

ICS ××.×××.××
B××

DB××

河北省地方标准

DB 13/ T ×××—××××

信息安全技术 工业控制系统安全保护技术规范

Information security technology- Technical specifications for safety
control of industrial control systems

(征求意见稿)

×××× - ×× - ×× 发布

×××× - ×× -×× 实施

河北省质量技术监督局

发布

目 次

前言.....	II
引言.....	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 系统能力要求.....	1
4.1 物理和环境安全.....	1
4.2 网络安全.....	2
4.3 主机安全.....	5
4.4 scada 安全.....	7
4.5 plc/dcs 安全.....	12
附录 A（规范性附录）	15
参考文献.....	20

前 言

本标准按照GB/T1.1-2009给出的规则起草。

本标准由河北省工业和信息化厅提出并归口。

本标准起草单位：河北省信息安全测评中心、河北金信网络技术开发服务有限公司、唐山港集团股份有限公司。

本标准主要起草人：陶卫江、张凤臣、闫利平、黄亮、张友平、李鹏、刘艳、梁志、王辙、崔健、李娜、李冀、任旭东、高飞、张争、付江、张桐、甘振旺、延海波、李超、和德明、侯志方、王会娟。

引 言

随着工业化和信息化的高度融合，工业控制系统的信息安全问题越来越受到关注。为了增强工业控制系统的安全防护能力，从技术上加强工业控制系统的防护能力，特制定本标准。

本标准在 GB/T30976.1-2014 等技术类标准的基础上，根据现有技术的发展水平，提出和规定了工业控制系统的最低安全保护技术要求，即技术安全要求，本标准即适用于工业控制系统的安全测评，又适用于指导工业控制系统的安全建设和管理，以及工业控制系统安全主管部门的监督检查。

信息安全技术

工业控制系统安全保护技术规范

1 范围

本标准规定的工业控制系统信息安全技术要求。

本标准适用于系统设计方、设备生产商、系统集成商、用户、资产所有人以及评估认证机构等对工业控制系统信息安全进行评估时使用。

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，仅所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/T30976.1-2014 工业控制系统信息安全第一部分：评估规范

3 术语和定义

GB/T30976.1-2014 中界定的以及下术语和定义适用于本标准。

4 系统能力要求

4.1 物理和环境安全

4.1.1 安全区域

4.1.1.1 物理安全周边

本项目包括但不限于：

- a) 应设置物理安全管理制度，规定了对组织机构场所和重要系统的物理访问控制；
- b) 重要区域（如中控机房和现场总线机房）应有相应的控制措施，如门禁、视频监控、消防、红外探测器等设备。

4.1.1.2 物理入口控制

本项目包括但不限于：

- a) 重要区域应设置有门禁，或配置有专人值守，控制人员的进出；
- b) 门窗应有防盗措施；
- c) 现场总线机房需具备门禁等防盗防破坏措施，禁止人员随意接触关键设备。

4.1.1.3 办公室、房间和设施的安全防护

本项目包括但不限于：

- a) 应有针对办公区域的管理措施，外部人员的访问应经过审批，并有专人陪同；
- b) 重要区域应设置有控制措施，如门禁、视频监控等。

4.1.1.4 外部和环境的安全防护

本项目包括但不限于：

- a) 重要区域应有防雷、防水、防火、温湿度控制等安全防护措施；
- b) 现场总线机房应有防雷、防水、防火等防护措施。

4.1.1.5 在安全区域工作

本项目包括但不限于：

在操作手册和岗位管理制度中应有操作规程对人员、设备的安全做出规定。

4.1.1.6 公共访问、交换区安全

本项目包括但不限于：

公共访问、交换区域应与生产系统应有隔离防护措施。

4.1.2 设备安全

4.1.2.1 设备安置和保护

本项目包括但不限于：

- a) 设备安装应合理、牢固；
- b) 关键设备需有物理安全防护措施，避免被盗窃和被破坏。

4.1.2.2 支持性设施

本项目包括但不限于：

应保证系统正常运行的支持性设备运行正常，例如电力系统等。

4.1.2.3 布缆安全

本项目包括但不限于：

通信线缆和电源线应隔离铺设，并且远离电磁辐射源，避免电磁干扰引起数据传输错误。

4.1.2.4 设备维护

本项目包括但不限于：

- a) 应指定责任部门和人员负责设施的定期维护管理；应有相关管理规定；
- b) 设备管理制度中应包括对各类设备维护维修等方面要求；
- c) 维护记录，内容应全面、真实。

4.1.2.5 组织机构场所外的设备安全

本项目包括但不限于：

场外的设备（如部署于现场环境的 plc 设备等）应具备防盗、防拆、坚固耐用等要求，应能够适应所处的物理环境。

4.1.2.6 设备的安全处置或再利用

本项目包括但不限于：

- a) 不同设备的存放环境应采取与其相应的保护措施，设备管理制度中应包括对设备的存放环境、报废或再利用等方面；
- b) 应有设备的报废或再利用清单；
- c) 重要设备在报废或再利用前应彻底清除内含有的敏感信息。

4.1.2.7 资产的移动

本项目包括但不限于：

设备管理制度应对资产的转移做出规定，包括转移过程有专人负责，转移流程，移动前后资产的存放环境等。

4.1.3 资源可用性

4.1.3.1 紧急电源

本项目包括但不限于：

- a) 控制系统应具备紧急电源设施，应可提供与紧急电源设施之间的切换；
- b) 紧急电源之间的切换应不会影响到现有的安全状态。

4.2 网络安全

4.2.1 网络访问控制

4.2.1.1 网络服务的策略

本项目包括但不限于：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 系统对外提供的服务应仅限业务范围之内；

- c) 应制定了对网络服务的访问控制策略;
- d) 如制定了规则, 应测试访问控制规则是否有效。

4.2.1.2 外部连接的用户鉴别

本项目包括但不限于:

- a) 网络与外部连接情况应与相关的管理制度且与网络拓扑结构相符;
- b) 系统内部终端连接外部网络情况应与相关的管理制度且与网络拓扑结构相符;
- c) 如与外部网络有连接, 应通过措施进行控制;
- d) 网络内部如有 vpn 接入, 应制定了有效的控制措施。

4.2.1.3 网络上设备标识

本项目包括但不限于:

- a) 网络上设备应有标识;
- b) 网络上设备标识, 应有标识命名规则;
- c) 网络设备标识应唯一。

4.2.1.4 远程诊断和配置端口的保护

本项目包括但不限于:

对设备远程维护端口应设置访问控制规则, 只允许特定 ip 可以访问。

4.2.1.5 网络隔离

本项目包括但不限于:

- a) 重要生产系统应部署在网络内部, 重要网段与其他网段间应采用可靠的技术手段进行隔离;
- b) 应根据部门职能、重要性划分出不同的子网。

4.2.1.6 网络连接控制

本项目包括但不限于:

重要网段与其他网段之间的访问应有访问控制措施。

4.2.1.7 经由非可信网络的访问

本项目包括但不限于:

应具备监视和控制所有经由不可信网络对控制系统访问的措施。

4.2.1.7.1 明确地对访问请求的批准

本项目包括但不限于:

控制系统应提供能力默认拒绝来自不可信网络的访问。

4.2.1.8 无线使用控制

本项目包括但不限于:

- a) 应具备对无线访问的授权、监视和限制的能力;
- b) 应具备认证机制保护无线访问。

4.2.1.8.1 对未授权的无线设备进行识别和报告

本项目包括但不限于:

- a) 应具备扫描物理环境内发射信号的无线设备的功能;
- b) 应具备对物理环境内发射信号的未授权的无线设备进行识别和报告的能力。

4.2.2 监视

4.2.2.1 审计记录

本项目包括但不限于:

- a) 系统应具备日志功能, 如果具备, 日志功能应开启;
- b) 应对网络系统中网络设备的运行状况、用户行为等进行日志记录;
- c) 日志记录应包含时间、日期、用户、事件等相关事项。

4.2.2.2 监视系统的使用

本项目包括但不限于：

系统日志应对系统资源使用情况进行记录，包括网络流量、资源占用率等。

4.2.2.3 日志信息的保护

本项目包括但不限于：

应对审计日志进行保护，避免受到预期的删除、修改和覆盖。

4.2.2.4 管理员和操作日志

本项目包括但不限于：

系统日志应对管理员登陆和操作进行记录，内容应包括用户名、日期、时间、登陆ip，操作内容及结果等。

4.2.2.5 故障日志

本项目包括但不限于：

应对系统故障或错误进行日志记录，记录内容应包括日期、时间、系统故障或系统错误内容等。

4.2.2.6 时钟同步

本项目包括但不限于：

a) 系统时间应与标准时区时间一致；

b) 如果与互联网有连接，windowstime 服务应运行，时间服务器应设置正确。

4.2.3 限制的数据流

4.2.3.1 网络分区

本项目包括但不限于：

a) 应具备控制系统网络与非控制系统网络的逻辑分区功能；

b) 应具备关键控制系统网络与其他控制系统网络的逻辑分区功能。

4.2.3.1.1 物理网络分区

本项目包括但不限于：

a) 控制系统网络与非控制系统网络之间应进行了物理划分；

b) 关键控制系统网络与其他控制系统网络之间应进行了物理划分。

4.2.3.1.2 与非控制系统网络的独立性

本项目包括但不限于：

控制系统与非控制系统网络之间是否有连接。

4.2.3.1.3 关键网络的逻辑和物理隔离

本项目包括但不限于：

应采取措施将关键控制系统与其他控制系统进行逻辑和物理隔离。

4.2.3.2 区域边界防护

本项目包括但不限于：

控制系统应具备边界防护设备，对所有区域边界的外部接口进行管理。

4.2.3.2.1 默认拒绝，例外允许

本项目包括但不限于：

边界防护设备，应具备默认拒绝，例外允许的原则进行功能配置。

4.2.3.2.2 孤岛模型

本项目包括但不限于：

边界安全设备应具备当检测到安全事件时拒绝所有访问的功能。

4.2.3.2.3 故障关闭

本项目包括但不限于：

边界设备应具备当边界防护机制出现操作故障时,可关闭所有访问的功能。

4.2.4 持续监视

4.2.4.1 持续监视

本项目包括但不限于:

控制系统应具备检测攻击的工具。

4.2.5 资源可用性

4.2.5.1 拒绝服务的防护

本项目包括但不限于:

应具备防护拒绝服务攻击的能力,或以降级模式运行,攻击事件不应应对任何功能安全相关系统产生不利影响。

4.2.5.1.1 管理通信负荷

本项目包括但不限于:

应提供管理通信负荷的能力(例如使用限速)来削减拒绝服务攻击事件。

4.2.5.1.2 限制拒绝服务攻击对其他系统和网络的影响

本项目包括但不限于:

应提供能力限制所有用户(人、软件进程和设备)引发拒绝服务攻击事件的能力,避免影响其他控制系统和网络。

4.3 主机安全

4.3.1 操作系统访问控制

4.3.1.1 安全登录规程

本项目包括但不限于:

- a) 应对登陆操作系统和数据库的用户进行身份鉴别;
- b) 应启用登录失败处理功能,可采取结束会话、限制非法登录次数和自动退出等措施;
- c) 当对服务器进行远程管理时,应采取必要措施防止鉴别信息在网络传输过程中被窃听。

4.3.1.2 用户标识和鉴别

本项目包括但不限于:

- a) 应为操作系统和数据库系统的不同用户分配不同的用户名,确保用户名具有唯一性;
- b) 应根据管理用户的角色分配权限,实现管理用户的权限分离,仅授予管理用户所需的最小权限;
- c) 应严格限制默认帐户的访问权限,重命名系统默认帐户;
- d) 应及时删除多余的、过期的账户,避免共享账户的存在。

4.3.1.3 口令管理系统

本项目包括但不限于:

- a) 操作系统和数据库系统管理用户身份鉴别信息应具有不易被冒用的特点,口令应有复杂度要求并定期更换;
- b) 修改系统默认口令。

4.3.1.4 系统实用工具的使用

本项目包括但不限于:

应设置访问控制规则,限制用户对资源的访问。

4.3.1.5 会话超时

本项目包括但不限于:

应根据安全策略设置登录终端的操作超时锁定。

4.3.1.6 联机时间的限定

本项目包括但不限于：

- a) 网络内是否存在安装在高风险位置的敏感应用程序；
- b) 如存在此类程序，应设置了联机时间（如无特殊要求，则设为正常办公时间）。

4.3.2 监视

4.3.2.1 审计记录

本项目包括但不限于：

- a) 系统应开启日志功能；
- b) 应对系统中系统关键事件、用户行为等进行日志记录；
- c) 日志记录需包含时间、日期、用户、事件等相关事项。

4.3.2.2 监视系统的使用

本项目包括但不限于：

应对系统资源使用情况进行记录，包括网络流量、资源占用率等。

4.3.2.3 日志信息的保护

本项目包括但不限于：

应对审计日志进行保护，避免受到预期的删除、修改和覆盖。

4.3.2.4 管理员和操作日志

本项目包括但不限于：

应对管理员登陆和操作进行记录，内容应包括用户名、日期、时间，操作内容及结果等。

4.3.2.5 故障日志

本项目包括但不限于：

应对系统故障或错误进行日志记录，记录内容包括日期、时间、系统故障或系统错误内容等。

4.3.2.6 时钟同步

本项目包括但不限于：

- a) 系统时间应与标准时区时间一致；
- b) 如果与互联网有连接，时间服务应运行，时间服务器应设置正确。

4.3.3 恶意代码防护

4.3.3.1 恶意代码保护

本项目包括但不限于：

- a) 系统应安装有恶意代码防护产品；
- b) 恶意代码防护产品的防护功能应配置和启用；
- c) 恶意代码防护产品的特征库应为最新版本。

4.3.3.2 恶意代码防护的中央管理和报告

本项目包括但不限于：

应具备对恶意代码防护机制进行集中管理和报告的功能。

4.3.4 限制的数据流

4.3.4.1 禁止所有的一般目的的个人通信

本项目包括但不限于：

系统边界设备的设置，应具备禁止传输和接收一般目的的个人通信功能，如 email 或即时通讯软件等。

4.3.5 资源可用性

4.3.5.1 最小功能化

本项目包括但不限于：

操作系统应禁止或限制了其他多余的功能、端口、协议和/或服务。

4.3.5.2 资源管理

本项目包括但不限于：

应提供安全功能对系统资源使用限制的能力，防止资源耗尽。

4.3.6 使用控制

4.3.6.1 对便携和移动设备的使用控制

本项目包括但不限于：

- a) 应具备安全措施对便携和移动设备进行禁用和控制；
- b) 应具备对便携和移动设备进行监视和记录的功能；
- c) 控制系统应具备限制代码和数据传入传出便携和移动设备的能力。

4.3.6.1.1 便携和移动设备的安全状态的实施

本项目包括但不限于：

- a) 应具备安全措施在控制系统提供授权连接前对便携和移动设备进行安全扫描；
- b) 应对扫描结果进行监视和记录。

4.3.6.2 移动代码

本项目包括但不限于：

- a) 系统是否提供禁用/控制使用移动代码的功能；
- b) 应提供监视和记录移动代码的功能；
- c) 应定义限制使用的移动代码技术列表。

4.3.6.2.1 移动代码的完整性

本项目包括但不限于：

应提供在允许代码执行前验证移动代码的完整性的能力。

4.3.7 数据保密性

4.3.7.1 信息存留

本项目包括但不限于：

操作系统硬盘被移作他用时，应清除其储存的数据资源，确保无法被其他用户获取。

4.4 scada 安全

4.4.1 标识和认证管理

4.4.1.1 用户（人）的标识和认证

本项目包括但不限于：

控制系统应提供标识和认证所有用户（人）的能力。

4.4.1.1.1 唯一标识和认证

本项目包括但不限于：

控制系统应对所有用户（人）提供唯一标识和认证的能力。

4.4.1.1.2 非可信网络的多因子认证

本项目包括但不限于：

通过非可信网络访问（远程访问）控制系统时，控制系统应为其提供多因子认证的能力。

4.4.1.1.3 对所有网络的多因子认证

本项目包括但不限于：

控制系统应为所有用户（人）访问控制系统提供多因子认证的能力。

4.4.1.2 软件进程和设备的标识和认证

本项目包括但不限于：

控制系统应提供标识和认证所有用户（软件进程和设备）的能力。

4.4.1.2.1 唯一标识和认证

本项目包括但不限于：

控制系统应对所有用户（软件进程、设备）提供唯一标识和认证的能力。

4.4.1.3 账号管理

本项目包括但不限于：

控制系统应提供对所有账户的管理，包括创建、激活、修改、禁用和移除账户的能力。

4.4.1.3.1 统一的账号管理

本项目包括但不限于：

控制系统应提供能力支持统一的帐号管理。

4.4.1.4 标识符管理

本项目包括但不限于：

控制系统应提供按照用户、组、角色和/或控制系统接口管理标识符（例如用户 id）的能力。

4.4.1.5 认证码管理

本项目包括但不限于：

- a) 控制系统应具有定义初始认证码的能力；
- b) 在控制系统安装完毕后，应可变更默认认证码；
- c) 应具备周期性更改认证码的功能；
- d) 应保护认证码存储和传输时不被未经授权的泄露和更改。

4.4.1.5.1 软件进程标识凭证的硬件安全

本项目包括但不限于：

对于软件进程和设备用户，控制系统应提供使用硬件机制的保护相关认证码的能力。

4.4.1.6 无线访问管理

本项目包括但不限于：

对参与无线通信的所有的用户（人、软件进程或设备），控制系统应提供标识和认证的能力。

4.4.1.6.1 唯一标识和认证

本项目包括但不限于：

对参与无线通信的所有的用户（人、软件进程或设备），控制系统应提供唯一标识和认证的能力。

4.4.1.7 口令认证的加强

本项目包括但不限于：

对于使用口令认证的控制系统，控制系统应提供能力，实施可配置的基于最小长度和不同字符类的口令强度。

4.4.1.7.1 对用户（人）的口令生成和口令有效期限制

本项目包括但不限于：

控制系统应为用户（人）提供口令重用次数限制和最小/最大有效期限制功能。

4.4.1.7.2 对所有用户的口令有效期限制

本项目包括但不限于：

控制系统应为所有用户提供实施口令最小和最大有效期限制的能力。

4.4.1.8 公钥基础设施证书

本项目包括但不限于：

当使用公钥基础设施 pki 时，控制系统应提供能力按照普遍接受的最佳实践运行 pki 或从现 pki 中获取公钥证书。

4.4.1.9 公钥认证加强

本项目包括但不限于：

使用公钥认证的控制系统，应具备证书有效性验证和标识映射功能。

4.4.1.9.1 公钥认证的硬件安全

本项目包括但不限于：

控制系统应提供能力，按照普遍接受的安全工业实践和推荐，通过硬件机制保护相关的私钥。

4.4.1.10 认证反馈

本项目包括但不限于：

在认证过程中，控制系统应提供将认证信息反馈模糊化的能力。

4.4.1.11 失败的登陆尝试

本项目包括但不限于：

控制系统应具备登录失败处理功能。

4.4.1.12 系统使用通知

本项目包括但不限于：

控制系统应具备在认证之前显示配置好的通知的功能。

4.4.2 使用控制

4.4.2.1 授权的执行

本项目包括但不限于：

在所有接口上，控制系统应具备权限分离和最小特权功能。

4.4.2.1.1 对所有用户执行授权

本项目包括但不限于：

在所有接口上，控制系统应提供能力按照权限分离和最小特权分配给所有用户（人、软件进程和设备）授权的功能。

4.4.2.1.2 许可映射到角色

本项目包括但不限于：

控制系统应为资产所有者提供修改许可到角色的映射能力。

4.4.2.1.3 主管越权

本项目包括但不限于：

控制系统应支持主管在可配置的时间内或事件顺序上手工越权于当前用户（人）的授权。

4.4.2.1.4 双授权

本项目包括但不限于：

在行为可能对工业流程产生严重影响之处，控制系统应支持双授权。

4.4.2.2 会话锁

本项目包括但不限于：

控制系统应具备用户超时锁定功能。

4.4.2.3 远程会话终止

本项目包括但不限于：

控制系统应提供在可配置的不活跃时间周期后自动终止远程会话或由用户手动终止远程会话的能力。

4.4.2.4 并发会话控制

本项目包括但不限于：

对任意给定用户（人、软件进程或设备），控制系统应提供将每个接口的并发会话的数目限制为一个可配置的数目的能力。

4.4.2.5 可审计的事件

本项目包括但不限于：

- a) 访问控制、请求错误、系统事件、备份和存储、配置变更、潜在侦查行为和审计日志事件；
- b) 每个审计记录应包括时间戳、源、类别、类型、事件 id 和事件结果。

4.4.2.5.1 中央管理的、系统范围的审计跟踪

本项目包括但不限于：

- a) 控制系统应具备对整个控制系统内多个元器件的审计记录进行中央管理的功能；
- b) 控制系统应具备审计记录输出功能。

4.4.2.6 审计存储容量

本项目包括但不限于：

控制系统应具备预防审计存储容量超出限制的功能。

4.4.2.6.1 达到审计记录存储容量上限时发出警告

本项目包括但不限于：

控制系统达到审计记录存储上限时应具备发出警告功能。

4.4.2.7 审计处理失败时的响应

本项目包括但不限于：

控制系统应具备对审计流程失败时提供适当响应的功能。

4.4.2.8 时间戳

本项目包括但不限于：

控制系统审计记录应包含时间戳。

4.4.2.8.1 内部时间同步

本项目包括但不限于：

控制系统应提供以可配置的频率同步内部系统时钟的能力。

4.4.2.8.2 时间源的完整性保护

本项目包括但不限于：

时间源应被保护不受未授权的变更，其变更应触发审计事件。

4.4.2.9 不可否认性

本项目包括但不限于：

控制系统应具备对给定用户（人）的行为提供不可否认性的能力。

4.4.2.9.1 所有用户的不可否认性

本项目包括但不限于：

控制系统应具备对对所有用户（人、软件进程、设备）的行为提供不可否认性的能力。

4.4.3 系统完整性

4.4.3.1 通信完整性

本项目包括但不限于：

控制系统应具备通信传输完整性的功能。

4.4.3.1.1 基于密码技术的完整性保护

本项目包括但不限于：

控制系统应提供能力采用密码技术来保证信息在传输过程中的完整性。

4.4.3.2 安全功能验证

本项目包括但不限于：

控制系统应具备在工厂验收测试（fat）、现场验收测试（sat）或预定维护时系统运行正常的安全功能或方法，且发现异常后可进行报告。

4.4.3.2.1 安全功能验证的自动化机制

本项目包括但不限于：

控制系统应提供自动化验证机制，在 fat、sat 或预定维护时测试系统安全的功能。

4.4.3.2.2 正常运行中的安全功能验证

本项目包括但不限于：

控制系统应支持正常运行时的安全功能测试。

4.4.3.3 软件和信息完整性

本项目包括但不限于：

控制系统应提供能力检测、记录、保护软件和信息不受未经授权的变更。

4.4.3.3.1 对破坏完整性进行自动通知

本项目包括但不限于：

应具备自动化方法验证软件和配置的完整性，并且在发现不符时能够通知管理人员。

4.4.3.4 输入验证

本项目包括但不限于：

控制系统应支持对输入的内容和语法进行检验。

4.4.3.5 确定性输出

本项目包括但不限于：

控制系统在遭受攻击无法保持正常运行时应提供将输出设为预定义状态的能力。

4.4.3.6 错误处理

本项目包括但不限于：

控制系统的错误信息应不包括除诊断信息以外的敏感信息。

4.4.3.7 会话完整性

本项目包括但不限于：

控制系统应具备会话完整性保护机制。

4.4.3.7.1 会话终止后会话 id 的失效

本项目包括但不限于：

在用户退出或会话终止（包括浏览器会话）后，控制系统应提供使其会话标识失效的能力。

4.4.3.7.2 唯一会话 id 的产生和承认

本项目包括但不限于：

控制系统应提供为每个会话生成唯一会话标识 id 的能力。

4.4.3.7.3 会话 id 的随机性

本项目包括但不限于：

控制系统应提供随机会话标识的能力，防止被追踪。

4.4.3.8 审计信息的保护

本项目包括但不限于：

控制系统应保护审计信息不被未授权的访问、修改和删除。

4.4.3.8.1 一次性写入介质的审计记录

本项目包括但不限于：

控制系统应提供在基于硬件的、一次性写入介质上生成审计记录的能力。

4.4.4 数据保密性

4.4.4.1 信息机密性

本项目包括但不限于：

控制系统应提供能力，对有读授权的信息在静态和传输过程中进行保密性保护。

4.4.4.1.1 静态和经由不可信网络传输的数据的机密性保护

本项目包括但不限于：

控制系统应提供能力保护静态信息和穿越不可信网络的远程访问会话的保密性。

4.4.4.1.2 区域边界的机密性保护

本项目包括但不限于：

控制系统应提供能力保护穿越所有区域边界的信息的机密性。

4.4.4.2 密码的使用

本项目包括但不限于：

控制系统应根据普遍接受的工业实践和推荐来使用密码算法、密钥长度以及密钥创建和管理机制。

4.4.5 限制的数据流

4.4.5.1 应用分离

本项目包括但不限于：

控制系统应基于实现分区模型的关键程度提供对应用、数据和服务进行分离的能力。

4.4.6 对事件的及时响应

4.4.6.1 审计日志的可访问性

本项目包括但不限于：

控制系统应为已授权的人和/或工具提供访问审计日志的能力。

4.4.6.1.1 对审计日志的编程式访问

本项目包括但不限于：

控制系统应使用应用编程接口 api 提供对审计日志的访问。

4.4.7 资源可用性

4.4.7.1 控制系统备份

本项目包括但不限于：

控制系统在正常生产的情况下，应有能力执行用户级和系统级备份的功能。

4.4.7.1.1 备份验证

本项目包括但不限于：

控制系统应提供能力验证备份机制的可靠性。

4.4.7.1.2 备份自动化

本项目包括但不限于：

控制系统应提供能力按照可配置的频率进行自动化备份。

4.4.7.2 控制系统恢复和重构

本项目包括但不限于：

发生中断后，控制系统应提供恢复和重构到已知安全状态的能力。

4.4.7.3 网络和安全配置设置

本项目包括但不限于：

控制系统应具备网络和安全配置功能，提供与现有部署网络和安全配置设置之间的接口。

4.4.7.3.1 对当前安全设置的机器可读的报告

本项目包括但不限于：

控制系统应具备生成安全配置报告的能力。

4.4.7.4 控制系统元器件清单

本项目包括但不限于：

控制系统应提供当前已安装的元器件及其关联属性列表的能力。

4.5 plc/dcs 安全

4.5.1 标识和认证管理

4.5.1.1 用户（人）的标识和认证

本项目包括但不限于：

控制系统应提供标识和认证所有用户（人）的能力。

4.5.1.1.1 唯一标识和认证

本项目包括但不限于：

控制系统应对所有用户（人）提供唯一标识和认证的能力。

4.5.1.1.2 非可信网络的多因子认证

本项目包括但不限于：

通过非可信网络访问（远程访问）控制系统时，控制系统应为其提供多因子认证的能力。

4.5.1.1.3 对所有网络的多因子认证

本项目包括但不限于：

控制系统应为所有用户（人）访问控制系统提供多因子认证的能力。

4.5.1.2 软件进程和设备的标识和认证

本项目包括但不限于：

控制系统应提供标识和认证所有用户（软件进程和设备）的能力。

4.5.1.2.1 唯一标识和认证

本项目包括但不限于：

控制系统应对所有用户（软件进程、设备）提供唯一标识和认证的能力。

4.5.1.3 失败的登陆尝试

本项目包括但不限于：

控制系统应具备登录失败处理功能。

4.5.2 使用控制

4.5.2.1 会话锁

本项目包括但不限于：

控制系统应具备用户超时锁定功能。

4.5.2.2 远程会话终止

本项目包括但不限于：

控制系统应提供在可配置的不活跃时间周期后自动终止远程会话或由用户手动终止远程会话的能力。

4.5.2.3 并发会话控制

本项目包括但不限于：

对任意给定用户（人、软件进程或设备），控制系统应提供将每个接口的并发会话的数目限制为一个可配置的数目的能力。

4.5.3 系统完整性

4.5.3.1 通信完整性

本项目包括但不限于：

控制系统应具备通信完整性功能。

4.5.3.1.1 基于密码技术的完整性保护

本项目包括但不限于：

控制系统应提供能力采用密码技术来保证信息在传输过程中的完整性。

4.5.3.2 会话完整性

本项目包括但不限于：

控制系统应具备会话完整性保护机制。

4.5.3.2.1 会话终止后会话 id 的失效

本项目包括但不限于：

在用户退出或会话终止（包括浏览器会话）后，控制系统应提供使其会话标识失效的能力。

4.5.3.2.2 唯一会话 id 的产生和承认

本项目包括但不限于：

控制系统应提供为每个会话生成唯一会话标识 id 的能力。

4.5.3.2.3 会话 id 的随机性

本项目包括但不限于：

控制系统应提供随机会话标识的能力，防止被追踪。

4.5.4 数据保密性

4.5.4.1 信息存留

本项目包括但不限于：

控制系统元器件被移除后，应清除其储存的相关数据，确保不被他人获取。

附录 A

(规范性附录)

表A规定了系统能力要求与安全级别的映射。

表 A 系统能力要求与安全级别的映射

系统能力要求			安全级别			
			第一级	第二级	第三级	第四级
1. 物理和环境安全	1.1 安全区域	1.1.1 物理安全周边		√	√	√
		1.1.2 物理入口控制	√	√	√	√
		1.1.3 办公室、房间和设施的安全防护	√	√	√	√
		1.1.4 外部和环境的安全防护		√	√	√
		1.1.5 在安全区域工作	√	√	√	√
		1.1.6 公共访问、交换区安全	√	√	√	√
	1.2 设备安全	1.2.1 设备安置和保护	√	√	√	√
		1.2.2 支持性设施	√	√	√	√
		1.2.3 布缆安全	√	√	√	√
		1.2.4 设备维护	√	√	√	√
		1.2.5 组织机构场所外的设备安全		√	√	√
		1.2.6 设备的安全处置或再利用		√	√	√
		1.2.7 资产的移动			√	√
	1.3 资源可用性	1.3.1 紧急电源	√	√	√	√
2. 网络安全	2.1 网络访问控制	2.1.1 网络服务的策略	√	√	√	√
		2.1.2 外部连接的用户鉴别	√	√	√	√
		2.1.3 网络上设备标识		√	√	√
		2.1.4 远程诊断和配置端口的保护	√	√	√	√
		2.1.5 网络隔离	√	√	√	√
		2.1.6 网络连接控制	√	√	√	√
		2.1.7 经由非可信网络的访问	√	√	√	√
		2.1.7.1 明确地对访问请求的批准		√	√	√
		2.2.8 无线使用控制	√	√	√	√
		2.2.8.1 对未授权的无线设备进行识别和报告			√	√
	2.2 监视	2.2.1 审计记录	√	√	√	√
		2.2.2 监视系统的使用	√	√	√	√

系统能力要求			安全级别			
			第一级	第二级	第三级	第四级
		2.2.3 日志信息的保护	√	√	√	√
		2.2.4 管理员和操作日志	√	√	√	√
		2.2.5 故障日志	√	√	√	√
		2.2.6 时钟同步	√	√	√	√
	2.3 限制的数据流	2.3.1 网络分区	√	√	√	√
		2.3.1.1 物理网络分区		√	√	√
		2.3.1.2 与非控制系统网络的独立性			√	√
		2.3.1.3 关键网络的逻辑和物理隔离				√
		2.3.2 区域边界防护	√	√	√	√
		2.3.2.1 默认拒绝，例外允许		√	√	√
		2.3.2.2 孤岛模型			√	√
		2.3.2.3 故障关闭			√	√
	2.4 持续监视	2.4.1 持续监视		√	√	√
	2.5 资源可用性	2.5.1 拒绝服务的防护	√	√	√	√
		2.5.1.1 管理通信负荷		√	√	√
		2.5.1.2 限制拒绝服务攻击对其他系统和网络的影响			√	√
3. 主机安全	3.1 操作系统访问控制	3.1.1 安全登录规程	√	√	√	√
		3.1.2 用户标识和鉴别	√	√	√	√
		3.1.3 口令管理系统	√	√	√	√
		3.1.4 系统实用工具的使用		√	√	√
		3.1.5 会话超时			√	√
		3.1.6 联机时间的限定			√	√
	3.2 监视	3.2.1 审计记录	√	√	√	√
		3.2.2 监视系统的使用	√	√	√	√
		3.2.3 日志信息的保护	√	√	√	√
		3.2.4 管理员和操作日志	√	√	√	√
		3.2.5 故障日志	√	√	√	√
		3.2.6 时钟同步	√	√	√	√
	3.3 恶意代码防护	3.3.1 恶意代码保护	√	√	√	√
		3.3.2 恶意代码防护的中央管理和报告			√	√
	3.4 限制的数据流	3.4.1 禁止所有的一般目的的个人通信			√	√
	3.5 资源可用性	3.5.1 最小功能化	√	√	√	√
		3.5.2 资源管理	√	√	√	√
	3.6 使用控制	3.6.1 对便携和移动设备的使用控制	√	√	√	√
		3.6.1.1 便携和移动设备的安全			√	√

系统能力要求			安全级别			
			第一级	第二级	第三级	第四级
		状态的实施				
		3.6.2 移动代码	√	√	√	√
		3.6.2.1 移动代码的完整性			√	√
	3.7 数据保密性	3.7.1 信息存留		√	√	√
4. SCADA 安全	4.1 标识和认证管理	4.1.1 用户（人）的标识和认证	√	√	√	√
		4.1.1.1 唯一标识和认证		√	√	√
		4.1.1.2 非可信网络的多因子认证			√	√
		4.1.1.3 对所有网络的多因子认证				√
		4.1.2 软件进程和设备的标识和认证		√	√	√
		4.1.2.1 唯一标识和认证			√	√
		4.1.3 账号管理	√	√	√	√
		4.1.3.1 统一的账号管理			√	√
		4.1.4 标识符管理	√	√	√	√
		4.1.5 认证码管理	√	√	√	√
		4.1.5.1 软件进程标识凭证的硬件安全			√	√
		4.1.6 无线访问管理	√	√	√	√
		4.1.6.1 唯一标识和认证		√	√	√
		4.1.7 口令认证的加强	√	√	√	√
		4.1.7.1 对用户（人）的口令生成和口令有效期限限制			√	√
		4.1.7.2 对所有用户的口令有效期限限制				√
		4.1.8 公钥基础设施证书		√	√	√
		4.1.9 公钥认证加强		√	√	√
		4.1.9.1 公钥认证的硬件安全			√	√
		4.1.10 认证反馈	√	√	√	√
		4.1.11 失败的登陆尝试	√	√	√	√
		4.1.12 系统使用通知	√	√	√	√
	4.2 使用控制	4.2.1 授权的执行	√	√	√	√
		4.2.1.1 对所有用户执行授权		√	√	√
		4.2.1.2 许可映射到角色		√	√	√
		4.2.1.3 主管越权			√	√
		4.2.1.4 双授权				√
		4.2.2 会话锁	√	√	√	√
		4.2.3 远程会话终止		√	√	√
		4.2.4 并发会话控制			√	√

系统能力要求			安全级别			
			第一级	第二级	第三级	第四级
		4.2.5 可审计的事件	√	√	√	√
		4.2.5.1 中央管理的、系统范围的审计跟踪			√	√
		4.2.6 审计存储容量	√	√	√	√
		4.2.6.1 达到审计记录存储容量上限时发出警告			√	√
		4.2.7 审计处理失败时的响应	√	√	√	√
		4.2.8 时间戳		√	√	√
		4.2.8.1 内部时间同步			√	√
		4.2.8.2 时间源的完整性保护				√
		4.2.9 不可否认性			√	√
		4.2.9.1 所有用户的不可否认性				√
	4.3 系统完整性	4.3.1 通信完整性	√	√	√	√
		4.3.1.1 基于密码技术的完整性保护			√	√
		4.3.2 安全功能验证	√	√	√	√
		4.3.2.1 安全功能验证的自动化机制			√	√
		4.3.2.2 正常运行中的安全功能验证				√
		4.3.3 软件和信息完整性		√	√	√
		4.3.3.1 对破坏完整性进行自动通知			√	√
		4.3.4 输入验证	√	√	√	√
		4.3.5 确定性输出	√	√	√	√
		4.3.6 错误处理		√	√	√
		4.3.7 会话完整性		√	√	√
		4.3.7.1 会话终止后会话 ID 的失效			√	√
		4.3.7.2 唯一会话 ID 的产生和承认			√	√
		4.3.7.3 会话 ID 的随机性				√
		4.3.8 审计信息的保护		√	√	√
		4.3.8.1 一次性写入介质的审计记录				√
	4.4 数据保密性	4.4.1 信息机密性	√	√	√	√
		4.4.1.1 静态和经由不可信网络传输的数据的机密性保护		√	√	√
		4.4.1.2 区域边界的机密性保护				√
		4.4.2 密码的使用	√	√	√	√
	4.5 限制的数	4.5.1 应用分离	√	√	√	√

系统能力要求			安全级别			
			第一级	第二级	第三级	第四级
	据流					
	4.6 对事件的及时响应	4.6.1 审计日志的可访问性	√	√	√	√
		4.6.1.1 对审计日志的程式访问			√	√
	4.7 资源可用性	4.7.1 控制系统备份	√	√	√	√
		4.7.1.1 备份验证		√	√	√
		4.7.1.2 备份自动化			√	√
		4.7.2 控制系统恢复和重构	√	√	√	√
		4.7.3 网络和安全配置设置	√	√	√	√
		4.7.3.1 对当前安全设置的机器可读的报告			√	√
		4.7.4 控制系统元器件清单		√	√	√
5. PLC/DCS 安全	5.1 标识和认证管理	5.1.1 用户（人）的标识和认证	√	√	√	√
		5.1.1.1 唯一标识和认证		√	√	√
		5.1.1.2 非可信网络的多因子认证			√	√
		5.1.1.3 对所有网络的多因子认证				√
		5.1.2 软件进程和设备的标识和认证		√	√	√
		5.1.2.1 唯一标识和认证			√	√
		5.1.3 失败的登陆尝试	√	√	√	√
	5.2 使用控制	5.2.1 会话锁	√	√	√	√
		5.2.2 远程会话终止		√	√	√
		5.2.3 并发会话控制			√	√
	5.3 系统完整性	5.3.1 通信完整性	√	√	√	√
		5.3.1.1 基于密码技术的完整性保护			√	√
		5.3.2 会话完整性		√	√	√
		5.3.2.1 会话终止后会话 ID 的失效			√	√
		5.3.2.2 唯一会话 ID 的产生和承认			√	√
		5.3.2.3 会话 ID 的随机性				√
	5.4 数据保密性	5.4.1 信息存留		√	√	√

参考文献

- [1]GB/T30976.1-2014《工业控制系统信息安全第1部分：评估规范》
