CSA 云安全联盟标准

CSA GCR C0XX—20XX

零信任应用安全实施规范

Zero Trust Application Security Implementation Specification

（征求意见稿）

20XX－XX－XX 发布

云安全联盟大中华区　　发布

目 次

前　言

本规范按照 GB/T 1.1-2020 《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由云安全联盟大中华区归口。

本文件起草单位：

本文件主要起草人：

1 范围

本标准规定了应用安全零信任系统实施的通用要求，并给出了应用安全零信任实施的典型场景。

本标准适用于车联网、工业互联网行业应用的零信任系统实施。

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，标注日期的引用文件，仅该日期所对应的版本适用于本文件；不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术　术语

GB/T 29242—2012　信息安全技术　鉴别与授权安全断言标记语言

T/CESA 1165—2021　零信任系统技术规范

3 术语和定义

下列数据和定义适用于本文件。

- **访问主体**　access subject

访问客体的主动实体。

注：访问主体如用户、终端设备、物联网设备等

- **访问客体**　access object

被访问的目标资源。

注：访问客体如服务器、数据库、打印服务、网络等。

- **零信任技术**　zero trust technology

旨在降低访问过程安全风险的持续动态安全访问控制技术。

注：零信任技术基于安全和信任状态对访问主体进行安全授权，并持续性的监测整个访问过程的安全性。

- **零信任系统**　zero trust system

基于零信任技术的相关产品和服务，或者是产品和服务的组合。

- **前装智能车载终端 telematic box**

符合严格的车规级标准，集成 2G 至 5G 无线通信模块，实现与车辆 CAN 总线直接通信，以收集关键的车辆状态和性能数据；支持数据向云端的传输，并能够接收云端指令执行远程操作，包括自检、远程查询、远程参数配置及固件远程升级等高级功能。

- **追踪器 tracker**

提供高精度的车辆定位管理，实时追踪车辆位置，根据不同配置，扩展功能包括 4G 通信、状态监测、异常事件通知等；支持 4G WiFi、蓝牙 4.0/3.0 数据传输，以及驾驶行为分析，能够统计行驶里程，进行远程设置和维护。

- **后装设备 on-board diagnostics**

实时监控发动机电控系统及车辆其他功能模块的工作状态，通过算法分析，精确诊断并报告工况异常和故障；通过读取车辆 CAN 总线信息，支持车队管理平台的构建，实现车队的量化管理、安全监控、效率优化和成本控制。

4 缩略语

下列缩略语适用于本文件。

- CAN 控制器局域网总线（Controller Area Network）
- DLC 可下载内容（Downloadable Content）
- OBU 车载单元（On Board Unit）
- CPU 中央处理器（Central Processing Unit）
- DDoS 分布式拒绝服务攻击（Distributed Denial of Service）
- SSH 安全外壳协议（Secure Shell）
- RDP 远程桌面协议（Remote Desktop Protocol）
- WAN 广域网（Wide Area Network）
- DCN 数据通信网络（Data Communication Network）

5 概述

零信任是一种网络安全架构，其核心理念是“永不信任，始终验证”。该架构不信任任何用户或设备，无论其位于网络内部还是外部，都必须经过严格的身份验证和授权。零信任

系统基于对网络环境的高度不信任，采取多层次的安全控制措施来保护企业的数据和资源。在这种模式下，用户和设备在访问企业资源时都需要进行身份验证和授权，以减少未经授权的访问和数据泄露的风险。

零信任系统的实施涉及多个角色，包括提供商、业务系统提供商、集成商、使用方、信息安全设备提供商和第三方测评机构等。这些角色需相互配合，共同完成安全防护建设。零信任系统的安全防护工作需贯彻企业安全体系规划、建设、运维等全生命周期过程，分为安全分析、安全设计、安全加固和效果核验四个步骤。

零信任系统适用于所有需要资源访问安全防护的场景，本标准提供了通用实施场景及车联网和工业互联网两种典型场景的具体技术要求。企业应根据自身的安全风险水平和投入，决定是否采用零信任系统。

6 零信任系统建设实施流程

6.1 安全防护能力建设

新建业务系统：零信任安全防护应贯穿业务系统全生命周期，包括规划、建设、运维，并在关键节点进行安全分析、设计、加固及核验。

存量业务系统：根据现有架构和安全状况，进行针对性的安全分析、设计，并逐步加固和核验。

6.2 安全分析

确定目标安全效果，分析业务系统安全防护的收益、潜在损失和资源成本，形成安全防护分析报告。

新建业务系统：结合行业特点和企业资源，进行安全分析。

存量业务系统：基于现有架构和安全措施，进行综合安全分析。

6.3 安全设计

在安全分析基础上，设计零信任安全防护方案，包括咨询、方案设计和评审。

新建业务系统：同步规划零信任安全防护，设计一体化方案和配套管理。

存量业务系统：针对发现的风险，设计解决方案，提升安全防护能力。

6.4 安全加固

根据安全设计方案，在业务系统上线前或停机期间进行加固。

技术措施：由相关部门组成实施小组，共同开展安全防护实施工作。

管理措施：落实管理制度，监督第三方服务提供商。

6.5 效果核验

对加固后的业务系统进行监视、测量、分析和评价，定期进行内部审核和管理评审，确保达到预期安全水平。

7 应用安全零信任实施通用要求

7.1 逻辑架构

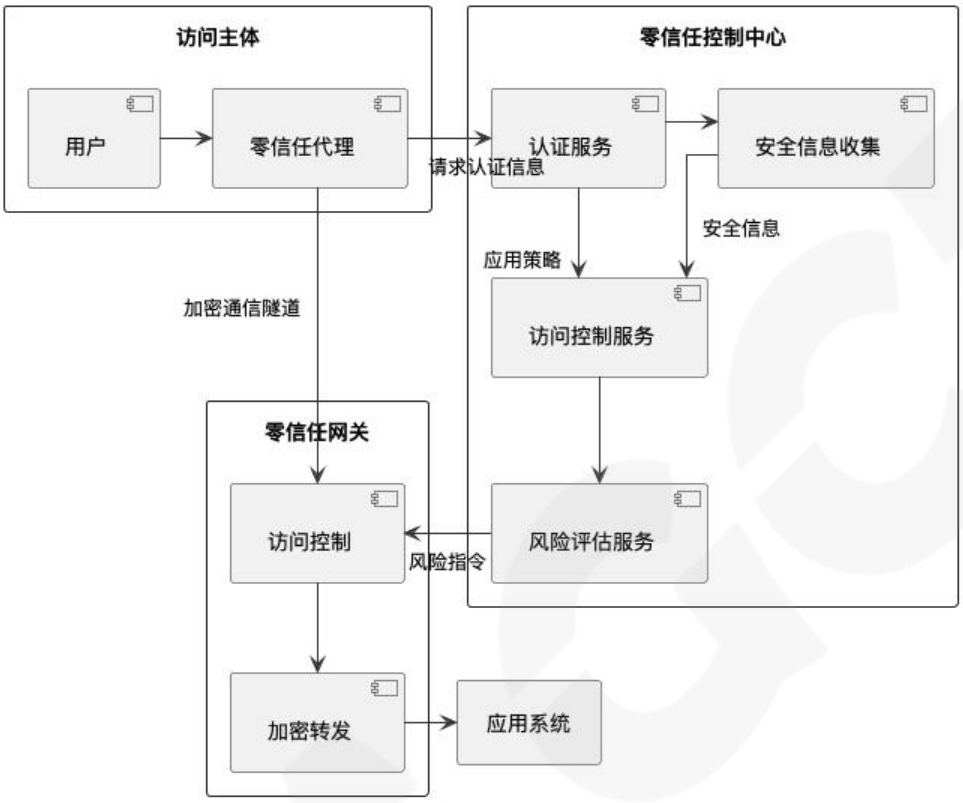

图 1 通用零信任架构图

本架构图展示了应用系统与零信任安全网关、零信任代理和零信任控制中心之间的交互关系，以及数据流向。

7.2 安全要求

应用安全零信任系统应满足行业应用业务安全的实际需要，应根据业务的访问对象、保护对象和安全要求等因素选择适当的零信任实现技术和方法。其基本要求包括以下几点：

a）认证和授权：零信任系统要求对用户进行认证和授权，确保只有经过验证的用户可以访问系统资源。通过多因素身份验证访问控制等技术来实现。

b）细粒度的访问控制：零信任系统需要实施细粒度的访问控制，以确保用户只能访问其所需的资源，而不是整个网络。这可以通过基于角色的访问控制、动态访问控制和上下文感知的访问控制等技术来实现。

c）实时威胁检测和响应：零信任系统需要实时监测和检测潜在的威胁，并采取相应的

措施进行响应。这可以通过实时日志分析、行为分析和威胁情报共享等技术来实现。

d）数据加密和隔离：零信任系统需要对数据进行加密和隔离，以防止未经授权的访问和数据泄露。这可以通过端到端加密、数据分类和分区、以及数据遗忘等技术来实现。

e）持续监测和审计：零信任系统需要进行持续的监测和审计，以确保系统的安全性和合规性。这可以通过日志记录、事件管理和审计工具等技术来实现。

7.3 性能要求

为了确保零信任系统在高负载情况下的稳定性和响应速度，我们对单节点网关的性能配置和测试指标有明确的要求。

7.3.1 单节点网关配置

在零信任架构中，单节点网关是处理用户请求的关键组件，因此必须具备足够的处理能力来应对预期的负载。以下是推荐的最低配置标准：

CPU：至少 8 核心，以确保在高并发请求下能够快速处理鉴权和数据传输任务。

内存：至少 16GB，以支持高效的数据处理和缓存机制，减少延迟。

磁盘：至少 500GB，用于存储日志、配置文件以及其他必要的数据，同时保证足够的空间以应对未来的扩展需求。

7.3.2 性能测试指标

性能测试是验证网关能否满足业务需求的重要环节。以下是必须满足的关键性能指标：

静态页面鉴权访问并发：网关应能够处理每秒 2000 至 8000 次的并发请求量（QPS）。这一指标反映了网关在面对大量用户请求时的处理能力，确保用户体验不受影响。

为了达到这些性能要求，建议进行定期的压力测试和性能监控，以便及时发现并解决潜在的性能瓶颈。此外，应考虑使用负载均衡技术分散请求，以提高系统的吞吐量和可用性。

7.4 部署要求

7.4.1 访问主体部署方式

访问主体部署功能要求应选择如下中的一种方式：

a）支持有零信任代理 的部署，设备操作系统类型：Windows、Macosx、Linux、Android、iOS 等；

b）支持无 零信任代理的部署模式，支持各类标准浏览器访问。

7.4.2 控制中心部署

1. 网络隔离和分段：

a) 部署控制中心时，需要放置在与业务网络隔离的安全区域，以确保控制中心不容易受到业务网络的攻击。

b) 业务网络和控制中心之间需要分段，根据安全策略和访问需求划分不同的网络区域，限制业务网络对控制中心的访问权限。

2. 数据保护和加密：

a) 对于在控制中心传输和存储的数据，需要加密保护，以防数据泄露和篡改。

b) 对于敏感数据，如资产信息、用户隐私数据等，需要采用更高级别的加密算法和保护措施，确保数据的安全性。

3. 高可用架构设计：

a) 部署多个控制中心实例，实现冗余和故障转移。当一个实例发生故障时，其他实例可以接管服务，保证系统的连续性。

b) 使用负载均衡器来分发流量，确保控制中心的负载均衡和高可用性。负载均衡器可以实时监控控制中心的状态，将流量动态分配给可用的实例。

4. 监控和告警系统：

a) 部署实时监控系统，对控制中心的性能和状态监控。通过监控系统，可以及时发现系统故障、性能下降等异常情况。

b) 设置告警规则，当控制中心的性能或状态异常时，及时发送告警通知给相关人

员，以便快速响应和处理问题。

5. 容灾和灾备计划：

a) 制定容灾和灾备计划，包括备用服务器、网络设备等基础设施的准备和配置，以应对自然灾害、硬件故障等突发情况。

b)定期进行容灾演练和测试，确保备用设备和系统能够正常运行，并能够在短时间内切换到备用设备，保证系统的连续性。

c) 定期备份控制中心的数据，包括配置信息、用户数据、日志等。备份数据应存储在安全可靠的位置，以便在需要时用于恢复。

d) 配置自动化的数据恢复机制，以便在发生故障或数据丢失时能够快速恢复数据，并尽量减少系统的停机时间。

6. 自动化运维和维护：

a) 配置自动化运维和维护工具，自动化地管理控制中心的配置和更新，减少人工操作和减少出错的可能性。

b) 定期进行系统巡检和维护，包括系统更新、安全补丁的安装、日志管理等，确保系统的稳定性和安全性。

7.4.3 零信任安全网关部署

零信任安全网关部署功能要求如下：

1. 高可用架构设计：

a) 部署多个零信任安全网关实例，实现冗余和故障转移。当一个实例发生故障时，其他实例可以接管服务，保证系统的连续性。

b) 使用负载均衡器分发流量，确保控制中心的负载均衡和高可用性。负载均衡器可以实时监安全控网关的状态，将流量动态分配给可用的实例。

2. 监控和告警系统：

a) 部署实时监控系统，监控安全网关的性能和状态。通过监控系统，可以及时发现系统故障、性能下降等异常情况。

b) 设置告警规则，当安全网关的性能或状态异常时，及时发送告警通知给相关人员，以便快速响应和处理问题。

3. 容灾和灾备计划：

a) 制定容灾和灾备计划，包括备用服务器、网络设备等基础设施的准备和配置，应对自然灾害、硬件故障等突发情况。

b) 定期执行容灾演练和测试，确保备用设备和系统能够正常运行，并能够在短时间内切换到备用设备，保证系统的连续性。

c) 定期备份安全网关的数据，包括配置信息、日志等。备份数据应存储在安全可靠的位置，以便在需要时用于恢复。

d) 配置自动化的数据恢复机制，以便在发生故障或数据丢失时能够快速恢复数据，并尽量减少系统的停机时间。

4. 自动化运维和维护：

a) 配置自动化运维和维护工具，自动化地管理安全网关的配置和更新，减少人工操作和减少出错的可能性。

b) 定期进行系统巡检和维护，包括系统更新、安全补丁的安装、日志管理等，确保系统的稳定性和安全性。

7.5 容灾要求

7.5.1 容灾架构

容灾架构示意图

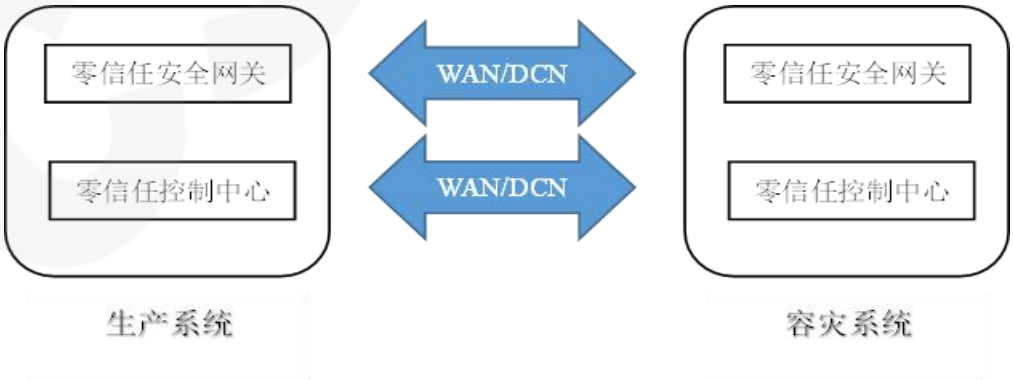

图 2 容灾示意图

当主节点发生故障时，备份节点会自动接管服务，并成为新的主节点。同时，备份节点会自动启动数据恢复和同步过程，确保数据的完整性和一致性。当主节点恢复后，系统会自

动切换回主节点，并继续提供服务。

7.5.2 容灾要求

控制中心和安全网关的容灾应符合以下要求：

a) 基础设施高可靠性：应支持备份、容错和冗余机制，确保在硬件故障或自然灾害等情况下系统能够持续运行。

b) 数据冷热分离部署：应支持将冷数据和热数据分别部署在不同的存储设备或节点上，提高数据的访问效率和存储利用率。

c) 数据存储高可靠性：数据存储应具备增量备份和全量备份的能力，并支持分布式存储和存储容量冗余设计，以防止数据丢失和提供高可用性。

d) 内存数据库数据持久化：应持久化存储内存数据库的数据，以便在故障恢复时能够快速恢复数据并保证数据的完整性。

e) 系统软件高可靠性：系统软件应经过充分的测试和验证，确保稳定性和可靠性。同时，应定期进行软件升级和补丁管理，修复潜在的漏洞并提升系统的安全性。

f) 支持自动故障恢复：系统应能够自动检测和识别故障，并采取相应的措施进行故障恢复。

g) 支持异地备份和灾备：系统应具备异地备份和灾备能力，即将数据备份到远程地点，并在发生灾难性故障时能够快速切换到备用数据中心或云服务提供商，实现快速的灾难恢复。

h) 支持灰度发布和回滚：在系统升级或发布新版本时，应支持灰度发布和回滚机制。

i) 支持监控和预警：系统应具备全面的监控和预警机制，能够实时监测系统的运行状态、性能指标和异常情况，并及时发出警报。

j) 支持容灾演练和测试：定期进行容灾演练和测试，验证容灾方案的有效性和可靠性。

8 车联网场景零信任实施技术要求

8.1 逻辑架构

车联网场景下，通过车辆与互联网的连接，实现车辆之间、车辆与基础设施之间的信息

共享和通信。系统逻辑架构见下图，主要包括：访问主体、零信任控制中心、零信任安全网关、车辆/车载设备、路侧设备、车联网应用系统。

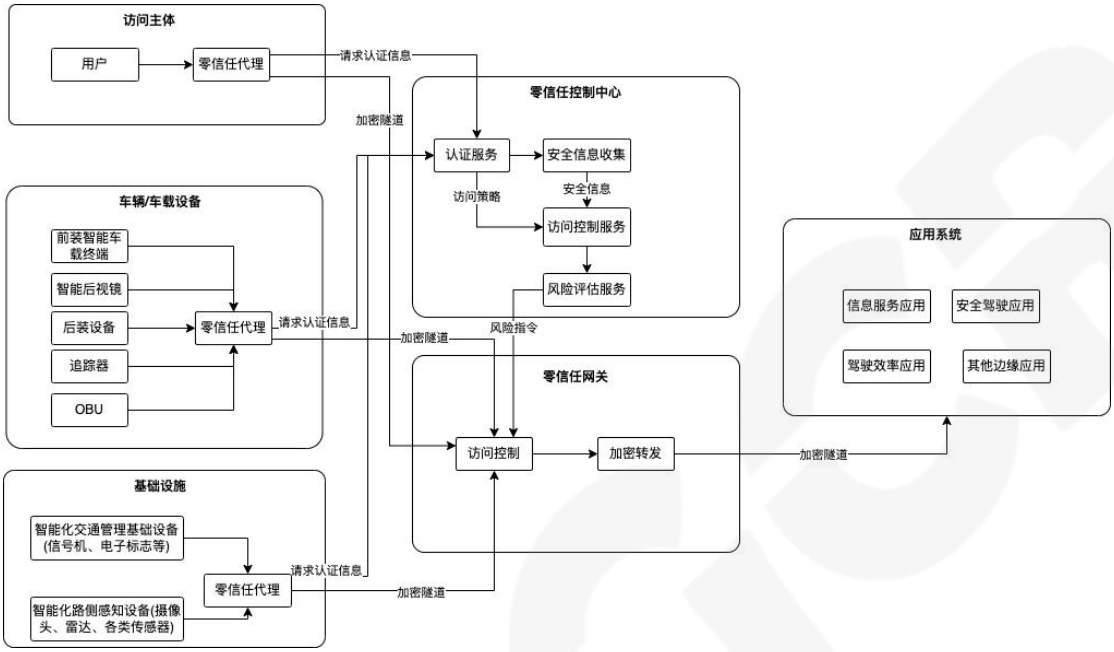

图 3 车联网零信任架构图

8.2 安全要求

在车联网中，使用零信任的安全要求主要体现在对车辆身份认证、数据加密传输、远程控制和远程监控等方面。由于车辆是移动的终端设备，其连接的网络环境可能不可靠，因此需要使用零信任的安全机制来保护车辆的安全和隐私。满足以下要求：

8.2.1 车辆身份认证要求

a) 车联网应支持强大的身份凭据和授权访问凭据防盗用功能，以确保只有合法的车辆和用户可以接入系统。

b) 车辆身份认证应采用多因素身份验证，包括但不限于基于设备的认证、车辆证书、数字签名和生物特征识别等。

c) 车辆身份认证应支持动态令牌和单次密码，以增加身份认证的安全性。

8.2.2 实施动态访问控制

a) 每个用户和设备的访问权限都需要进行动态控制，只有在经过验证和授权后才能获得相应的访问权限。

b) 权限可以根据用户的行为和环境的变化进行动态调整，确保只有合法的用户和设备能够访问系统。

8.2.3 数据加密传输要求

a) 车联网应支持双向数据加密传输，使用强加密算法如国密 SM2、SM3、SM4 等，确保数据在传输过程中的机密性和完整性。

b) 数据传输通道应采用 TLS/SSL 等安全协议，以保护数据在传输过程中的安全性。

c) 车联网应支持端到端的加密传输，确保数据在车辆、车载设备和应用系统之间的安全传输。

8.2.4 远程控制和远程监控要求

a) 远程控制和远程监控功能应受到严格的访问控制，只有经过授权的用户才能进行远程操作。

b) 远程控制和远程监控应支持权限分离，确保系统管理员、安全员和审计员的访问权限分别独立控制。

c) 远程控制和远程监控应采用安全的通信协议和加密算法，防止数据被篡改或泄露。

d) 车联网应支持远程设备锁定和远程数据擦除功能，以防止车辆被盗或数据泄露的风险。

8.2.5 设备安全要求

a) 终端设备、车载设备和路侧设备应具备操作系统基础病毒防护、安全文件加密、自身进程异常中断保护和系统漏洞修复等功能，以防止恶意软件和攻击的入侵。

b) 终端设备、车载设备和路侧设备应定期进行安全性评估和漏洞扫描，及时修补系统漏洞和弱点。

8.2.6 服务器安全要求

a) 车联网应用系统所在服务器应具备操作日志审计功能，记录所有操作和事件，以便进行安全审计和故障排查。

b) 服务器应具备 DDoS 防护能力，以应对来自网络的分布式拒绝服务攻击。

c) 服务器上的关键服务如 SSHD/RDP 等应加固，采取安全配置和访问控制措施，以防止未经授权的访问和攻击。

8.2.7 应用系统安全要求

a) 车联网应用系统应强制要求用户使用复杂密码，并定期更新密码，以提升系统的密码安全性。

b) 高危服务应关闭或限制访问，终端高危端口应屏蔽，以减少系统的攻击面。

c) 车联网应用系统应定期进行安全性评估和漏洞扫描，及时修补系统漏洞和弱点。

8.2.8 实施持续监控和响应

a) 建立安全事件监控和响应机制，持续监控和分析系统进行，及时发现和响应安全事件。

b) 建立漏洞管理和紧急修复机制，及时修补系统漏洞和弱点。

8.3 性能要求

参考 7.3 性能要求。

8.4 部署要求

参考 7.4 部署要求。

8.5 容灾要求

参考 7.5 容灾要求。

9 工业互联网场景零信任实施技术要求

9.1 逻辑架构

工业互联网场景下，通过网络连接工业设备、工业控制系统和企业管理系统，实现设备之间及设备与系统之间的信息共享和通信。系统逻辑架构如下图所示，主要包括：访问主体、零信任控制中心、零信任安全网关、工业设备、工业互联网系统（访问客体）。

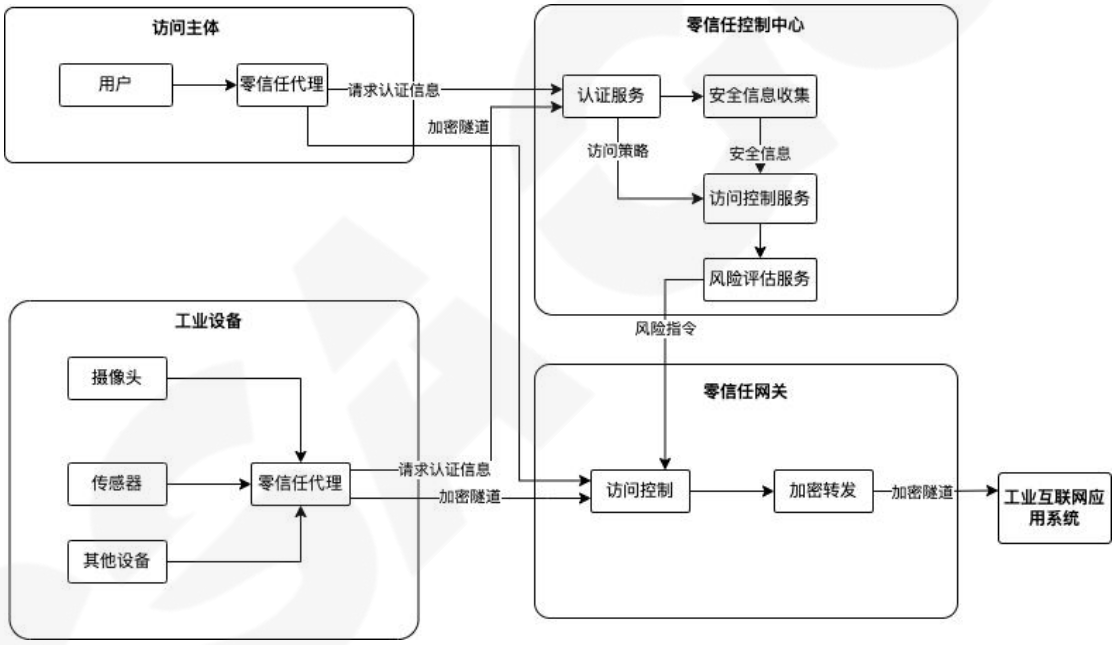

图 4 工业互联网零信任架构图

9.2 安全要求

在工业互联网中，使用零信任的安全要求主要涵盖设备身份认证、数据加密传输、远程访问和远程监控等方面。虽然工业设备通常是固定的终端设备，且其连接的网络环境相对可靠，但由于工业设备的特殊性，其安全性要求较高。因此，工业互联网需要使用零信任的安全机制来保护设备的安全和数据的机密性。具体安全要求如下：

1. 终端设备身份认证要求：

a) 工业互联网应支持身份凭据和授权访问凭据防盗用等功能，以确保只有合法的工业互联网终端设备和用户可以接入系统。

b) 工业互联网终端设备身份认证应采用多因素身份验证，包括但不限于基于设备的认证、设备证书、数字签名等。

c) 工业互联网终端设备身份认证应支持动态令牌和单次密码，以增加身份认证的安全性。

2. 实施动态访问控制：

a) 每个用户和设备的访问权限都需要进行动态控制，只有在经过验证和授权后才能获得相应的访问权限。

b) 权限可以根据用户的行为和环境的变化进行动态调整，确保只有合法的用户和设备能够访问系统。

3. 数据加密传输要求：

a) 工业互联网应支持双向数据加密传输，使用强加密算法如国密 SM2、SM4 等，确保数据在传输过程中的机密性和完整性。

b) 数据传输通道应采用 TLS1.2 等安全协议，以保护数据在传输过程中的安全性。

c) 工业互联网应支持端到端的加密传输，确保数据在工业互联网终端设备和应用系统之间的安全传输。

4. 远程控制和远程监控要求：

a) 远程控制和远程监控功能应受到严格的访问控制，只有经过授权的用户才能进行远程操作。

b) 远程控制和远程监控应支持权限分离，确保系统管理员、安全员和审计员的访问权限分别独立控制。

c) 远程控制和远程监控应采用安全的通信协议和加密算法，防止数据被篡改或泄露。

d) 工业互联网应支持远程设备锁定和远程数据擦除功能，以防止工业互联网终端设备数据泄露的风险。

5. 设备安全要求：

a) 终端设备应具备操作系统基础病毒防护、安全文件加密、自身进程异常中断保

护和系统漏洞修复等功能，以防止恶意软件和攻击的入侵。

b) 终端设备应定期进行安全性评估和漏洞扫描，及时修补系统漏洞和弱点。

6. 服务器安全要求：

a) 工业互联网应用系统所在服务器应具备操作日志审计功能，记录所有操作和事件，以便进行安全审计和故障排查。

b) 服务器应具备 DDoS 防护能力，以应对来自网络的分布式拒绝服务攻击。

c) 服务器上的关键服务如 SSHD/RDP 等应加固，采取安全配置和访问控制措施，以防止未经授权的访问和攻击。

7. 应用系统安全要求：

a) 工业互联网应用系统应强制要求用户使用复杂密码，并定期更新密码，以提升系统的密码安全性。

b) 高危服务应关闭或限制访问，终端高危端口应屏蔽，以减少系统的攻击面。

c) 工业互联网应用系统应定期进行安全性评估和漏洞扫描，及时修补系统漏洞和弱点。

8. 实施持续监控和响应：

a) 建立安全事件监控和响应机制，持续监控和分析系统，及时发现和响应安全事件。

b) 建立漏洞管理和紧急修复机制，及时修补系统漏洞和弱点。

9.3 性能要求

参考 7.3 性能要求。

9.4 部署要求

参考 7.4 性能要求。

9.5 容灾要求

参考 7.5 容灾要求。