

a） 对维护人员实施必要的管理，包括组织内部人员的全程陪同；

b） 开发并实现必要的安全防护措施，确保对 ICS 的维护不会对正常运行造成影响；

c） 确保维护人员进行维护诊断活动对 ICS 处理、存储和传输的信息不造成破坏性影响；

d） 确保维护人员进行维护诊断活动不会对 ICS 处理、存储和传输的机密信息造成泄露。

B.10.6 及时维护（MA-6）

控制：

a） 组织应确保获得维护支持，并保障在【赋值：组织定义的 ICS 组件失效时间】内获得配件支持。

补充指导：

a） 组织评估确定那些在其不能正常工作会给组织业务、人员和财产等造成重大影响的 ICS 组件；

b） 组织行为的获得维护支持通常是指适当的合同保障；

c） 相关安全控制：CM-8、CP-2。

控制增强：

a） 组织应【赋值：按定义的时间间隔】对 ICS 及组件进行预防性的维护诊断；

b） 组织应启用一定的机制将预防性维护诊断数据导入管理系统。

B.11 系统与信息完整性（SI）

B.11.1 系统与信息完整性策略和规程（SI-1）

控制：

组织应：

a) 制定并发布正式的系统与信息完整性策略，内容包括目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及依从关系等；
b) 制定并发布正式的系统与信息完整性规程，以推动该策略及相关安全控制的实施；
c) 按【赋值：组织定义的时间间隔】，对系统与信息完整性策略及规程进行评审和更新。

补充指导：

a) 系统与信息完整性策略和章程应与相关法律、法规、规章、制度及标准相一致。
b) 系统与信息完整性策略可以包含在组织的通用信息安全策略中，需要时，可以为一般的安全程序或特殊 ICS 制定系统与信息完整性策略和规程。

控制增强：无

B.11.2 缺陷修复（SI-2）

控制：

组织应：

a) 对系统中存在的缺陷进行标识、报告并进行纠正；
b) 在缺陷相关的软件和固件升级包在安装前，验证其有效性并评估可能带来的后果；
c) 在软件和固件升级包发布后，在适当的时间进行升级并明确升级和维护频率；
d) 将缺陷修复并入组织的配置管理过程之中。

补充指导：

a) 识别软件缺陷对 ICS 的影响，及时安装最新发布的安全相关补丁和服务包。
b) 安装补丁应该格外小心，一方面补丁可修补系统脆弱性，但同时也可能引入更大的风险；另一方面，许多 ICS 使用供应商已不再支持旧版本的操作系统，因此提供的修补程序可能不适用。在更新补丁之前一定要在测试系统中经过仔细的测试，明确可能导致的副作用，并制定详细的回退计划。
c) 补丁机制通常都是自动的，在 ICS 中，如有必要，应将补丁安装安排在停机的时候进行。
d) 相关安全控制：CA-2、CA-7、CM-3、CM-5、CM-8、MA-2、IR-4、RA-5、SA-10、SA-11、SI-11。

控制增强：

a) 统一管理缺陷修补程序和自动化升级程序；

增强补充指导：

1) 在组织不集中管理弱点修补和自动化更新的情况下，组织按一般的裁剪指导，使用非自动化机制或规程作为补偿控制。

b) 根据【赋值：组织定义的频度】采用自动化机制，根据 ICS 及组件的状态实施缺陷修复；

增强补充指导：

1) 在 ICS 不支持使用自动化机制进行并报告有关弱点修补状态的情况下，组织应按裁剪指导，使用非自动化机制或规程作为补偿控制。

c) 根据【赋值：组织定义的基准】来度量缺陷识别与缺陷修复间的关系；
d) 组织采用自动化的补丁管理工具，以方便缺陷修复。

B.11.3 恶意代码防护（SI-3）

控制：

组织应：

a) 在 ICS 网络中建立恶意代码防护机制，以检测和清除恶意代码；
b) 按照【赋值：组织定义的管理政策和程序】，更新恶意代码防护机制；
c) 按照【赋值：组织定义的安全策略】，按【赋值：组织定义的时间间隔】扫描和实时检测恶意代码；

d) 关注恶意检测和清除过程中的误操作,以及可能对 ICS 运行造成的影响。

补充指导:

a) 恶意代码防护软件版本和恶意代码库要及时更新;

b) 恶意代码防护软件和恶意代码库在安装前应经过测试;

c) 恶意代码通常由以下几种方式传播:通过电子邮件、电子邮件附件、网络访问、可移动介质,或者通过利用系统的脆弱性;

d) 在恶意代码检测和清除过程中,对系统的可用性可能会产生潜在的影响,应考虑接受误诊误测;

e) 相关安全控制:CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。

控制增强:

a) 集中管理恶意代码防护机制;

增强补充指导:

1) 在认真考虑并验证恶意代码防范机制对 ICS 运行性能没有负面影响后,才确定使用。

b) 自动升级恶意代码防护机制;

增强补充指导:

1) 在该 ICS 不支持使用自动化机制来更新恶意代码防范机制的情况下,组织应按裁剪指导,使用非自动化机制或规程作为补偿控制。

c) 防止非特权用户绕过恶意代码保护功能;

d) 组织应限制便携式设备在 ICS 中的使用;

e) 组织应根据【赋值:组织定义的周期】检测恶意代码防护机制的有效性。

B.11.4 系统监控(SI-4)

控制:

组织应:

a) 监控 ICS 运行,及时发现可能受到的攻击;

b) 标识对 ICS 的非授权访问;

c) 部署监控设备,收集【赋值:组织定义的必要信息】,跟踪组织感兴趣的行为;

d) 根据风险提示,方便提高监控级别;

e) 根据法律、法规和政策要求调整系统监控。

补充指导:

a) 系统监控包括外部和内部监控,外部监控是指对系统边界发生事件的监控,内部监控是指对系统内部发生事件的监控;

b) 系统监测能力是通过各种工具和系统来实现,包括 IDS/IPS、恶意代码监控软件、审计软件和网络监控软件等;

c) 监控工具和系统通常部署在系统边界或靠近核心系统;

d) 监控系统收集信息的粒度由组织监控目标和系统能力来决定的;

e) 组织应确保使用不对 ICS 运行产生负面影响的监视工具和技术;

f) 相关安全控制:AC-3、AC-4、AC-8、AC-17、AU-2、AU-6、AU-7、AU-9、AU-12、CA-7、IR-4、PE-3、RA-5、SC-7。

控制增强:

a) 组织应将独立的入侵检测工具通过通用协议整合到组织层面的 IDS 中;

b) 组织应采用自动化工具来支持事件的实时分析;

增强补充指导:

1） 在ICS不支持使用自动化机制来支持实时事件分析的情况下，组织应按裁剪指导，使用非自动化机制或规程作为补偿控制。

c） 组织应将入侵检测工具与访问控制、流量控制等机制整合，以快速响应攻击；

d） 系统应监控进出的非正常和未授权通信；

e） 系统应根据【赋值：组织定义的显式或潜在的威胁】进行实时报警；

f） 系统应具有防止非授权用户绕开入侵检测/防御系统的能力；

增强补充指导：

1） 在ICS不具备非特权用户规避入侵检测和预防能力的情况下，组织应按裁剪指导，使用合适的补偿控制（例如，强审计）。

g） 当【赋值：组织定义的可疑事件】发生时，系统应能够实时通知设置的干系人；

h） 组织应保护对入侵监测工具所获得的信息的未授权访问、修改和删除；

i） 组织应根据定义的周期测试和演练入侵检测工具和系统；

j） 组织应规定：加密流量是系统监控工具可见的；

k） 组织应分析边界通信流量，必要时，分析内部特定点的通信流量，以发现可能存在的异常；

l） 组织应采用自动化机制，在发生定义的不正常的活动与安全影响时，提醒安全人员；

m） 组织应分析通信流量与事件间的关系，并根据分析结果调整监控设备，以降低误报和漏报率；

n） 组织应采用无线入侵检测系统，以识别流氓的无线设备，并检测无线通信流量、无线攻击尝试和潜在违反组织无线使用策略的行为。

B.11.5 安全报警（SI-5）

控制：

组织应：

a） 接收外部组织持续的信息安全报警、警告和安全指令；

b） 必要时发布内部信息安全报警、警告和安全指令；

c） 向【赋值：组织定义的干系人】推送信息安全报警、警告和安全指令；

d） 按照既定的时间框架实现安全指令。

补充指导：

a） 安全报警和安全指令由国家互联网应急响应中心（CNCERT/CC）等机构发布；

b） 由于这些安全报警和安全指令可能对组织ICS产生一定的影响，遵守这些报警和指令，实施相应的防护是必须的；

c） 相关安全控制：SI-2。

控制增强：

a） 组织采用自动化机制及时获取组织所需的这些安全报警和安全指令。

B.11.6 安全功能验证（SI-6）

控制：

组织应：

a） 验证在异常发生时，ICS按照定义的动作实现了准确的安全功能；

b） 在系统启动或重启时实施安全验证或者按【赋值：组织定义的时间间隔】实施安全验证；

c） 将失败的测试情况通知相关人员。

补充指导：

a） 安全功能验证适应于所有的安全功能；

b） 对于那些不能够执行自动化测试的安全功能，组织可以实现补偿安全控制，或显式地接受不

需要执行验证的风险；

c) 一般地，不建议依据标识的异常就宕机或重启动 ICS；

d) 相关安全控制：CA-7、CM-6。

控制增强：

a) 系统应提供自动安全验证失败通知功能；

b) 系统应提供自动安全验证支持功能；

c) 应向组织相关负责人报告安全功能验证结果。

B.11.7 软件和信息完整性(SI-7)

控制：

a) 组织应检测与保护软件和信息，以防止对软件和信息未经授权的更改。

补充指导：

a) 对 ICS 采用完整性校验应用软件，以查找信息篡改、错误和删除的迹象；

b) 采用软件工程实践中现成的通用完整性机制，如奇偶检验、循环冗余检验、散列加密等；

c) 采用工具自动监控完整性信息；

d) 在检测到完整性受到破坏后具有恢复的措施；

e) 组织应确保使用的完整性验证应用没有负面影响 ICS 的运行性能；

f) 相关安全控制：SA-12、SC-8、SC-13、SI-3。

控制增强：

a) 组织应按【赋值：组织定义的频度】重新评估软件和信息的完整性；

b) 组织应提供自动化机制，在软件和信息完整性异常时通知相关负责人；

增强补充指导：

1) 在组织不使用自动化工具来通告完整性不适用的情况下，组织应按裁剪指导，使用非自动化机制或规程作为补偿控制。

c) 组织应集中管理完整性验证工具；

d) 在传输和使用过程中，组织应提供明显的防篡改包。

B.11.8 输入验证(SI-8)

控制：

a) 组织应验证授权人员输入信息的有效性。

补充指导：

a) 对输入信息进行语法和语义检查，包括字符集、长度、数值范围和可接受的值等；

b) 通过检查防止非法命令被有意/无意地输入到系统，造成系统运行异常；

c) 相关安全控制：CM-3、CM-5。

控制增强：

a) 提供手动重写机制用于输入验证，确保该功能仅用于授权人员，并对该功能进行审计；

b) 确保按【赋值：组织定义的时间间隔】对输入验证错误的审查；

c) 在收到无效输入时，确保 ICS 按照预定的方式运行；

d) 对无效输入的响应不应该影响正常运行时序；

e) 按组织预定义的格式和内容限制系统输入。

B.11.9 错误处理(SI-9)

控制：

ICS 应：

a） 确定潜在的安全相关错误条件；

b） 在错误日志中产生足以用于纠错的错误信息；

c） 仅向授权人员显示错误信息。

补充指导：

a） 组织应仔细考虑错误信息的结构和内容；

b） 在组织策略和运行需求的指导下，错误信息的内容可被系统标识和处理；

c） 敏感信息，如账号、密码等不应出现在错误日志中；

d） 相关安全控制：AU-2、AU-3。

控制增强：无

B.11.10 信息处理和留存（SI-10）

控制：

a） 组织应根据可相关法律、法规、规章、制度、标准以及运行要求，对 ICS 的输出信息进行处理和留存。

补充指导：

a） 信息处理和留存应涵盖信息的全生命周期。

b） 相关安全控制：AC-16、AU-5、AU-11、MP-2、MP-4。

控制增强：无

B.11.11 可预见失效预防（SI-11）

控制：

组织应：

a） 确定在特定运行环境中信息组件的平均故障时间；

b） 提供可替代的工业控制系统组件、对组件进行激活和建立主备切换的机制。

补充指导：

a） 虽然平均故障时间是可靠性问题，本控制关注提供安全功能的特定系统组件；

b） 主备切换应不影响系统的可靠性、稳定性和安全性；

c） 除切换期间或维护原因，备用系统应一直可用；

d） 相关安全控制：CP-2、CP-10、MA-6。

控制增强：

a） 组织应在不迟于平均故障时间内，或【赋值：组织定义的时间间隔】内，实现主备组件的切换；

b） 组织应禁止在无监督的情况下实施切换；

c） 组织应在定义的时间间隔内手动完成主备组件的切换；

d） 如果检测到系统组件故障，组织应确保备用系统组件成功并透明地在定义的时间段内发挥作用。

B.11.12 输出信息过滤（SI-12）

控制：

a） 组织应确认软件和应用输出的信息与期望的内容相吻合。

补充指导：

a） 重点是检测无关的内容，防止多余的内容被显示。

b） 相关安全控制：SI-3、SI-4。

控制增强：无

B.11.13 内存防护（SI-13）

控制：

a） ICS 应执行安全保护措施，以防代码在内存中进行未授权的执行。

补充指导：

a） 部分攻击行为专注于非执行区域内存攻击；内存防护的安全保障措施包括，数据执行预防和地址空间布局随机化处理。

b） 相关安全控制：SC-3。

控制增强：无

B.11.14 故障安全程序（SI-14）

控制：

a） 组织应定义 ICS 发生故障时的安全处理程序。

补充指导：

a） 故障条件包括，关键系统组件之间的通信损失，系统组件和操作设备之间的通信故障等。

b） 故障安全程序包括，提醒操作人员，并提供后续步骤的具体指令（什么也不做，恢复系统设置，关闭程序，重新启动系统，或与指定的人员联系等）。

c） 相关安全控制：CP-12、CP-13、SC-24、SI-13。

控制增强：无

B.11.15 入侵检测和防护（SI-15）

控制：

a） 组织应在 ICS 安全建设方案中考虑部署入侵检测和防护系统（IDS/IPS）。

补充指导：

a） 部署 IDS/IPS 产品应不影响 ICS 正常运行。

b） 相关安全控制：PL-2。

控制增强：无

B.12 介质保护（MP）

B.12.1 介质保护策略和规程（MP-1）

控制：

组织应：

a） 制定并发布正式的介质保护策略，其中应包含目的、范围、角色、责任、管理承诺、各部门间的协调以及合规性；

b） 制定并发布正式的介质保护规程，以推动介质保护策略以及相关安全控制的实施；

c） 按【赋值：组织定义的时间间隔】，对介质保护策略和规程进行评审和更新。

补充指导：

a） 通过该控制来有效实现介质保护族中安全控制和安全增强的策略和规程；

b） 应与相关的法律、法规、制度、政策和标准保持一致；

c） 介质保护策略可作为组织信息安全策略的一部分；

d） 介质保护规程一般可针对安全程序予以开发，也可针对特殊的 ICS 予以开发；

e) 在开发系统和服务获取策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.12.2 介质访问（MP-2）

控制：

a) 组织应规定介质的访问策略，严格控制对组织介质的访问。

补充指导：

a) 介质包括数字介质和非数字介质，其中，数字介质包括：硬盘、光盘、软盘、U 盘等，非数字介质包括文档、缩微胶片等；

b) 相关安全控制：AC-3、IA-2、MP-4、PE-2、PE-3、PL-2。

控制增强：

a) 默认禁止访问；

b) 加密保护。

B.12.3 介质标记（MP-3）

控制：

a) 组织应按照【赋值：组织定义的规范】标记介质的分发范围、访问要求、处理要求、销毁要求等。

补充指导：无

控制增强：无

B.12.4 介质存储（MP-4）

控制：

组织应：

a) 在受控区域中，采取物理控制措施并安全地存储磁带、外置/可移动硬盘、U 盘或其他 Flash 存储介质、软盘、CD、DVD 等介质。

b) 定义设施内用来存储信息和存放工业控制系统的受控区域。

c) 为这些介质提供持续保护，直到利用经批准的设备、技术和规程对其进行破坏或净化。

补充指导：

a) 介质包括数字介质和非数字介质。

b) 相关安全控制：CP-6、MP-2。

控制增强：

a) 加密存储，物理安全保护；

b) 严格访问控制。

B.12.5 介质传输（MP-5）

控制：

组织应：

a) 在受控区域之外传递磁带、外置/可移动硬盘、U 盘或其他 Flash 存储介质、软盘、CD 和 DVD 时，采用适当的安全防护措施进行保护和控制。

b) 维护介质在受控区域之外传递过程的可核查性。

c) 对介质传递相关活动进行记录。

d) 只允许授权人员参与介质传递有关的活动。

补充指导：

a) 介质包括数字介质和非数字介质。

b) 相关安全控制：CP-6、MP-2、MP-3、MP-4。

控制增强：

a) 组织控制区域外加强介质保护；

b) 文档化介质传输相关活动；

c) 加强介质传输过程中对委托人管理；

d) 在介质传输过程中进行加密处理。

增强补充指导：

1) 在 ICS 不支持密码机制的情况下，组织应按裁剪指导，使用补偿控制（例如，实现物理安全措施）。

B.12.6 介质销毁（MP-6）

控制：

组织应：

a) 根据介质销毁有关规定和标准，在介质报废、组织控制外使用、回收使用前，采用销毁技术和规程对介质进行销毁。

b) 所采用的销毁机制的强度、覆盖范围应与介质中信息的安全类别或级别相匹配。

补充指导：

a) 该控制适用于组织所有的介质；

b) 销毁前应确保介质内的信息不能恢复或重建；

c) 销毁技术，包括清除、密码清除、物理破坏，以防止信息泄露；

d) 组织确定合适的销毁方法是必要的，其他的方法不能应用于介质销毁；

e) 组织应使用批准的销毁技术和程序；

f) 相关安全控制：MA-2、MA-4、RA-3。

控制增强：

a) 介质销毁前的审阅、批准、跟踪、文件与验证机制；组织审查和批准的介质销毁，以确保符合组织政策，跟踪、文件销毁行动，并验证该销毁过程的合规性。

b) 组织测试销毁设备和销毁程序，以验证预期的处理结果。

c) 组织按定义的方式销毁便携式存储设备。

d) 组织应按国家相关法律、法规规定销毁涉密和受控设备。

B.12.7 介质使用（MP-7）

控制：

a) 组织应采取安全防护措施限制或禁止在 ICS 系统和组件中介质（包含数字介质和非数字介质）的使用。

补充指导：

a) ICS 中介质包括数字介质和非数字介质；

b) 数字介质包括磁带、外置/可移动硬盘、U 盘或其他 Flash 存储介质、软盘、CD 和 DVD 等；

c) 非数字介质包括文件、文档或胶片；

d) 该控制应包括具有拍照、存储功能的智能手机、平板电脑、阅读器、相机等；

e) 组织应采用技术和非技术手段（如：政策、流程和行为规范等）来规范介质的使用；

f) 相关安全控制：PL-4。

控制增强：

a) 组织应禁止未标识的便携式设备在ICS使用；
b) 组织应禁止使用不方便实施销毁和净化处理的介质。

B.13 事件响应(IR)

B.13.1 事件响应策略和规程(IR-1)

控制：

组织应：

a) 制定并发布正式的的事件响应策略，其中应包含目的、范围、角色、责任、管理承诺、各部门间的协调以及合规性；
b) 制定并发布正式的事件响应规程，以推动事件响应方针策略及与相关安全控制的实施；
c) 按【赋值：组织定义的时间间隔】，对事件响应策略和规程进行评审和调整。

补充指导：

a) 有效实现该族中的安全控制和控制增强，编制所需要的策略和规程。
b) 该策略和规程应与应用的法律、法规、政策、规章、制度、标准和指南是一致的。
c) 事件响应策略可作为组织信息安全策略的一部分。
d) 事件响应规程可针对一般性的安全程序予以开发；也可针对特殊ICS予以开发。
e) 在开发配置管理策略中，组织的风险管理战略是一个重要的因素。

控制增强：无

B.13.2 事件响应培训(IR-2)

控制：

组织应：

a) 制定事件响应培训计划，并按【赋值：组织定义的时间间隔】对ICS用户进行符合其角色和责任的事件响应培训；
b) 按【赋值：组织定义的时间间隔】或在ICS发生变更时向ICS用户提供符合其角色和责任的事件响应培训。

补充指导：

a) 事件响应培训包括用户培训—标识和报告来自内外源的嫌疑活动。
b) 相关安全控制：AT-3、CP-4、IR-8。

控制增强：

a) 组织把模拟事件和事件响应结合起来进行培训，以便支持人员在危机情况下的有效响应；
b) 组织使用自动化机制，提供更全面、更真实的培训环境。

B.13.3 事件响应测试与演练(IR-3)

控制：

组织应：

a) 按【赋值：组织定义的时间间隔】以【赋值：组织定义的测试和演练方法】测试ICS的响应能力，以判断事件响应的有效性，并记录测试结果。
b) 评审事件响应测试和演练的结果；如有不合格项应启动纠正措施。

补充指导：

a) 事件响应培训包括用户培训—标识和报告来自内外源的嫌疑活动。
b) 相关安全控制：CP-4、IR-8。

控制增强：

a） 组织使用自动化机制，更全面、更有效地测试或演练事件响应能力。

增强补充指导：

1） 自动化机制可以提供更全面、更有效的测试或演练事件响应能力，因为自动化机制可以提供更完整的覆盖事件响应问题，选择更真实的测试或演练场景和环境，以及更有效地强调响应能力。

B.13.4 事件处理（IR-4）

控制：

组织应：

a） 具有应对安全事件的事件处理能力，包括准备、检测和分析、控制、消除和恢复。

b） 协调事件处理活动与应急规划活动。

c） 将当前事件处理活动的经验，纳入事件响应规程、培训及测试/演练，并相应地实施变更。

补充指导：

a） 与事件有关的信息可以从一些不同的源中获取，包括但不限于：审计监视，网络监视，物理访问监视和用户报告。

b） 相关安全控制：CP-2、CP-4、IR-2、IR-3。

控制增强：

a） 组织使用自动化机制，例如在线的事件管理系统，支持事件处理过程；

b） 组织关注 ICS 的动态重新配置，作为事件响应能力的一部分；

增强补充指导：

1） 动态重新配置，例如：路由规则的改变，访问控制列表的改变，入侵检测系统参数的改变，以及防火墙和网关过滤规则的改变。

c） 组织标识事件类别（例如：有目标的有意攻击，无目标的有意攻击，由于设计或实现中的错误和忽略），并定义响应中所采取的合适动作，确保使命/业务运行的继续；

d） 组织建立事件信息和单个事件响应的联系，以实现对有关事件做出及时正确的响应；

e） ICS 一旦出现【赋值：组织定义的安全损坏列表】中的损坏，组织为此实现可配置的能力，使其停止运行。

B.13.5 事件监控（IR-5）

控制：

a） 组织应跟踪和记录 ICS 安全事件，并建立相应的文档。

补充指导：

a） 与事件有关的信息可以从不同的源中获得，包括但不限于：审计监视、网络监视、物理访问监视和用户或管理人员的报告。

b） 应当引起重视或进行重点监控的事件包括：网络流量突然增大、磁盘空间溢出或空闲磁盘空间明显减少、异常高的 CPU 使用率、新用户账号创建、试图或实际使用超级管理员级的账号、账户锁定、用户不工作时，账号仍在使用、清除日志文件、以不常用的大量事件塞满日志文件、防病毒或 IDS 警报、不可用的防病毒软件和其他安全控制措施、不期望的补丁变更、非法外联、请求系统信息、配置设置的非期望更改、非期望的系统关闭或重启等。

c） 相关安全控制：AU-6、IR-6、IR-7、SC-5。

控制增强：

a） 组织使用自动化机制，支持安全事件的跟踪，支持事件信息的收集和分析。

B.13.6 事件报告(IR-6)

控制:

组织应:

a) 在规定时间内,向组织的事件响应部门报告可疑的安全事件。

b) 向相关主管部门报告安全事件信息。

补充指导:

a) 通过该控制来强调组织内特定的事件报告需求以及正式的事件报告需求;

b) 报告的安全事件类型,报告的内容和时间,以及指定的报告机构,应与可用的国家法律、法规、制度、标准和指南是一致的;

c) 相关安全控制:IR-4、IR-5。

控制增强:

a) 应使用自动化机制,支持安全事件的报告;

b) 向合适的组织官员,报告 ICS 中与所报告的安全事件相关的弱点、不足和脆弱性。

B.13.7 事件响应支持(IR-7)

控制:

a) 组织应提供事件响应支持资源,集成组织事件响应能力,即为 ICS 用户提供设备和支持,以便处理和报告安全事件。

补充指导:

a) 在组织中,事件响应支持资源的实现可能涉及一个支持小组。

b) 相关安全控制:AT-2、IR-4。

控制增强:

a) 组织使用自动化机制,增加与事件响应有关信息和支持的可用性;

b) 组织在其事件响应能力和外部提供方之间,建立一种直接协作的关系;向外部提供方,标识组织的事件响应小组成员。

B.13.8 事件响应计划(IR-8)

控制:

组织应:

a) 制定事件响应计划,该计划应包括:实施路线图;事件响应的结构和组织;满足组织的有关使命、规模、结构和功能的特殊要求;定义可报告事件;定义必要的资源和管理支持,以维护和增强事件响应能力;

b) 评审和批准事件响应计划,并向组织内事件响应人员发布;

c) 按【赋值:组织定义的时间间隔】评审该事件响应计划;

d) 针对系统/组织的变更或事件响应计划在实施、执行或测试中遇到的问题,更新计划;

e) 将事件响应计划的变更通报组织内相关部门和人员;

f) 使事件响应计划处于受控状态。

补充指导:

a) 组织应有一个正式的、集中的、协调一致的途径来响应事件;

b) 组织有关事件响应的使命、战略和目标,帮助确定其事件响应能力的结构;

c) 相关安全控制:AT-2、IR-4、SA-9。

控制增强:无

B.14 教育培训(AT)

B.14.1 教育培训策略和规程(AT-1)

控制:

组织应:

a) 制定并发布正式的教育培训策略,其中应包含目的、范围、角色、责任、管理承诺、部门间的协调以及合规性;

b) 制定并发布正式的教育培训规程,以推动教育培训策略及相关安全控制的实施;

c) 按【赋值:组织定义的时间间隔】,对教育培训策略和规程进行评审和调整。

补充指导:

a) 为有效实现该族中的安全控制和控制增强,编制所需要的策略和规程。

b) 该策略和规程应与应用的法律、制度、政策、规章、标准和指南是一致的。

c) 学习与培训策略可作为组织信息安全策略的一部分。

d) 学习与培训规程可针对一般性的安全程序予以开发;当需要时,可针对特殊 ICS 予以开发。

e) 在开发配置管理策略中,组织的风险管理战略是一个重要的因素。

控制增强:无

B.14.2 安全意识培训(AT-2)

控制:

组织应:

a) 为包括管理员、高级管理层、承包商在内的 ICS 用户提供安全意识培训;

b) 在新用户的培训中纳入安全意识培训;

c) 按【赋值:组织定义的时间间隔】或系统变更需要培训时,进行安全意识培训,安全意识培训内容应包括 ICS 特定安全方针策略,安全操作程序,ICS 安全趋势和安全漏洞等。

补充指导:

a) 组织应根据安全策略的需要以及 ICS 安全需求,以确定适当的安全意识培训内容,内容包括信息安全、用户操作维护安全和应对可能的安全事件处理技术等;

b) ICS 安全意识培训包括 ICS 特定策略、标准的操作规程、安全趋势以及脆弱性的评审以及它们的定期评审;

c) ICS 的意识培训大纲应与组织所建立的有关安全意识和培训策略的需求相一致;

d) 培训时机包括:新用户培训、ICS 调整或【赋值:组织定义的培训周期】;

e) 相关安全控制:AT-3、AT-4、PL-4。

控制增强:

a) 组织开展包括实际练习的安全意识培训以模拟实际的安全攻击;

b) 组织开展包括识别和报告内部潜威胁的安全意识培训。

B.14.3 基于角色的安全培训(AT-3)

控制:

组织应:

a) 为 ICS 中的安全角色和具有安全职责的人员提供安全培训;

b) 在新用户的培训中纳入安全培训;

c) 按【赋值:组织定义的时间间隔】或系统变更需要培训时,进行安全培训,安全培训内容应包括

ICS 特定安全方针策略，安全操作程序，ICS 安全趋势和安全漏洞等。

补充指导：

a) 组织在分配个人的角色和责任，进行 ICS 授权访问或满足组织的特定安全要求时，进行基于角色的安全培训，并确定适当的安全培训内容；

b) 安全培训包括初始的 ICS 特定策略、标准的操作规程、安全趋势以及脆弱性的评审以及它们的定期评审；

c) ICS 的培训大纲应与组织所建立的有关安全培训策略的需求相一致；

d) 培训时机包括：在对 ICS 进行授权访问或执行人员任务分配时、在 ICS 调整后或者根据【赋值：组织定义的培训周期】；

e) 相关安全控制：AT-2、AT-4、PL-4。

控制增强：

a) 组织根据初始或定义的频度的人员和角色培训；

b) 组织开展包括实际操作的安全培训，以增强安全培训的目标；

c) 组织应向内部人员提供安全培训，使能够识别 ICS 存在的异常行为。

B.14.4 安全培训记录（AT-4）

控制：

组织应：

a) 记录并监视 ICS 安全培训活动，包括基本的安全意识培训和具体的 ICS 安全培训；

b) 在【赋值：规定的时间】内保留培训记录。

补充指导：

a) 应维护安全培训记录。

b) 相关安全控制：AT-2、AT-4。

控制增强：无

B.15 标识与鉴别（IA）

B.15.1 标识与鉴别策略和规程（IA-1）

控制：

组织应：

a) 制定并发布正式的标识与鉴别策略，内容包括目的、范围、角色、责任、管理承诺、组织实体间的关系等；

b) 制定并发布正式的标识与鉴别规程，以推动标识与鉴别方针策略及与相关安全控制的实施；

c) 按【赋值：组织定义的时间间隔】，对标识与鉴别策略及规程进行评审和更新。

补充指导：

a) 标识与鉴别策略和规程应与相关的法律、法规、政策、策略及标准相一致；

b) 标识与鉴别策略可以包含在组织的通用信息安全策略中，也为一般的安全程序或特殊 ICS 制定标识与鉴别规程。

控制增强：无

B.15.2 组织内用户的标识与鉴别（IA-2）

控制：

a) 组织应唯一标识和鉴别组织用户（员工、供应商人员及访客等）或代表该用户的进程。

补充指导：

a） 用户的所有访问都要被唯一的标识和鉴别，确保用户名具有唯一性，且专供用户个人使用；

b） 当用户功能可以归为同一类（比如控制室操作员）时，用户身份鉴别与认证可以基于角色、组或者设备；

c） 对于一些 ICS，操作员及时响应很重要，身份识别与认证要求绝不能影响系统的本地紧急响应，对这些系统的访问可以通过合适的物理安全措施来限制；

d） 对于一定的 ICS，操作员的即刻交互能力是至关重要的；

e） ICS 的本地紧急措施并非受到标识与鉴别需求的束缚，对这些系统的访问可受到合适的物理安全控制的限制；

f） 在某些情况下，组织认为不适用该控制，可以在安全计划中记录原因，并选取必要的补偿控制。例如，为了建立远程访问，可能需要远程人员的人工语音鉴别，需要一些人工的动作；

g） 相关安全控制：AC-2、AC-3、IA-4、IA-5。

控制增强：

a） 对已授权账户的网络访问，使用多因子鉴别；

b） 对未授权账户的网络访问，使用多因子鉴别；

c） 对已授权账户的本地访问，使用多因子鉴别；

d） 对未授权账户的本地访问，使用多因子鉴别；

增强补充指导：

1） 在该 ICS 不支持多因子鉴别的情况下，组织应按裁剪指导，使用合适的补偿控制（例如，实现物理安全措施）。

e） 对未授权账户的本地和网络访问，使用口令或个人标识码；

f） ICS 对本地访问，使用口令或个人标识码；

g） 组织应仅当与个体或特定鉴别员一起使用时，才使用组鉴别；要求在使用组鉴别机制前，要用个体鉴别机制对个体进行鉴别；

h） 对未授权账户的远程访问，使用多因子鉴别，其中一个因子要由与该 ICS 分离的设备提供。

B.15.3 设备标识与鉴别（IA-3）

控制：

a） 在建立一个或多个本地、远程、网络连接前，组织应【赋值：定义的特定设备和设备类型列表】。

补充指导：

a） 要求逐一予以标识与鉴别的设备，可以按类型或按特定设备予以定义，或按组织认为合适的组合类型和设备予以定义；

b） 针对标识和组织鉴别解决方案（例如，国家标准 GB/T 28455—2012《信息安全技术 引入可信第三方的实体鉴别及接入架构规范》等），ICS 一般使用强制访问控制（MAC）或传输控制协议来标识和鉴别本地网和广域网上的设备；

c） 设备鉴别机制所要求的强度，是由 ICS 的安全分类来确定的；

d） 在 ICS 不支持设备标识与鉴别的情况下，组织应按裁剪指导，使用合适的补偿控制（例如，实现物理安全措施）；

e） 相关安全控制：IA-4、IA-5。

控制增强：

a） 在建立远程网络连接前，ICS 应以密码技术为基础，使用设备之间的双向鉴别来鉴别设备；

b） 在建立网络连接前，ICS 以密码技术为基础，使用设备之间的双向鉴别来鉴别设备；

c） 组织针对动态地址分配，标准化动态主机控制协议（DHCP）的专用信息以及赋予设备的时间；

并当把这些信息赋予一个设备时，对专用信息进行审计。

B.15.4 标识符管理（IA-4）

控制：

组织应：

a) 按照授权策略分配个人、组、角色或设备标识符；

b) 选择用于识别个人、组、角色或设备的标识符；

c) 将标识符分配给指定的个人、组、角色或设备；

d) 在【赋值：组织定义的时间间隔】内防止对标识符的重用；

e) 在【赋值：组织定义的时间间隔】内清除不活动的标识符。

补充指导：

a) 通用设备标识符，包括强制访问控制（MAC）或互联网协议（TCP/IP）的地址，或设备独特的令牌标识符；

b) 管理用户标识符，不可用于共享的 ICS 账户（例如：贵宾账户和匿名账户）；

c) 用户标识符是 ICS 的一个与个体相关联的账户的名字，在这样实例中，账户管理活动（AC-2）更强调标识符管理；

d) 在用户职能作为单一小组（例如，控制屋操作员）的情况下，用户标识可以是基于角色的、基于小组的、或是基于设备的；

e) 相关安全控制：AC-2I、A-2、IA-3。

控制增强：

a) 应禁止使用 ICS 账户标识符作为用户电子邮件账户的公共标识符；

b) 应要求接受用户 ID 和口令的登记，应具有监督人员的授权，并在指定登记授权前由人来完成；

c) 应要求多种形式个体身份的认证，如对该登记授权给出有文件的证据，或给出文件以及生物特征的组合；

d) 应按【赋值：组织定义的方式】标识用户状态的特征，唯一地标识用户，以此来管理用户标识符；

e) ICS 动态地管理标识符、属性以及相关联的访问授权。

B.15.5 鉴别符管理（IA-5）

控制：

组织应：

a) 在初始鉴别分发时验证鉴别接收对象（个人、组、角色或设备）的身份；

b) 确定【赋值：组织定义的初始鉴别的内容】；

c) 确保鉴别对于其预期使用具有足够强的机制；

d) 建立和实现管理规程，覆盖鉴别的初始分发、丢失或受损处置以及收回过程；

e) 在工业控制系统安装之前变更鉴别的默认内容；

f) 建立鉴别的最小和最大生存时间、限制以及再用条件；

g) 按【赋值：组织定义的时间间隔】变更或更新鉴别；

h) 保护鉴别内容，以防未授权泄露和更改；

i) 要求个人采取由设备或特定安全措施来保护鉴别；

j) 在组/角色账户的成员发生变化时变更这些账户的鉴别。

补充指导：

a) ICS 认证设备包括：PKI 证书、生物特征、口令、密钥卡等；

b） 许多 ICS 设备和软件通常采用厂商缺省认证证书以进行安装和配装，应及时更换；

c） 相关安全控制：AC-2、AC-3、AC-6、CM-6、IA-2、IA-4。

控制增强：

a） 对于基于 PKI 的鉴别，ICS 应：

1） 针对一个接受的可信物，通过构造一个具有状态信息的认证路径，来确认证书；

2） 对对应的私钥，执行授权访问；

3） 把所认证的身份映射为用户账户；

b） 组织要求接受【赋值：组织定义的鉴别符类型或特定鉴别符的注册过程】，在由指定组织官员赋予注册授权之前由人来承担；

c） 组织使用自动化工具来确定该鉴别符对抵御企图揭示或损坏该鉴别符的攻击而言是否具有充分的强度；

d） 组织要求 ICS 部件供应商或制造者在交付之前，提供唯一的鉴别符或改变默认的鉴别符；

e） 对于基于口令的鉴别，ICS 应：

1） 实施按组织就敏感情况、字符个数、大写小写字符和数字的混合，以及特殊字符等方面定义的需求的最小口令复杂性；

2） 当创建新口令时，实施按【赋值：组织定义的字符个数】；

3） 在口令存储和传输中，对口令加密处理；

4） 实施按【赋值：组织定义的口令最大和最小生存期】的限制；

5） 实施按【赋值：组织定义的生成次数】，禁止口令复用；

f） 组织保护鉴别符，使其相称于所访问信息的保密性和敏感性；

g） 组织确保口令没有被嵌入在访问脚本中或存储在功能键上；

h） 由于存在一些在多个 ICS 上拥有账户的个体，因此组织采取【赋值：组织定义的措施】，管理破坏性风险；

增强补充指导：

当一个个体在多个 ICS 上拥有账户的时候，存在以下风险：一旦一个账户被破坏，并且该个体是使用同样的用户标识符和鉴别符，那么其他账户也将被破坏。可选的方案包括但不限于：

1） 在所有的系统上有同样的标识符，但鉴别符不同；

2） 在每一系统上有不同的用户标识符号和鉴别符号；

3） 使用某种形式的单一签名机制；

4） 在所有系统上使用某种形式的一次性口令。

i） 组织应规定对授权账户的网络访问，使用【赋值：组织定义的一次性鉴别机制】；

j） 组织应规定对未被授权账户的网络访问，使用【赋值：组织定义的一次性鉴别机制】。

B.15.6 鉴别反馈（IA-6）

控制：

a） ICS 应隐蔽鉴别过程期间鉴别信息的反馈，以保护该信息免遭未授权个体的利用。

补充指导：

a） 来自 ICS 的反馈不提供可使未授权用户损害鉴别机制的信息。

b） 相关安全控制：PE-18。

控制增强：无

B.15.7 密码模块鉴别（IA-7）

控制：

a) ICS 使用满足相关法律、法规、政策、规定、标准和指南等需求的鉴别相关的密码模块。

补充指导：

a) 密码模块应符合相关密码管理部门规定和标准；

b) 应在认真考虑安全需要以及对系统性能的潜在结果之后，确定要使用的密码技术。例如，组织考虑由于使用密码技术而引入的潜在因素是否负面影响了该 ICS 的运行性能；

c) 相关安全控制：AC-2、IA-2、IA-4。

控制增强：无

B.15.8 组织外用户的标识与鉴别（IA-8）

控制：

a) ICS 应逐一标识和鉴别非组织的用户或标识和鉴别代表非组织用户所执行的过程。

补充指导：

a) 非组织用户是组织内用户以外的 ICS 用户。非组织用户访问 ICS 的身份验证需要保护专有或隐私相关的信息。组织使用风险评估方法，以确定身份验证的需求，并考虑可扩展性、实用性和安全性的平衡。

b) 相关安全控制：AC-2、IA-2、IA-4、MA-4、RA-3、SA-12。

控制增强：

a) ICS 接受并鉴别其他相关机构发布的单子标识与鉴别；

b) ICS 只接受经权威机构批准的第三方认证；

c) 组织只采用相关权威机构批准的 ICS 组件第三方认证。

B.16 访问控制（AC）

B.16.1 访问控制策略和规程（AC-1）

控制：

组织应：

a) 制定并发布正式的访问控制策略，内容包括目的、范围、角色、责任、管理承诺、组织实体间的协调关系以及依从关系等；

b) 制定并发布正式的访问控制章程，以推动访问控制方针策略及与相关安全控制的实施；

c) 按【赋值：组织定义的时间间隔】，对访问控制策略及规程进行评审和更新。

补充指导：

a) 访问控制策略和章程应与相关的法律、法规、规章、制度、策略及标准相一致；

b) 访问控制策略可以包含在组织的通用信息安全策略中，也可为一般的安全程序或特殊 ICS 制定访问控制规程。

控制增强：无

B.16.2 账户管理（AC-2）

控制：

a) 组织应管理 ICS 账户，包括建立、激活和修改、审核、失效和删除账户；

b) 组织应按【赋值：组织定义的时间间隔】审核 ICS 账户。

补充指导：

a) 账户管理包括账户类型的识别（个人、组、系统），组成员条件的确定和相关授权的分配；

b) 账户类型可以是基于角色、基于设备、基于属性等；

c) 应识别 ICS 的授权用户和特定的访问控制权利；
d) 应明确地授权和监督客人和匿名账户的使用；
e) ICS 使用者或用户属性发生变化时，应通知账户管理人；
f) 在为物理访问 ICS(例如，工作站，硬件部件，场站设备)预先定义了一些特权账号的情况下，或在 ICS 不支持账号管理(例如，一些远程终端单元，基站)的情况下，组织按一般的裁减指导，使用合适的补偿控制(例如，提供增强的物理安全、人员管理、入侵检测和审计措施)；
g) 应要求产品或设备供应商告知系统存在的默认账户和口令；
h) 应删除、禁用或对默认账户提供安全维护，严格限制默认账户的访问权限，重命名系统默认账户，修改默认账户的默认口令；
i) 相关安全控制：AC-3、AC-4、AC-5、AC-6、AC-10、AC-17、AC-19、AC-20、AU-9、IA-2、IA-4、IA-5、IA-8、CM-5、CM-6、CM-11、MA-3、MA-4、MA-5、PL-4、SC-13。

控制增强：

a) 应使用自动机制来支持对 ICS 账户的管理。对于某些 ICS 部件(如现场设备)，账户管理的自动机制不可用的情况下，组织按裁减指导，使用非自动化机制或规程作为一个补偿控制；
b) 在规定的时间周期后应及时删除临时的和非常时期的账户；
c) 在规定的时间周期后及时删除非活动的账户；
d) 应使用自动机制来审计账户的创建、修改、失效和终止等活动，需要时通知相关人员。

B.16.3 强制访问控制(AC-3)

控制：

a) ICS 应根据应用策略执行指定的系统访问控制授权。

补充指导：

a) 组织应采用访问控制策略(如：基于身份的策略、基于角色的策略、基于规则的策略)和相关访问控制机制(如：访问控制列表、访问控制许可、密码技术)实现 ICS 用户与对象(包括设备、文件、程序、进程、域)间的访问控制；
b) 为提供更佳的安全，除在 ICS 层面实现访问控制外，必要时还应在应用层面实现强制访问控制；
c) 针对所有主体和客体，应实施基于角色的访问控制策略；
d) 针对 ICS 范围内属性相同的主体和客体，执行统一策略；
e) 应限制将信息传递给未授权的主体和客体；
f) 应限制将权限授予给未授权的主体和客体；
g) 应限制对主体、客体、工业控制系统或其组件安全属性的变更；
h) 应限制对访问控制策略的更改；
i) 强制访问控制机制不应对 ICS 正常运行产生不利影响；
j) 相关安全控制：AC-2、AC-4、AC-5、AC-6、AC-16、AC-17、AC-18、AC-19、AC-20、AC-21、AC-22、AU-9、CM-5、CM-6、CM-11、MA-3、MA-4、MA-5、PE-3。

控制增强：

a) 基于【赋值：组织定义的权利要求】的组织策略和规程，执行二元访问授权；
b) 在【赋值：组织规定的用户集和资源集】上，执行【赋值：组织定义的非自主访问控制策略】；
c) ICS 执行自主访问控制(DAC)策略；
d) 除了安全状态外，应禁止 ICS 访问【赋值：组织规定的、与安全有关的信息】；
e) 在非安全的地方，加密或存储【赋值：组织定义的非在线的关键或敏感的信息】。

B.16.4 信息流强制访问控制(AC-4)

控制:

a) ICS 应按应用策略,执行控制系统中的信息流和系统间的信息流授权。

补充指导:

a) 信息流控制规定了信息在系统内和系统间流转路径;

b) 信息流控制策略和执行机制通常采用制定源和目的方式;

c) 信息流控制通常基于信息和信息路径的特征;

d) 该控制指导配置其他安全控制的授权;

e) 相关安全控制:AC-3、AC-17、AC-19、AC-21、CM-6、CM-7、SA-8、SC-2、SC-5、SC-7、SC-18。

控制增强:

a) ICS 应使用信息对象、源对象、目的对象等显式的安全属性,作为流控制决策的基础,执行信息流控制;

b) ICS 应使用受保护的过程域,作为流控制决策的基础,执行信息流控制;

c) ICS 应基于特定策略,执行动态的系统信息流控制;

d) 防止来自旁路的内容检测机制的加密数据;

e) 执行【赋值:组织定义的在其他数据类型】中嵌入数据类型的限制;

f) 执行元数据上的信息流控制;

g) 使用硬件机制,执行【赋值:组织定义的信息流】控制;

h) 使用【赋值:组织定义的安全策略】,执行信息流控制;

增强补充指导:

1) 【赋值:组织定义的安全策略过滤器】,应包括:欺诈词过滤器、文件类型检测过滤器、结构化数据过滤器、非结构化数据过滤器、元数据内容过滤器、隐藏内容过滤器等;

2) 结构化数据可被应用和个体予以理解。

i) 当 ICS 不能做出信息流控制决策时,系统使用人对【赋值:组织定义的安全策略过滤器】进行评审;

j) 应为授权管理员提供了一种使用【赋值:组织定义的安全控制过滤器】的能力;

k) 应为授权管理员提供了配置【赋值:组织定义的安全控制过滤器】的能力,以便支持不同安全策略;

l) 在不同安全域间传送信息时,ICS 应按数据类型的规约和用法,标识信息流;

m) 在不同安全域间传送信息时,ICS 应把信息分解为与策略有关的一些子部分;

n) 在不同安全域间传送信息时,ICS 应把数据结构和内容限制为【赋值:组织定义的安全策略】需求的策略过滤器;

增强补充指导:

1) 限制文件长度,限制允许的枚举,限制字符集,限制模式以及其他数据对象,这样可以减少潜在恶意的范围,减少不被许可的内容。限制的例子包括但不限于:字符数据域仅包含可打印的 ASCII;字符数据域仅包含字母、数字;字符数据域不包含特定字符;基于【赋值:组织定义的安全策略】,执行域的最大长度和文件长度。

o) 在不同安全域间传送信息时,ICS 应按安全策略检测不被许可的信息,并阻止传输这些信息;

增强补充指导:

1) 支持这一增强的措施有:检测所有传输的信息是否是恶意的;针对传输的信息,实现特定词列表搜索;对元数据(例如:安全属性)应用以上同样的保护措施。

p) ICS 执行互连系统上信息的安全策略;

增强补充指导：

1） 在不同安全策略的互连系统间传输信息，可能存在破坏安全策略的风险。由于安全策略的破坏不可能绝对地予以阻止，因此信息拥有者所提出的策略指导往往是在互连系统的策略增强点上予以实现。

2） 当需要时，特定体系结构方案是强制的，以便减少可能没被发现的脆弱性。例如，体系结构方案包括：禁止在互连系统之间信息传输（即：仅实现访问，单向传输机制）；使用硬件机制来执行单一信息流决策；实现完整测试、再分等机制，以便重新赋予安全属性以及相关联的安全标记。

q） ICS 应逐一标识并鉴别信息传输源域和目的域；把安全属性和信息进行绑定，支持信息流策略的实施；跟踪安全属性绑定以及信息传输相关联的问题。

B.16.5 职责分离（AC-5）

控制：

组织应：

a） 在必要时，分离个体的职责，以便防止恶意活动；

b） 建立职责分离文档；

c） 通过 ICS 访问授权，实现分离的职责。

补充指导：

a） 根据需要建立适当的职责分离来消除在个人职责方面的利益冲突。

b） 限制和控制特殊权限的分配和使用，根据用户的角色分配权限，实现用户的权限分离。如实现管理用户、操作系统特权用户的权限分离。

c） 某些情况下，ICS 不合适或不支持实施职责分离，应记录不实施的原因，并选择使用合适的补偿控制（例如，提供增强的人员安全和审计）。

d） 组织认真考虑单个个体执行多重关键角色的合适性。

e） 相关安全控制：AC-3、PL-2。

控制增强：无

B.16.6 最小授权（AC-6）

控制：

a） 组织应使用最小授权概念，只允许被授权的用户（和代表用户的过程）对完成所赋予的任务是必要的且符合组织使命和业务的功能进行访问。

补充指导：

a） 针对特定的职责和 ICS（包括特定的协议、端口和服务），利用最小特权的概念，依照必要的风险评估来充分地降低运行、资产和个人的风险；

b） 该控制定义的访问授权，是由 AC-3 实现的；

c） 组织依据风险评估，针对特定的职责和工业控制系统，使用最小授权这一概念，目的是为了准确地缓解组织运行和资产、个体其他组织和国家的风险；

d） 仅授予管理用户所需的最小权限；

e） 在 ICS 不支持特权区分的情况下，组织应按裁减指导，选择使用合适的补偿控制（例如，提供增强的人员安全和审计）；

f） 组织应认真考虑单个个体执行多重关键特权的合适性；

g） 相关安全控制：AC-2、AC-3、AC-5、CM-6、PL-2。

控制增强：

a) 组织应显式地对【赋值:组织定义的安全功能】(硬件、软件和固件中所开发的安全功能)和安全有关的信息列表授予访问权。

增强补充指导:

1) 安全功能的例子有:建立系统账户,配置访问授权(即允许,特权),设置要审计的事件以及设置入侵检测参数。

2) 显式地被授权的人员,例如有:安全管理员、系统和网络管理员、系统安全官员、系统维护人员、系统程序设计人员和其他被赋予特权的用户。

b) 组织要求系统具有访问【赋值:组织定义安全功能和安全有关的信息列表】的 ICS 账户的用户或角色,当访问其他系统功能时,使用非授权的账户或角色,并且对于这样的功能,如果方便的话,审计任意对授权账户或角色的使用。

c) 组织按【赋值:运行需要而定义的授权要求】,授权网络访问,并在安全计划中为这样访问记录理由。

d) ICS 提供分离的过程域,以便能精细地分配用户授权。

e) 组织限定指定的系统管理人员,向 ICS 的超级用户账户授权。

增强补充指导:

1) 超级用户账户一般被描述为市场上不同类型现成操作系统的"根"或"管理员"。

2) 限制系统授权的例子有:在配置组织的 ICS 时,对于那些日常工作的用户就不授予访问超级用户账户的权利。

3) 在这一增强控制中的应用中,组织可以区分为本地 ICS 账户所赋予的权利和为域账户所赋予的权利。其中域账户是由组织提供的,从而可仍然能控制系统针对关键安全参数的配置,以及为了充分缓解风险所必要的其他配置。

f) 组织应禁止向组织之外的用户授权访问 ICS。

B.16.7 失败登录控制(AC-7)

控制:

a) ICS 应在【赋值:组织定义的时间周期】内,按【赋值:组织定义的次数】,限制用户连续无效的访问尝试;

b) 自动按【赋值:组织定义的时间周期】,锁死账户,直到管理员予以释放;

c) 当未成功尝试超出最大次数时,依据【赋值:组织定义的延迟算法】,延迟下一次登入执行。

补充指导:

a) 由于可能存在服务拒绝,因此在【赋值:组织定义的时间周期】后,自动锁死通常是临时的,并可能自动释放;

b) 如果要选择延迟算法,那么组织应基于部件的能力,为不同的 ICS 选择使用不同的算法;

c) 对不成功登入尝试的响应,可以通过系统或通过应用层予以实现;

d) 某些情况下,ICS 不支持账号、节点锁定、延迟登录,或存在重大的负面性能影响,组织应按裁减指导,选择使用合适的补偿控制(例如,建立日志或记录所有不成功的登录尝试,当组织定义的数个连续的无效访问尝试予以执行时,通过报警或其他手段,警示 ICS 的安全人员);

e) 相关安全控制:MP-5、MP-6、SC-13。

控制增强:

a) 系统自动锁死账户或节点,直到不成功尝试超出最大次数时才予以释放;

b) 系统为插入在 ICS 中的移动设备提供附加的保护,即在【赋值:组织定义的连续不成功登入】尝试后,净化来自移动设备的信息。

B.16.8 系统使用提示(AC-8)

控制:

a) 设置鉴别警示信息,在允许用户访问前,显示经过批准的、校准过的通告信息,并保持在屏幕上,直到用户采取了明确的行动。

补充指导:

a) 显示只有授权的用户才能访问计算机的一般性的告警通知。

b) 描述未授权访问可能导致的后果。

c) 在ICS不支持系统使用提示的情况下,组织应按裁减指导,使用合适的补偿控制(例如,在ICS设施上公布物理通告)。

d) 相关安全控制:PL-2。

控制增强:无

B.16.9 以前访问提示(AC-9)

控制:

a) ICS应通知成功登入(访问)的用户,以及最后一次登入的日期和时间。

补充指导:

a) 期望该控制覆盖两个方面:传统的系统登入以及以其他类型的结构化配置(例如,面向服务的体系结构)而出现的对ICS的一般性访问。

b) 在该ICS不支持以前访问提示的情况下,组织按裁减指导,使用合适的补偿控制。

控制增强:

a) ICS通知成功登入/访问的用户,以及自最后一次成功登入/访问以来未成功登入/访问尝试的次数;

b) ICS通知在【赋值:组织定义的时间周期】内,选择:成功登入/访问;未成功登入/访问的尝试的用户和次数;

c) ICS通知在【赋值:组织定义的时间周期】内,对用户账户的安全设置改变的用户。

B.16.10 并发会话控制(AC-10)

控制:

a) ICS按【赋值:组织定义的当前会话数】,限制每一系统账户的当前会话数量。

补充指导:

a) 对于整个ICS的账户,组织可通过账户类型或账户组合,定义当前最大会话数量。

b) 该控制强调了对一个给定ICS账户的当前会话,并没有强调单个用户通过多系统账户的当前会话。

c) 在ICS不支持并发会话控制的情况下,组织应按裁减指导,使用合适的补偿控制(例如,提供更强的审计措施)。

d) 相关安全控制:PL-2。

控制增强:无

B.16.11 会话锁定(AC-11)

控制:

a) ICS应在【赋值:组织定义的不活动时间周期】后,或接受的用户请求,通过会话锁,禁止对系统进一步访问;

b） 应保持会话锁，直到用户通过标识和鉴别规程，重新建立访问。

补充指导：

a） 会话锁定是当用户停止工作，离开 ICS 所采取的一种临时措施，但并不希望中断会话；ICS 使用会话锁定以防止访问已规约的工作站或节点；

b） 组织可以在操作系统层或应用层实现这会话锁；

c） 会话锁定不能替代断开系统登入；

d） ICS 在指定的工作站和节点所【赋值：定义的时间段】后，自动激活会话锁定；

e） 在某些情况中，不建议为 ICS 操作员的工作站/节点设立会话锁定（例如，当在紧急情况中需要操作员即可予以响应的话）；

f） 在 ICS 不支持会话锁定的情况下，组织按裁减指导，使用合适的补偿控制（例如，提供更强的物理安全、人员安全以及审计措施）；

g） 相关安全控制：AC-7、PL-2。

控制增强：

a） 当在具有显示屏的设备上启动 ICS 会话锁机制时，该机制应以公共可观察的模式放在相关联的显示屏上，隐藏该屏幕上以前可见的信息。

B.16.12 会话终止（AC-12）

控制：

a） 在【赋值：组织定义的条件或需要终止会话的事件】触发时自动终止用户会话。

补充指导：

a） 该控制终止用户端发起的逻辑会话，而 SC-10 终止物理会话，如：网络连接；

b） 会话终止与用户的逻辑会话相关的所有进程，除非是由用户（即会话所有者）在会话结束后继续运行的特定进程；

c） 需要自动终止会话的条件或事件包括：组织定义的用户活动期间，特定类型的事件，限制使用时间等；

d） 相关安全控制：SC-10。

控制增强：

a） ICS 应提供用户端发起会话的退出能力，无论是否认证后获得【赋值：组织定义的信息资源】；

b） ICS 应向用户显式地提示会话已被安全终止。

B.16.13 未标识鉴别的许可行为（AC-13）

控制：

组织应：

a） 在 ICS 内设置未标识鉴别用户的特定行为动作；

b） 在 ICS 安全规程中记录并说明不需要进行标识鉴别用户动作的原因。

补充指导：

a） 该控制主要用于某些特定情况下，不需进行标识和鉴别即可操作 ICS；

b） 组织应允许有限数量的不需要进行标识和鉴别的操作；

c） 组织也可以标注出那些通常需要标识和鉴别，在紧急情况下，可以绕过标识和鉴别的行为；

d） 相关控制：CP-2、IA-2。

控制增强：

a） 无需标识和鉴别的组织许可行为仅用于实现组织业务目标。

B.16.14 远程访问(AC-14)

控制：

a) 组织应授权、监督和控制所有对 ICS 的远程访问。

补充指导：

a) 只有在必要时，并经过批准和认证的情况下才可以进行远程访问；

b) 远程访问要采取多因素认证；

c) 在 ICS 没有实现这一控制的任何或所有部件的情况下，组织按裁减指导，使用其他机制或规程作为一个补偿控制；

d) 相关安全控制：AC-2、AC-3、AC-18、AC-19、AC-20、CA-3、CA-7、CM-8、IA-2、IA-3、IA-8、MA-4、PE-17、PL-4、SC-10、SI-4。

控制增强：

a) 组织利用自动机制来监督和控制远程访问方式；部分 ICS 可能不支持远程访问；

增强补充指导：

1) 在 ICS 不支持使用自动化机制来监控远程访问的情况下，组织按裁减指导，使用非自动化机制或规程作为补偿控制。

b) 利用密码技术来保护远程访问会话的机密性和完整性，防止鉴别信息在网络传输过程中被窃听和篡改；

增强补充指导：

1) 相关密码技术的采用绝对不能影响 ICS 正常运行；

2) ICS 的安全目的通常按可用性、完整性和保密性这一次序的优先级。在认真考虑安全需要以及有关系统性能的潜在结果的基础上，确定要使用的密码技术；

3) 在 ICS 不支持使用密码机制来保护远程会话保密性和完整性的的情况下，或由于对安全(safety)、性能或可靠性具有重大的负面影响，或 ICS 部件不能使用密码机制的情况下，组织按裁减指导，使用合适的补偿控制(例如，为远程会话提供更强的审计，或限制关键人员远程访问特权)。

c) ICS 通过【赋值：组织定义的访问控制点的数目】，路由所有远程访问；

d) 组织仅迫于运行方面的要求，授权执行远程访问并访问与安全有关的信息，远程授权访问要在工业控制系统安全计划中记录其理由；

e) 工业控制系统使用鉴别和加密技术保护对系统的无线访问；

f) 组织监控对工业控制系统的授权远程访问，包括按【赋值：组织定义的时间间隔】，扫描未授权的无线访问点；

g) 对那些不期望使用的无线访问，在工业控制系统部件中嵌入的内部无线网络发挥作用或部署前，组织应关闭或取消其功能；

h) 组织应禁止用户独自配置无线网络；

i) 组织确保用户保护了有关远程访问的信息，以免造成未授权的使用和信息泄露；

j) 组织确保远程访问【赋值：组织定义的安全功能和安全有关信息的列表】的会话，使用了附加的【赋值：组织定义的安全措施】，并进行了相应的审计；

k) 除了特定运行需求所显式标识的部件外，组织应断掉工业控制系统中点对点无线网络的能力；

l) 除了特定运行需求所显式标识的部件外，组织断掉被认为是不安全的网络协议。

B.16.15 无线访问(AC-15)

控制:

组织应:

a) 建立无线访问使用规范;

b) 监控对 ICS 的无线访问;

c) 强化对无线访问需求管理,如非必须,关闭无线访问。

补充指导:

a) 无线技术包括但不限于:802.11x、蓝牙、微波等;

b) 无线网络使用提供凭证保护和相互验证等功能协议,如 EAP/TLS、PEAP 等;

c) 某些情况下,无线信号可能辐射到组织控制以外区域;

d) 相关安全控制:AC-2、AC-3、CM-8、IA-2、PL-4、SI-4。

控制增强:

a) 使用基于【选择:用户和/或设备】的认证和加密技术保护无线接入 ICS;

b) 组织监测未经授权的无线连接,包括扫描未经授权的无线接入点,对发现的未经授权的连接采取适当的措施;

c) 必要时,组织应禁止 ICS 组件内部嵌入式无线网络功能;

d) 组织应禁止用户自主配置无线网络功能;

e) 组织应管制控制范围内的无线网络。

B.16.16 移动设备的访问控制(AC-16)

控制:

组织应:

a) 建立移动设备使用规范;

b) 授权移动设备连接到 ICS 应满足组织规范要求;

c) 监控非授权移动设备接入 ICS;

d) 强化移动设备接入 ICS 需求管理;

e) 禁用 ICS 自动执行移动设备可执行代码功能;

f) 对到组织认为存在风险的区域的个人发放特殊配置的移动设备;

g) 对到组织认为存在风险的区域的进行检查或维护的移动设备采用领取归还方式。

补充指导:

a) 移动设备包括但不限于:移动硬盘、USB 设备、笔记本电脑、智能手机等;

b) 组织控制的移动设备包括:组织内部设备,组织有权要求提供特定安全要求的设备;

c) 移动设备的使用规范包括:配置管理、认证和授权、实施强制性保护软件、扫描设备的恶意代码、更新防病毒软件、扫描关键软件更新和修补程序、进行操作系统和其他常驻软件完整性检查、禁用不必要的硬件等;

d) 组织移动设备带出和返还策略包括:确定关注点、定义设备所需配置、带出前检查和返还后检查等;

e) 在 ICS 没有实现这一控制的任何或所有部件的情况下,组织按裁减指导,使用其他机制或规程作为补偿控制;

f) 相关控制包括:AC-3、AC-7、AC-18、AC-20、CA-9、CM-2、IA-2、IA-3、MP-2、MP-4、MP-5、PL-4、SC-7、SC-43、SI-3、SI-4。

控制增强:

a) 组织应限制 ICS 内可读写、可移动设备的使用；
b) 组织应禁止 ICS 内使用个人所有的可移动设备；
c) 组织应禁止 ICS 内使用未标记的可移动设备；
d) 组织应禁止在涉密系统中使用非涉密移动设备；
e) 组织采用【选择：全设备加密、容器加密】来保护【赋值：组织定义的移动设备】信息的机密性和完整性；
f) 组织应考虑关闭不用的或不必要的 I/O 端口；
g) 组织应禁止使用移动设备中的无线功能。

B.16.17 外部系统的使用(AC-17)

控制：

组织应建立一些术语和条件，允许授权个体：

a) 从外部访问工业控制系统；
b) 使用外部系统处理、存储和传输组织信息。

其中，所建立的术语和条件，要与其他组织所拥有的、运行的、维护的外部系统所建立的任何可信关系是一致的。

补充指导：

a) 外部系统是组织边界外的系统，通常组织对这些系统的安全性不具体控制；
b) 外部系统包括个人或其他组织拥有的系统和设备；
c) 相关安全控制：AC-3、AC-14、CA-3、PL-4、SA-9。

控制增强：

a) 组织应禁止授权的个体使用外部系统来访问工业控制系统，或处理、存储、传输组织收集的信息，除非存在以下情况：
   1) 可以验证外部系统上所要求的安全控制的实现，像组织工业控制系统安全策略和安全计划中所规约的那样；
   2) 已批准了工业控制系统与外部系统的连接，或批准了组织内实体使用外部系统进行处理的协议。
b) 组织对授权个体有关使用外部信息系统上组织控制的可移动媒介，施加一些限制。

B.16.18 信息共享(AC-18)

控制：

组织应：

a) 促进信息共享，并监控授权用户是否按【赋值：组织定义的共享策略】将信息共享给其他用户；
b) 采用【赋值：组织定义的自动化机制或手动过程】，以帮助用户在决策信息共享。

补充指导：

a) 相关安全控制：AC-3。

控制增强：

a) 信息共享|自动决策支持

ICS 基于共享伙伴的访问权限和被共享信息的共享属性来执行自动共享决策。

b) 信息共享|信息检索

ICS 执行【赋值：定义组织信息共享的限制】来实现信息检索服务。

B.17 审计与问责(AU)

B.17.1 审计与问责策略和规程(AU-1)

控制:

组织应:

a) 制定并发布正式的安全审计策略,内容包括目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及依从关系等;

b) 制定并发布正式的安全审计章程,以推动审计和可核查性方针策略及与相关安全控制的实施;

c) 按【赋值:组织定义的时间间隔】,对审计和可核查性方针策略及规程进行评审和更新。

补充指导:

a) 安全审计策略和章程应与相关的法律、可执行命令,指令、策略、规则及标准相一致。

b) 安全审计策略可以包含在组织的通用信息安全策略中,作为其一部分。

c) 相关安全控制:PM-9。

控制增强:无

B.17.2 审计事件(AU-2)

控制:

a) 组织应明确规定审计事件范围和审计内容。审计范围应覆盖到ICS的每个用户,审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。

补充指导:

a) 安全审计的目的是为了记录那些与ICS安全相关的重要的审计事件,应该指明哪些ICS部件需要执行审计行为;

b) 现场设备审计事件应包括:用户登录、退出事件,连接超时事件,配置变更,时间/日期变更,审计接入,ID/密码创建和修改等;

c) 审计行为会影响ICS的效率,因此,应该基于风险评估确定哪些事件需要进行常规审计,哪些事件需要相应于特殊环境的审计;

d) 大多数ICS的审计发生在应用层上;

e) 相关安全控制:AC-6、AU-3、MA-4、MP-2、SI-4。

控制增强:

a) 应提供编辑审计记录的能力,这些记录来自多重部件,这些部件遍布于系统的逻辑层面、物理层面及相关于时序的审计痕迹中;

b) 提供对审计事件选择的集中管理能力,事件选择被单独的系统部件所审计;

c) 组织应定义审计事件进行【赋值:组织定义的时间间隔】的审核和升级。

B.17.3 审计记录的内容(AU-3)

控制:

a) 审计记录应包含足够的信息,以便确定什么事件发生了、事件的来源、事件的结果等。

补充指导:

a) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

b) 相关安全控制:AU-2、AU-8。

控制增强：

a） 审计记录应使用主题、类型、位置等信息标识审计事件；

b） 组织应集中管理审计内容。

B.17.4 审计存储能力（AU-4）

控制：

a） 组织应规定【赋值：审计记录的保存期限】，并保证审计记录的存储空间。

补充指导：

a） 为方便安全事故提供事后调查和满足信息保留要求和规定，应在指定时间内保存审计记录，直到这些记录不会被行政、法律、审计或者其他操作目的所使用。审计记录和报表保存时间应不少于三个月，现场设备应至少支持 2 048 个事件记录；

b） 应分配足够的审计记录存储空间，减少空间不足的可能性；

c） 相关安全控制：AU-2、AU-5、AU-6、AU-7。

控制增强：无

B.17.5 审计失效响应（AU-5）

控制：

ICS 应：

a） 对于审计处理失效的事件，向【赋值：组织定义的人员】报警；

b） 采取赋值：【选择：组织定义的动作】，例如：停止系统的运行，重写原有的审计记录，停止生成新的审计记录等。

补充指导：

a） 审计处理失效包括软硬件错误、审计获取机制失败、审计存储空间达到或超出极限等；

b） 组织可针对不同审计处理失效（例如，由于类型、位置、严重程度或这些因素的组合），选择定义附加的措施；

c） 该控制应用于每个审计数据存储库（即存储审计记录的 ICS 部件），应用于组织的整个审计存储能力（即组合了所有审计数据存储库）；

d） 一般地，不能在 ICS 上执行审计记录的处理，而在隔离的信息系统上进行处理；

e） 在 ICS 不支持审计的情况下，包括对审计失效的响应，组织应按裁剪指导，使用合适的补偿控制（例如，在隔离的信息系统上提供审计能力）；

f） 相关安全控制：AU-4、SI-12。

控制增强：

a） 对审计处理失效｜审计存储能力的响应

在【赋值：组织定义的时间段】内，当分配给审计记录的存储量达到【赋值：组织定义的最大审计记录存储容量】的某一百分比时，ICS 向【赋值：组织定义的人员、角色或岗位】提供一个警示。

b） 对审计处理失效｜实时报警的响应

当【赋值：组织定义的、要求实时报警的审计失效事件】发生时，ICS 在【赋值：组织定义的实时报警时间段】内，向【赋值：组织定义的人员，角色和岗位】发出报警。

c） 对审计处理失效｜可配置的流量阈值的响应

ICS 执行可配置的流量阈值，反映对审计能力的限制，并【选择：拒绝、延迟】网络流量超出这些阈值。

d） 对审计处理失效｜失效宕机的响应

当发生【赋值：组织定义的审计事件】发生时，ICS 调用【选择：完全宕掉系统，部分宕掉系统；降低运

行模式，仅具有有限可用的业务处理能力】，除非存在一种可选的审计能力。

B.17.6 审计信息的监控、分析和报告（AU-6）

控制：

a） 组织应按【赋值：组织定义的时间间隔】对审计记录数据进行分析，并生成审计报告。

补充指导：

a） 应按【赋值：组织定义的时间间隔】的回顾、分析审计记录，这些记录包含了不恰当或不寻常的行为；

b） 调查可疑行为和入侵行为；

c） 生成审计报表，并向相关人员报告这些事件，同时采取必要的措施；

d） 相关安全控制：AC-2、AC-3、AT-3、AU-7、CM-5。

控制增强：

a） 采用自动的机制，将审计监控、分析、报告联结成一个完整的审计过程；

b） 采用自动的机制，对存在安全隐患的不安全或者异常行为向安全人员发出警告。

B.17.7 审计简化和报告生成（AU-7）

控制：

a） 提供审计简化和报告生成能力。

补充指导：

a） 审计简化和报告生成能力，可有效支持 AU-6 中所描述的及时的审计评审、分析和报告需求，支持安全事件之后的事实研究；

b） 审计简化和报告工具并不警示原始的审计纪律；

c） 审计简化和报告生成一般不在 ICS 上执行，而在隔离的信息系统上进行；

d） 在某些情况下，ICS 不支持审计简化和报告生成，组织应按裁剪指导，使用合适的补偿控制（例如，在隔离的信息系统上提供审计能力）；

e） 相关安全控制：AU-6。

控制增强：

a） ICS 基于可选的事件准则，为关切的事件提供自动化处理审计记录的能力。

B.17.8 时间戳（AU-8）

控制：

a） 应使用内部时钟，为审计记录生成时间戳。

补充指导：

a） 由 ICS 生成的审计事件应包括日期和时间等时间信息。

b） 相关安全控制：AU-3。

控制增强：

a） ICS 按【赋值：组织定义的时间间隔】，同步内部系统时钟。

B.17.9 审计信息保护（AU-9）

控制：

a） 应保护审计信息和审计工具，避免受到未授权访问、修改、删除或覆盖等行为的破坏。

补充指导：

a） 审计信息包括审计 ICS 行为的所有信息，包括审计记录、审计设置、审计报告等。

b） 相关安全控制：AC-3、AC-6、MP-2、MP-4、PE-2。

控制增强：

a） ICS 在所执行的硬件上，在一次性写入的媒介上生成审计记录；

b） ICS 按【赋值：组织定义的时间间隔】，把审计记录反馈到一个与被审计系统不同的系统或媒介上；

c） ICS 使用加密机制来保护审计记录和审计工具的完整性；

d） 组织对访问审计功能的授权，只限制为一个具有特权的用户子集；保护审计记录的非本地访问，仅为授权的账户，并执行授权的功能。

B.17.10 抗抵赖（AU-10）

控制：

a） 应防止个体否认执行过一个特定的动作。

补充指导：

a） 审计信息包括审计 ICS 行为的所有信息，包括审计记录、审计设置、审计报告等。

b） 相关安全控制：SC-12、SC-8。

控制增强：

a） ICS 在所执行的硬件上，在一次性写入的媒介上生成审计记录；

b） ICS 按【赋值：组织定义的时间间隔】，把审计记录反馈到一个与被审计系统不同的系统或媒介上；

c） ICS 使用加密机制来保护审计记录和审计工具的完整性；

d） 组织对访问审计功能的授权，只限制为一个具有特权的用户子集；

e） 保护审计记录的非本地访问，仅为授权的账户，并执行授权的功能。

B.17.11 审计信息保留（AU-11）

控制：

a） 组织应按【赋值：组织定义的时间长度】保留审计记录，提供事件方式时回顾、分析支持。

补充指导：

a） 组织保留审核记录，直至确定不再需要；

b） 审计记录通常根据事件发生时所采取的动作和响应过程进行分类；

c） 相关安全控制：AU-4、AU-5。

控制增强：无

B.17.12 审计生成（AU-12）

控制：

a） ICS 应提供可审计事件的审计记录的生成能力；

b） 应允许【赋值：组织定义的人员或角色】对特定组件可审计事件进行审计；

c） 应对 AU-2 定义的事件按照 AU-3 所需的内容生成审计记录。

补充指导：

a） ICS 组件均应可以对事件生成审计记录；

b） 生成的审计日志应是一组事件列表；

c） 生成的审计日志通常是一个事件的子事件；

d） 在 ICS 不支持使用自动化机制来生成审计记录的情况下，组织应按裁剪指导，使用非自动化的机制或规程作为一个补偿控制；

e) 相关安全控制：AC-3、AU-2、AU-3、AU-6、AU-7。

控制增强：

a) 应按时间相关将审计记录从【赋值：组织定义的系统组件】转换为系统的（逻辑或物理）审计跟踪记录；

b) 应产生系统的（逻辑或物理）审计跟踪记录的标准化格式；

c) 提供在【组织内定义的时间范围】内，进行 ICS 审核的能力。

B.18 系统与通信保护（SC）

B.18.1 系统与通信保护策略和规程（SC-1）

控制：

组织应：

a) 制定并发布正式的系统与通信保护策略，其中应包含目的、范围、角色、责任、管理承诺、各部门间的协调以及合规性；

b) 按【赋值：组织定义的时间间隔】，对系统与通信保护策略和规程进行评审和调整。

补充指导：

a) 期望通过该控制，为有效实现该族中的安全控制和安全控制增强，编制所需要的策略和规程。

b) 该策略和规程应与应用的法律、法规、规章、制度、政策、标准和指南是一致的。

c) 系统与通信保护策略可作为组织信息安全策略的一部分。

d) 系统与通信保护规程可针对一般性的安全程序予以开发；当需要时，也可针对特殊 ICS 予以开发。

e) 在开发系统与通信保护策略中，组织的风险管理策略是一个重要的因素。

控制增强：无

B.18.2 应用分区（SC-2）

控制：

a) ICS 应能分离用户功能和系统管理功能。

补充指导：

a) ICS 管理功能，例如管理数据库、网络部件、工作站或服务器所必要的功能，并一般需要授权用户的访问。

b) 用户功能与系统管理功能的分离，或是逻辑的，或是物理的，并可通过使用不同的计算机、不同的集中处理单元、不同的操作系统、不同的网络地址等方法实现，以及通过这些方法的组合或其他合适的方法。

c) 在 ICS 没有把用户功能与信息系统管理职能予以隔离的情况下，组织应按裁剪指导，使用补偿控制（例如，提供更强的审计措施）。

d) 相关安全控制：SA-4、SA-8、SC-3。

控制增强：

a) ICS 禁止在一般（即非授权）用户的接口上，渗透与 ICS 管理有关的功能。

增强补充指导：

1) 期望通过该控制增强确保管理选择对一般用户是不可用的。例如，不给出管理选择，直到用户依据管理授权已合适地建立了一个会话。

B.18.3 安全功能隔离(SC-3)

控制:

a) ICS 应能隔离安全功能和非安全功能。

补充指导:

a) 通过隔离边界的手段(以划分和域来实现之),ICS 可以隔离安全功能和非安全功能,控制对执行这些安全功能的硬件、软件和固件的访问,并保护其完整性。

b) ICS 为每一个执行的过程,维护一个隔离的执行域。

c) 在 ICS 不支持安全功能隔离的情况下,组织应按裁剪指导,使用补偿控制(例如,提供更强的审计措施,限制网络连接)。

d) 相关安全控制:AC-3、AC-6、SA-4、SA-5、SA-8、SA-13、SC-2、SC-7。

控制增强:

a) ICS 实现基本的硬件隔离机制,以支持安全功能的隔离。

b) ICS 把执行访问控制策略和信息流控制策略的安全功能与非安全功能隔离开来,与来自其他安全功能隔离开来。

c) ICS 实现隔离边界,最小化包含安全功能的边界内所涉及的非安全功能。

d) 组织把安全功能实现为一些相对独立的模块,避免模块之间存在不必要的接口。

e) 组织把安全功能实现为一个层次结构,最小化设计层次之间的接口,并避免高层在功能或正确性方面依赖低层。

B.18.4 共享资源中的信息(SC-4)

控制:

a) ICS 应禁止通过共享的系统资源进行未授权的、无意的信息传输。

补充指导:

a) 通过该控制,可禁止以前用户/角色的动作所产生信息,包括信息的加密表示,在资源释放回信系统之后,对当前获得对一个共享的资源访问的任意用户/角色(或当前过程)是可用的。即控制共享资源中的信息,其中涉及客体复用问题。

b) 相关安全控制:AC-3、AC-4、MP-6。

控制增强:

a) ICS 没有诸如内存、输入/输出队列、网络接口卡等共享资源,而这些在不同安全层上的资源仅用于与系统运行的接口。

B.18.5 拒绝服务防护(SC-5)

控制:

a) ICS 应防止或抵御【赋值:组织定义的拒绝服务攻击类型列表】中的拒绝服务攻击。

补充指导:

a) 边界保护设备可过滤一定类型的包,以保护组织内部网络上的设备,免遭受到拒绝服务攻击的直接影响。使用组合的增大容量和带宽以及服务容余,可减少遭受某些拒绝服务攻击的影响。

b) 相关安全控制:SC-6、SC-7。

控制增强:

a) ICS 限制用户针对其他 ICS 或网络,发起拒绝服务攻击的能力。

b) ICS 为了限制拒绝服务攻击的信息泛滥之影响,管理多余的能力、带宽或其他容余。

c) ICS 安全失效。

增强补充指导：

1） 所谓安全失效是一种条件，可通过应用一组系统机制来实现，以确保在管理接口上的边界保护设备（例如：路由器，防火墙，门禁，以及驻留在受保护的通用子网上被称为非军事区或 DMZ 的应用网关），在其运行失效的事件中，没有互连系统之外的信息进入该系统。

2） 运行失效可能与任何一个过程、设备或机制是有关系的。

3） 边界保护设备的任何一个失效，均不能导致或引起该保护设备之外的信息进入该设备，也不可能失效地允许未授权的信息释放。

B.18.6 资源优先级（SC-6）

控制：

a） ICS 应能通过优先级来控制资源使用。

补充指导：

a） 优先级保护有助于防止低优先级过程延迟或干扰 ICS 服务于高优先级的过程。

b） 该控制并不适用于 ICS 中那些只有单一用户/角色的部件。

控制增强：无

B.18.7 边界保护（SC-7）

控制：

a） 组织应监视并控制在系统边界上的通信，以及系统内关键的边界上的通信；

b） 连接外部网络或 ICS，应通过得到管理的、并与组织安全体系结构所安排的边界保护设备相一致的接口。

补充指导：

a） 限制外部信息流仅能流向管理接口中组织的服务器，并禁止外部流量似乎欺诈一个内部地址。

b） 管理接口使用边界保护设备，例如包括：在一个有效安全体系结构（例如：驻留在称为非军事区或 DMZ 的受保护子网中受到防火墙和应用网关保护的路由器）中所组织的代理，网关，路由器，防火墙，门禁，或加密隧道。

c） 在安全控制的实现以及这样服务中，组织要考虑商业电子通信服务的固有共享本质。

d） 一般地，公共访问 ICS 的信息是不允许的。

e） 相关安全控制：AC-4、AC-17、CA-3、CM-7、CP-8、IR-4、RA-3、SC-5、SC-13。

控制增强：

a） 组织通过不同的物理网络接口，真正把公共可访问的 ICS 部件分配给不同的子网。

b） ICS 阻止公共访问到组织的内部网络，除非通过管理接口进行合适的调解，使用边界保护设备。

c） 组织限制 ICS 访问点的数量，以便允许更全面的监视通信边界内外的网络流量。

d） 组织应：

1） 为每一个外部电子通信服务实现一个管理接口；

2） 为每一个管理接口建立一个通信流策略；

3） 当需要时，使用安全控制来保护正在传送的那些信息的保密性和完整性；

4） 为每一个支持使命/业务需要以及持续需要的通信流策略的例外，建立相应的文档；

5） 按【赋值：组织定义的时间间隔】，评审通信流策略的例外；

6） 去除不再被显式的使命和业务需要的通信流策略例外。

e） 在管理接口上的控制系统，拒绝默认的网络流量，允许除了例外的网络流量（即拒绝所有例外的流量）。

f） 当出现边界保护机制运行失效时，组织禁止未授权地释放 ICS 边界之外的信息，或未授权地经

过 ICS 边界的通信。

增强补充指导：

1） 组织选择一种合适的失效模式(例如，失败是封闭的，失败是开放的)。

g） ICS 禁止远程设备与系统建立非远程的连接，以防与外边的、具有外部网络资源的通信路径进行通信。

h） ICS 按【赋值：组织定义的通信流量】，通过边界保护设备管理外部网络。

增强补充指导：

1） 外部网络是组织控制之外的网络；

2） 代理服务器支持登入个体的传输控制协议(TCP)会话，并锁死特定的统一资源分配(URL)、域名和互联网协议地址；

3） 代理服务按【赋值：组织定义的授权网站和未授权网站】。

i） 在管理接口上的 ICS，拒绝解析外部 ICS 威胁的网络流量并审计内部用户。

增强补充指导：

1） 可以解析一个对外部系统的安全威胁的检测内部活动，有时是使用穷举检测；

2） 在 ICS 边界上的穷举检测分析，包括网络流量(流入和流出的)监控，以便指示对外部系统安全的内部威胁。

j） 组织禁止未授权地过度过滤通过管理接口的信息。

增强补充指导：

1） 严格控制协议格式；

2） 对系统报警进行监控；

3） 对加密进行监控；

4） 除非需要断开所有外部网络连接；

5） 对数据报文头进行必要的拆装和组装；

6） 对网络流量进行分析。

k） 检测通信进入，以确保该通信是从授权源进入的，并路由到授权目标。

l） 实现基于主机的边界保护机制。

增强补充指导：

1） 基于主机的边界保护机制，其例子是基于主机的防火墙。

m） 组织通过物理上不同的子网以及对该系统其他部分的管理接口，把【赋值：组织定义的关键信息安全工具】与其他内部 ICS 部件隔离开来。

n） 实现保护边界，防止穿过边界保护机制的未授权物理连接。

o） ICS 通过指定的管理接口，按访问控制和审计的意图，路由所有网络化的授权访问。

p） ICS 禁止揭示构成一个管理接口的特定系统部件(或设备)。

增强补充指导：

1） 期望通过该控制增强来保护 ICS 部件的网络地址，这样的地址是管理接口的一部分，可通过通用根据和技术来发现的，以便标识一个网络上的设备；

2） 网络地址要求在了解访问知识之前，是不能予以揭示的(例如：不能发布或进入域名系统)。

q） 组织使用自动化机制，严格符合协议格式。

增强补充指导：

1） 严格符合协议格式所使用的自动化机制，其例子有包深度检测防火墙和 XML 网关；

2） 这些设备在应用层上验证是否符合协议的规格说明，并支持标识在网络上或传输层上运行的设备不可能检测到的大量脆弱性。

B.18.8 传输完整性(SC-8)

控制：

a) ICS 应保护传输信息的完整性。

补充指导：

a) 该控制适用于内外网之间的通信；

b) 如果组织依赖商业服务方提供传输服务，作为一种商品项，而完全不是一个贡献性服务，那么传输完整性所需要的安全控制的实现，就可能更难获得必要的保障；

c) 当实际上不可能通过合同方式获得必要的有效安全控制和保障时，组织要么实现合适的补偿安全控制，要么就显式地接受附加的风险；

d) 相关安全控制：AC-17、PE-4。

控制增强：

a) 组织应使用加密机制来识别传输中对信息的改变。

增强补充指导：

1) 在认真考虑安全需要和系统性能上的潜在结果的基础上，确定要使用的密码技术。例如，组织考虑使用密码技术是否对该 ICS 运行性能引入了负面影响的潜在因素。组织揭示所有可能的密码技术完整性机制(例如，数字签名，哈什函数)，每一机制均有不同的延迟影响。

b) ICS 维护准备传输中信息汇聚期间、打包期间和传输期间的信息完整性。

增强补充指导：

1) 在数据汇聚点或协议传送点上，信息可能被有意或恶意的修改，损害信息的完整性。

c) 组织应使用加密技术，来实现数字签名。

B.18.9 传输机密性(SC-9)

控制：

a) ICS 应保护传输信息的保密性。

补充指导：

a) 该控制适用于内外网之间的通信；

b) 如果组织依赖商业服务方提供传输服务，传输保密性所需要的安全控制是必要的；

c) 当实际上不可能通过合同方式获得必要的有效安全控制和保障时，组织要么实现合适的补偿安全控制，要么就显式地接受附加的风险；

d) 相关安全控制：AC-17、PE-4。

控制增强：

a) 组织使用加密机制来防止传输中对信息的未授权泄露；

增强补充指导：

1) ICS 的安全目的通常具有保密性，完整性和可用性的有序优先级；

2) 在认真考虑安全需要和系统性能上的潜在结果的基础上，确定要使用的密码技术。例如，组织考虑使用密码技术是否对该 ICS 运行性能引入了负面影响的潜在因素。

b) ICS 维护准备传输中信息汇聚期间、打包期间和传输期间的信息保密性；

c) 组织使用密码技术，来保护传输中受控的非秘密信息；

d) 当用于传输秘密的、涉及国家安全信息的网络之等级低于被传输的信息之等级时，组织使用密码技术，来保护该信息；

e) 组织使用密码技术，来保护网络上同样秘密等级的信息，当这样信息必须与没有必要的访问批

准的个体予以隔离时；

f) 组织使用密码技术，来保护传输中秘密的、涉及国家安全的信息；

g) 组织使用密码技术，来保护传输中源信息和方法信息。

B.18.10 网络中断(SC-10)

控制：

a) 在会话结束时或在不活动的时间周期之后，ICS 应终止与该通信会话相关的网络连接。

补充指导：

a) 该控制适用于内外网；

b) 终止与通信会话相关的网络连接，例如包括重新分配开发系统层上所关联的 TCP/IP 地址/端口对，或重新分配应用层上的网络指派，如果多应用会话使用一个开放系统层的网络连接的话；

c) 不活动的时间周期作为组织认为必要的时间周期，可以是网络访问类型的一个时间周期的集合，或是特定访问的一个时间周期的集合；

d) 在一个会话结束上或在【赋值：组织定义的非活动时间段】之后，ICS 不能终止网络连接的情况下，或由于对性能，安全(safety)或可靠性具有重大负面影响，ICS 不能终止网络连接的情况下，组织按裁剪指导，使用补偿控制(例如，提供更强的审计措施，限制关键人员的远程访问特权)。

控制增强：无

B.18.11 密钥建立与管理(SC-11)

控制：

a) 组织应为 ICS 内所需要的密码技术，建立并管理加密密钥。

补充指导：

a) 加密密钥的建立和管理，可以通过使用人为的规程或支持人为规程的自动化机制予以实施。

b) 相关安全控制：SC-13。

控制增强：

a) 组织维护用户丢失加密密钥的事件中的信息的可用性；

b) 组织使用密钥管理技术和过程，产生、控制和分布对称加密密钥；

c) 组织使用密钥管理技术和过程，产生、控制和分布对称或非对称加密密钥；

d) 组织使用批准的 3 级证书或前置密钥化资料的 PKI，产生、控制和分布非对称加密密钥；

e) 组织使用批准的 3 级证书或 4 级证书以及保护用户私钥的 PKI，产生、控制和分布非对称加密密钥。

增强补充指导：

1) 在认真考虑安全需要和系统性能上的潜在结果的基础上，确定要使用的密钥，包括密钥管理。例如，组织考虑使用密码技术是否对该 ICS 运行性能引入了负面影响的潜在因素。

2) 期望在 ICS 中使用密钥管理来支持内部非公共的使用。

B.18.12 密码技术的使用(SC-12)

控制：

a) ICS 应使用符合相关法律、法规、方针政策、规章制度、标准和指南的密码模块，实现所需要的密码技术的保护。

补充指导：

a) 使用密码技术应遵守相关标准和法律规定。

b) 密码技术的使用应不影响 ICS 正常运行。

c) 相关安全控制：AC-2、AC-3、AC-7、AC-17、AC-18、AU-9、AU-10、CM-11、CP-9、IA-3、IA-7、MA-4、MP-2、MP-4、MP-5、SA-4、SC-8、SC-12、SI-7。

控制增强：无

B.18.13 公共访问保护(SC-13)

控制：

a) ICS 应保护公共可用信息和应用的完整性和可用性。

补充指导：

a) 该控制的意图是，确保组织显式地强调公共信息和应用的保护需求，以及与可能实现的、作为其他安全控制一部分的这样保护的关联；

b) 一般地，对 ICS 的公共访问是不允许的。

控制增强：

a) ICS 应禁止公共访问。

B.18.14 安全属性的传输(SC-14)

控制：

a) ICS 应将安全属性与系统间交换的信息关联起来。

补充指导：

a) 安全属性可以显式地或隐式地与 ICS 中所包含的信息相关联；

b) 与该控制有关的控制有：AC-3、AC-4、AC-16。

控制增强：

a) ICS 验证系统间交换的安全属性的完整性。

B.18.15 证书管理(SC-15)

控制：

a) 组织应按合适的证书策略发布公钥证书或按合适的证书策略从批准的服务提供方那里获得公钥证书。

补充指导：

a) 对于用户证书，每个组织按策略的要求，从一个得到批准的、共享的服务提供方那里获得证书；

b) 该控制关注证书及系统外的可见性；

c) 相关安全控制：SC-12。

控制增强：无

B.18.16 移动代码(SC-16)

控制：

组织应：

a) 定义可接受的和不可接受的移动代码及移动代码技术；

b) 对可接受的移动代码及移动代码技术，建立用法限制和实现指南；

c) 授权、监视并控制 ICS 中移动代码的使用。

补充指导：

a) 基于移动代码的恶意使用可能对 ICS 导致破坏，组织应就 ICS 是否使用移动代码做出相应的

决策；

b） 代码技术，例如包括：Java，JavaScript，ActiveX，PDF，VBScript 等；

c） 用法限制和实现指南适用于安装在组织服务器端的移动代码，也适应于工作站和移动设备；

d） 与移动代码相关的策略和规程，强调了防止 ICS 中不可接受的移动代码的开发、获得或引入；

e） 相关安全控制：AU-2、AU-12、CM-2、CM-6、SI-3。

控制增强：

a） 为了标识未授权的移动代码，ICS 实现发现和检查机制，必要时采取纠正措施。

增强补充指导：

1） 发现未授权移动代码时，纠正措施包括：锁定、隔离和报警等。

b） 组织应确保部署在 ICS 中的移动代码的获得、开发和使用满足【赋值：组织定义的移动代码】需求。

c） ICS 禁止下载和执行已禁止的移动代码。

d） ICS 禁止在软件应用中自动执行移动代码。

B.18.17 会话鉴别（SC-17）

控制：

a） ICS 应提供保护通信会话真实性的机制。

补充指导：

a） 该控制关注通信会话保护；

b） 该控制的目的是建立每一通信会话的信任基础；

c） 该控制仅在组织认为必要时实现；

d） 在 ICS 不能保护通信会话真实性的情况下，组织应按裁剪指南，使用补偿控制（例如，审计措施）；

e） 相关安全控制：SC-8、SC-10、SC-11。

控制增强：

a） ICS 应在用户退出或终止会话后让会话身份标识符失效；

b） ICS 应提供明显容易的退出功能；

c） ICS 应为每一会话生成唯一的会话身份标识符，并仅认可系统生成的会话身份标识符；

d） ICS 应按【赋值：组织定义的随机需求】，生成唯一的会话身份标识符。

B.18.18 已知状态中的失效（SC-18）

控制：

a） 针对【赋值：组织定义的失效类型】，ICS 失效于【赋值：组织定义的已知状态】，保持失效中系统状态信息。

补充指导：

a） 在已知状态中失效，可按组织的使命和业务需要来强调安全。

b） 在已知状态中失效，有助于防止在 ICS 和部件失效事件中丧失保密性、完整性和可用性。

c） 在已知安全状态中失效，有助于防止系统失效导致损害个体或破坏特性的状态。

d） 保留 ICS 状态信息，可支持系统对使命和业务过程的较少破坏，重新启动并返回到组织的运行模式。

e） 相关安全控制：CP-2、CP-10、CP-12、SC-7。

控制增强：无

B.18.19 剩余信息保护(SC-19)

控制：

a) ICS 应保护剩余信息的保密性和完整性。

补充指导：

a) 该控制的目的是剩余信息的保密性和完整性保护。

b) 组织可选择不同的机制来实现保密性和完整性保护。

c) 相关安全控制：AC-3、AC-6、CA-7、CM-3、CM-5、CM-6、PE-3、SC-8、SC-13、SI-3、SI-7。

控制增强：

a) 应确保 ICS 内的文件、目录和数据等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除；

b) 应保证用户鉴别信息等敏感信息所在的存储空间被释放或再分配给其他用户前得到完全清除；

c) 可提供加密机制保护剩余信息的保密性和完整性。

增强补充指导：

1) 加密机制是保护组织信息的保密性和完整性的基础，组织应根据安全需求来选择对应强度的加密机制。

B.18.20 执行程序隔离（SC-20）

控制：

a) 组织应让 ICS 各类执行程序运行在相互隔离的域中。

补充指导：

a) 让 ICS 各类执行程序运行在相互隔离的域中，并各自使用分离的地址空间，处于分离的地址空间的各可执行程序异常时不会影响其他程序；

b) ICS 产品所采用的操作系统一般均正常地址空间分离；

c) 相关安全控制：AC-3、AC-4、AC-6、SA-4、SA-5、SA-8、SC-2、SC-3。

控制增强：

a) 采用硬件分离实现可执行程序隔离。

附 录 C
（规范性附录）
工业控制系统安全控制基线

根据工业控制系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，结合信息安全等级保护标准划分及实施效果分析，结合工业控制系统的基本特征（参见附录 A），结合以往诸多工业控制系统的安全实践，将附录 B 中适用于工业控制系统的安全控制分为三个级别：一级、二级和三级，每个级别对应安全控制如表 C.1。安全控制基线及其设计考虑，以及基线的选择和裁剪指导见本标准正文内容。

表 C.1 安全控制基线

编号	控制名	级别		
		一级	二级	三级
访问控制（AC）				
AC-1	访问控制策略和规程	AC-1	AC-1	AC-1
AC-2	账户管理	AC-2	AC-2 a)b)c)d)	AC-2 a)b)c)d)
AC-3	强制访问控制	AC-3	AC-3 b)	AC-3 b)
AC-4	信息流强制访问控制	—	AC-4	AC-4
AC-5	职责分离	—	AC-5	AC-5
AC-6	最小授权	—	AC-6 a)b)c)e)f)	AC-6 a)b)c)d)e)f)
AC-7	失败登录控制	AC-7	AC-7	AC-7
AC-8	系统使用提示	—	AC-8	AC-8
AC-9	以前访问提示	—	—	AC-9
AC-10	并发会话控制	—	—	AC-10
AC-11	会话锁定	—	AC-11 a)	AC-11 a)
AC-12	会话终止	—	AC-12	AC-12
AC-13	未标识鉴别的许可行为	—	AC-13	AC-13
AC-14	远程访问	AC-14	AC-14 a)b)c)d)	AC-14 a)b)c)d)
AC-15	无线访问	AC-15	AC-15 a)	AC-15 a) b)c)d)e)
AC-16	移动设备的访问控制	AC-16	AC-16 d)e)f)	AC-16 a)b)c)d)e)f)g)
AC-17	外部系统的使用	AC-17	AC-17 a)b)	AC-17 a)b)
AC-18	信息共享	—	AC-18	AC-18
教育培训（AT）				
AT-1	教育培训策略和规程	AT-1	AT-1	AT-1
AT-2	安全意识培训	AT-2	AT-2 b)	AT-2 a)b)
AT-3	基于角色的安全培训	AT-3	AT-3 b)	AT-3 a)b)c)
AT-4	安全培训记录	AT-4	AT-4	AT-4

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
审计与问责(AU)				
AU-1	审计与问责策略和规程	AU-1	AU-1	AU-1
AU-2	审计事件	AU-2	AU-2 c)	AU-2 a)b)c)
AU-3	审计记录的内容	AU-3	AU-3 a)	AU-3a)b)
AU-4	审计存储能力	AU-4	AU-4	AU-4
AU-5	审计失效响应	AU-5	AU-5 a)b)	AU-5 a)b)c)
AU-6	审计信息的监控、分析和报告	AU-6	AU-6 a)	AU-6 a)b)
AU-7	审计简化和报告生成	—	AU-7 a)	AU-7 a)
AU-8	时间戳	AU-8	AU-8 a)	AU-8 a)
AU-9	审计信息保护	AU-9	AU-9 b)	AU-9 a)b)c)d)
AU-10	抗抵赖	—	—	AU-10 a)b)c)d)
AU-11	审计信息保留	AU-11	AU-11	AU-11
AU-12	审计生成	AU-12	AU-12	AU-12 a)b)c)
安全评估与授权(CA)				
CA-1	安全评估与授权策略和规程	CA-1	CA-1	CA-1
CA-2	安全评估	CA-2	CA-2 a)b)	CA-2 a)b)c)d)e)
CA-3	ICS 连接管理	CA-3	CA-3	CA-3 a)b)
CA-4	实施计划	CA-4	CA-4	CA-4 a)
CA-5	安全授权	CA-5	CA-5	CA-5
CA-6	持续监控	CA-6	CA-6 a)	CA-6 a)b)
CA-7	渗透测试	—	—	CA-7
CA-8	内部连接	CA-8	CA-8	CA-8
配置管理(CM)				
CM-1	配置管理策略和规程	CM-1	CM-1	CM-1
CM-2	基线配置	CM-2	CM-2 a)c)f)	CM-2 a)b)c)d)e)f)
CM-3	配置变更	—	CM-3 b)	CM-3 a)b)c)d)
CM-4	安全影响分析	CM-4	CM-4	CM-4 a)b)
CM-5	变更的访问限制	—	CM-5 a)b)c)	CM-5 a)b)c)d)e)f)g)
CM-6	配置设置	CM-6	CM-6 a)b)c)	CM-6 a)b)c)d)
CM-7	最小功能	CM-7	CM-7 a)b)	CM-7 a)b)c)
CM-8	系统组件清单	CM-8	CM-8 a)b)c)d)e)	CM-8 a)b)c)d)e)f)
CM-9	配置管理计划	—	CM-9	CM-9

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
应急计划(CP)				
CP-1	应急计划策略和规程	CP-1	CP-1	CP-1
CP-2	应急计划	CP-2	CP-2 a)b)c)e)	CP-2 a)b)d)f)
CP-3	应急计划培训	CP-3	CP-3 a)	CP-3 a)
CP-4	应急计划测试和演练	CP-4	CP-4 a)b)d)	CP-4 a)b)c)d)
CP-5	备用存储设备	—	CP-5 a)b)c)	CP-5 a)b)c)
CP-6	备用处理设备	—	CP-6 a)b)c)d)e)	CP-6 a)b)c)d)e)
CP-7	通信服务	—	CP-7 a)b)c)	CP-7 a)b)c)
CP-8	系统备份	CP-8	CP-8 a)b)c)	CP-8 a)b)c)d)e)f)
CP-9	系统恢复与重建	CP-9	CP-9 b)c)d)	CP-9 b)c)d)
标识与鉴别(IA)				
IA-1	标识与鉴别策略和规程	IA-1	IA-1	IA-1
IA-2	组织内用户的标识与鉴别	IA-2 a)	IA-2 a)b)c)d)g)h)	IA-2 a)b)c)d)g)h)
IA-3	设备标识与鉴别	—	IA-3	IA-3
IA-4	标识符管理	IA-4	IA-4	IA-4
IA-5	鉴别符管理	IA-5	IA-5 a)b)c)	IA-5 a)～j)
IA-6	鉴别反馈	IA-6	IA-6	IA-6
IA-7	密码模块鉴别	IA-7	IA-7	IA-7
IA-8	组织外用户的标识与鉴别	IA-8 a)b)c)	IA-8 a)b)c)	IA-8 a)b)c)
事件响应(IR)				
IR-1	事件响应策略和规程	IR-1	IR-1	IR-1
IR-2	事件响应培训	IR-2	IR-2	IR-2 a)b)
IR-3	事件响应测试与演练	—	IR-3 a)	IR-3 a)
IR-4	事件处理	IR-4	IR-4 a)b)	IR-4 a)b)c)d)e)
IR-5	事件监控	IR-5	IR-5 a)	IR-5 a)
IR-6	事件报告	IR-6	IR-6 a)b)	IR-6 a)b)
IR-7	事件响应支持	IR-7	IR-7 a)b)	IR-7 a)b)
IR-8	事件响应计划	IR-8	IR-8	IR-8
维护(MA)				
MA-1	维护策略和规程	MA-1	MA-1	MA-1
MA-2	受控维护	MA-2	MA-2 a)b)	MA-2 a)b)c)
MA-3	维护工具	—	MA-3 a)b)c)d)e)	MA-3 a)b)c)d)e)
MA-4	远程维护	MA-4	MA-4 a)b)c)	MA-4 a)b)c)d)e)f)g)

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
MA-5	维护人员	MA-5	MA-5	MA-5 a)b)c)d)
MA-6	及时维护	—	MA-6	MA-6 a)b)
介质保护(MP)				
MP-1	介质保护策略和规程	MP-1	MP-1	MP-1
MP-2	介质访问	MP-2	MP-2 a)	MP-2 a)b)
MP-3	介质标记	—	MP-3	MP-3
MP-4	介质存储	—	MP-4 a)b)	MP-4 a)b)
MP-5	介质传输	—	MP-5 b)c)d)	MP-5 b)c)d)
MP-6	介质销毁	MP-6	MP-6a)b)c)	MP-6a)b)c)d)
MP-7	介质使用	MP-7	MP-7 a)b)	MP-7 a)b)
物理与环境安全(PE)				
PE-1	物理与环境安全策略和规程	PE-1	PE-1	PE-1
PE-2	物理访问授权	PE-2	PE-2	PE-2
PE-3	物理访问控制	PE-3	PE-3 a)	PE-3 a)
PE-4	传输介质的访问控制	PE-4	PE-4 a)	PE-4 a)b)
PE-5	输出设备的访问控制	PE-5	PE-5	PE-5
PE-6	物理访问监控	PE-6	PE-6 a)	PE-6 a)
PE-7	访问日志	PE-7	PE-7 a)b)	PE-7 a)b)
PE-8	电力设备与电缆	—	PE-8 a)b)	PE-8 a)b)
PE-9	紧急停机	—	PE-9	PE-9
PE-10	应急电源	—	PE-10 a)	PE-10 a)b)
PE-11	应急照明	PE-11	PE-11	PE-11
PE-12	消防	PE-12	PE-12 a)b)c)	PE-12 a)b)c)d)
PE-13	温湿度控制	PE-13	PE-13	PE-13
PE-14	防水	PE-14	PE-14 a)	PE-14 a)
PE-15	交付和移除	PE-15	PE-15	PE-15
PE-16	备用工作场所	PE-16	PE-16	PE-16
PE-17	防雷	PE-17	PE-17	PE-17
PE-18	电磁防护	—	PE-18	PE-18
PE-19	信息泄露	—	—	PE-19
PE-20	人员和设备追踪	PE-20	PE-20	PE-20

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
规划(PL)				
PL-1	安全规划策略和规程	PL-1	PL-1	PL-1
PL-2	系统安全规划	PL-2	PL-2	PL-2 a)～g)
PL-3	行为规则	PL-3	PL-3	PL-3 a)
PL-4	信息安全架构	—	PL-4	PL-4 a)b)
PL-5	安全活动规划	—	PL-5	PL-5
人员安全(PS)				
PS-1	人员安全策略和规程	PS-1	PS-1	PS-1
PS-2	岗位分类	PS-2	PS-2	PS-2
PS-3	人员审查	PS-3	PS-3	PS-3
PS-4	人员离职	PS-4	PS-4	PS-4
PS-5	人员调离	PS-5	PS-5	PS-5
PS-6	访问协议	PS-6	PS-6	PS-6
PS-7	第三方人员安全	PS-7	PS-7	PS-7
PS-8	人员处罚	PS-8	PS-8	PS-8
风险评估(RA)				
RA-1	风险评估策略和规程	RA-1	RA-1	RA-1
RA-2	安全分类	RA-2	RA-2	RA-2
RA-3	风险评估	RA-3	RA-3	RA-3
RA-4	脆弱性扫描	RA-4	RA-4 a)b)c)d)e)h)	RA-4 a)b)c)d)e)f)g)h)i)
系统与服务获取(SA)				
SA-1	系统与服务获取策略和规程	SA-1	SA-1	SA-1
SA-2	资源分配	SA-2	SA-2	SA-2
SA-3	生存周期支持	SA-3	SA-3	SA-3
SA-4	服务获取	SA-4	SA-4 a)b)d)	SA-4 a)b)c)d)
SA-5	系统文档	SA-5	SA-5 a)b)c)	SA-5 a)b)c)
SA-6	软件使用限制	SA-6	SA-6	SA-6 a)b)
SA-7	用户安装软件	SA-7	SA-7	SA-7
SA-8	安全工程原则	—	SA-8	SA-8
SA-9	外部系统服务	SA-9	SA-9	SA-9 a)b)
SA-10	开发人员的配置管理	—	SA-10	SA-10 a)b)
SA-11	开发人员的安全测试	—	SA-11	SA-11 a)b)c)
SA-12	供应链保护	—	SA-12	SA-12 a)～h)

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
SA-13	可信赖性	—	SA-13	SA-13
SA-14	关键系统部件	—	SA-14	SA-14 a)b)
系统与通信保护(SC)				
SC-1	系统与通信保护策略和规程	SC-1	SC-1	SC-1
SC-2	应用分区	—	SC-2	SC-2
SC-3	安全功能隔离	—	—	SC-3
SC-4	共享资源中的信息	—	SC-4	SC-4
SC-5	拒绝服务防护	SC-5	SC-5	SC-5
SC-6	资源优先级	SC-6	SC-6	SC-6
SC-7	边界保护	SC-7	SC-7 a)b)c)d)e)h)	SC-7 a)b)c)d)e)f)h)i)
SC-8	传输完整性	—	SC-8 a)	SC-8 a)
SC-9	传输机密性	—	SC-9 a)	SC-9 a)
SC-10	网络中断	—	SC-10	SC-10
SC-11	密钥建立与管理	SC-11	SC-11 a)	SC-11 a)
SC-12	密码技术的使用	SC-12	SC-12	SC-12
SC-13	公共访问保护	SC-13	SC-13	SC-13
SC-14	安全属性的传输	—	SC-14 a)	SC-14 a)
SC-15	证书管理	—	SC-15	SC-15
SC-16	移动代码	—	SC-16 a)b)c)d)	SC-16 a)b)c)d)
SC-17	会话鉴别	SC-17	SC-17 a)b)c)	SC-17 a)b)c)d)
SC-18	已知状态中的失效	SC-18	SC-18	SC-18
SC-19	剩余信息保护	SC-19	SC-19 a)b)	SC-19 a)b)c)
SC-20	执行程序隔离	SC-20	SC-20	SC-20
系统与信息完整性(SI)				
SI-1	系统与信息完整性策略和规程	SI-1	SI-1	SI-1
SI-2	缺陷修复	SI-2	SI-2 a)b)	SI-2 a)b)
SI-3	恶意代码防护	SI-3	SI-3 a)b)c)d)	SI-3 a)b)c)d)e)
SI-4	系统监控	SI-4	SI-4 b)d)e)f)	SI-4 b)d)e)f)
SI-5	安全报警	SI-5	SI-5 a)	SI-5 a)
SI-6	安全功能验证	—	SI-6	SI-6
SI-7	软件和信息完整性	—	SI-7 a)b)	SI-7 a)b)
SI-8	输入验证	—	SI-8	SI-8
SI-9	错误处理	—	SI-9	SI-9

表 C.1（续）

编号	控制名	级别		
		一级	二级	三级
SI-10	信息处理和留存	SI-10	SI-10	SI-10
SI-11	可预见失效预防	—	SI-11	SI-11
SI-12	输出信息过滤	—	SI-12	SI-12
SI-13	内存防护	—	—	SI-13
SI-14	故障安全程序	—	—	SI-14
SI-15	入侵检测和防护	—	SI-15	SI-15
程序管理(PM)				
PM-1	程序管理计划	组织级部署,适应于所有基线		
PM-2	信息安全高管			
PM-3	信息安全资源			
PM-4	行动和里程碑计划			
PM-5	安全资产清单			
PM-6	安全性能度量			
PM-7	组织架构			
PM-8	关键基础设施计划			
PM-9	风险管理策略			
PM-10	安全授权过程			
PM-11	业务流程定义			

参 考 文 献

[1] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[2] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

[3] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[4] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

[5] NIST Special Publication 800-82 Guide to Industrial Control Systems(ICS)Security