ICS 71.020
CCS G 00

T/GLAC

中 国 卫 星 导 航 定 位 协 会 团 体 标 准

T/CLAC 26—2025

北斗安全生产应用 化工园区安全管理系统技术要求

BDS safety production application——Technical requirements of safety management system for chemical industry park

2025－06－25 发布　　2025－06－25 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。

本文件由中国卫星导航定位协会提出并归口。

本文件起草单位：上海华谊信息技术有限公司、武汉梦芯科技有限公司、新锐科创(湖北)科技有限公司、南京北路智控科技股份有限公司、苏州真趣信息科技有限公司、南光石油化工有限公司、中石化石油工程地球物理有限公司北斗运营服务中心、罗维智联(北京)科技有限公司、中国石油北斗运营服务中心、浙江中星卫星通信有限公司、北京市中位协北斗时空技术研究院、蓝鲸高领（北京）标准化技术服务有限公司。

本文件主要起草人：王玉杰、马骏、苗国睿、祝青、吴磊、赵明、王庆、贺玮、牛炳乾、曹鹏志、田鑫、孙京侨、段永辉。

北斗安全生产应用 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构成、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（以下简称“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 3836.1 爆炸性环境 第1部分：设备 通用要求

GB/T 3836.2 爆炸性环境 第2部分：由隔爆外壳“d”保护的设备

GB/T 3836.4 爆炸性环境 第4部分：由本质安全型“i”保护的设备

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

GM/T 0054 信息系统密码应用基本要求

JT/T 794—2019 道路运输车辆卫星定位系统车载终端技术要求

T/GLAC 21—2025 道路运输车辆北斗卫星导航系统定位模块技术要求及测试方法

3 术语和定义

GB/T 39267界定的以及下列术语和定义适用于本文件。

3.1

北斗基准站 BDS reference station

在位置坐标已知点上架设高精度BDS观测设备、通信终端等设备，并在一定时间内连续观测、记录卫星信号，将数据传输给数据中心或经处理后直接播发差分改正数据的设施。

[来源：GB/T 39267—2020,2.1.25，有修改]

3.2

北斗人员定位卡 BDS personnel location card

一种基于BDS、RFID（射频识别）、UWB、蓝牙等技术的定位设备，具备感知并传输佩戴者实时定位、身份等信息的能力。

3.3

北斗形变监测站 BDS deformation monitoring station

基于BDS高精度定位技术，对地表、工程结构物的位移、沉降、倾斜等形变进行实时、连续、自动化监测的设施。

3.4

工程结构物 engineering structure

由工程材料建造而成，能承受和传递荷载，为化工园区内安全生产提供空间或平台，满足园区内生产安全性、适用性和耐久性要求的承重骨架或实体。

注：化工园区内常见的工程结构物包含储罐、管廊、楼宇等。

3.5

化工园区 chemical industry park

由多个相关联的化工企业构成，以发展石化和化工产业为导向、地理边界和管理主体明确、基础设施和管理体系完整的工业区域。

注：化工园区一般包括两种类型，包含有关部门批准设立或认定的专业化工园区、有关部门批准设立或认定的经济（技术）开发区、高新技术产业开发区或其他工业园区中相对独立设置的化工园（区）。

[来源：GB/T 39218—2020,3.1,有修改]

3.6

蓝牙信标 bluetooth beacon

一种内置在室分天线内或独立架设在室内，保证蓝牙信号覆盖，能满足蓝牙短距离通信协议的模组设备。

[来源：YD/T 4086—2022,3.1.3,有修改]

3.7

敏感数据 sensitive data

一旦泄露、篡改或滥用可能危害个人权益、企业安全或公共利益的信息。

注：敏感数据通常包含个人信息、业务和系统数据，其中个人信息定义见GB/T 35273，业务数据指与园区安全生产行为和应急管理相关的数据，例如危险化学品储量、重大危险源参数、应急方案等，系统数据指与系统安全、审计相关的数据，例如加密密钥、权限令牌、未脱敏的用户操作记录等。

3.8

信道 channel

在两点之间按规定特性传输信号的途径。

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）

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

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）

NMEA:美国国家海洋电子协会（National Marine Electronics Association）

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

POI:兴趣点（Point of Interest）

RMS:均方根（Root Mean Square）

RS232:推荐标准232（Recommended Standard 232）

RS485:推荐标准485（Recommended Standard 485）

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

RTCM:海事无线电技术委员会（Radio Technical Commission for Maritime Services）

RTK:实时动态定位（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 总体要求

5.1 一般要求

系统的感知和管理对象应包含人员、车辆、生产设备、工程结构物等实体，其中人员包含作业人员、管理人员和临时出入人员，车辆包含危险化学品运输车、工程作业车和临时车辆等。

系统应采用开放的软件平台框架，其兼容性、可靠性、可维护性和安全性能满足化工园区安全生产管理的需求。

5.2 系统架构

系统基于BDS高精度定位、蓝牙、UWB等技术，通过对园区内人员、车辆、化工生产设备的实时位置，以及工程结构物的形变情况进行实时监测，实现化工园区安全生产合规管理。系统架构分为感知层、传输层、数据层、服务层、应用层，见图1。

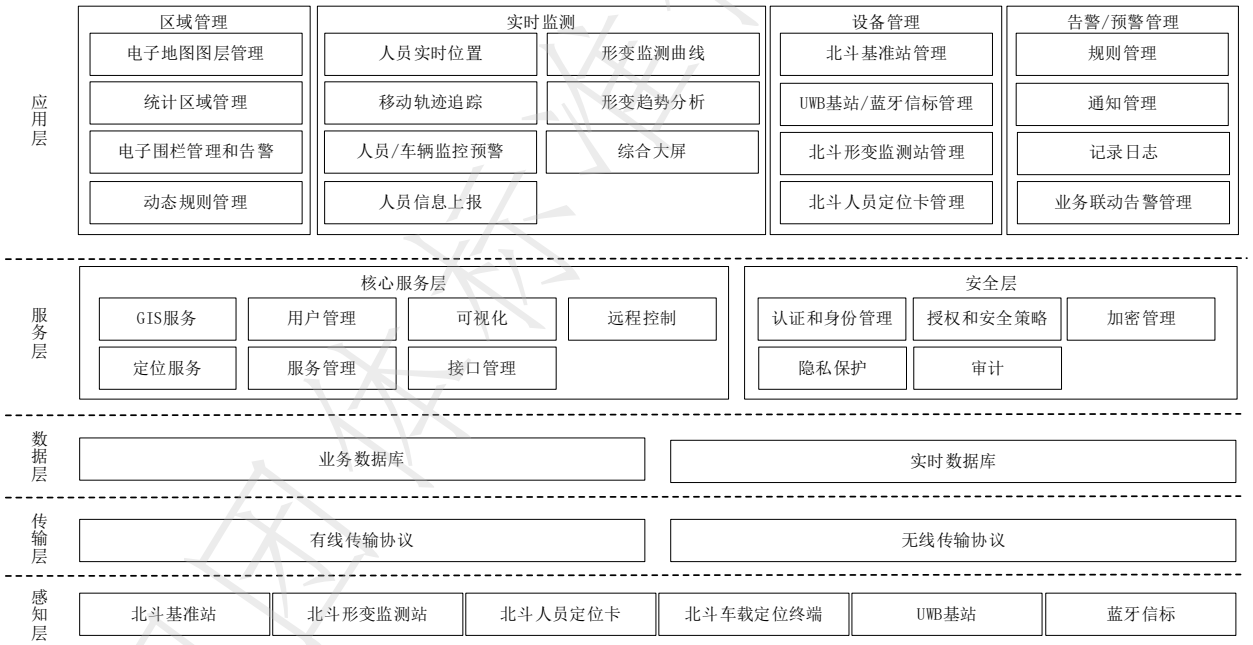

图1 基于北斗的化工园区安全管理系统架构

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、解析并传输化工园区人员、车辆、生产设备的定位数据，以及工程结构物的形变数据，包含北斗基准站、北斗形变监测站、北斗人员定位卡、北斗车载定位终端、UWB 基站和蓝牙信标；
b) 传输层：负责通过有线或无线数据传输协议将感知层获得的数据传输至数据层；
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：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、实时监测预警、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 北斗基准站

北斗基准站使系统能对化工园区内的人员、车辆、工程结构物进行精准定位，应支持下列功能：

a) 信号接收处理：仅支持接收和处理 GB/T 39414（所有部分）规定的信号。
b) 通信：
——支持 4G/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；
——支持符合 RTCM 3.0 及以上版本和 NMEA 0183 的数据格式。
c) 能远程配置和远程监控北斗基准站状态，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。

6.1.2 北斗形变监测站

北斗形变监测站通过对化工园区内工程结构物进行实时高精度定位监测，及时发现潜在的不均匀沉降、结构失稳变形等安全隐患，应支持下列功能：

a) 信号接收处理：仅支持接收和处理 GB/T 39414（所有部分）规定的信号。
b) 通信：
——支持 4G/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；
——支持符合 RTCM 3.0 及以上版本和 NMEA 0183 的数据格式。
c) 能远程配置及远程监控北斗形变监测站状态，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。

6.1.3 北斗人员定位卡

北斗人员定位卡通过BDS、UWB、蓝牙等定位技术实现室内外人员实时定位，并能结合系统实现人员状态监控、电子围栏报警、历史轨迹追溯等，应支持下列功能：

a) 应支持 RTK 与蓝牙 RSSI/UWB 等融合定位；
b) 应仅支持接收和处理 BDS 卫星信号；
c) 应具备 TTS 语音播报功能；
d) 应具备 SOS 报警功能；
e) 应具备人员动态、静态状态检测功能；
f) 宜具备 NFC 功能；
g) 应支持有线充电或无线充电；
h) 应至少支持 4G/5G/Wi-Fi/NB-IoT 等通信协议中的一种；
i) 应支持本地或远程配置参数。

6.1.4 北斗车载定位终端

北斗车载定位终端安装在危险化学品运输车、工程作业车和临时车辆上，为系统提供获取车辆实时定位信息的能力，应支持下列功能：

a) 支持北斗独立定位；
b) 支持接收 BDS 播发的信号实现定位、测速和授时功能；
c) 支持 T/GLAC 21—2025 中 6.5 规定的组合定位功能；
d) 安装在危险化学品运输车上的终端支持防水、防尘和防爆功能。

6.1.5 UWB 基站

UWB基站部署于化工园区内BDS信号无法满足定位精度要求或存在严重信号遮挡的区域，应支持下列功能：

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。

6.1.6 蓝牙信标

蓝牙信标部署于化工园区内BDS信号无法有效覆盖或存在严重遮挡的区域，应支持下列功能：

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。

6.2 传输层

传输层为系统提供有线和无线数据传输功能，应支持下列数据传输协议：

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、Wi-Fi、蓝牙、NB-IoT 等。

6.3 数据层

6.3.1 业务数据库

用于存储化工园区安全管理相关业务数据，包含但不限于系统录入的企业、人员、固定资产等台账数据，门禁、作业票、巡检工单等作业管理数据等。业务数据库应支持根据管理对象自动关联下列数据：

a） 人员：特殊工种和资质、安全培训记录、历史违规记录等数据；
b） 车辆：种类、载运介质、车载人员信息、行驶路线许可等数据；
c） 风险区域监管：双重预防机制、特殊作业票、气体泄漏监测、应急预案、安全教育考试等数据；
d） 重大危险源管理：位置、工艺参数、安全状态/校验周期等数据；
e） 危险化学品管理：类别、特性、储量监管、运输管控、危险废物处置等数据。

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、形变监测数据，以及气体检测、视频监控等第三方业务系统联动的实时数据。

6.4 服务层

6.4.1 核心服务层

6.4.1.1 GIS 服务

GIS服务应符合下列要求：

a） 地图绘制：支持二维和三维地图的分层绘制；
b） 地图浏览：支持自定义显示地图的范围，并对地图进行放大、缩小、漫游等操作；
c） 图层控制：支持图层切换、图层叠置和图层显示控制；
d） 图层渲染：支持按单值分类、要素属性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；
e） 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

用户管理应符合下列要求：

a） 支持用户的增加、删除、查询和修改；
b） 支持根据化工园区实际的安全管理层级和职责分工，为企业、部门、人员等用户配置系统访问权限和数据查看范围；
c） 支持密码、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

可视化应符合下列要求：

a） 支持使用计算机、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（剖）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等 POI 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

远程控制应支持对系统中的感知设备进行远程控制、系统配置和恢复。

6.4.1.5 定位服务

定位服务应符合下列要求：
a） 支持 BDS 定位数据（含 RTK）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

接口管理应支持第三方系统调用下列数据：
a） 基础数据：包含内部作业人员、承包商人员、访客人员、内部/外部车辆、感知设备、作业许可等数据；
b） 展示用数据：包含区域内人数、区域内监测点数量、各类报警数量占比、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

认证和身份管理应符合下列要求：
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配置和管理角色功能；
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

授权和安全策略应符合下列要求：
a） 支持为用户访问特定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

加密管理应符合下列要求：
a） 支持加密密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

隐私保护应符合下列要求：

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，当系统应用部署在移动通信终端上时，个人信息的收集应符合 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

审计应符合下列要求：

注：审计指由第三方机构对系统进行评估，以确保系统能保障各类数据的安全性、完整性、可用性和合规性，并为系统持续改进提供依据。

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

区域管理应符合下列要求：

a) 电子地图图层管理：
   1) 图层显示：支持化工园区内人员、车辆的实时位置和工艺管线、重大危险源分布、应急疏散通道、消防设施、有毒有害气体扩散模拟范围等图层叠加显示，以及支持与来自第三方系统的图层数据叠加显示；
   2) 支持图层的添加、删除、修改和查询。
b) 分区管理和统计：支持基于园区功能分区和临时分区内的定位数据对区域内的人员、设备、车辆、工程结构物进行统计和管理。

注：常见的功能分区包含工艺装置区、仓储物流区、公用工程区、辅助生产区、安全与环保区、管理服务区等。

c) 电子围栏管理和告警：
   1) 支持自定义电子围栏，并对电子围栏进行添加、删除、修改和查询等操作，电子围栏属性包含范围、生效/有效时间、限定进入人数等；
   2) 支持设置基于电子围栏的自定义告警规则，实现人员出入和聚集的告警。
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

实时监测应符合下列要求：

a) 人员实时位置：
   1) 支持基于电子地图显示人员的实时位置及分布情况；
   2) 支持按照人员类型和区域分类，并在地图上以不同的颜色标识。
b) 移动轨迹追踪：支持基于电子地图显示人员的实时和历史移动轨迹。
c) 人员/车辆监控预警：支持基于预定义管理规则的对人员越界、超员/聚集、缺员、滞留、禁行以及车辆超速等情况进行监控与告警/预警，对园区易燃易爆场所以及实施动火/受限空间作业等特殊作业的区域应实施在线人数自动统计和滞留、离岗/串岗等违规行为告警。
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：支持基于储罐、管廊、楼宇等大型基础设施的形变监测实时数据绘制并展示形变量、形变速率、加速度等曲线。
f) 形变分析预警：
   1) 支持基于形变监测的历史数据统计、分析监测点位的形变趋势、管理规则进行告警/预警；
   2) 支持基于自定义形变阈值设置和报警，当形变值超过阈值时，系统自动进行告警/预警。
g) 综合大屏显示：支持基于显示大屏对多种监测内容进行一屏或分屏展示。

6.5.3 设备管理

设备管理应符合下列要求：

a) 设备注册：
   1) 支持单独和批量注册，并为设备分配唯一标识；
   2) 支持名称、用户、厂商、位置、型号、通信协议等属性信息录入；
   3) 支持实时更新相关设备信息，包含但不限于北斗基准站服务账号、UWB 基站实时信号强度、蓝牙信标实时信号强度、定位优先级、北斗形变监测站数据格式及定位频率、北斗人员定位卡绑定人员信息及定位频率等。

注：定位优先级指根据系统设置、实时信号强弱判断采用某中定位方式或定位方式的顺序。

b) 设备注销：支持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：支持设备属性信息和设备配置参数的变更。
d) 设备信息查询：支持设备属性信息、设备运行信息和设备采集信息的查询，其中设备采集信息包含配置参数、历史命令、在线记录、安装位置及运行状态等。
e) 支持设备群组管理。

6.5.4 告警/预警管理

告警/预警管理应符合下列要求：

a) 规则管理：支持对人员越界、超员/聚集、缺员、滞留、禁行，车辆超速和形变监测的告警/预警类型、规则策略及阈值配置进行管理；
b) 通知管理：支持对自定义人员群组和车辆组群以短信、邮件、大屏显示、广播等方式推送告警/预警信息，通知包含事件的类型、时间、地点、对象等信息，支持通知配置管理；
c) 记录日志：支持将人员越界、超员/聚集、缺员、滞留、禁行，车辆超速和形变监测的告警/预警历史以日志形式归类、记录和留档；
d) 业务联动告警管理：支持依据重大危险源安全管理、双重预防机制、特殊作业管理、封闭管理、敏捷应急等第三方业务系统接入的数据自定义告警/预警管理规则。

注：敏捷应急指一种利用快速响应、迭代改进、跨职能协作、持续学习等敏捷思维和方法应对突发事件和危机的管理模式。

7 性能要求

7.1 硬件性能

7.1.1 北斗基准站

北斗基准站应符合下列性能要求：

a) 静态测量精度（RMS）：
——水平定位精度：优于±(2.5 mm+0.5×10^{-6}×D)；
——高程定位精度：优于±(5.0 mm+0.5×10^{-6}×D)。
b) 动态测量精度（RMS）：
——水平定位精度：优于±(8 mm +1×10^{-6}×D)；
——高程定位精度：优于±(15 mm+1×10^{-6}×D)。

注：D为基线长度，单位为毫米（mm）。

c) 防水防尘等级：不低于 GB/T 4208—2017 中规定的 IP68。
d) 工作温度：-40 ℃～85 ℃。
e) 电源：内置锂电池容量≤15000 mAh，断电情况下的运行时间不少于 48 h。
f) MTBF：≥60000 h。

7.1.2 北斗形变监测站

北斗形变监测站应符合下列性能要求：

a) 静态测量精度（RMS）：
——水平定位精度：优于±(2.5 mm+0.5×10^{-6}×D)；
——高程定位精度：优于±(5.0 mm+0.5×10^{-6}×D)。
b) 动态测量精度（RMS）：

——水平定位精度优于±(8 mm+1×10^{-6}×D)；
——高程定位精度优于±(15 mm+1×10^{-6}×D)。
注：D为基线长度，单位为毫米（mm）。

c) 防水防尘等级：不低于 GB/T 4208—2017 规定的 IP68。
d) 工作温度：-40 ℃～85 ℃。
e) 接收机：主机平均功耗≤1.3 W。
f) 电源：锂电池电池容量≥7500 mAh，断电情况下的运行时间不少于 48 h。
g) 防爆等级：不低于 GB/T 3836.1、GB/T 3836.2、GB/T 3836.4 规定的 Ex ib IIC T4 Gb 的要求。
h) MTBF≥50000 h。

7.1.3 北斗人员定位卡

北斗人员定位卡应符合下列性能要求：
a) 室外定位精度：单点定位精度应≤5 m，RTK 定位精度应≤1 m；
b) 室内定位精度：UWB 定位精度应≤1 m，蓝牙定位精度应≤5 m；
c) BDS 频点：应至少支持 B1I；
d) UWB 频段：应支持 7163 MHz～8812 MHz；
e) 蓝牙：宜支持 4.0 或更高版本协议；
f) NFC 工作频率：宜支持 13.56 MHz；
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 5 s 每次的上报频率连续工作 18 h 以上；
i) 防爆等级：应不低于 GB/T 3836.1、GB/T 3836.2、GB/T 3836.4 规定的 Ex ib IIC T4 Gb 的要求。

7.1.4 北斗车载定位终端

北斗车载定位终端应符合下列性能要求：
a) 防爆性能不低于 GB/T 3836.1、GB/T 3836.2、GB/T 3836.4 规定的 Ex ib IIC T4 Gb 的要求；
b) 机壳防水防尘性能应符合 JT/T 794—2019 中 4.6 的要求；
c) 定位精度、测速精度、授时精度、灵敏度、组合定位、功耗符合 T/GLAC 21—2025 中第 7 章的要求。

7.1.5 UWB 基站

UWB基站应符合下列性能要求：
a) UWB 频段：支持 7163 MHz～8812 MHz；
b) 定位精度：≤1 m；
c) 续航能力：免布线型的基站续航时间不低于 3 a；
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 GB/T 3836.1、GB/T 3836.2、GB/T 3836.4 规定的 Ex ib IIB T4 Gb 或 Ex db IIC T4 Gb 的要求。

7.1.6 蓝牙信标

化工园区用蓝牙信标应符合下列性能要求：
a) 定位精度：≤5 m；
b) 外壳防护等级：不低于 GB/T 4208—2017 中规定的 IP67；
c) 续航能力：电池续航时间不低于 5 a；
d) 防爆等级：不低于 GB/T 3836.1、GB/T 3836.2、GB/T 3836.4 规定的 Ex ib IIC T4 Gb 的要求。

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 3 s，回复用户请求的响应时间应不大于 2 s。

7.2.2 事务处理

系统应每秒处理至少 500 个用户请求，数据库每秒处理至少 3000 条记录的插入、更新和查询操作。

7.2.3 并发用户数

系统应至少支持 1000 个用户同时访问。

7.2.4 稳定性

系统应具备在 1s 内处理不少于 500 个用户请求或不少于 800 个用户并发访问后，无内存泄漏和性能下降的能力，且 MTBF≥5000 h。

7.2.5 网络带宽

系统的网络带宽应支持每秒 100 Mbps 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) 如用户在一次身份鉴别后保持在线状态超过 15 min（无操作或持续会话），应周期性重新鉴别用户身份，确保权限未变更；若身份状态异常（如权限降级、账户冻结），系统应自动注销该用户并强制重新认证；
k) 应在用户执行关键或修改口令等不可逆操作前，再次鉴别用户身份；
l) 应实现用户与人员实体、设备实体及场景实体的绑定。

8.2 口令安全

口令安全要求如下：

a) 口令在登录过程中应不可见；
b) 口令具备一定的复杂程度，满足系统安全策略的要求；
c) 用户初次登录时应更改默认初始口令；
d) 口令信息应采用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独立通信信道通知，避免与业务数据混传。

8.3 权限管理安全

系统对于权限管理的设计和实现符合下列要求：

a) 应遵循最小授权原则；
b) 访问授权操作应在 TEE 中执行；
c) 应检测人机交互过程中的访问控制状态；
d) 访问控制策略应包含检查用户访问或操作的数据；

e） 加密数据或敏感数据应仅对已授权用户开放访问权限；
f） 宜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符合下列要求：
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） 记录关键行为日志；
e） 对日志记录过程中的异常（如磁盘满、服务中断）进行捕获并处理，确保日志服务持续可用，异常恢复后自动补传未记录数据；
f） 对日志输入内容中的恶意字符、敏感数据进行过滤，验证时间戳、IP 地址等字段的格式合法性，防止日志被注入与伪造；
g） 采取安全措施防止攻击者访问日志；
h） 不在日志中保存敏感数据。

8.5 数据安全

8.5.1 数据加密

数据加密的设计和实现符合下列要求：
a） 密码服务应采用经国家密码管理部门认证核准的产品或方案，使用国密算法的应用符合 GM/T 0054 的要求；
b） 应加密存储本地及云端敏感数据；
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进行密码运算；
e） 在加密失败或报错时，应重新加密；
f） 应最小化敏感数据加密存储的时间和数量；
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、编码等措施提升密钥安全性。

8.5.2 数据保护

数据保护符合下列要求：
a） 应定义敏感数据的范围，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） 应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，应最小化敏感数据存储时长和备份数量；
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） 在设计网页登录表单时，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） 验证通信源和通道源；
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） 采用时间戳与随机数组合的方式实施重放检测，防止旧报文重放攻击，确保数据传输的时序性与唯一性；

注1：重放检测指通过验证数据时间戳、随机数、序列号等信息，识别并拦截重复历史数据的安全机制。

注2：重放攻击指攻击者通过截获并重复发送历史通信数据（如身份认证报文、控制指令），试图欺骗系统执行非法操作的攻击方式。

e） 对会话标识符的创建/识别等进行安全管理；

f） 禁止将多个服务的套接字绑定到同一端口，单端口仅允许绑定唯一服务，避免端口冲突导致的服务劫持风险；

g） 建立跟踪网络传输流量机制，支持自定义流量阈值，并控制网络传输流量不超过自定义阈值。

参 考 文 献

[1] GB/T 39218—2020 智慧化工园区建设指南
[2] YD/T 4086—2022 适用于移动室内分布系统的蓝牙定位技术要求