ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36323—2018

信息安全技术
工业控制系统安全管理基本要求

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

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：[redacted]、中国科学院自动化研究所、和利时集团、全球能源互联网研究院有限公司、浙江大学、气象能源系统研发设计有限公司、深圳赛西信息技术有限公司、广州数控设备有限公司、北京江南天安科技有限公司、中电长城网际系统应用有限公司、北京匡恩网络科技有限责任公司。

引　言

随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统，包括分布式控制系统(DCS)、监控与数据采集(SCADA)系统和可编程逻辑控制器(PLC)等产品

[redacted]

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

信息安全技术
工业控制系统安全管理基本要求

1 范围

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

本标准适用于非涉及国家秘密的工业控制系统建设、运行、使用、管理等相关方进行工业控制系统安全管理的机制和落实，也可供工业控制系统安全测评标准和检查工作作业参考使用。

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。

注：PLC主要执行各类运算、顺序控制、定时等指令，用于控制工业生产装备的动作，是工业控制系统的基础单元。

3.5

安全控制基线　security control baseline

安全控制选择过程的起始点和选择基点。

注：安全控制基线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。

AC：访问控制(Access Control)

AT：意识和培训(Awareness and Training)

AU：审计和可核查性(Audit and Accountability)

CA：安全评估和授权(Security Assessment and Authorization)

CM：配置管理(Configuration Management)

CP：应急规划(Contingency Planning)

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

IA：标识和鉴别(Identification and Authentication)

ICS：工业控制系统(Industrial Control System)

IR：事件响应(Incident Response)

MA：维护(Maintenance)

MP：介质保护(Media Protection)

PE：物理和环境保护(Physical and Environmental Protection)

PL：规划(Planning)

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

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)

求整合到ICS中，形成了ICS安全管理基本框架(如图1所示)。该框架在确定ICS安全管理具体意图、理解需求期望并明确ICS体系范围的基础上，将ICS安全管理活动分为顶层承诺、规划评估、资源支持、策略实施、绩效评价与持续改进六个方面。其中，顶层承诺方面需要组织获得管理层的承诺，确定ICS安全管理的方针，明确组织各相关成员在ICS管理活动中的角色和权责；规划评估中组织应确定规

框架各阶段所需的基本控制措施，并在附录 A 中给出了针对不同级别的工业控制系统安全管理要求对应表，用以指导组织根据自身工业控制系统的不同安全级别选择安全管理基本控制措施，并根据工业控制系统安全控制应用指南、安全分级等相关标准，对所选安全管理基本控制措施进行剪裁、选择等操作。

5.2 顶层承诺

5.2.1 管理层承诺

组织应依据 GB/T 22080—2016 的 5.1 作出针对 ICS 安全的承诺。

5.2.2 方针

组织应依据 GB/T 22080—2016 的 5.2 制定适用于 ICS 安全的方针，此外，还应制定相应的将 ICS 安全的方针与组织信息安全整体方针保持一致，并作为其有机组成部分。

5.2.3 成立 ICS 安全联合管理团队

为确保 ICS 安全的实施落实，组织应：

b) 向最高管理者报告 ICS 安全管理基本框架绩效；

c) 接受联合管理团队的定期汇报。

5.3 规划评估

5.3.1 应对风险和机会的措施

5.3.1.1 总则

组织应依据 GB/T 22080—2016 中 6.1.1 作出针对 ICS 总则，同时还应在总则中加入对于 ICS 安全运行和维护的期望。

5.3.1.2 ICS 信息安全风险评估

组织应依据 GB/T 22080—2016 中 6.1.2 定义并应用针对 ICS 的风险评估过程，同时还应考

5.5.2 ICS 信息安全风险评估

组织应依据 GB/T 22080—2016 中 8.1 开展针对 ICS 信息安全的风险评估工作。在风险评估过程中，依据 GB/T 32919—2016 附录 A 中的内容，充分考虑 ICS 与传统信息系统的差异性。

5.5.3 ICS 信息安全风险处置

见 GB/T 22080—2016 中 8.3，并依据 ICS 特点开展风险处置。

5.6 绩效评价

5.6.1 监视、测量、分析和评价

见 GB/T 22080—2016 中 9.1，同时还应持续监控已实施的安全控制措施，识别安全违规事件，检测 ICS 中的安全异常事件的发生。

5.6.2 内部审核

见 GB/T 22080—2016 中 9.2，并依据 ICS 特点开展内部审核。

5.6.3 管理评审

见 GB/T 22080—2016 中 9.3，并依据 ICS 特点开展管理评审。

5.7 持续改进

5.7.1 不符合及纠正措施

见 GB/T 22080—2016 中 10.1，并依据 ICS 特点采取纠正措施。

5.7.2 持续改进

组织应持续改进 ICS 安全管理基本框架的适宜性、充分性和有效性，并在 ICS 生产业务或系统安全防护发生重大变更时向联合管理团队和最高管理层汇报。

6 ICS 安全管理基本控制措施

6.1 安全控制措施分类

本标准从管理制度、运维管理和技术管理三方面给出安全控制，共十六个安全控制族，其对照关系如表 1 所示：

表 1 安全控制[illegible]分

	安全控制族	安全控制类	族标识符
	安全评估和授权(Security Assessment and Authorization)	管理制度	CA
	系统和服务获取(System and Services Acquisition)	管理制度	SA
	规划(Planning)	管理制度	PL
	风险评估(Risk Assessment)	管理制度	RA
	人员安全(Personnel Security)	运维管理	PS

表 1（续）

族标识符	安全控制族
CP	应急规划(Contingency Planning)
PE	物理和环境安全(Physical and Environmental Protection)
CM	配置管理(Configuration Management)
SI	系统和信息完整性(System and Information Integrity)
MP	介质保护(Media Protection)
IR	事件响应(Incident Response)
AT	意识和培训(Awareness and Training)
MA	维护(Maintenance)
IA	标识鉴别(Identification and Authentication)

安全控制类	
运维管理	
运维管理	
运维管理	
运维管理	
运维管理	
技术管理	

括：目的、范围、角色、责任、

和授权策略及与相关安全控

：判定安全措施有效性的评

，并判断是否满足相关安全

6.2 安全评估和授权(CA)

6.2.1 安全评估和授权方针策略及规程(CA-1)

本项要求包括：

a) 应制定并发布安全评估和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) 应制定并发布安全评估和授权方针策略及规程，以推动安全评估和授权策略及与相关安全控制的实施；

c) 应定期对安全评估与授权策略和规程进行评审和更新。

6.2.2 安全评估(CA-2)

本项要求包括：

a) 应制定安全评估计划，该评估计划应包括：应评估的安全控制措施；判定安全措施有效性的评估流程；评估环境、队伍、角色及责任；

b) 应定期对 ICS 采取的安全措施实施的正确性、有效性进行评估，并判断是否满足相关安全需求；

c) 应

记录；

c) 应定期评审 ICS 与外部的连接情况，以验证 ICS 连接是否符合规定要求；

d) 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；

e) 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。

6.2.4 行动计划与时间节点(CA-4)

本项要求包括：

a) 制定行动计划和时间节点，在其中记录下检测到的弱点行动，以改正并安全控制措施评估中发现的对已知不足的缺陷和系统中的已知漏洞；

b) 根据系统审核、后果分析和持续监控的情况，每季度至少更新一次现有的行动计划和时间节点；

c) 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。

6.2.5 安全授权(CA-5)

本项要求包括：

a) 应指定一位高层管理人员作为 ICS 的授权责任人；

b) ICS 未经授权责任人正式授权，不得投入运行；

c) 应对 ICS 定期或发生重大变更时，重新进行安全授权；

d) 应识别并定期评审反应组织机构信息保护需要的保密性或不泄露协议的要求；

e) 开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

6.2.6 持续监控(CA-6)

本项要求包括：

a) 应制定持续的监控策略，并实施持续的监控计划，计划内容包括：被监控的目标、监控的频率、以及对监控进行评估的频率；

b) 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；

c) 组织应定期规划、安排并进行评估，公开或不公开该评估信息，以便确保符合所有脆弱性缓解过程；

d) 应根据组织的连续监控策略，实施安全控制评估；

e) 应根据组织的连续监控战略，对组织已确定的度量指标，进行安全状态监控；

f) 应对评估和监控产生的安全相关信息进行关联和分析，并根据分析结果，采取相应的响应措施；

g) 应定期向相关人员报告信息系统安全状态。

6.2.7 渗透测试(CA-7)

本项要求包括：

a) 应定期对 ICS 进行渗透测试，要明确渗透测试的频率与目标

b） 应为每个内部连接建立文件，包括连接的接口特性，安全性要求和传输信息的性质；

c） 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。

6.3 系统和服务获取(SA)

6.3.1 系统及服务获取的方针策略及规程(SA-1)

本项要求包括：

a） 应制定并发布系统服务及获取的方针策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调及合规性；

b） 应制定并发布系统服务及获取的规程，以推动系统服务及获取的方针策略及与相关安全控制的实施；

c） 应定期对系统服务及获取的方针策略及规程进行评审和更新。

6.3.2 资源配置(SA-2)

本项要求包括：

a） 应在业务过程规划中明确提出 ICS 或系统服务的安全需求；

b） 应明确、配置保护信息系统及相关服务所需的资源，形成相关文档并将其作为资本计划和投资管理过程的组成部分；

c） 应在组织的工作计划和预算文件中考虑信息

i) 组织应有限制地获取市场上现成信息技术产品，这些产品应是那些已通过国家安全相关部门评估的产品类[illegible]

配置、使用、管理及运行维护信息以及系统管理员功能相关的脆弱性；

b) 应提供描述系统、组件或服务的用户文档，文档应包括：用户可访问的安全功能描述及其有效使用方法；用户对系统、组件或服务的安全使用方法及安全维护责任；

c) 当文档不可用时或不存在时，[illegible]应获得的 ICS 文档；

d) 当需要时，获取并保护描述 ICS 中所使用的安全控制的功能特性的文档，该文档具有充分的详细程度，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；

e) 当需要时，获取并保护描述了 ICS 与安全有关的外部接口文档，该文档应充分详细，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；

f) 当需要时，获取并保护以子系统以及安全控制的实现细节来描述 ICS 高层设计的文档，并具有充分的详细程度，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；

g) 当需要时，获取并保护描述了 ICS 与安全有关外部接口的文档，该文档具有充分的详细程度，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；

h) 当需要时，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；

i) 应基于风险管理策略要求对 ICS 文档进行保护；

j) ICS 文档应分发到指定的角色或个人。

[illegible]外部 ICS 服务(SA-9)

本项要求包括：

a) 外部 ICS 服务的提供商应遵从组织[illegible]

6.3.7 开发者配置管理(SA-7)

本项要求信息系统、系统组件及系统服务的开发者：

a) 应在系统、组件或服务的设计、开发、实现和运行的过程中实施配置、变更管理，并形成相关文档；

b) 信息系统的变更应经过批准，考虑系统、组件及服务变更的安全影响并形成文档；

c) 应跟踪系统、组件及服务的安全缺陷及应对措施；

d) 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；

e) 在开发人员和集成人员能实施配置管理活动中的情况

6.3.10 开发过程、标准及工具(SA-10)

本项要求包括：

a) ICS、系统组件或系统服务的开发人员应遵循软件工程的开发流程；

b) 应明确安全需求、开发过程中需遵循的标准及可使用的工具，并记录工具的配置信息与特殊选项；

c) 应对开发过程中的工具与变更进行管理；

d) 应定期对开发过程、标准、工具及配置文件进行审核。

6.3.11 网络服务安全(SA-11)

本项要求包括：

a) 安全特性、服务级别以及所有网络服务的管理要求应予以确定并包括在所有网络服务协议中，无论这些服务是由内部提供的还是外包的。

6.4 人员安全(PS)

6.4.1 人员安全的方针策略及规程(PS-1)

本项要求包括：

a) 应制定并发布人员安全的方针策略，各策略中应包括目的、范围、角色、管理承诺、协调各组织实体的方式、合规性；

b) 应制定并发布人员安全管理规程，规程应基于方针策略及相关安全控制的实施；

c) 应定期对人员安全的方针策略及规程进行评审和更新。

6.4.2 岗位风险评估(PS-2)

本项要求包括：

a) 应建立 ICS 岗位分类机制；

[illegible]

6.4.3 人员审查(PS-3)

本项要求包括：

a) 应在授权访问 ICS 之前进行人员审查；

b) 应在人员离职或岗位调动时对其进行审查；

c) 组织应确保每个访问涉及秘密信息处理、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；

d) 组织应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。

6.4.4 人员离职(PS-4)

本项要求包括：

a) 应终止离职人员对 ICS 系统的访问权限；

b) 应删除与离职人员相关的任何身份鉴别信息；

供系统安全需求的概要描述及

评估过程中发现问题时，应及时

续变化进行沟通；

更改；

的安全分类、描述系统的运营环境及与其他系统的关联关系、

针对这些安全需求的安全控制等；

c) 应定期对 ICS 系统安全规划进行评审和更新；

d) 当 ICS 系统或运行环境发生变化，或者在系统安全规划实施或
更新系统安全规划；

e) 向指定的角色或个人分发系统安全规划，并针对安全规划的后

f) 应对 ICS 系统安全规划的内容进行保护，以防止泄露或未授权

g) 对影响 ICS 系统安全的活动，在其实施前应进行规划及人

6.5.3 行为规则：PL-3：

本项要求包括：

a) 应建立用户对 ICS 进行访问等行为规则，明确其以责及其对

b) 应签订用户协议，确保用户在授权访问信息及 ICS 之前，已
约束；

c) 在行为规则中，组织应显式限制对社会网站等使用，限制在
统的账户信息；

d) 应定期对用户信息系统等实行监督检查并记录检查结果；

6.6.2 安全分类(RA-2)

本项要求包括：

a) 应依据适用的法律、法规、规章及相关标准，对 ICS 进行安全分类；

b) 应在 ICS 安全规划文件中包含 ICS 的安全分类及分类依据；

c) 安全分类应通过主管部门的审查和批准。

6.6.3 安全风险评估(RA-3)

本项要求包括：

a) 应制定 ICS 及相关信息系统的安全风险评估计划，明确风险评估的对象、内容及评估流程；

b) 应按安全风险评估计划在系统上线前或系统维修期间对指定系统实施风险评估，并形成风险评估报告；

c) 应将风险评估结果向相关人员通报，并定期对风险评估的结果进行评审；

d) 当系统或其运行环境发生重大变更(包括发现新的威胁和漏洞)，或出现其他可能影响系统

部门的协调、合规性；

b) 应制定并发布应急想规规程以推动应急想规划方针策略及与相关安全控制的实施；

c) 应定期对应急想规划方针策略及规程进行评审和更新。

6.7.2 应急计划(CP-2)

本项要求包括：

a) 应制定 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) 应制定 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) 应按已确定的应急计划角色设置，将应急计划分发下去；

d) 应定期评审和更新应急计划，以反映组织、ICS 或运行环境的变更；

e) 组织应协调应急计划与其他计划间的一致性；

f) 组织应规划应急处理时的信息处理、通信和环境等支撑能

i) 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；

j) 组织应维护硬件计划，保障异地运行时全部业务功能不受影响或很少受影响；

k) 应协调处理应急规划活动与事件处理活动；

l) 应急计划变更时，应告知相关方；

m) 对应急计划进行安全管理，以防泄露和未授权更改；

n) 应制定 ICS 故障的应急预案，以便在 ICS 发生故障时，可及时启动应急预案。

6.7.3 应急培训(CP-3)

本项要求包括：

a) 应制定应急培训计划，并向具有相应角色和职责的 ICS 用户提供应急培训；

b) 应定期或在 ICS 变更时，对相应人员进行应急培训；

c) 模拟事件场景以配合应急培训，提高人员在危难时刻具备高效的应对能力；

d) 使用自动化机制提供更加全面、真实的培训环境。

6.7.4 应急计划的测试和演练(CP-4)

本项要求包括：

a) 应测试和演练 ICS 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 ICS 完整恢复和重建到已知状态；

d) 应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) 应定期或应急计划变更时，进行应急计划的测试和演练；

f) 组织协调应急计划与其他相关计划相一致的测试和演练

状态；

i) 组织应采用自动化机制，[illegible]底、有效地测试和演练应急计划。

6.7.5 备用存储场所(CP-5)

本项要求包括：

a) 应建立备用存储场所，包括许可[illegible]

[illegible]

b) 对备用存储设备进行记录，保证其可[illegible]

c) 明确当发生区域性破坏或灾难时，备用存储设备[illegible]

[illegible]

本项要求包括：

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

b) 应按照已制定的ICS备份策略对用户级信息、系统级信息及ICS文档进行备份，增量备份应每天一次，全量备份应每周一次；

c) 应采取安全防护措施，保护备份信息的保密性、完整性和可用性；

d) 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；

e) 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；

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

g) 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；

h) 建立异[illegible]灾备中心，利用通信网络将信息实时备份到异地灾备中心；

i) 建设备份系统，实现ICS数据的自动备份。

6.7.9 ICS 恢复和重建(CP-9)

本项要求包括：

a) 应在 ICS 中断、受损或失败后将其恢复和重建到一个已知状态；

b) 应将系统状态变量作为恢复指标之一，并将其作为系统重建的一个部分；

c) 组织提供一套补偿的安全控制，定期将系统恢复到确定的状态；

d) 组织提供一套在规定的时间间隔内，将 ICS 组件恢复到安全和运行状态；

e) 按组织规定的时间内，配置实时或准实时的失败恢复能力；

f) 组织应对备份/恢复所用的硬件、软件和固件实施保护；

g) 应定期测试恢复信息，以验证可靠性和信息完整性。

6.8 物理和环境安全(PE)

6.8.1 物理和环境保护方针策略与规程(PE-1)

本项要求包括：

a) 应制定并发布物理和环境保护方针策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性；

b) 应制定并发布物理和环境保护规程，以推动物理和环境保护方针策略及与相关安全控制的实施；

[redacted]

a) 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。

6.8.5 输出设备的访问控制(PE-5)

本项要求包括：

a) 应对 ICS 输出设备进行物理访问控制以

b) 控制对输出设备的物理访问；

c) 确保只有授权人员获得输出信息；

d) 组织应对输出设备进行标记，标明该标

e) 组织应对输出设备可输出的信息。

6.8.6 物理访问监控(PE-6)

本项要求包括：

a) 应监视 ICS 物理访问以检测物理安

b) 组织应设置防盗报警系统，识别潜

c) 组织应采用自动化设备识别入侵，

d) 组织应采用视频监控，并保留视频

e) 应定期对物理访问日志进行审查；

f) 应在发生事件或发现事件迹象的情

d) 组织提供给 ICS 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[illegible]能力；

e) 组织提供 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。

6.8.11 应急照明(PE-11)

本项要求包括：

a) 应为 ICS 部署应急照明并进行维护，确保其在断电情况下的可用性；

b) 应在应急照明设施中包含紧急通道和疏散通道指示牌。

6.8.12 消防(PE-12)

本项要求包括：

a) 应为 ICS 部署火灾检测和消防系统或设备，并维护该设备；

b) 应为消防系统或设备配备独立电源；

c) 应使用防火设备或系统，该设备或系统在火灾事故中[illegible]

b） 应评估备用工作场所安全控制措施的可行性和有效性；

c） 应提供安全事件发生时与信息安全人员沟通的渠道。

6.8.17 信息泄露(PE-17)

本项要求包括：

a） 应避免因电磁泄露、传导等方式造成的信息泄露。

6.9 配置管理(CM)

6.9.1 配置管理方针策略和规程(CM-1)

本项要求包括：

a） 应制定并发布配置管理方针策略，内容至少应包括目的、范围、角色、责任、管理层承诺[illegible]

[illegible]门的协调、合规性；

b） 应制定并发布配置管理规程，以推动配置管理方针策略及与相关安全控制的实施，该规程应与相关法律、制度、策略、规章、标准和指南保持一致；

c） 应定期对配置管理方针策略及规程进行评审和更新。

6.9.2 [illegible]基线配置(CM-2)

本项要求包括：

a） 应制定、记录并维护 ICS 当前的配置基线；

b） 应定期或在系统发生重大变更、安装和更新系统组件后，对基线配置进行评审和更新；

c） 应保留旧版本 ICS 基线配置，以便必要时恢复配置；

d） 应定期根据组织要求，在系统部件进行整体安装和升级等情况下评审并调整 ICS 的基线配置；

e） 组织为开发和测试环境，维护一个基线配置，该配置与组织运行的基线配置是采用不同方式管理的；

f） 组织保留被认为可支持回滚的、老的基线配置版本；

g） 组织使用自动化机制，及时维护 ICS 配置，确保保持完整、准确、就绪可用的基线；

h） 组织应开发并维护已授权在组织 ICS 予以执行的软件列表，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；

i） 组织应开发并维护没有被授权可在组织 ICS 上执行的软件列表，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。

6.9.3 配置变更控制(CM-3)

本项要求包括：

a） 应明确系统受控配置列表中，包含了哪些变更内容；

b） 应评审所提交的 ICS 变更事项，并根据其影响结果，进行批准或否决，[illegible]

[illegible]更决策形成文件；

[illegible]更记录；

[illegible]动进行评审；

[illegible]管理部门，协调和监管配置变更的相关活动；

[illegible]应测试、确认这些对 ICS 的变更，并建立相应的文档；

[illegible]建立 ICS 配置变更记录文档，通知指定批准机构，强调在规定期限内[illegible]

[illegible]禁止变更，并在接受到指定的批准后，建立对 ICS 完成变更的文档；

c） 应将 ICS 相关的配置变[illegible]

d） 应保留对 ICS 配置的变[illegible]

e） 应对系统配置变更的活[illegible]

f） 应明确配置变更控制的[illegible]

g） 组织在实现 ICS 变更前[illegible]

h） 组织使用自动化机制，来[illegible]

[illegible]收有接受到的批准将[illegible]

i) 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，开发调整基线；

j) 组织需在配置变更管理部门中设置一个信息安全代表作为部门成员；

k) 变更控制管理部门和配置变更频率/条件应得到管[illegible]的批准；

l) 在 ICS 不支持自动生成配置变更审计记录的情况下，需要采用其他控制措施；

m) 应对获得的[illegible]进行阻止，只限于必要的变更，且对所有的变更加以严格控制。

6.9.4 变更安全影响分析(CM-4)

本项要求包括：

a) 在实施变更之前，应对 ICS 配置变更进行分析，判断该变更可能带来的潜在安全影响；

b) 在新软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[illegible]发生的安全影响；

c) 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[illegible]

6.9.5 对变更的访问限制(CM-5)

本项要求包括：

a) 应定义、记录、批准和实施与 ICS 变更相关的物理和逻辑访问限制；

b) 应限制 ICS 开发方和在线方对生产环境中[illegible]

c) 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；

d) 组织应使用自动化机制[illegible]

e) 组织应[illegible]系统配置在[illegible]期评审并重新评估 ICS 开发人员/集成人员的权利；

h) 组织应保护软件库，以免引入未授权的代码或恶意代码；

i) ICS 实现自动功能或机制，以发现不恰当的系统变更。

6.9.6 配置设置(CM-6)

本项要求包括：

a) 应依据安全配置检查清单，实[illegible]品的配置，并实现与运行需求一致的模式；

b) 应基于 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) 应根据相关策略和规程，监控配置设置项的变更；

d) 应使用自动机制，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) 应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；

f) 组织使用自动化机制，集中管理、应用并验证配置[illegible]设置；

g) 组织使用自动化机制，对未授权改变的配置改版作出响应；

h) 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；

i) ICS 在引入到生产环境前，应证实其符合安全配置指南；

j) 应有规程来控制在系统上运行的安全软件。

6.9.7 配置最小功能化(CM-7)

本项要求包括：

a) 应对信息系统按照仅提供最小功能进行配置，并按照定义的列表，对非必要功能、端口、协议和服务的使用进行合理性论证；

b) 应定期对信息系统进行评审，发现和排除不必要的功能、端口、协议和服务；

c) 应实现并消除不必要的功能、端口、协议和服务，实现对ICS进行风险控制；

d) 组织使用自动化机制，应对授权软件程序、未授权软件程序的执行；

e) 组织应确保提供了满足组织需求的功能、端口、协议和服务。

6.9.8 ICS 部件清单(CM-8)

本项要求包括：

a) 应制定ICS组件清单，并形成文件。该清单应能准确反映当前ICS，符合已授权的ICS边界，达到追踪和报告所需要的详细程度；

b) 当一个完整的组件安装和移除，或系统更新时，应更新系统组件清单；

a) 应对系统中存在的漏洞进行标识、报告并进行纠正；

b) 漏洞相关的软件和固件升级包在安装前，应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，应在适当的时间进行升级并明确升级和维护频率；

d) 应将漏洞修复并入组织的配置管理过程之中；

e) 统一管理漏洞修补程序和自动化升级程序；

c) 应向承担系统管理、监控或安全职责的相关人员传达安全警报建议和指示；

d) 应按照时间计划实施安全指示并通报完成情况；

e) 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。

6.10.6 安全功能验证(SI-6)

本项要求包括：

a) 应验证既定的安全功能是否正确运行；

b) 应在系统启动或重启时实施安全验证或者定期实施安全验证；

a) 应确定在特定运行环境中信息组件的平均故障间隔时间；
b) 应提供可替代的 ICS 组件、对组件进行激活和建立主备切换的机制；
c) 组织应在不迟于平均故障间隔时间内，或定期实现主备组件的切换；
d) 组织应禁止在无监督的情况下实施切换；
e) 组织应在定义的时间间隔内手动完成主备组件的切换；
f) 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。

6.10.12 信息的输出过滤(SI-12)

本项要求包括：

a) 应确认软件和应用输出的信息与期望内容相吻合。

6.10.13 内存防护(SI-13)

本项要求包括：

a) 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。

6.10.14 入侵检测和防护(SI-14)

本项要求包括：

a) 应在工业控制系统的安全建设方案中考虑部署入侵检测系统。

6.11 介质保护(MP)

6.11.1 介质保护方针策略与规程(MP-1)

本项要求包括：

a) 应制定并发布介质保护方针策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性；

存储介质、软盘、CD、DVD 等介质；

b) 应定义设施内用来存储信息和存放 ICS 的受控区域；

c) 应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；

d) 加密存储，物理安全保护；

e) 严格访问控制。

6.11.5 介质传递(MP-5)

本项要求包括：

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，应采用适当的安全防护措施进行保护和控制；

b) 应维护介质在受控区域之外传递过程的可[redacted]

c) 应对介质传递相关活动进行记录；

d) 应只允许授[redacted]

6.12.2 事件响应培训(IR-2)

本项要求包括：

a) 应制定事件响应培训计划，并定期对 ICS 用户进行符合其角色和责任的事件响应培训；

b) 应定期或在 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；

c) 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；

d) 组织使用自动化机制，提供更全面、更真实的培训环境。

6.12.3 事件响应测试和演练(IR-3)

本项要求包括：

a) 应定期以规定的测试方法测试方案的响应能力，以判断事件响应的有效性，并记录测试结果；

b) 应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；

c) 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；

d) 测试数据应认真地加以选择、保护和控制。

6.12.4 事件处理(IR-4)

本项要求包括：

a) 应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) 应协调事件处理活动与应急规划活动；

c) 应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；

d) 向有关的组织官员报告 ICS 中与所报告的安全事件相关的弱点、不足和脆弱性。

6.12.7 事件响应帮助(IR-7)

本项要求包括：

a) 应提供事件响应支持资源，该资源是组织的事件响应能力必不可少的，以向 ICS 用户处理、报告安全事件提供咨询和帮助；

b) 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；

c) 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。

6.12.8 事件响应计划(IR-8)

本项要求包括：

a) 应制定事件响应计划，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) 应评审事件响应计划并获得批准，并向组织内事件响应人员分发；

c) 应定期评审事件响应计划；

d) 应针对系统/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) 应将事件响应计划的变更通报组织内相关部门和人员；

f) 应使事件响应计划处于受控状态。

6.13 意识和培训(AT)

6.13.1 安全意识培养和安全培训方针策略和规程(AT-1)

本项要求包括：

a) 应制定并发布安全意识培养[redacted]

a) 应为 ICS 中的安全角色和具有安全职责的人员提供安全培训；
b) 应在新用户的培训中纳入安全培训；
c) 应定期或系统变更需要培训时，进行安全培训；
d) 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；
e) 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；
f) 组织根据初始或定义的频度开展人员和角色培训；
g) 组织应向内部人员提供安全培训，使其能够识别 ICS 存在的异常行为。

6.13.4 安全培训记录(AT-4)

本项要求包括：

a) 应记录并监视 ICS 安全培训活动，包括基本的安全意识培训和特定的 ICS 安全培训；
b) 应在规定的时间内保留培训记录。

6.14 访问控制(AC)

6.14.1 访问控制方针策略和规程(AC-1)

本项要求包括：

a) 应制定并发布访问控制策略和规程，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性；
b) 应制定并发布访问控制规程，以推动访问控制方针策略及与相关安全控制的实施；
c) 应定期对访问控制方针策略及规程进行评审和更新。

6.14.2 账户管理(AC-2)

本项要求包括：

a) 应建立[illegible]账号类型(即个人的、组织的、系统的、应用的、访客的/匿名的和临时的)，以支持不同的业务职能；
b) 应指定 ICS 账号管理员；
c) 应建立明确的组和角色的条件；
d) 应建立 ICS、组和角色的授权用户，明确每个账号的访问权限和其他必需的属性；
e) 创建 ICS 账号时，应获得相关人员的批准；
f) 应建立、激活、修改、关闭和注销账号的制度；
g) 应对 ICS 使用进行授权和监视；
h) 当账号需要删除、关闭、转移、变更时，应通报账号管理员；
i) 定期检查账号是否符合账号管理要求(如，是否符合系统[illegible]

[illegible]

a) ICS 资源的逻辑访问需得到授权和批准；
b) 针对所有主体和客体，应实施基于角色的访问控制策略；
c) 针对 ICS 范围内属性相同的主体和客体，执行统一策略；
d) 应限制将信息传递给未授权的主体和客体；
e) 应限制将权限授予给未授权的主体和客体；
f) 应限制对主体、客体、ICS 或其组件安全属性的变更；
g) 应对新创建或修改后的客体，限制变更其已经关联的安全属性；
h) 应限制对访问控制策略的再变更；
i) 应确保访问控制策略，不会对 ICS 的运营产生不利影响；
j) 在组织规定的用户和 ICS 相关资源上，执行组织定义的非自主访问控制策略；
k) 基于组织策略和规程，执行二元访问授权；
l) ICS 执行自主访问控制(DAC)策略；
m) 除了安全状态外，应禁止 ICS 访问公共网络等组织规定的、与安全有关的信息；
n) 在非安全的地方，加密或存储 ICS 安全相关的非在线关键或敏感信息。

6.14.4 信息流执行(AC-4)

本项要求包括：
a) ICS 内或互连系统间的信息流动需得到授权和批准；
b) 应建立组织机构与外部方交换信息和软件的协议；
c) 包含在电子邮件发送中的信息应给予适当的保护；
d) 应建立并实施策略和规程，以保护与业务系统互联相关的信息；
e) 应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。

6.14.5 职责的分割(AC-5)

本项要求包括：
a) 必要时，分离个体的职责，以便防止恶意活动；
b) 应定义 ICS 的访问授权策略，以支持职责分割；
c) 在 ICS 不能支持职责分割的情况下，应采取安全防护措施，对一个人承担多个角色进行有效管理。

6.14.6 最小权限(AC-6)

本项要求包括：
a) 组织应基于最小权限，对用户进行访问授权，使其根据组织使命、业务职能，来完成指定任务；
b) 组织应显式地对硬件、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；
c) 组织要求 ICS 系统具有访问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，审计任意对

6.14.7 不成功的录入尝试(AC-7)

本项要求包括：

a) ICS 应在组织规定的时间间隔内，按定义的次数，限制用户连续无效的访问尝试；

b) 自动按照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，延迟下一次登入执行；

d) 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；

e) 系统为插入在 ICS 中的移动设备提供附加的保护，即在 ICS 用户连续不成功登入定义次数后，净化来自移动设备的信息。

6.14.8 会话封锁(AC-8)

本项要求包括：

[illegible]

[illegible]屏幕上以前可见的信息；

d) ICS 应尽量采用会话锁定的方式，防止其他人对特定的工作站/节点的访问。在 ICS 操作员工作站/节点不适宜使用会话锁定的情况下，应采用其他适当的控制措施(例如，增加物理安全、人员安全和审计措施)。

6.14.9 远程访问(AC-9)

本项要求包括：

a) 授权、监督和控制所有对 ICS 的远程访问；

b) 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；

c) 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；

d) ICS 通过组织定义的访问控制点的数目，路由所有远程访问；

e) 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；

f) 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；

g) 组织监控对工业控制系统的授权远程访问，包括定期扫描未授权的无线访问点；

[illegible]

[illegible]织应禁止用户独自配置无线网络；

[illegible]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；

[illegible]织确保远程访问组织定义的安全功能和安全有关信息列表的会话，使用了附加的组织认可安全措施，并进行了相应的审计；

[illegible]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点对点无线网络的能力；

[illegible]除了特定运行需求所显式标识的部件外，组织限制被认为是不安全的网络协议。

6.14.10 无线访问(AC-10)

要求包括：

c) 应建立无线连接的使用限制、配置、连接要求和[illegible]

d) 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。

6.14.13 对程序源代码的访问控制(AC-13)

本项要求包括：

a) 应制定规程管理程序、代码和源程序库；

b) 应限制访问程序源代码。

6.15 维护(MA)

6.15.1 系统维护方针策略与规程(MA-1)

本项要求包括：

a) 应制定并发布 ICS 系统维护方针策略，应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性；

b) 应制定并发布 ICS 系统维护规程，以推动 ICS 系统维护方针策略及与相关安全控制的实施；

c) 应定期对 ICS 系统维护方针策略及规程进行评审和更新。

6.15.2 受控维护(MA-2)

本项要求包括：

a) 应根据厂商或供应商的规格说明以及组织的要求，对 ICS 组件的维护和修理进行规划、实施、

k) 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。

6.15.3 维护工具(MA-3)

本项要求包括：

a) 应批准、控制并监视 ICS 维护工具的使用；

b) 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；

c) 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；

d) 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

诺、相关部门的协调、合规性；

b) 应制定并发布审计和可核查性规程，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) 应定期对审计和可核查性方针策略及规程进行评审和更新。

6.16.2 审计事件(AU-2)

本项要求包括：

a) 组织应明确规定审计事件的范围和审计内容。应至少对以下 ICS 事件进行审计：成功和未成功的账号登录事件、账号管理事件、客体访问、策略变更、特权功能、进程跟踪、系统事件等；

b) 应与需要审计信息的其他相关部门进行安全审计协调，增强相互间的支持，并帮助确定审计事件清单；

c) 应提供已确定的审计事件清单，并阐述其足以支撑安全事件事后调查的理由；

d) 应确定需连续审计的事件清单；

e) 应[illegible]根据安全威胁情况的变化及时对审计事件清单进行评审和更新；

f) 组织应定义审计事件进行定期的审核和升级；

g) 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；

[illegible]

h) 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。

6.16.3 审计记录内容(AU-3)

本项要求包括：

a) 应在审计记录中至少包含：事件类型、事件发生的时间和地点、事件来源、事件结果、与事件相关实体或主体的身份等；

b) 审计记录应使用主题、类型、位置等信息标识审计事件；

c) 组织应集中管理审计内容。

6.16.4 对审计处理失败的响应(AU-4)

本项要求包括：

a) 应在审计处理失败时向相关人员报警。

c) 应使用自动化机制将禁会审查、分析及报告的过程以支持对可疑活动进行的调查程响应；

d) 应对不同审计库上的审计记录进行关联性分析，以使感知 ICS 整体的安全态势。

6.16.6 审计归约和报告生成(AU-6)

本项要求包括：

a) 应具有审计归约和报告生成的功能，支持按需审计评审、分析和报告要求以及安全事件事后调查；

b) 不应改变原始的审计记录；

c) 应尽量在隔离的系统而不是 ICS 本身进行审计归约和报告生成。

6.16.7 时间戳(AU-7)

本项要求包括：

a) 应使用 ICS 内部时钟生成审计记录的时间戳；

b) 应定期对内部时钟与权威时间源进行同步。

6.16.8 审计信息的保护(AU-8)

本项要求包括：

a) 应保护审计信息和审计工具，以[illegible]受未授权访问、篡改、删除；

b) 应定期将审计记录备份到与所审系统或组件不同物理位置的系统或组件之中；

c) 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；

d) 应采用加密机制保护审计信息和审计工具的完整性；

e) 组织对访问审计功能的授权，只限制为一个[illegible]

d) 应尽量使用自动化机制生成审计记录；

e) 应按时间相关将审计记录从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；

f) 应产生系统的(逻辑或物理)审计跟踪记录的标准化格式；

g) 提供在组织规定的时间范围内，进行 ICS 审核的能力。

6.17 标识和鉴别(IA)

6.17.1 标识与鉴别方针策略和规程(IA-1)

本项要求包括：

a) 应制定并发布标识与鉴别方针策略，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性；

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

c) 应定期对标识与鉴别方针策略及规程进行评审和更新。

6.17.2 组织用户的标识与鉴别(IA-2)

本项要求包括：

系统应唯一标识和鉴别组织用户(或代表组织用户执行过程)，供应商人员或访客等户或代表该用户的进程；

授权账户的网络访问，使用多因子鉴别；

授权账户的本地访问，使用多因子鉴别；

未授权账户的本地访问，使用多因子鉴别；

已授权账户的网络访问，使用多因子鉴别；

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，要用体鉴别机制对个体进行鉴别；

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；

未授权账户的本地和网络访问，使用口令或个人标识码；

S 对本地访问，使用口令或个人标识码。

6.17.3 设备的标识与鉴别(IA-3)

本项要求包括：

建立一个或多个本地、远程、网络连接前，应定义的特定设备和/或设备类型列表；

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；

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；

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；

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

h) 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；

i) 应按组织规定标识用户状态的特征，单一地标识用户，以此来管理用户标识符；

j) ICS动态地管理标识符、属性以及相关联的访问授权。

6.17.5 鉴别管理（IA-5）

本项要求包括：

a) 初始鉴别分发时，应验证鉴别接收对象（个人、组、角色或设备）的身份；

b) 应确定组织规定的初始鉴别的内容；

c) 应确保鉴别对于其预期[illegible]具有足够强的机制；

d) 应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) 在信息系统安装之前应变更鉴别的默认内容；

f) 应建立鉴别的最小和最大生存时间、限制以及再用条件；

g) 应定期变更/更新鉴别；

h) 应保护鉴别内容，以防未授权泄露和更改；

i) 应要求个人采取由设备或特定安全措施来保护鉴别；

j) 当组/角色账户的成员发生变化时，应变更这些账户的鉴别；

k) 对于基于PKI的鉴别，ICS应：

1) 针对一个接受的可信赖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账户；

l) 组织要求接受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；

m) 组织使用自动化工具来确定鉴别符对抗御企图揭示或猜[illegible]

a) 系统应使用密码模块鉴别机制，该密码模块应满足相应的法律法规、规章和标准。

6.17.8 非组织用户的标识与鉴别(IA-8)

本项要求包括：

a) 信息系统应唯一标识和鉴别非组织用户(信息系统用户)或代表非组织用户的进程；

b) ICS 接受并鉴别其他相关机构发布的单子标识与鉴别；

c) ICS 只接受经权威机构批准的第三方认证；

d) 组织只采用相关权威机构批准的 ICS 组件第三方认证。

附 录 A
（资料性附录）
不同安全级别的 ICS 安全管理基本要求对应表

为便于对不同安全级别的工业控制系统进行适于其级别的安全管理，本附录结合第 6 章中的 ICS 安全管理基本控制措施，给出了各级 ICS 安全管理基本要求对应表作为安全控制基线（见表 A.1），四个级别分级可依据 GB/T 36324—2018 等标准。针对 ICS 安全管理基本控制措施的裁剪方式参见 GB/T 32919—2016。

表 A.1 不同安全级别的 ICS 安全管理基本要求对应表

要求	安全级			
	第一级	第二级	第三级	第四级
安全评估和授权(CA)				
安全评估和授权方针策略及规程(CA-1)	a)～c)	a)～c)	a)～c)	a)～c)
安全评估(CA-2)	a)～c)	a)～d)	a)～f)	a)～f)
ICS 连接管理(CA-3)	a)～c)	a)～c)	a)～e)	a)～e)
监控计划与时间节点(CA-4)	a)～b)	a)～b)	a)～c)	a)～c)
安全授权(CA-5)	a)～c)	a)～c)	a)～c)	a)～e)
持续监控(CA-6)	a)	a)～b)	a)～c)	a)～g)
渗透测试(CA-7)	—	—	a)	a)～c)
内部系统的连接(CA-8)	a)～b)	a)～b)	a)～b)	a)～c)
系统和服务获取(SA)				
系统及服务获取的方针策略及规程(SA-1)	a)～c)	a)～c)	a)～c)	a)～c)
资源配置(SA-2)	a)～c)	a)～c)	a)～c)	a)～c)
系统开发生命周期(SA-3)	a)～c)	a)～c)	a)～c)	a)～c)
采购过程(SA-4)	a)～b)	a)～e)	a)～f)	a)～l)
ICS 信息系统文档(SA-5)	a)～c)	a)～f)	a)～f)	a)～j)
外部 ICS 服务(SA-6)	a)～c)	a)～c)	a)	

表 A.1（续）

要求	安全级			
	第一级	第二级	第三级	第四级
6.4.7 第三方人员安全(PS-7)	a)～d)	a)～d)	a)～d)	a)～d)
6.4.8 人员处罚(PS-8)	a)	a)	a)	a)
6.5 规划(PL)				
6.5.1 安全规划策略及规程(PL-1)	a)～c)	a)～c)	a)～c)	a)～c)
6.5.2 系统安全规划(PL-2)	a)～d)	a)～d)	a)～d)	a)～g)
6.5.3 行为规则(PL-3)	a)～b)	a)～b)	a)～c)	a)～d)
6.5.4 信息安全架构(PL-4)	—	a)～c)	a)～d)	a)～d)
6.5.5 安全活动				
6.6.1 物理访问控制(PE-1)				
6.6.2 物理访问监控(PE-2)				
6.6.3 传输介质访问控制(PE-3)				
6.6.4 输出设备访问控制(PE-4)				
6.6.5 物理访问记录(PE-5)				

表 A.1（续）

要求	安全级			
	第一级	第二级	第三级	第四级
6.8.7 访问记录(PE-7)		a)～b)	a)～d)	

表 A.1（续）

要求	安全级			
	第一级	第二级	第三级	第四级
6.10.12 信息的输出过滤(SI-12)	—	a)	a)	a)
6.10.13 内存防护(SI-13)	—	—	a)	a)
6.10.14 入侵检测和防护(SI-14)	—	a)		
6.12.2 事件响应培训(IR-2)	a)～b)	a)～b)	a)～d)	a)～d)
6.12.3 事件响应测试和演练(IR-3)	—	a)～c)	a)～c)	a)～d)
6.12.4 事件处理(IR-4)	a)～c)	a)～e)	a)～h)	a)～h)
6.12.5 事件监控(IR-5)	a)	a)～b)	a)～b)	a)～b)
6.12.6 事件报告(IR-6)	a)～b)	a)～d)	a)～d)	a)～d)
6.12.7 事件响应帮助(IR-7)	a)	a)～c)	a)～c)	a)～c)
12.8 事件响应计划(IR-8)	a)～f)	a)～f)	a)～f)	a)～f)
13 意识和培训(AT)				
13.1 安全意识培养和安全培训方针策略和规程(AT-1)	a)～c)	a)～c)	a)～c)	a)～c)
13.2 安全意识培训(AT-2)	a)～d)	a)～e)	a)～f)	a)～f)
13.3 基于角色的安全培训(AT-3)	a)～d)	a)～e)	a)～g)	a)～g)
13.4 安全培训记录(AT-4)	a)～b)	a)～b)	a)～b)	a)～b)
14 访问控制(AC)				
14.1				

表 A.1（续）

要求	安全级			
	第一级	第二级	第三级	第四级
6.14.8 会话封锁(AC-8)	—	a)～b)	a)～b)	a)～d)
6.14.9 远程访问(AC-9)	a)	a)～e)	a)～e)	a)～m)
6.14.10 无线访问(AC-10)	a)～c)	a)～d)	a)～h)	a)～k)
6.14.11 移动设备的访问控制(AC-11)	a)～g)	a)～j)	a)～n)	a)～n)
6.14.12 外部 ICS 的使用(AC-12)	a)～b)	a)～b)	a)～d)	a)～d)
6.14.13 对程序源代码的访问控制(AC-13)	a)～b)	a)～b)	a)～b)	a)～b)
6.15 维护(MA)				
6.15.1 系统维护方针策略与规程				

参 考 文 献

[1] GB/T 36324—2018 信息安全技术 工业控制系统信息安全分级规范

[2] 关于加强工业控制系统信息安全管理的通知(工信部协〔2010〕451 号)

[3] 电力监控系统安全防护规定(国家发改委令第 14 号)

[4] 电力行业信息系统安全等级保护基本要求(电监信息〔2012〕62 号)

[5] 电力行业网络与信息安全管理办法(国能安全〔2014〕317 号)

[6] 电力行业信息安全等级保护管理办法(国能安全〔2014〕318 号)

[7] NIST SP 800-82 Guide to Industrial Control Systems(ICS)Security

[8] NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations