控制应用程序、现场总线的接收-发送模块、现场设备层设备接收-发送模块的程序的信任链或安全可控链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复；应构建基于系统的整个完整链路的可信的或安全可控的时钟源、可信的或安全可控的同步和校时机制，防范恶意干扰和破坏。

g) 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。

9.3.2 安全区域边界设计技术要求

9.3.2.1 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受保护的区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警并做出相应处置。

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、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实时的对程序内存空间、操作系统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。

9.3.2.2 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；保证信息系统的外部通信接口经授权后方可传输数据；应确保云计算平台具有独立的资源池。

应能够识别、监控虚拟机之间、虚拟机；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；应确保云租户的四级业

务应用系统具有独立的资源池。

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限监控。

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监测和告警。

应在关键区域边界处部署相应形态的文件级代码检测或文件运行行为检测的安全系统，对恶意代码进行检测和清除。

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；对确认的违规行为及时报警并做出相应处置。

9.3.2.3 移动互联安全区域边界设计技术要求

9.3.2.3.1 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。

9.3.2.3.2 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。

9.3.2.4 物联网系统安全区域边界设计技术要求

本项要求包括：

a) 物联网系统区域边界访问控制

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，控制粒度为节点级；应提供网络最大流量及网络连接限制机制；应能够根据通信协议特性，控制不规范数据包的出入；应对进出网络的信息内容进行过滤，实现对通信协议的命令级的控制。

b) 物联网系统区域边界准入控制

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；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) 物联网系统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深度检测和过滤，对通信报文进行合规检查；根据协议特性，设置相对应基于白名单控制机制。

9.3.2.5 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

应在安全区域边界设置实时监测告警机制，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。

9.3.3 安全通信网络设计技术要求

9.3.3.1 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，且做出相应处置。

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，并在发现完整性呗破坏时进行恢复。

c) 通信网络数据传输保密性保护

采用由密码等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

应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其所有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，进行动态关联感知。

9.3.3.2

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；**应支持使用硬件加密设备对重要通信过程进行密码运算和密钥管理。**

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；**应确保外部通信接口经授权后方可传输数据。**

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。

应通过安全管理中心集中管理，并对确认的违规行为进行报警，且做出相应处置。

9.3.3.3 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。

9.3.3.4 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性保护。

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。**应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。**

9.3.3.5 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) **总线网络安全审计**

应支持工控总线网络审计，可通过总线审计的接口对访问控制、请求错误、系统事件、备份和存储事件、配置变更、潜在的侦查行为等事件进行审计。

b) 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。

c) 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校验机制，以实现无线网络数据传输完整性保护。

d) 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。

e) 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。

f) 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。

g) 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 PPS 阈值的通信进行控制并报警。

h) 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。

9.3.4 安全管理中心设计技术要求

9.3.4.1 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、控制和可信管理，包括用户身份、可信证书、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。**应通过系统管理员对下载到感知设备上的应用软件进行授权。**

在进行工业控制系统安全设计时，安全管理中心系统应具有自身运行监控与告警、系统日志记录等功能。

9.3.4.2 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，**并确保标记、授权和安全策略的数据完整性。**

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，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，**并采取必要措施保证密钥安全。**

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；**应通过安全管理员分析系统面临的安全风险和安全态势。**

9.3.4.3 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及时处理。

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网络安全信息进行分类管理与查询，并生成统一的审计报告。系统对各类安全报警和日志信息进行关联分析。**系统通过各设备安全日志信息的关联分析提取出少量的、或者是概括性的重要安全事件或发掘隐藏的攻击规律，进行重点报警和分析，并对全局存在类似风险的系统进行安全预警。**

9.3.5 系统安全保护环境结构化设计技术要求

9.3.5.1 安全保护部件结构化设计技术要求

第四级系统安全保护环境各安全保护部件的设计应基于形式化的安全策略模型。安全保护部件应划分为关键安全保护部件和非关键安全保护部件，防止违背安全策略致使敏感信息从关键安全保护部件流向非关键安全保护部件。关键安全保护部件应划分功能层次，明确定义功能层次间的调用接口，确保接口之间的安全交换。

9.3.5.2 安全保护部件互联结构化设计技术要求

第四级系统各安全保护部件之间互联的接口功能及其调用关系应明确定义；各安全保护部件之间互联时，需要通过可信验证机制相互验证对方的可信性，确保安全保护部件间的可信连接。

9.3.5.3 重要参数结构化设计技术要求

应对第四级系统安全保护环境设计实现的与安全策略相关的重要参数的数据结构给出明确定义，包括参数的类型、使用描述以及功能说明等，并用可信验证机制确保数据不被篡改。

10 第五级系统安全保护环境设计

略。

11 定级系统互联设计

11.1 设计目标

定级系统互联的设计目标是：对相同或不同等级的定级系统之间的互联、互通、互操作进行安全保护，确保用户身份的真实性、操作的安全性以及抗抵赖性，并按安全策略对信息流向进行严格控制，确保进出安全计算环境、安全区域边界以及安全通信网络的数据安全。

11.2 设计策略

定级系统互联的设计策略是：遵循 GB 17859—1999 对各级系统的安全保护要求，在各定级系统的计算环境安全、区域边界安全和通信网络安全的基础上，通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护。

11.3 设计技术要求

11.3.1 安全互联部件设计技术要求

应通过通信网络交换网关与各定级系统安全保护环境的安全通信网络部件相连接，并按互联互通的安全策略进行信息交换，实现安全互联部件。安全策略由跨定级系统安全管理中心实施。

11.3.2 跨定级系统安全管理中心设计技术要求

11.3.2.1 系统管理

应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的系统管理。应通过系统管理员对安全互联部件与相同和不同等级的定级系统中与安全互联相关的系统资源和运行进行配置和管理，包括用户身份管理、安全互联部件资源配置和管理等。

11.3.2.2 安全管理

应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的安全管理。应通过安全管理员对相同和不同等级的定级系统中与安全互联相关的主/客体进行标记管理，使其标记能准确反映主/客体在定级系统中的安全属性；对主体进行授权，配置统一的安全策略，并确保授权在相同和不同等级的定级系统中的合理性。

11.3.2.3 审计管理

应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的审计管理。应通过安全审计员对安全互联部件的安全审计机制、各定级系统的安全审计机制以及与跨定级系统互联有关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及时处理。

附 录 A
（资料性附录）
访问控制机制设计

A.1 自主访问控制机制设计

系统在初始配置过程中，安全管理中心首先需要对系统中的主体及客体进行登记命名，然后根据自主访问控制安全策略，按照主体对其创建客体的授权命令，为相关主体授权，规定主体允许访问的客体和操作，并形成访问控制列表。自主访问控制机制结构如图 A.1 所示。

用户登录系统时，首先进行身份鉴别，经确认为合法的注册用户可登录系统，并执行相应的程序。当执行程序（主体）发出访问系统中资源（客体）的请求后，自主访问控制安全机制将截获该请求，然后查询对应的访问控制列表。如果该请求符合自主访问控制列表规定的权限，则允许其执行；否则将拒绝执行，并将此行为记录在审计记录中。

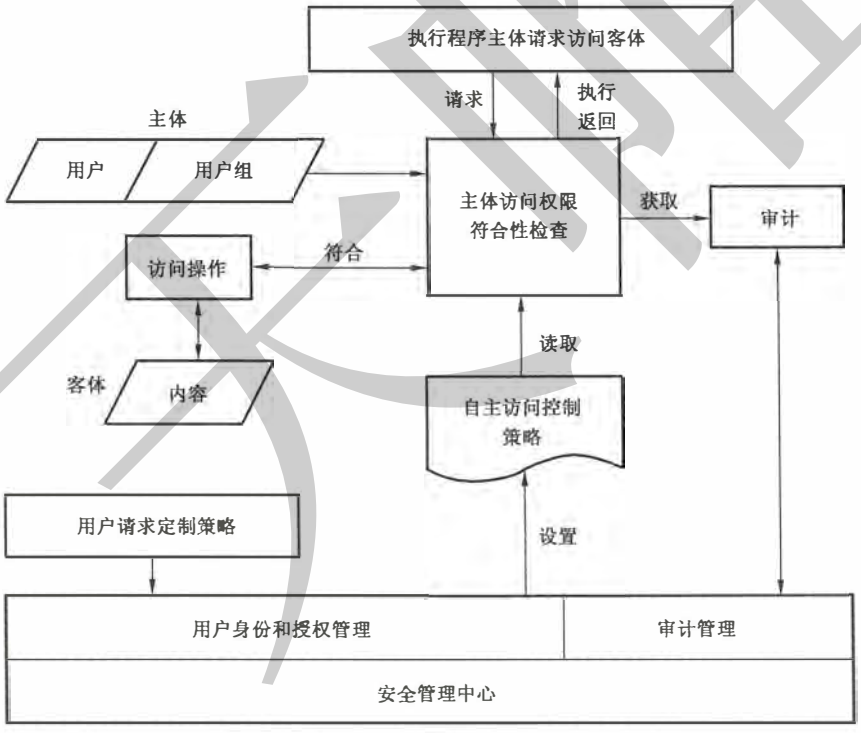

图 A.1 自主访问控制机制结构

A.2 强制访问控制机制设计

系统在初始配置过程中，安全管理中心需要对系统中的确定主体及其所控制的客体实施身份管理、标记管理、授权管理和策略管理。身份管理确定系统中所有合法用户的身份、工作密钥、证书等与安全相关的内容。标记管理根据业务系统的需要，结合客体资源的重要程度，确定系统中所有客体资源的安全级别及范畴，生成全局客体安全标记列表；同时根据用户在业务系统中的权限和角色确定主体的安全级别及范畴，生成全局主体安全标记列表。授权管理根据业务系统需求和安全状况，授予用户（主体）访

问资源(客体)的权限,生成强制访问控制策略和级别调整策略列表。策略管理则根据业务系统的需求,生成与执行主体相关的策略,包括强制访问控制策略和级别调整策略。除此之外,安全审计员需要通过安全管理中心制定系统审计策略,实施系统的审计管理。强制访问控制机制结构如图 A.2 所示。

系统在初始执行时,首先要求用户标识自己的身份,经过系统身份认证确认为授权主体后,系统将下载全局主/客体安全标记列表及与该主体对应的访问控制列表,并对其进行初始化。当执行程序(主体)发出访问系统中资源(客体)的请求后,系统安全机制将截获该请求,并从中取出访问控制相关的主体、客体、操作三要素信息,然后查询全局主/客体安全标记列表,得到主/客体的安全标记信息,并依据强制访问控制策略对该请求实施策略符合性检查。如果该请求符合系统强制访问控制策略,则系统将允许该主体执行资源访问。否则,系统将进行级别调整审核,即依据级别调整策略,判断发出该请求的主体是否有权访问该客体。如果上述检查通过,系统同样允许该主体执行资源访问,否则,该请求将被系统拒绝执行。

系统强制访问控制机制在执行安全策略过程中,需要根据安全审计员制定的审计策略,对用户的请求及安全决策结果进行审计,并且将生成的审计记录发送到审计服务器存储,供安全审计员管理。

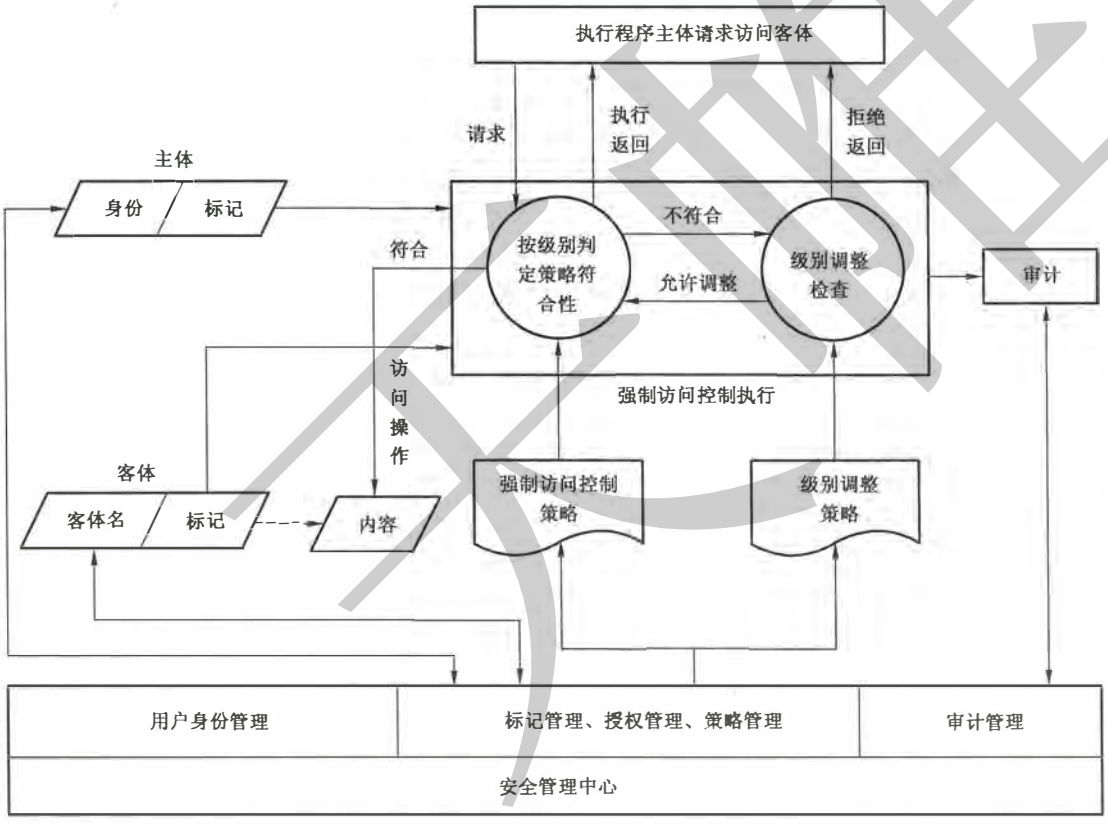

图 A.2　强制访问控制机制结构

附 录 B
（资料性附录）
第三级系统安全保护环境设计示例

B.1 概述

根据“一个中心”管理下的“三重保护”体系框架，构建安全机制和策略，形成定级系统的安全保护环境。该环境分为如下四部分：安全计算环境、安全区域边界、安全通信网络和安全管理中心。每个部分由1个或若干个子系统(安全保护部件)组成，子系统具有安全保护功能独立完整、调用接口简洁、与安全产品相对应和易于管理等特征。安全计算环境可细分为节点子系统和典型应用支撑子系统；安全管理中心可细分为系统管理子系统、安全管理子系统和审计子系统。以上各子系统之间的逻辑关系如图 B.1 所示。

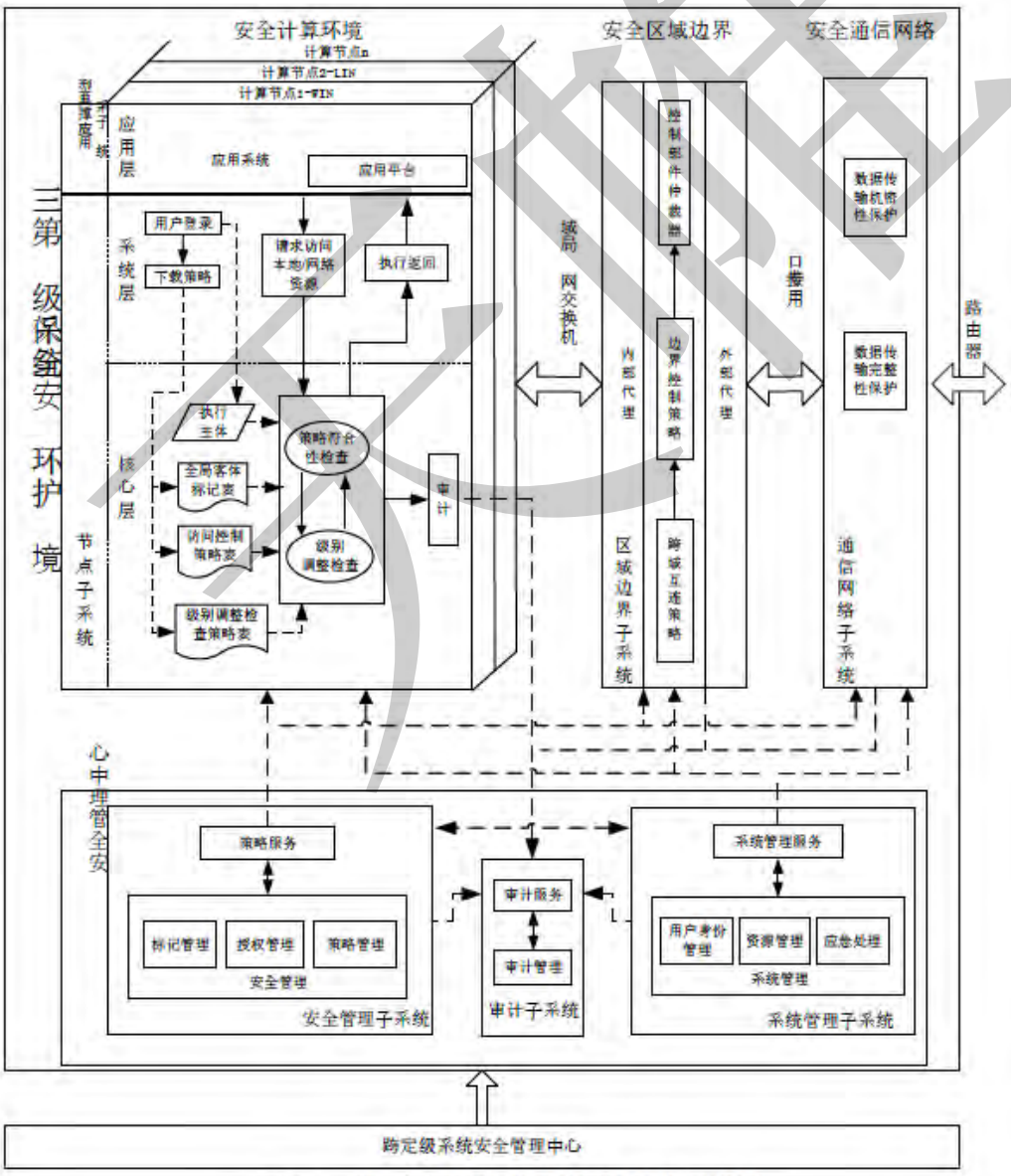

图 B.1 第三级系统安全保护环境结构与流程

B.2 各子系统主要功能

第三级系统安全保护环境各子系统的主要功能如下：

a) 节点子系统

节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成防护层，通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，为典型应用支撑子系统的正常运行和免遭恶意破坏提供支撑和保障。

b) 典型应用支撑子系统

典型应用支撑子系统是系统安全保护环境中为应用系统提供安全支撑服务的接口。通过接口平台使应用系统的主客体与保护环境的主客体相对应，达到访问控制策略实现的一致性。

c) 区域边界子系统

区域边界子系统通过对进入和流出安全保护环境的信息流进行安全检查，确保不会有违反系统安全策略的信息流经过边界。

d) 通信网络子系统

通信网络子系统通过对通信数据包的保密性和完整性的保护，确保其在传输过程中不会被非授权窃听和篡改，以保障数据在传输过程中的安全。

e) 系统管理子系统

系统管理子系统负责对安全保护环境中的计算节点、安全区域边界、安全通信网络实施集中管理和维护，包括用户身份管理、资源配置和可信库管理、异常情况处理等。

f) 安全管理子系统

安全管理子系统是系统的安全控制中枢，主要实施标记管理、授权管理及可信管理等。安全管理子系统通过制定相应的系统安全策略，并要求节点子系统、区域边界子系统和通信网络子系统强制执行，从而实现对整个信息系统的集中管理。

g) 审计子系统

审计子系统是系统的监督中枢。安全审计员通过制定审计策略，并要求节点子系统。区域边界子系统。通信网络子系统。安全管理子系统。系统管理子系统强制执行，实现对整个信息系统的行为审计，确保用户无法抵赖违反系统安全策略的行为，同时为应急处理提供依据。

B.3 各子系统主要流程

第三级系统安全保护环境的结构与流程可以分为安全管理流程与访问控制流程。安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等。访问控制流程则在系统运行时执行，实施自主访问控制、强制访问控制等。

a) 策略初始化流程

节点子系统在运行之前，首先由安全管理员、系统管理员和安全审计员通过安全管理中心为其部署相应的安全策略。其中，系统管理员首先需要为定级系统中的所有用户实施身份管理，即确定所有用户的身份、工作密钥、证书等。同时需要为定级系统实施资源管理，以确定业务系统正常运行需要使用的执行程序等。安全管理员需要通过安全管理中心为定级系统中所有主、客体实施标记管理，即根据业务系统的需要，结合客体资源的重要程度，确定其安全级，生成全局客体安全标记列表。同时根据用户在业务系统中的权限和角色确定其安全标记，生成全局主体安全标