ICS 35.240.01
CCS L 77

T/CASME

中 国 中 小 商 业 企 业 协 会 团 体 标 准

T/CASME XXXX—2024

楼宇自控系统安全技术要求

Safety technical requirements for building automation systems

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2024－XX－XX 发布　　2024－XX－XX 实施

中国中小商业企业协会　　发 布

楼宇自控系统安全技术要求

1 范围

本文件规定了楼宇自控系统安全技术的术语和定义、系统总体架构、平台层安全要求、传输层安全要求、感知层安全要求。

本文件适用于楼宇自控系统的设计、建设、运维等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 35273 信息安全技术 个人信息安全规范

GB/T 37044 信息安全技术 物联网安全参考模型及通用要求

GM/T 0026 安全认证网关产品规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

密钥 key

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

4 系统总体架构

4.1 系统架构

4.1.1 楼宇自控系统架构如图 1。

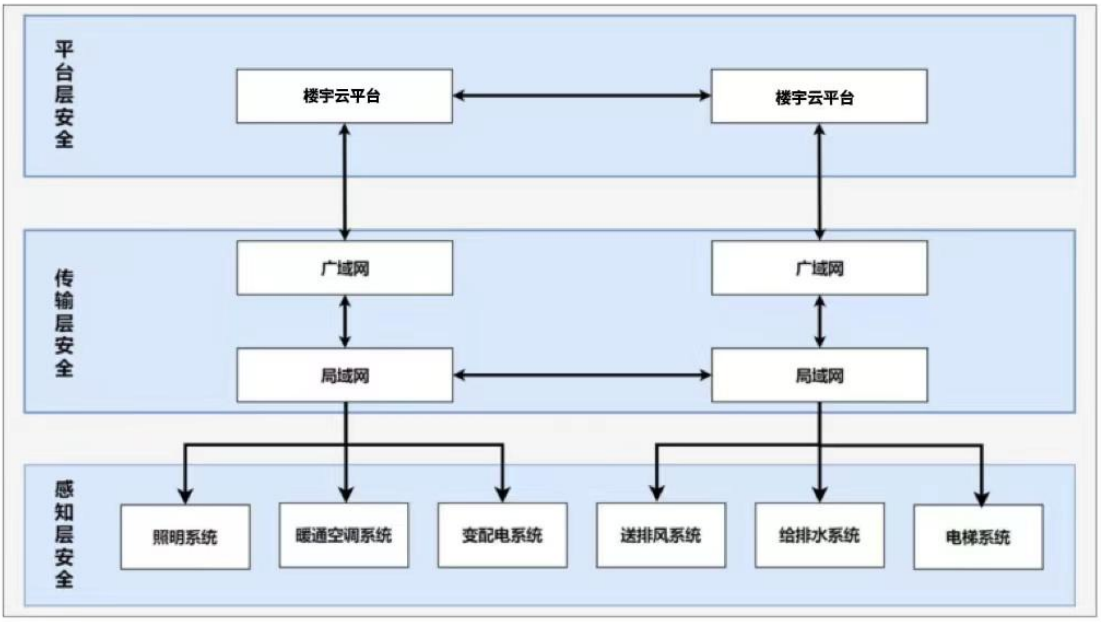

图 1　楼宇自控系统架构

4.1.2　楼宇自控系统架构应包括以下内容：

——楼宇自控系统应包括平台层、传输层以及感知层三部分；

——平台层安全面向智能终端设备提供服务，如设备注册、数据采集、数据监控、安全服务等；

——传输层安全提供网络连接功能，智能终端设备通过通信层，实现发现、组网、控制等操作，并可连接到平台层，实现平台对智能终端设备的注册、管理、控制等；

——感知层安全应包括智能终端设备、网关设备、人机交互终端设备等。

4.2　安全体系架构

4.2.1　楼宇自控系统安全体系架构如图 2。

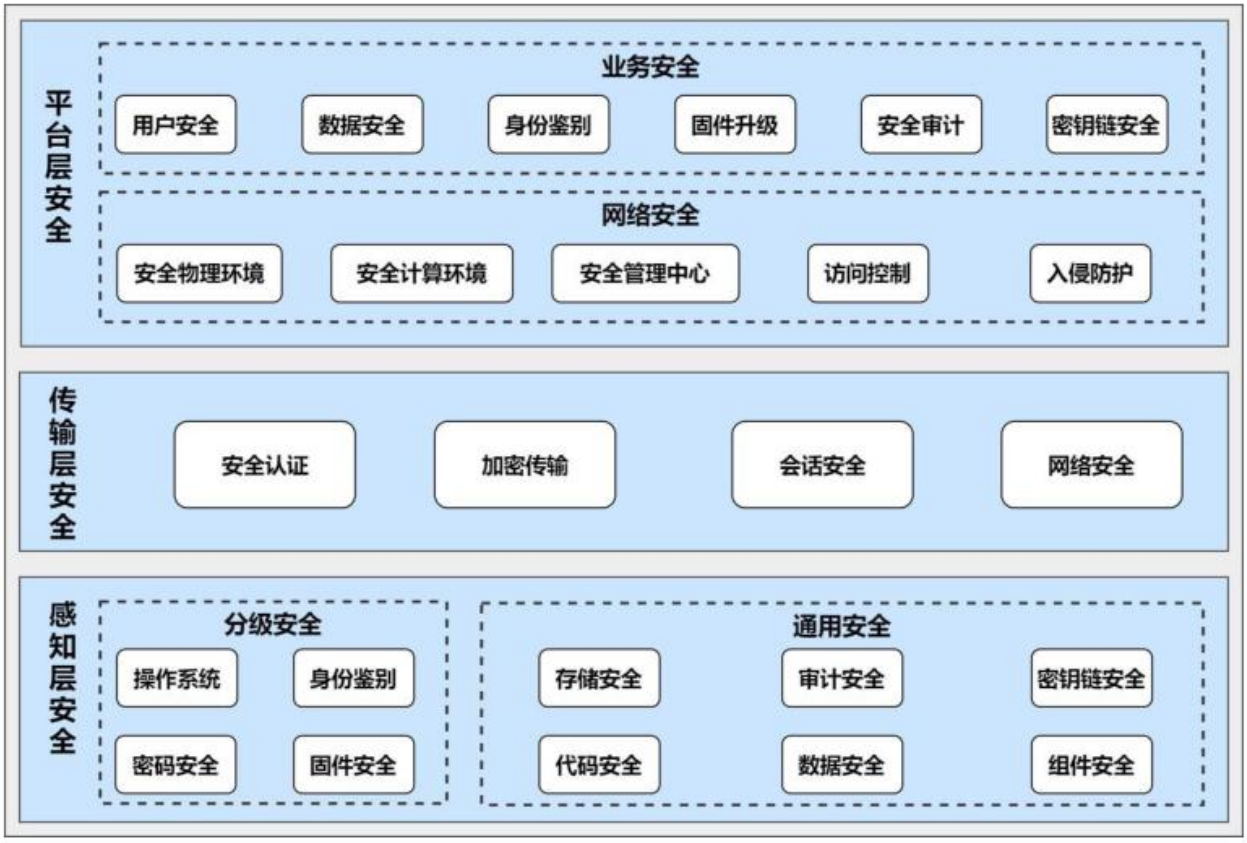

图 2　楼宇自控系统安全体系架构

4.2.2　楼宇自控系统安全体系架构应包括以下内容：

——应由平台层安全、传输层安全以及感知层安全三部分构成；

——平台安全应分为网络安全和业务安全，网络安全以等级三级为基础，增加访问控制和入侵防护两个方面；

——传输安全应包括安全认证、加密传输、会话管理、网络防御等方面；

——感知安全应分为分级安全部分和通用安全部分，安全要求应符合 GB/T 37044 的相关规定。

5　平台层安全要求

5.1　网络安全

5.1.1　物理环境

应通过云主机管理器实现同一物理机上不同云主机之间相互隔离，用户仅能访问属于自己的云主机资源，保证云主机不受周边云主机的影响，避免云主机之间发生恶意攻击或数据窃取等情况。

5.1.2 存储安全

5.1.2.1 应通过虚拟化层实现云主机间存储访问隔离，隔离用户数据，防止恶意云主机用户盗取其他用户的数据，保证数据安全。

5.1.2.2 数据存储宜采用多重备份机制，每一份数据都可有一个或者多个备份，以防存储设备（如硬盘）出现故障引起数据丢失或影响系统正常使用。

5.1.3 入侵保护安全

5.1.3.1 应通过网络平面隔离和防火墙，控制和审计云主机的网络流量，保证内部网络传输安全。

5.1.3.2 Web 应用防火墙宜采用黑、白名单机制相结合的完整防护体系，通过精细的配置将多种 Web 安全检测方法连结成一套完整的解决方案，并整合成熟的 DDos 攻击抵御机制，能够在 Web 环境中抵御各类 Web 安全威胁和拒绝服务攻击，拦截如 Web 漏洞攻击，SQL 注入、XSS 跨站、获取敏感信息等常见的攻击行为。

5.1.4 数据安全

数据安全应包括下列内容：

——数据传输过程中应对用户的数据进行加密，保证在数据传输过程中数据不会泄漏，防止数据的交叉泄漏和非法访问；

——密钥管理员应通过 API 或控制台进行主密钥的产生与管理操作，还可通过访问控制为密钥实现访问控制功能，直接通过使用 API 进行少量数据的加解密。还可通过信封加密技术实现大量数据的本地加解密；

——对所有信息系统的日志和权限审批记录均应采用碎片化分布式离散存储技术进行长期保存，对用户的操作行为进行日志监控；

——用户云服务期满后，设备管理平台应自动消除原有服务器上磁盘和内存数据，使得原用户数据无法恢复，保证对用户退库后的设备进行完全的数据销毁。

5.2 业务安全

5.2.1 用户注册、登录和注销

用户账号的相关过程应符合下列要求：

——应对用户注册的过程进行有效保护；

——应对用户注册或登录涉及的用户密码，进行加密处理后才能传输；

——应有效防止用户登录、密码重置、忘记密码等流程进行密码暴力破解；

——应对所有请求参数进行有效校验，保证会话的完整性；

——应保证用户注销账号的权利，确保用户数据能够完整和安全地删除。

5.2.2 设备入网认证和用户绑定

设备入网认证和用户绑定应符合下列要求：

——应对设备的身份进行有效验证，需要保证平台内设备的身份信息唯一，不应预测，并拥有足够的长度和复杂度；

——应保证用户绑定设备的过程安全可靠，确保用户和设备身份准确。

5.2.3 用户和设备身份鉴权

设备交互过程，包含了APP与云端交互，以及云端与设备交互，平台的服务包括设备的鉴权，用户鉴权，设备控制和状态的上报。交互过程的身份鉴权应符合下列要求：

——应对设备的身份凭证进行有效验证，不应直接使用设备 ID 等身份索引标识符号直接作为交互的凭证；

——应对用户的身份凭证进行有效验证，不应直接使用用户 ID 等身份索引标识符号直接作为交互的凭证；
——应对用户和设备的绑定关系进行严格的校验，防止用户和非其绑定关系的设备进行交互。

5.2.4 固件升级

固件升级应符合下列要求：
——应保证在固件升级下发固件信息的完整性和准确性；
——应保证固件的完整性和不应抵赖性，对固件进行安全有效的算法验证；
——应能够在下发固件的时候，同时下发固件的校验值，宜使用 SM3 等算法。

5.2.5 日志审计

日志审计应符合下列要求：
——应审计用户的所有操作时间，包括事件的日期、时间、类型、设备标识和结果，对不正常的事件，如频繁大量或不符合的业务参数进行有效记录和告警；
——应审计设备的异常状态，包括系统资源的使用情况，设备状态的频繁变化等，进行有效的记录和告警；
——应保护审计记录，保证无法删除、修改或覆盖等；
——应保证日志存储时间满足《中华人民共和国网络安全法》等相关法律法规的规定和要求。

5.2.6 用户信息保护

平台应满足GB/T 35273中的个人信息安全的有关规定。

6 传输层安全要求

6.1 安全认证要求

6.1.1 集成平台要求

6.1.1.1 应支持标准的认证授权机制，提供认证授权网关的服务或模块供各子系统平台使用，达到单点登录和用户权限统一维护的效果，各子系统平台应能将自己的认证和授权部分接入集成平台由集成平台统一管理，也可脱离集成平台独立运行。
6.1.1.2 集成平台和子系统平台在直接进行物联网设备接入时应实现设备的认证和授权机制，做到只有已知的设备才能接入平台，避免非法设备随意接入平台对系统的正常运行产生影响。

6.1.2 认证机制

认证机制中应避免使用一些终端依赖的机制，对于设备的接入，应采用基于非对称秘钥机制进行身份认证。

6.1.3 授权机制

授权机制应根据不同的客体采用不同的机制，支持基于角色的细粒度访问控制（RBAC）。平台在集成各子系统平台时除提供单点登录的方案外，还应支持标准的授权机制。

6.2 安全接入要求

6.2.1 对于保密性一般的数据接入，如封闭的内网环境，平台应对内网提供 HTTP 的 API。
6.2.2 对于保密性高的数据接入，平台应对外仅提供 HTTPS 的 API，不应对外提供 HTTP 的 API；终端应用程序对接时不应忽略证书错误。
6.2.3 对于保密性极高的数据接入，平台应对外仅提供 HTTPS 的 API，不应对外提供 HTTP 的 API；TLS 版本应大于等于 1.2，终端应用程序对接时不应忽略证书错误，终端应用程序应实现证书锁定（SSL/TLS Pining）。
6.2.4 平台应能够拦截未经授权的访问，为每个受信的终端应用程序颁发终端唯一标识、终端秘钥。终端唯一标识可对外公开，终端秘钥不应对外公开。

6.2.5 终端应用程序调用平台提供的 API 时，平台应能够验证认证信息，能够防止重放攻击，并能够验证请求的内容未经篡改。

6.2.6 平台应实现仅允许受信的终端应用程序调用其有权访问的 API，对超出访问权限的调用进行拦截。在平台中，每个受信的终端应用程序应配置有 0 到多条 API 访问规则，每条访问规则应确切地描述终端“允许调用”系统中的哪一个或那些 API，以及允许调用的频次等，或者是描述终端“不应调用”系统中的哪一个或那些 API。

7 感知层安全要求

7.1 安全分级原则

楼宇设备依据自身在身份认证、硬件、操作系统、固件等安全能力，依次划分三个安全等级，安全能力从低到高分别为：Leve11、Leve12、Leve13，以满足不同应用场景的安全需求。本文件依次对不同安全等级的楼宇设备提出安全需求，楼宇设备应满足Leve11中的全部安全要求，Level2至Leve13为宜满足的可选安全要求，并应符合下列规定：

——Level1 级楼宇设备应在使用密钥时可以进行软件级隔离并保障一定的安全性并可抵抗大规模软件攻击，应支持如软件沙箱、白盒加密等技术；

——Leve12 级楼宇设备应在使用密钥时可以进行逻辑级隔离并可以抵御大规模软件攻击、可在操作系统层被攻破的情况下仍然保障密钥的安全性，应支持如可信执行环境、安全 MCU 芯片等技术；

——Leve13 级楼宇设备应支持物理隔离安全性、芯片级防篡改保护机制并具备可抵御芯片级攻击能力，可在物理设备层被攻破的情况下仍然保障密钥的安全性，应支持安全芯片或同等安全能力的安全单元。

7.2 应用程序安全要求

7.2.1 应用程序内部存储要求

内部存储应符合下列要求：

——系统私有目录本地部分存放的配置文件等信息，通过安全的加密方式保存，包括严格的读写执行权限设置；

——系统数据库不应存储用户相关的敏感信息；

——在设备本地不存储所有楼宇设备的令牌等涉及设备安全的信息；

——在未授权拿到令牌之前，应用程序不应主动获取楼宇设备的信息；

——应用程序系统配置文件不应出现敏感信息。

7.2.2 应用系统日志要求

系统日志应符合下列要求：

——应用程序系统不应打印和存放任何交互日志文件；

——应用程序系统不应打印和存放任何从楼宇设备获取的信息的日志文件。

7.2.3 应用代码安全要求

代码安全应符合下列要求：

——签名应校验客户端完整性；

——对核心业务代码应进行混淆；

——应具备反调试功能；

——应用程序禁止存在病毒、木马、恶意脚本/代码，以及发送恶意广告、吸费、恶意消耗流量的行为；

——软件安装包应进行完整性保护并确保完整性校验流程安全可靠；

——应用程序执行从文件中读取的命令或调用外部脚本时要严格限制该文件的脚本的修改权限，防止注入攻击；

——应用程序应设置对外交互组件的访问权限；

——应对涉及现实或虚拟货币应用的口令输入框实现安全输入机制；
——涉及现实或虚拟货币的应用应实现 root 检测及风险控制；
——应用程序不应缓存敏感信息；
——应用程序只申请业务必要的权限；
——应用程序应实现自动检测更新机制；
——应用的保持登录选项，应能够让用户自主选择和取消；
——应对涉及现实或虚拟货币操作的应用提供会话保护机制；
——应对涉及现实或虚拟货币交易操作提供重认证；
——对于每一个需要授权访问的 Web 请求，应核实用户的会话标识是否合法、用户是否被授权执行这个操作；
——对 Web 用户的最终认证处理过程应放到服务器进行；
——在 Web 服务器端对所有来自不可信数据源的数据进行校验，拒绝任何没有通过校验的数据。若输出到 Web 客户端的数据来自不可信的数据源，则应对该数据进行相应的编码或转义；
——Web 应用程序的会话标识应具备随机性、唯一性，身份验证成功后，应更换会话标识；
——通过 Web 上传文件时，应在服务器端采用白名单方式对上传到 Web 内容目录下的文件类型进行严格的限制。

7.3 密钥安全要求

加解密部件涉及密钥安全的安全性应符合GM/T 0026的规定。

7.4 加解密部件的功能要求

7.4.1 加解密部件应包括对网络数据信息的加密和解密两个部分，即将网络数据从明文数据加密为密文数据或从密文数据解密为明文数据，加解密部件可根据实际需要对 IP 数据进行加密和解密处。

7.4.2 加解密部件应具备动态更换密钥的能力，并与其它加解密部件同步，在变更密钥过程中，不应影响正在进行的网络通信。

7.4.3 应用于互联网加解密网络通讯的加密网闸，应满足点对点，以及点对多点的主从通讯方式应用场景的加解密要求，也适用于独立上云的子系统或设备的应用场景；应用于楼宇自控系统内部的加解密通讯的加密模块或类似的加密产品，应满足点对点、点对多点构成的主从通讯方式和对等通讯方式应用场景的加解密要求。

7.4.4 针对公有云的应用，应采用虚拟加密网闸代替实体加密网闸，应具备与实体加密网闸相类似的功能，同时应获得密管中心发放的证书和密钥，以及实时认证和激活。

7.5 关键技术指标要求

加解密部件的关键技术指标应包括网速、延迟和丢包率，并应符合如下要求：
——网速：≥100 MHz；
——网络延迟：≤30 ms；
——丢包率：≤10-4。

《楼宇自控系统安全技术要求》团体标准

编制说明

一、工作简况

（一）任务来源

随着信息技术的飞速发展和城市化进程的加快，楼宇自控系统作为智慧城市建设的重要组成部分，其重要性与日俱增。楼宇自控系统通过集成多种智能设备和技术，实现了对建筑物内部环境、设备设施及能源使用的全面监控与管理，极大地提高了建筑运行效率和居住舒适度。然而，随着系统复杂性的增加，其问题也日益凸显，首先，不同厂商之间的设备通信协议不统一，系统集成时需要大量的定制开发工作，增加了开发成本和时间。其次，现有系统多侧重于设备的自动化控制，但在智能调节、预测性维护等高级功能方面仍有待提升。最后，系统的通信协议、设备接口等存在安全漏洞，容易受到黑客攻击和病毒侵害；数据安全保护措施不完善，可能导致数据泄露和损坏。

因此，制定楼宇自控系统安全技术要求的团体标准具有重要意义。一是通过标准化工作，推动设备通信协议的统一和互操作性的提升，降低系统集成难度和成本。二是明确系统智能化功能的要求，推动新技术在楼宇自控系统中的应用，提升系统的智能化水平。三是对系统的安全性能进行详细规定，包括系统架构安全、数据安全、设备安全、应用安全以及安全监测与防护等方面，确保系统的安全稳定运行。

（二）编制过程

为使本标准在楼宇自控系统安全技术市场管理工作中起到规范信息化管理作用，标准起草工作组力求科学性、可操作性，以科学、谨慎的态度，在对我国现有楼宇自控系统安全技术市场相关管理服务体系文件、

模式基础上，经过综合分析、充分验证资料、反复讨论研究和修改，最终确定了本标准的主要内容。

标准起草工作组在标准起草期间主要开展工作情况如下：

1、项目立项及理论研究阶段

标准起草组成立伊始就对国内外楼宇自控系统安全技术相关情况进行了深入的调查研究，同时广泛搜集相关标准和国外技术资料，进行了大量的研究分析、资料查证工作，确定了楼宇自控系统安全技术市场标准化管理中现存问题，结合现有产品实际应用经验，为标准起草奠定了基础。

标准起草组进一步研究了楼宇自控系统安全技术需要具备的特殊条件，明确了技术要求和指标，为标准的具体起草指明了方向。

2、标准起草阶段

在理论研究基础上，起草组在标准编制过程中充分借鉴已有的理论研究和实践成果，基于我国市场行情，经过数次修订，形成了《楼宇自控系统安全技术要求》标准草案。

3、标准征求意见阶段

形成标准草案之后，起草组召开了多次专家研讨会，从标准框架、标准起草等角度广泛征求多方意见，从理论完善和实践应用多方面提升标准的适用性和实用性。经过理论研究和方法验证，起草组形成了《楼宇自控系统安全技术要求》（征求意见稿）。

（三）主要起草单位及起草人所做的工作

1、主要起草单位

协会、企业等多家单位的专家成立了规范起草小组，开展标准的编制工作。

经工作组的不懈努力，在 2024 年 8 月，完成了标准征求意见稿的编写工作。

2、起草人所做工作

广泛收集相关资料。在广泛调研、查阅和研究国际标准、国家标准、行业标准的基础之上，形成本标准草案稿。

二、标准编制原则和主要内容

（一）标准编制原则

本标准依据相关行业标准，标准编制遵循“前瞻性、实用性、统一性、规范性”的原则，注重标准的可操作性，本标准严格按照《标准化工作指南》和 GB/T 1.1《标准化工作导则 第一部分：标准的结构和编写》的要求进行编制。标准文本的编排采用中国标准编写模板 TCS 2009 版进行排版，确保标准文本的规范性。

（二）标准主要技术内容

本标准报批稿包括 7 个部分，主要内容如下：

1　范围

本文件规定了楼宇自控系统安全技术的术语和定义、系统总体架构、平台层安全要求、传输层安全要求、感知层安全要求。

本文件适用于楼宇自控系统的设计、建设、运维等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 35273 信息安全技术 个人信息安全规范

GB/T 37044 信息安全技术 物联网安全参考模型及通用要求

GM/T 0026 安全认证网关产品规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

密钥 key

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

4 系统总体架构

4.1 系统架构

4.1.1 楼宇自控系统架构如图 1。

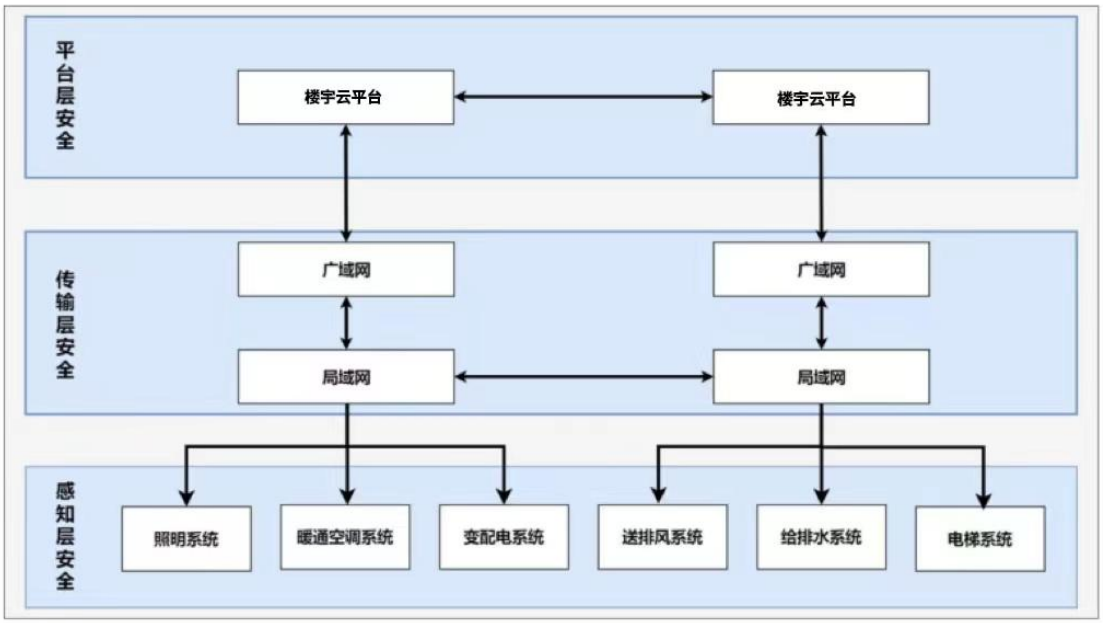

图 1 楼宇自控系统架构

4.1.2 楼宇自控系统架构应包括以下内容：

——楼宇自控系统应包括平台层、传输层以及感知层三部分；

——平台层安全面向智能终端设备提供服务，如设备注册、数据采集、数据监控、安全服务等；