6.1.4 安全计算环境

6.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

6.1.4.2 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限；

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

6.1.4.3 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应关闭不需要的系统服务、默认共享和高危端口。

6.1.4.4 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

6.1.4.5 可信验证

可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.1.4.6 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

6.1.4.7 数据备份恢复

应提供重要数据的本地数据备份与恢复功能。

6.1.5 安全管理制度

6.1.5.1 管理制度

应建立日常管理活动中常用的安全管理制度。

6.1.6 安全管理机构

6.1.6.1 岗位设置

应设立系统管理员等岗位，并定义各个工作岗位的职责。

6.1.6.2 人员配备

应配备一定数量的系统管理员。

6.1.6.3 授权和审批

应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

6.1.7 安全管理人员

6.1.7.1 人员录用

应指定或授权专门的部门或人员负责人员录用。

6.1.7.2 人员离岗

应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

6.1.7.3 安全意识教育和培训

应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

6.1.7.4 外部人员访问管理

应保证在外部人员访问受控区域前得到授权或审批。

6.1.8 安全建设管理

6.1.8.1 定级和备案

应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

6.1.8.2 安全方案设计

应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

6.1.8.3 产品采购和使用

应确保网络安全产品采购和使用符合国家的有关规定。

6.1.8.4 工程实施

应指定或授权专门的部门或人员负责工程实施过程的管理。

6.1.8.5 测试验收

应进行安全性测试验收。

6.1.8.6 系统交付

本项要求包括：

a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b) 应对负责运行维护的技术人员进行相应的技能培训。

6.1.8.7 服务供应商选择

本项要求包括：

a) 应确保服务供应商的选择符合国家的有关规定；

b) 应与选定的服务供应商签订与安全相关的协议，明确约定相关责任。

6.1.9 安全运维管理

6.1.9.1 环境管理

本项要求包括：

a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等方面。

6.1.9.2 介质管理

应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

6.1.9.3 设备维护管理

应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理。

6.1.9.4 漏洞和风险管理

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

6.1.9.5 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

6.1.9.6 恶意代码防范管理

本项要求包括：

a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

6.1.9.7 备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

6.1.9.8 安全事件处置

本项要求包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b) 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

6.2 云计算安全扩展要求

6.2.1 安全物理环境

6.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

6.2.2 安全通信网络

6.2.2.1 网络架构

本项要求包括：

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b) 应实现不同云服务客户虚拟网络之间的隔离。

6.2.3 安全区域边界

6.2.3.1 访问控制

应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

6.2.4 安全计算环境

6.2.4.1 访问控制

本项要求包括：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；

b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。

6.2.4.2 数据完整性和保密性

应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

6.2.5 安全建设管理

6.2.5.1 云服务商选择

本项要求包括：

a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

6.2.5.2 供应链管理

应确保供应商的选择符合国家有关规定。

6.3 移动互联安全扩展要求

6.3.1 安全物理环境

6.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

6.3.2 安全区域边界

6.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入安全网关设备。

6.3.2.2 访问控制

无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

6.3.3 安全计算环境

6.3.3.1 移动应用管控

应具有选择应用软件安装、运行的功能。

6.3.4 安全建设管理

6.3.4.1 移动应用软件采购

应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

6.4 物联网安全扩展要求

6.4.1 安全物理环境

6.4.1.1 感知节点设备物理防护

本项要求包括：

a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。

6.4.2 安全区域边界

6.4.2.1 接入控制

应保证只有授权的感知节点可以接入。

6.4.3 安全运维管理

6.4.3.1 感知节点管理

应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

6.5 工业控制系统安全扩展要求

6.5.1 安全物理环境

6.5.1.1 室外控制设备物理防护

本项要求包括：

a) 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

b) 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

6.5.2 安全通信网络

6.5.2.1 网络架构

本项要求包括：

a) 工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；

b) 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

6.5.3 安全区域边界

6.5.3.1 访问控制

应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

6.5.3.2 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b) 应对无线连接的授权、监视以及执行使用进行限制。

6.5.4 安全计算环境

6.5.4.1 控制设备安全

本项要求包括：

a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

7 第二级安全要求

7.1 安全通用要求

7.1.1 安全物理环境

7.1.1.1 物理位置选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

7.1.1.2 物理访问控制

机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

7.1.1.3 防盗窃和防破坏

本项要求包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；

b) 应将通信线缆铺设在隐蔽安全处。

7.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

7.1.1.5 防火

本项要求包括：

a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

7.1.1.6 防水和防潮

本项要求包括：

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

7.1.1.7 防静电

应采用防静电地板或地面并采用必要的接地防静电措施。

7.1.1.8 温湿度控制

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。

7.1.1.9 电力供应

本项要求包括：

a) 应在机房供电线路上配置稳压器和过电压防护设备；

b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

7.1.1.10 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

7.1.2 安全通信网络

7.1.2.1 网络架构

本项要求包括：

a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

7.1.2.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

7.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.3 安全区域边界

7.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

7.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

7.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为。

7.1.3.4 恶意代码防范

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

7.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.4 安全计算环境

7.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.1.4.2 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限；

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

7.1.4.3 安全审计

本项要求包括：

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.1.4.4 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应关闭不需要的系统服务、默认共享和高危端口；

c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

7.1.4.5 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

7.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.4.7 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

7.1.4.8 数据备份恢复

本项要求包括：

a) 应提供重要数据的本地数据备份与恢复功能；

b) **应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。**

7.1.4.9 剩余信息保护

应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

7.1.4.10 个人信息保护

本项要求包括：

a) **应仅采集和保存业务必需的用户个人信息；**

b) **应禁止未授权访问和非法使用用户个人信息。**

7.1.5 安全管理中心

7.1.5.1 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

7.1.5.2 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

7.1.6 安全管理制度

7.1.6.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。