ICS 71.020
CCS G00

T/GLAC

中 国 卫 星 导 航 定 位 协 会 团 体 标 准

T/XXX XXXX—XXXX

基于北斗的化工园区安全管理系统技术要求

Technical requirements for safety management system of chemical industry park based on BDS

（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。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国卫星导航定位协会　　发 布

目　　次

前　言

本文件按照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专利的责任。

本文件由上海华谊信息技术有限公司提出。

本文件由中国卫星导航定位协会归口。

本文件起草单位：

本文件主要起草人：

基于北斗的化工园区安全管理系统技术要求

1 范围

本文件规定了基于北斗的化工园区安全管理系统的架构、功能、性能和安全性要求。

本文件适用于基于北斗的化工园区安全管理系统的设计、部署和验收。

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 4208—2017 外壳防护等级（IP代码）

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39267 北斗卫星导航术语

GB/T 39414（所有部分） 北斗卫星导航系统空间信号接口规范

GB/T 41391 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

NMEA 0183 海洋电子设备接口标准（Standard For Interfacing Marine Electronic Devices）

RTCM 3.X GNSS实时差分数据传输标准（Real-Time GNSS Data Transmission Standard）

3 术语和定义

GB/T 39267界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件

AOA:到达角度（Angle of Arrival）

BDS:北斗卫星导航系统(BeiDou Navigation Satellite System)

CA：证书授权（Certificate Authority）

CORS:连续运行卫星定位导航服务系统(Continuous OperationalReference System)

GIS:地理信息系统（Geographic Information System）

LoRa:远距离无线电（Long Range Radio）

MQTT:消息队列遥测传输协议（Message Queuing Telemetry Transport）

MTBF:平均无故障工作时间（Mean Time Between Failure）

NB-IoT:窄带物联网（Narrow Band Internet of Things）

NFC:近场通信（Near Field Communication）

NTRIP:通过互联网进行RTCM网络传输的协议（Networked Transport of RTCM via Internet Protocol）

RSSI:接收的信号强度指示（Received Signal Strength Indication）

RTK:实时动态测量（Real-Time Kinematic）

TCP:传输控制协议（Transmission Control Protocol）

TDOA:到达时间差（Time Difference of Arrival）

TEE:可信执行环境（Trusted Execution Environment）

TOF:飞行时间（Time of Flight）

TTS:文本到语音（Text To Speech）

USB:通用串行总线（Universal Serial Bus）

UWB:超宽带（Ultra Wide Band）

Wi-Fi:无线网络通信技术（Wireless Fidelity）

5 系统构成

基于北斗的化工园区安全管理系统分为感知层、传输层、数据层、服务层、应用层，见图1。

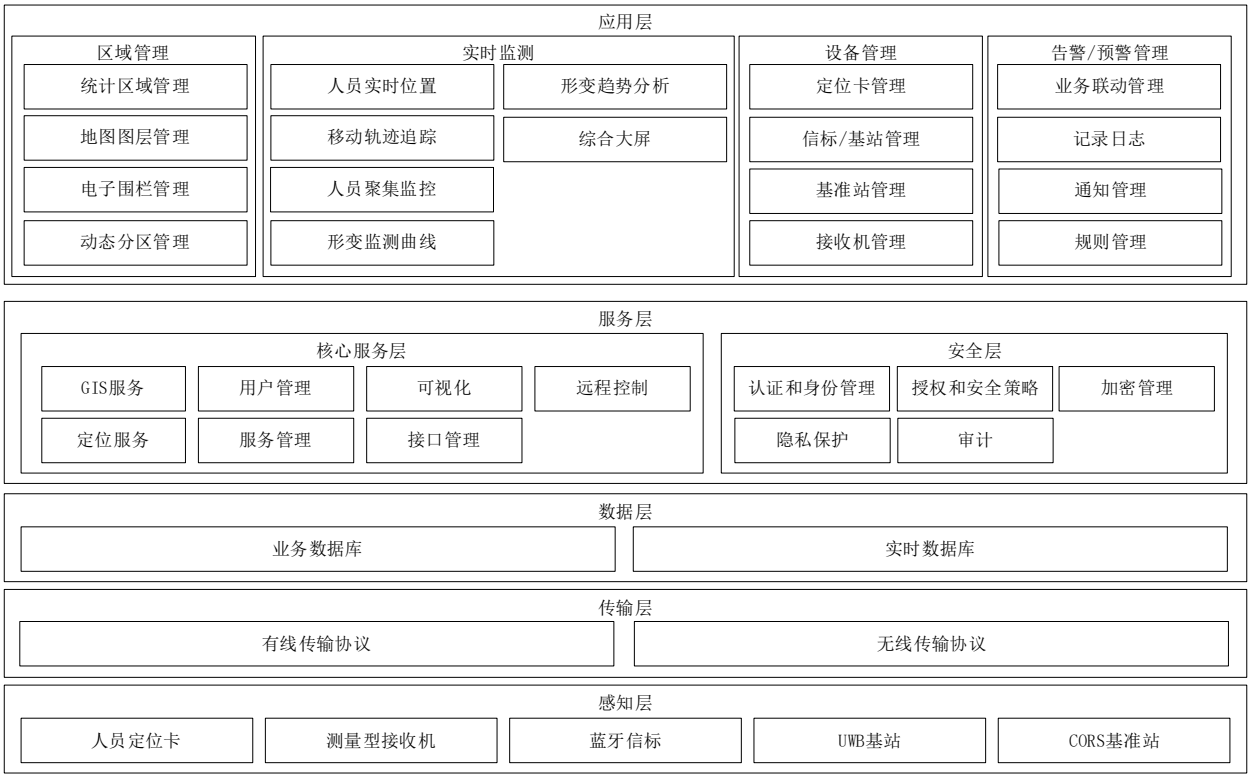

图1 基于北斗的化工园区安全管理系统架构

其中：

a) 感知层：基于物理感知设备的集合，通过多种定位设备，收集并解析定位数据，通过多种传输协议传输至数据层；
b) 传输层：包含本系统的各项数据传输的有线或无线通信涉及的技术体制与通信协议等；
c) 数据层：用于储存并处理来自感知层的数据，分为业务数据和实时数据；
d) 服务层：构建在云上，为系统应用提供中间件支持和多种基础服务，包含核心服务层和安全层；
e) 应用层：为用户提供区域管理、实时监测、设备管理、告警/预警管理等服务；

6 功能要求

6.1 感知层

6.1.1 人员定位卡

人员定位卡应满足下列功能要求：

a) 支持 RTK+蓝牙 RSSI/UWB 等融合定位；
b) RTK 支持仅接收和处理 BDS 卫星信号；
c) 具备 TTS 语音播报功能；
d) 具备 SOS 报警功能；
e) 具备动静检测功能，可识别人员状态；
f) 宜具备 NFC 刷卡功能；
g) 至少支持磁吸式/TYPE-C/无线等充电方式；
h) 至少支持 4G/5G/WiFi/NB-IoT 等通信；

i） 支持本地或远程配置参数。

6.1.2 UWB 基站

UWB基站应满足下列功能要求：

a） 支持 TOF、TDOA、AOA 等算法的室内场景 UWB 定位；

b） 支持本地或远程配置参数。

6.1.3 蓝牙信标

蓝牙信标应满足下列功能要求：

a） 支持基于蓝牙 RSSI 的三角定位；

b） 采用稳定的免充电电池供电，免布线；

c） 支持本地或远程配置参数。

6.1.4 测量型接收机

测量型接收机应支持下列功能：

a） 信号接收处理：支持仅接收和处理 GB/T 39414（所有部分）规定的信号。

b） 通信：

——支持 4G/LoRa/Wi-Fi/NB-IoT 等多种无线通信方式之一；

——支持串口、网口、USB 等多种有线通信方式；

——支持 TCP、NTRIP、MQTT 通信协议；

——满足 RTCM 3.X、NMEA 0183 数据格式要求。

c） 支持远程配置及远程监控接收机状态，包含内置网络连接状态、内置电池剩余电量及外置电源电压等信息。

6.1.5 CORS 基准站

CORS基准站应支持下列功能：

a） 信号接收处理：支持仅接收和处理 GB/T 39414（所有部分）规定的信号。

b） 通信：

——支持 4G/LoRa/Wi-Fi/NB-IoT 等多种无线通信方式之一；

——支持串口、网口、USB 等多种有线通信方式；

——支持 TCP、NTRIP、MQTT 通信协议；

——满足 RTCM 3.X、NMEA 0183 数据格式要求。

c） 远程配置及远程监控基准站状态，包含内置网络连接状态、内置电池剩余电量及外置电源电压等信息。

6.2 传输层

传输层为系统提供有线和无线数据传输功能，其中：

a） 有线数据传输协议包含：以太网、USB、串口（RS232/RS485）等。

b） 无线数据传输协议包含：4G、5G、LoRa、Wi-Fi、蓝牙、NB-IoT 等。

6.3 数据层

6.3.1 业务数据库

用于存储化工园区业务相关数据，包含系统录入的园区台账数据（企业/车辆/人员/设备等）、作业管理基础数据（门禁/作业票/巡检工单等）及园区安全生产管理相关的其他业务基础数据。

6.3.2 实时数据库

用于存储对园区感知对象的实时监测数据，包含感知层采集上传的人员定位实时数据、形变监测实时数据，以及第三方业务系统联动的实时数据（如视频监控等）。

6.4 服务层

6.4.1 核心服务层

6.4.1.1 GIS 服务

GIS服务应支持下列功能：

a) 地图绘制：支持二维和三维地图的绘制；
a) 地图浏览：包含自定义显示地图的范围，进行放大、缩小、漫游等操作；
b) 图层控制：包含图层切换、图层叠置和图层显示控制；
c) 图层渲染：按单值、要素值和分级等维度显示专题图，专题图图层要素渲染符合石油化工领域信息空间要素表达的规范；
d) 查询检索：检索满足属性约束条件或空间约束条件的地理信息数据，包括空间查询、属性查询和组合查询。

6.4.1.2 用户管理

用户管理服务应支持下列功能：

a) 用户的增加、删除、查询和修改；
b) 根据权限修改并浏览指定账户的信息；
c) 提供密码、短信验证码、生物特征识别等多种登录方式。

6.4.1.3 可视化

可视化功能应满足下列要求：

a) 支持使用微型计算机、移动通信终端、显示大屏等设备进行可视化展示和交互操作；
b) 支持各类信息的分级、分类、分区展示；
c) 支持按历史趋势、历史断面、主题排序、阈值筛选、动态等方式显示信息；
d) 支持各类信息数据的画面联动；
e) 支持信息与风险位置数据的关联展示；
f) 支持数据按照表格、仪表盘、雷达图、柱状图、饼图、趋势图、三维模型等方式进行图元展示；
g) 支持报表等可视化结果的生成、导入和导出。

6.4.1.4 远程控制

应支持对系统中的物联网实体进行远程控制、系统配置和恢复。

6.4.1.5 定位服务

定位服务为定位数据接入、解算、播发提供服务，应支持下列功能：

a) 支持卫星定位（含 RTK）数据的实时接入、动态/静态解算、动态播发；
b) 支持蓝牙 RSSI 定位数据的实时接入、动态解算；
c) 支持 UWB 定位数据的实时接入、动态解算；
d) 支持基于不同类型定位数据的动态融合解算。

6.4.1.6 服务管理

服务管理应符合下列要求：

a) 支持构建服务目录，查询当前已部署的服务以及正在运行的服务状态等信息；
b) 当系统服务出现异常时，支持将异常情况报告给管理员；
c) 提供对服务定义、更新和访问策略的管理功能。

6.4.1.7 接口管理

接口管理为第三方系统提供数据接口配置调用相关服务，应支持下列数据的调用：

a) 基础数据：包含内部人员、承包商人员、访客人员、内部/外部车辆、获取监测设施等数据；
b) 展示用数据：包含区域内人数、区域内监测点数量、各类报警占比、当天未处理的报警数据、大屏在线统计、在线人员详情等数据；
c) 历史数据：包含人员历史轨迹、车辆历史轨迹、监测历史曲线、报警历史记录等数据。

6.4.2 安全层

6.4.2.1 认证和身份管理

认证/身份管理功能为用户系统提供数据接入认证、用户访问认证、网络安全认证等相关服务，应符合下列要求：

a) 支持 CA 认证；
b) 支持建立身份管理策略和管理机制；
c) 支持基于预定义身份管理测量配置角色功能；
d) 支持确认用户对特定资源的访问和使用权限。

6.4.2.2 授权和安全策略

授权和安全策略服务应符合下列要求：

a) 支持为用户访问特点功能或数据提供授权；
b) 支持自定义安全策略和应用。

6.4.2.3 加密管理

加密管理服务为数据存储和网络通信提供加密服务，应符合下列要求：

a) 支持加密秘钥管理和加密模式的选择；
b) 支持对敏感数据进行加密存储；
c) 使用加密传输确保通信安全。

6.4.2.4 隐私保护

隐私保护包含下列功能：

a) 支持对数据进行加密、脱敏、去标识化，其中个人信息的收集和管理应符合 GB/T 35273 的要求，使用部署在移动终端上的应用收集个人信息时，应符合 GB/T 41391 的要求；
b) 支持对数据传输双方身份进行隐私保护；
c) 支持用户进行隐私设置和自定义隐私内容。

6.4.2.5 审计

审计为相关方提供用户行为记录和审计能力，应支持下列功能：

a) 操作行为管理：支持查询用户登录、用户点击记录、远程控制等记录；
b) 审计策略管理：支持定义审计事件过滤规则，并根据规则对事件进行筛选；
c) 日志管理：支持记录软硬件故障、系统重要事件等详细信息。

6.5 应用层

6.5.1 区域管理

区域管理模块应包含下列功能：

a) 地图图层管理：支持二维地图分层绘制、管理和三维地图分层绘制、组合展示、管理等操作；
b) 统计区域管理：支持依据园区业务及人员定位相关逻辑的区域管理；
c) 电子围栏管理：支持通过电子围栏实现人员出入及聚集的告警；
d) 动态规则管理：支持基于不同的时间/地点/角色对特定区域制定动态管理规则。

6.5.2 实时监测

实时监测模块应包含下列功能：

a) 人员实时位置：支持展示基于地图展示人员的实时位置信息；
b) 移动轨迹追踪：支持基于地图追踪展示人员的实时和历史移动轨迹；
c) 人员聚集监控：支持基于配置好的管理规则对人员聚集情况进行监控告警；
d) 人员信息上报：支持人员自动或手动上报位置、紧急求救等信息；
e) 形变监测曲线：支持基于测量型接收机的实时监测数据绘制并展示形变量、形变速率、加速度等曲线；

f） 形变趋势分析：支持基于测量型接收机的历史数据统计分析监测点位的形变趋势，结合管理规则进行告警/预警；
g） 综合大屏：支持基于大屏对多种监测内容的一屏或分屏展示。

6.5.3 设备管理

设备管理为定位卡、测量型接收机、蓝牙信标、UWB基站、CORS基准站以及其他设备提供管理能力，应支持下列功能：

a） 设备注册：
   1） 设备的单独和批量注册，并为设备分配唯一标识；
   2） 设备名称、用户、厂商、位置、型号、通信协议等属性信息录入；
   3） 设备参数配置，保障平台能实时同步设备信息。
b） 设备注销：设备单独或批量注销，注销后支持自定义保留设备历史信息的时效。
c） 设备变更：设备属性信息和设备配置参数的变更。
d） 信息查询：设备属性信息、设备运行信息、指定设备的采集信息、空间位置属性的查询，其中设备运行信息包含配置参数、历史命令、在线记录、运行状态等。
e） 支持设备群组管理。

6.5.4 告警/预警管理

告警/预警管理应包含下列功能：

a） 规则管理：支持对人员定位和形变监测的告警/预警逻辑及阈值配置进行管理；
b） 通知管理：支持对人员定位和形变监测的告警/预警形式（例如，短信/邮件等方式）进行配置管理。支持向部分或全部人员广播通知信息；
c） 记录日志：支持将人员定位和形变监测的告警/预警历史以日志形式进行归类、记录和留档；
d） 业务联动管理：支持基于第三方业务系统（如工作票/视频监控等）接入的数据自定义告警/预警管理规则。

7 性能要求

7.1 硬件性能

7.1.1 人员定位卡

人员定位卡符合下列性能要求：

a） 室外场景定位精度应不低于亚米级；
b） 室内场景定位精度应≤5m；
c） BDS 频点应至少支持 B1I；
d） UWB 频段应支持 7163MHz～8812MHz 或 3.1GHz～10.6GHz；
e） 蓝牙频段采用 2.4GHz，并符合国际通用标准；
f） NFC 功能宜支持 13.56MHz 或 900MHz；
g） 外壳防护等级应不低于 GB/T 4208—2017 中规定的 IP65；
h） 续航能力应支持设备按 5s/次的上报频率连续工作 18h 以上；
i） 防爆等级应不低于 Ex ib IIC T4 Gb。

7.1.2 UWB 基站

UWB基站应符合下列性能要求：

a） UWB 频段：支持 7163MHz～8812MHz 或 3.1GHz～10.6GHz；
b） 定位精度：不低于亚米级；
c） 续航能力：免布线型的续航时间不低于 3y；
d） 外壳防护等级：不低于 GB/T 4208—2017 中规定的 IP67；
e） 防爆等级：不低于 Ex ib IIB T4 Gb 或 Ex db IIC T4 Gb。

7.1.3 蓝牙信标

蓝牙信标应符合下列性能要求：

a) 蓝牙频段：2.4GHz，符合国际通用标准；
b) 定位精度：≤5m；
c) 外壳防护等级：不低于 IP67；
d) 续航能力：电池续航时间不低于 5y；
e) 防爆等级：不低于 Ex ib IIC T4 Gb。

7.1.4 测量型接收机

测量型接收机应符合下列性能要求：

a) 静态测量精度：
——水平精度不低于±(2.5mm+0.5ppm) RMS；
——高程精度不低于±(5.0mm+0.5ppm) RMS。
b) 动态测量精度：
——水平精度不低于±(8mm+1ppm) RMS；
——高程精度不低于±(15mm+1ppm) RMS。
c) 防水防尘等级不低于 IP68。
d) 工作温度在-40℃～+85℃之间。
e) 主机平均功耗≤1.3W。
f) 内置锂电池容量不低于 7500mAh，在断电情况下能至少运行 48h。
g) 防爆等级不低于 Ex ib IIC T4 Gb。
h) MTBF 不小于 50000h。

7.1.5 CORS 基准站

CORS基准站应符合下列性能要求：

a) 静态测量精度：
——水平精度不低于±(2.5mm+0.5ppm) RMS；
——高程精度不低于±(5.0mm+0.5ppm) RMS。
b) 动态测量精度：
——水平精度不低于±(8mm+1ppm) RMS；
——高程精度不低于±(15mm+1ppm) RMS。
c) 防水防尘等级不低于 IP68。
d) 在-40℃～+85℃的温度区间内能正常工作。
e) 主机平均功耗≤2.5W。
f) 内置锂电池容量不低于 15000mAh，在断电情况下能至少运行 48h。
g) MTBF 不小于 60000h。

7.2 系统/软件性能

7.2.1 响应时间

系统页面加载时间应不大于 3s，用户请求的响应时间应不大于 2s。

7.2.2 事务处理

系统能够每秒处理 500 个用户请求，数据库每秒可处理 3000 条记录的插入、更新和查询操作。

7.2.3 并发用户数

系统至少支持 1000 个用户同时访问本系统。

7.2.4 稳定性

系统能在高负载和长时间运行后依然保持稳定，且不出现内存泄漏、性能下降等问题。

7.2.5 网络带宽

系统的网络带宽需支持每秒 100Mbps 的数据传输速率。

8 安全性要求

8.1 身份鉴别安全

系统对身份鉴别的设计和实现符合下列要求：

a) 应建立并使用标准的、已通过测试的身份鉴别策略；
b) 应根据业务安全要求选择身份鉴别方式，宜采用多因素身份鉴别方式；
c) 应支持使用包含调用第三方身份鉴别服务的方法实现身份鉴别的集中实现；
d) 鉴别过程应在 TEE 中执行，且仅在每次用户登录时进行身份鉴别；
e) 应遵循最小化授权原则；
f) 在进行关键的安全操作时，宜采用多种方式进行身份鉴别；
g) 应验证 CA 证书，检查证书的状态和证书持有者的有效性和一致性；
h) 应避免鉴别过程被绕过，且在处理身份鉴别的过程中透露无用信息；
i) 应对鉴别尝试的频率进行限制，在连续多次登录失败时可强制锁定账户；
j) 如在一次身份鉴别后，进行较长时间的通话，应周期性重新鉴别用户的身份，以确保其权限没有改变，如身份发生改变，则注销该用户，并强制重新执行身份鉴别；
k) 应在用户执行关键或不可逆操作（如修改口令）前，再次鉴别用户身份；
l) 应避免使用过于严格的账户锁定机制；
m) 应实现用户与主体的绑定。

8.2 口令安全

口令安全性要求如下：

a) 口令在登录过程中应不可见；
b) 宜使用强口令，口令的复杂度满足安全策略的要求，不应使用弱口令、空口令或已泄露的口令；
c) 用户初次登录时应更改默认初始口令。
d) 口令信息应进行加密存储等保护措施，加密过程应在 TEE 中执行，口令、加密密钥的保存时间符合安全策略的要求；
e) 应使用安全的口令传输；
f) 用户信息改变时应使用单独的信道通知。

8.3 权限管理安全

系统对于权限管理的设计和实现应符合下列要求：

a) 遵循最小授权原则；
b) 访问授权操作在 TEE 中执行；
c) 检测人机交互访问控制状态；
d) 访问控制策略包含检查用户访问或操作的数据；
e) 加密数据或敏感数据仅对已授权用户开放访问权限；
f) 账户审计并强制失效长期不使用的账户，建议明确允许账户不使用的最长期限，支持账户的强制失效，并在账户停止时终止会话。

8.4 日志安全

日志记录的设计和实现应从下列方面提升安全性：

a) 通过安全存储、完整性验证等方式保护日志文件；
b) 在 TEE 中执行日志记录操作；
c) 日志条目中增加由可信第三方机构签发的时间戳；
d) 关键行为记录日志；
e) 对日志记录进行完善的异常捕获处理，确保功能可靠性；

f） 对日志中的特殊元素进行过滤和验证；
g） 采取安全措施防止攻击者访问日志；
h） 避免在日志中保存敏感数据。

8.5 数据安全

8.5.1 数据加密

系统应对敏感数据进行加密，数据加密的设计和实现符合下列要求：
a） 密码服务应经国家密码管理部门认证核准后使用；
b） 应加密存储本地敏感数据；
c） 应在 TEE 中执行数据的加密过程；
d） 应确保密码运算过程安全，基于指定的算法和特定长度的密钥来进行密码运算；
e） 在加密失败或报错时，应重新加密；
f） 应最少化加密信息的存储；
g） 应执行安全策略和流程实现加、解密的密钥管理；
h） 应支持可信的随机数生成器；
i） 应通过规定密钥强度、有效期、编码方式等方式提升秘钥安全性。

8.5.2 数据保护

数据保护符合下列要求：
a） 应定义应用中的敏感和隐私数据的范围，以及有权访问这些数据的用户范围；
b） 敏感数据应进行加密存储和传输；
c） 对敏感数据进行完整性检查；
d） 在不影响系统功能、性能、安全性的情况下，最小化敏感数据存储时间和备份数量；
e） 不应在错误消息、进程信息、调试信息、日志文件、源代码或注释中出现敏感数据；
f） 在设计 WEB 登录表单的时，可考虑禁止浏览器的口令自动填充功能；
g） 应在资源释放前清理敏感数据；
h） 在判断无用后，应及时清除在服务器上缓存的或临时拷贝的敏感数据；
i） 不应在用户端保存敏感数据；
j） 当敏感数据丢失或破坏时，可通过备份数据进行数据恢复。

8.5.3 网络安全

网络安全应符合下列要求：
a） 验证通信通道源；
b） 对来自网络的数据进行验证；
c） 对信道中传输的消息进行完整性验证；
d） 使用时间戳和随机数组合的方式进行重放检测；
e） 对会话安全进行管理，例如会话标识符的创建/识别等；
f） 避免将多个套接字绑定到相同端口；
g） 支持建立跟踪网络传输流量机制，控制网络传输流量不超过被允许的值。

参 考 文 献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 38674-2020 信息安全技术 应用软件安全编程指南