8.3.1.5 工业控制系统安全计算环境设计技术要求

本项要求包括：

a) 工业控制身份鉴别

现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理，**防止未经授权的修改**。

b) 现场设备访问控制

应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。**只有获得授权的用户才能对现场设备进行组态下装、软件更新、数据更新、参数设定等操作**。

c) **现场设备安全审计**

在有冗余的重要应用环境，双重或多重控制器可采用实时审计跟踪技术，确保及时捕获网络安全事件信息并报警。

d) **现场设备数据完整性保护**

应采用密码技术或应采用物理保护机制保证现场控制层设备和现场设备层设备之间通信会话完整性。

e) 现场设备数据保密性保护

应采用密码技术支持的保密性保护机制或应采用物理保护机制，对现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息等进行保密性保护。

f) 控制过程完整性保护

应在规定的时间内完成规定的任务，数据应以授权方式进行处理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和处理事件，保护系统的同步机制、校时机制，保持控制周期稳定、现场总线轮询周期稳定；**现场设备应能识别和防范破坏控制过程完整性的攻击行为，应能识别和防止以合法身份、合法路径干扰控制器等设备正常工作节奏的攻击行为；在控制系统遭到攻击无法保持正常运行时，应有故障隔离措施，应使系统导向预先定义好的安全的状态，将危害控制到最小范围**。

8.3.2 安全区域边界设计技术要求

8.3.2.1 通用安全区域边界设计技术要求

本项要求包括：

a) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，**应对源及目标计算节点的身份、地址、端口和应用协议等进行可信验证**，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

b) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制，由安全管理中心集中管理，**并对确认的违规行为及时报警**。

d) 区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管

理中心。

e) 可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、区域边界安全管控程序等进行可信验证，并在区域边界设备运行过程中定期对程序内存空间、操作系统内核关键内存区域等执行资源进行可信验证，并在检测到其可信性受到破坏时采取措施恢复，并将验证结果形成审计记录，送至管理中心。

8.3.2.2 云安全区域边界设计技术要求

本项要求包括：

a) 区域边界结构安全

应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击；应实现不同租户间虚拟网络资源之间的隔离，并避免网络资源过量占用；应保证云计算平台管理流量与云租户业务流量分离。

应能够识别、监控虚拟机之间、虚拟机与物理机之间的网络流量；提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务。

b) 区域边界访问控制

应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云租户设置不同虚拟机之间的访问控制策略；应建立租户私有网络实现不同租户之间的安全隔离；应在网络边界处部署监控机制，对进出网络的流量实施有效监控。

c) 区域边界入侵防范

当虚拟机迁移时，入侵防范机制可应用于新的边界处；应将区域边界入侵防范机制纳入安全管理中心统一管理。

应向云租户提供互联网内容安全监测功能，对有害信息进行实时检测和告警。

d) 区域边界审计要求

根据云服务商和云租户的职责划分，收集各自控制部分的审计数据；根据云服务商和云租户的职责划分，实现各自控制部分的集中审计；当发生虚拟机迁移或虚拟资源变更时，安全审计机制可应用于新的边界处；为安全审计数据的汇集提供接口，并可供第三方审计。

8.3.2.3 移动互联安全区域边界设计技术要求

8.3.2.3.1 区域边界访问控制

应对接入系统的移动终端，采取基于 SIM 卡、证书等信息的强认证措施；应能限制移动设备在不同工作场景下对 WiFi、3G、4G 等网络的访问能力。

8.3.2.3.2 区域边界完整性保护

移动终端区域边界检测设备监控范围应完整覆盖移动终端办公区，并具备无线路由器设备位置检测功能，对于非法无线路由器设备接入进行报警和阻断。

8.3.2.4 物联网系统安全区域边界设计技术要求

本项要求包括：

a) 区域边界访问控制

应能根据数据的时间戳为数据流提供明确的允许/拒绝访问的能力；应提供网络最大流量及网络连接数限制机制；应能够根据通信协议特性，控制不规范数据包的出入。

b) 区域边界准入控制

应在安全区域边界设置准入控制机制，能够对设备进行认证，保证合法设备接入，拒绝恶意设备接入；应根据感知设备特点收集感知设备的健康性相关信息如固件版本、标识、配置信息校验值等，并能够对接入的感知设备进行健康性检查。

c) 区域边界协议过滤与控制

应在安全区域边界设置协议过滤，能够对物联网通信内容进行过滤，对通信报文进行合规检查，根据协议特性，设置相对应控制机制。

8.3.2.5 工业控制系统安全区域边界设计技术要求

本项要求包括：

a) 工控通信协议数据过滤

对通过安全区域边界的工控通信协议，应能识别其所承载的数据是否会对工控系统造成攻击或破坏，应控制通信流量、帧数量频度、变量的读取频度稳定且在正常范围内，保护控制器的工作节奏，识别和过滤写变量参数超出正常范围的数据，该控制过滤处理组件可配置在区域边界的网络设备上，也可配置在本安全区域内的工控通信协议的端点设备上或唯一的通信链路设备上。

b) 工控通信协议信息泄露防护

应防止暴露本区域工控通信协议端点设备的用户名和登录密码，采用过滤变换技术隐藏用户名和登录密码等关键信息，将该端点设备单独分区过滤及其他具有相应防护功能的一种或一种以上组合机制进行防护。

c) 工控区域边界安全审计

应在安全区域边界和设置实时检测告警机制，通过安全管理中心集中管理，对确认的违规行为及时向安全管理中心和工控值守人员报警并做出相应处置。

8.3.3 安全通信网络设计技术要求

8.3.3.1 通用安全通信网络设计技术要求

本项要求包括：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。

b) 通信网络数据传输完整性保护

应采用由密码技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

应采用由密码技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 可信连接验证

通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其关键执行环节的执行资源进行可信验证，并将验证结果形成审计记录，送至管理中心。

8.3.3.2 云安全通信网络设计技术要求

本项要求包括：

a) 通信网络数据传输保密性

应支持云租户远程通信数据保密性保护。

应对网络策略控制器和网络设备(或设备代理)之间网络通信进行加密。

b) **通信网络可信接入保护**

应禁止通过互联网直接访问云计算平台物理网络;应提供开放接口,允许接入可信的第三方安全产品。

c) 通信网络安全审计

应支持租户收集和查看与本租户资源相关的审计信息;应保证云服务商对云租户通信网络的访问操作可被租户审计。

8.3.3.3 移动互联安全通信网络设计技术要求

本项要求包括:

a) 通信网络可信保护

应通过VPDN等技术实现基于密码算法的可信网络连接机制,通过对连接到通信网络的设备进行可信检验,确保接入通信网络的设备真实可信,防止设备的非法接入。

8.3.3.4 物联网系统安全通信网络设计技术要求

本项要求包括:

a) 感知层网络数据新鲜性保护

应在感知层网络传输的数据中加入数据发布的序列信息如时间戳、计数器等,以实现感知层网络数据传输新鲜

b) 异构网安全接入保护

应采用接入认证等技术建立异构网络的接入认证系统,保障控制信息的安全传输;应根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素,划分不同的子网或网段,并采取相应的防护措施。

8.3.3.5 工业控制系统安全通信网络设计技术要求

本项要求包括:

a) 现场总线网络数据传输完整性保护

应采用适应现场总线特点的报文短、时延小的密码技术支持的完整性校验机制或应采用物理保护机制,实现现场总线网络数据传输完整性保护。

b) 无线网络数据传输完整性保护

应采用密码技术支持的完整性检验机制,以实现无线网络数据传输完整性保护。

c) 现场总线网络数据传输保密性保护

应采用适应现场总线特点的报文短、时延小的密码技术支持的保密性保护机制或应采用物理保护机制,实现现场总线网络数据传输保密性保护。

d) **无线网络数据传输保密性保护**

应采用由密码技术支持的保密性保护机制,以实现无线网络数据传输保密性保护。

e) **工业控制网络实时响应要求**

对实时响应和操作要求高的场合,应把工业控制通信会话过程设计为三个阶段:开始阶段,应完成对主客体身份鉴别和授权;运行阶段,应保证对工业控制系统的实时响应和操作,此阶段应对主客体的安全状态实时监测;结束阶段,应以显式的方式结束。在需要连续运行的场合,人员交接应不影响实时性,应保证访问控制机制的持续性。

f) **通信网络异常监测**

应对工业控制系统的通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发现异常进行报警；在有冗余现场总线和表决器的应用场合，可充分监测各冗余链路在同时刻的状态，捕获可能的恶意或入侵行为；应在相应的网关设备上进行流量监测与管控，对超出最大 PS 阈值的通信进行控制并报警。

g) 无线网络攻击的防护

应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，应对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽，可综合采用检测和干扰、电磁屏蔽、微波暗室吸收、物理保护等方法，在可能传播的频谱范围将无线信号衰减到不能有效接收的程度。

8.3.4 安全管理中心设计技术要求

8.3.4.1 系统管理

可通过系统管理员对系统的资源和运行进行配置、控制和可信及密码管理，包括用户身份、可信证书及密钥、可信基准库、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。

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。

在进行云计算平台安全设计时，安全管理应提供查询云租户数据及备份存储位置的方式；云计算平台的运维应在中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

在进行物联网系统安全设计时，应通过系统管理员对感知设备、感知网关等进行统一身份标识管理；应通过系统管理员对感知设备状态（电力供应情况、是否在线、位置等）进行统一监测和处理。

8.3.4.2 安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略，维护策略库和度量值库。

应对安全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管理操作，并进行审计。

在进行云计算平台安全设计时，云计算安全管理应具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力；应具有对网络安全态势进行感知、预测和预判的能力。

在进行物联网系统安全设计时，应通过安全管理员对系统中所使用的密钥进行统一管理，包括密钥的生成、分发、更新、存储、备份、销毁等。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制系统设备的可用性和安全性进行实时监控，可以对监控指标设置告警阈值，触发告警并记录；应通过安全管理员在安全管理中心呈现设备间的访问关系，及时发现未定义的信息通讯行为以及识别重要业务操作指令级的异常。

8.3.4.3 审计管理

应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计；应通过运维审计系统对管理员的运维行为进行安全审计；应通过租户隔离机制，

确保审计数据隔离的有效性。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制现场控制设备、网络安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的网络安全监控和报警、网络安全日志信息进行集中管理。根据安全审计策略对各类安全信息进行分类管理与查询，并生成统一的审计报告。系统对各类网络安全报警和日志信息进行关联分析。

9 第四级系统安全保护环境设计

9.1 设计目标

第四级系统安全保护环境的设计目标是：按照GB 17859—1999对第四级系统的安全保护要求，建立一个明确定义的形式化安全策略模型，将自主和强制访问控制扩展到所有主体与客体，相应增强其他安全功能强度；将系统安全保护环境结构化为关键保护元素和非关键保护元素，以使系统具有抗渗透的能力；保障基础计算资源和应用程序可信，确保所有关键执行环节可信，对所有可信验证结果进行动态关联感知。

9.2 设计策略

第四级系统安全保护环境的设计策略是：在第三级系统安全保护环境设计的基础上，遵循GB 17859—1999的4.4中相关要求，通过安全管理中心明确定义和维护形式化的安全策略模型。依据该模型，采用对系统内的所有主、客体进行标记的手段，实现所有主体与客体的强制访问控制。同时，相应增强身份鉴别、审计、安全管理等功能，定义安全部件之间接口的途径，实现系统安全保护环境关键保护部件和非关键保护部件的区分，并进行测试和审核，保障安全功能的有效性。第四级系统安全保护环境在使用密码技术设计时，应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。

第四级系统安全保护环境的设计通过第四级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。所有计算节点都应基于可信计算技术实现开机到操作系统启动，再到应用程序启动的可信验证，并在应用程序的所有执行环节对其执行环境进行可信验证，主动抵御病毒入侵行为，同时验证结果，进行动态关联感知，形成实时的态势。

9.3 设计技术要求

9.3.1 安全计算环境设计技术要求

9.3.1.1 通用安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，将强制访问控制扩展到所有主体与客体；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，终止违例进程等；确保审计记录不被破坏或非授权访问以及防止审计记录丢失等。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，校验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。

g) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源。在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h) 可信验证

可基于可信根对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的所有执行环节对系统调用的主体、客体、操作可信验证，并对中断、关键内存区域等执行资源进行可信验证，并在检测到其可信性受到破坏时采取措施恢复，并将验证结果形成审计记录，送至管理中心，进行动态关联感知。

i) 配置可信检查

应将系统的安全配置信息形成基准库，实时监控或定期检查配置信息的修改行为，及时修复和基准库中内容不符的配置信息，可将感知结果形成基准值。

j) 入侵检测和恶意代码防范

应通过主动免疫可信计算检验机制及时识别入侵和病毒行为，并将其有效阻断。

9.3.1.2

本项要求包括：

a) 用户身份鉴别

应支持注册到云计算服务的云租户建立主子账号，并采用用户名和用户标识符标识主子账号用户身份。

当进行远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制。

b) 用户账号保护

应支持建立云租户账号体系，实现主体对虚拟机、云数据库、云网络、云存储等客体的访问授权。

c) 安全审计

应支持对云服务商和云租户远程管理时执行的特权命令进行审计。

应支持租户收集和查看与本租户资源相关的审计信息，保证云服务商对云租户系统和数据的访问操作可被租户审计。

d) 入侵防范

应支持对云租户进行行为监控，对云租户发起的恶意攻击或恶意对外连接进行检测和告警。

e) 数据保密性保护

应提供重要业务数据加密服务，加密密钥由租户自行管理；应提供加密服务，保证虚拟机在迁 移过程中重要数据的保密性。

f) 数据备份与恢复

应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云租户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性；应建立异地灾难备 份中心，提供业务应用的实时切换。

g) 虚拟化安全

应实现虚拟机之间的CPU、内存和存储空间安全隔离，能检测到非授权管理虚拟机等情况，并进行告警；应禁止虚拟机对宿主机物理资源的直接访问，应能对异常访问进行告警；应支持不同云租户虚拟化网络之间安全隔离；应监控物理机、宿主机、虚拟机的运行状态，并提供接口供安全管理中心集中监控。

h) 恶意代码防范

物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对Web应用恶意代码检测和防护的能力。

i) 镜像和快照安全

应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供安全加固的操作系统镜像或支持对操作系统镜像进行自加固。

9.3.1.3 移动互联安全计算环境设计技术要求

本项要求包括：

a) 用户身份鉴别

应对移动终端用户实现基于口令或解锁图案、数字证书或动态口令、生物特征等方式的两种或两种以上的组合身份鉴别；应基于硬件为身份鉴别机制构建隔离的运行环境。

b) 标记和强制访问控制

应确保用户或进程对移动终端系统资源的最小使用权限；应根据安全策略，控制移动终端接入访问外设，外设类型至少应包括扩展存储卡、GPS等定位设备、蓝牙、NFC等通信外设，并记录日志。

c) 应用管控

应具有软件白名单功能，能根据白名单控制应用软件安装、运行；应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。**应确保移动终端为专用终端，不得处理与系统无关的业务。**

d) 安全域隔离

应能够为重要应用提供基于容器、虚拟化等系统级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。

e) 移动设备管控

应基于移动设备管理软件，实行对移动设备全生命周期管控，保证移动设备丢失或被盗后，通过网络定位搜寻设备的位置、远程锁定设备、远程擦除设备上的数据、使设备发出警报音，确保在能够定位和检索的同时最大程度地保护数据。

f) 数据保密性保护

应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译；应实现对扩展存储设备的加密功能，确保数据存储的安全。

g) 可信验证

应能对移动终端的引导程序、操作系统内核、应用程序等进行可信验证，确保每个部件在加载前的真实性和完整性。

9.3.1.4 物联网系统安全计算环境设计技术要求

本项要求包括：

a) 感知层设备身份鉴别

应采用密码技术支持的鉴别机制实现感知层网关与感知设备之间的双向身份鉴别，确保数据来源于正确的设备；应对感知设备和感知层网关进行统一入网标识管理和维护，并确保在整个生存周期设备标识的唯一性；应采取措施对感知设备组成的组进行组认证以减少网络拥塞。

b) 感知层设备访问控制

应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，根据安全策略对其他设备进行权限检查；感知设备进行更新配置时，根据安全策略对用户进行权限检查。

9.3.1.5 工业控制系统安全计算环境设计技术要求

本项要求包括：

a) 工业控制身份鉴别

现场控制层设备、现场设备层设备以及过程监控层设备应实施唯一性的标识、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理，防止未经授权的修改。

b) 现场设备访问控制

应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。只有获得授权的用户才能对现场设备进行组态下装、软件更新、数据更新、参数设定等操作，才能对控制器的操作界面进行操作。

OPC 服务器和客户机可分别单独放置在各自的安全区内，以访问控制设备进行隔离保护，应对进出安全区的信息实行访问控制等安全策略。

c) 现场设备安全审计

在有冗余的重要应用环境，双重或多重控制器应采用实时审计跟踪技术，确保及时捕获网络安全事件信息并报警。

d) 现场设备数据完整性保护

应采用密码技术或应采用物理保护机制保证现场控制层设备和现场设备层设备之间通信会话完整性。

e) 现场设备数据保密性保护

应采用密码技术支持的保密性保护机制或应采用物理保护机制，对现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息等进行保密性保护。

f) **程序安全执行保护**

应构建从工程师站组态逻辑通过通讯链路下装到现场控制层的控制设备进行接收、存储的信任链或安全可控链，构建控制回路中从控制设备启动程序到操作系统（如果有的）直至到调用