Q/JD

奇点新源国际技术开发（北京）有限公司 企业标准

Q/JD-01A-03-2018

SmartWall-智慧墙入侵探测系统

SmartWall-Intrusion Detection System

2018-03 修订　　2018-03 实施

奇点新源国际技术开发（北京）有限公司　　发 布

文件修订记录

文件名称		SmartWall-智慧墙入侵探测系统		文件编号	Q/JD-01A-112018	
序号	修订单号	修订内容	修订人	修订日期	修订状态	备注
1	/	/	原桂龙	2016.11	B/0	初版
2	201803	1）修订目录编码问题。 2）修订 7 检验规则内容。	杨超	2018.03	B/1	第一次修订
分发范围	最高管理层 01□　营销中心 02□　产品研发中心 03□　应用研发中心 04□ 生产运营中心 05□　售后运营中心 07□　综合部 06□　财务中心 08□ 质量部 09□　管廊事业部 10□　质检部 11□					

目次

企业标准信息公共服务平台
公开 2020年09月18日 12点03分

前　　言

为了保证产品的质量，本公司特参照有关入侵报警系统的国家标准及行业标准，制定出本企业标准，作为组织生产和检验产品的依据，其中的各项技术要求将随企业的技术进步及产品的改进而修订。

本标准由奇点新源国际技术开发（北京）有限公司负责起草。

本标准由奇点新源国际技术开发（北京）有限公司负责解释。

本标准首次发布时间：2016-11-10。

本标准第一次修订时间：2018-03-10。

企业标准信息公共服务平台
公开　2020年09月18日 12点03分

SmartWall-智慧墙入侵探测系统

1 范围

本标准规定了 SmartWall-智慧墙入侵探测系统的构成、技术要求、试验方法、检验规则、包装等，其是检验和验收本系统的基本依据。

2 规范性引用文件

下列文件对本文件的应用是必不可少的，凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本（包括所有的修改）适用于本文件。

IEC 62642-1: 2010	Alarm systems - Intrusion and hold-up systems - Part 1: System（报警系统-入侵和拦截系统-第一部分：系统要求）
GB16796-2009	安全防范报警设备安全要求和试验方法（5.4.3/5.4.4/5.4.5/5.4.6/5.4.8）
GB/T 191-2008	包装储运图是标志
GB 6388-1986	运输包装收发货标志

3 术语和定义

3.1 探测节点

具备射频信号收发能力，对目标的入侵、靠近防区或用户的主动操作等做出相应的响应的装置。

3.2 智能探测线缆

系统底层的核心物理构件，嵌入探测节点、信号传输线、供电线的线缆，它能够按照不同的组网策略执行微波的收发工作，实现无线传感探测。

3.3 智慧墙

系统底层的核心逻辑构件，由两条物理上平行部署的智能探测线缆组成，系统启动后其自然形成一道密不透风的“自适应微波阵列”墙，实现无线传感功能。

3.4 智慧墙分站（CC）

系统上层构件（指智慧墙管理平台和 NC）与底层构件（指智慧墙和智能探测线缆）的连接枢纽，

能够实现 IP 网络与智能探测线缆之间的物理连接以及协议转换。

- 实现光纤接入 IP 网络，并且通过 IP 网络与系统上层构件通信；
- 本身直接接入智能探测线缆，并且向智能探测线缆供电；
- 负责下属的智能探测线缆发现、自检和状态监控；
- 负责下发微波组网方案和升级任务；
- 负责上传从智能探测线缆采集到的传感信号；
- 具备接地接口，实现对智能探测线缆首端的感应雷防护；
- 1 个 CC 智能归属于 1 个 NC，1 个 CC 最多能够接入 4 根智能探测线缆，分别组成 2 道智慧墙。

3.5 入侵行为智能识别软件（NC）

智能分析和定位人员入侵并过滤干扰的软件，部署在 Linux 操作系统中，管理人员需要通过智慧墙管理平台才能对其进行配置和管理：

- 通过 IP 网络与系统其它构件通信；
- 负责下发智慧墙的部署设计、微波阵列的组网方案、CC 和智能探测线缆的升级任务；
- 负责分析微波信号变化规律、产生人员入侵事件、定位人员入侵位置；
- 负责监控下属的智慧墙分站 CC 的运行状态；
- 1 个入侵行为智能识别软件只能归属于 1 个智慧墙管理平台，1 个入侵行为智能识别软件能够管理多个智慧墙分站 CC。

3.6 智慧墙管理平台（MP）

系统顶层中心构件，采用 B/S 架构，部署在 Linux 操作系统中。管理人员通过 Chrome Web 浏览器，就能够在 IP 可达的任何客户端监控周界运行：

- 通过 IP 网络与系统其它构件通信；
- 负责记录、存储和下发系统的各项配置，包括记录智慧墙的部署设计、配置透地微波阵列的组网方案、监控区域/防区组/防区的划分、CC 和智能探测线缆的远程升级；
- 负责集中记录并展现人员入侵的发生和结束的时间和地点，同时进行各项告警功能；
- 负责集中记录并展现 NC/CC/智慧墙/智能探测线缆等设备的运行状态，同时进行各项告警功能；

1 个智慧墙管理平台，能够管理多个入侵行为智能识别软件。

3.7 监控区域

入侵探测系统能够探测到的入侵范围。

3.8 防区

防区是对监控区域的细致划分，不受物理设备的限制，可跨多道智慧墙组成防区或将一道智慧

墙分为多个防区，可按业务需求缩小或扩大，可随管理员意愿随时布防或撤防。

3.9 布防

防区的工作模式之一，防区处于布防模式下，智慧墙实时感知倒入侵后将智能管理平台显示和记录报警信息。

3.10 撤防

防区的工作模式之一，防区处于撤防模式下，智慧墙实时感知入侵后仅记录下入侵事件，智能管理平台不会显示报警信息。

3.11 身份认证

在防区处于布防模式下，佩戴经过授权的合法巡检卡终端的人员进入智慧墙实时监控区域，系统感知入侵后会与终端进行鉴权通信，通过后将在管理平台显示巡检事件并记录；非法人员或佩戴未授权终端的人员进行实时监控区域正常报警显示。

3.12 多点入侵识别

系统可以识别同一防区内间隔 15 米以上同时发生的多个入侵行为的功能。

3.13 抗风险容限

系统前端探测器非连续的损坏可由其它探测器自动弥补漏洞，不影响系统正常工作。

3.14 非接触式主动探测

系统主动发射探测信号形成空间场探测防区，靠近非接触状态即可感知入侵行为并报警，可以有效预防跨越突防行为。

4 系统组成

本系统由周界探测设备、控制与传输设备、智能分析与呈现设备、网络互联等设备等组成。

4.1 系统架构图

探测设备包括一组或多组智能探测线缆（探测器）；控制和传输设备包括智慧墙分站（CC）、传输光缆、交换机等；分析与呈现设备包括入侵智能识别服务器（NC）、智能管理平台、用户操作终端以及通信接口等。

基本系统结构如图 1 所示。

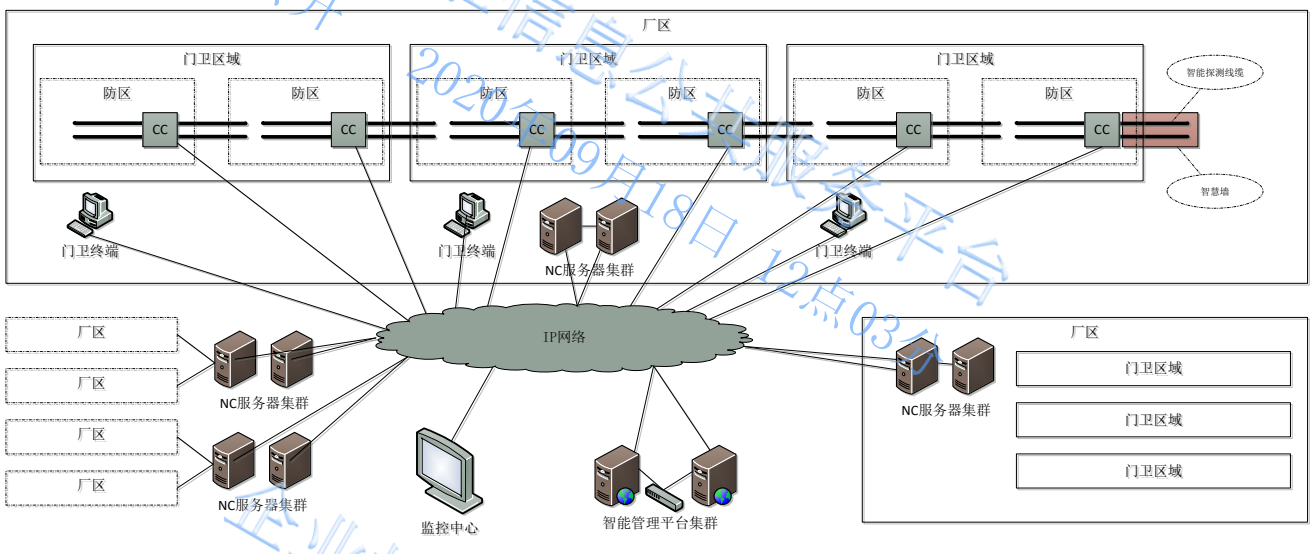

图 1 基本系统结构

支持多个智慧墙探测系统联网，接入本地或远程报警控制中心。

5 技术要求

5.1 功能要求

5.1.1 主动非接触式入侵探测

系统利用微波阵列形成主动立体的探测场，实时感知入侵目标并生成报警信号，即入侵者在没有触碰探测设备的情况下，系统即能发现并报警。

5.1.2 报警灵敏度可调

系统实际探测距离远近可以通过系统参数进行调整。

5.1.3 入侵探测告警

防区布防模式下，管理平台接收到入侵信号时，向用户发出报警。

5.1.4 精确定位

防区报警时，系统可以定位入侵行为发生的位置，定位精度 2~5 米。

5.1.5 多点入侵告警

防区布防模式下，系统可以识别同一防区内间隔 15 米以上同时发生的多个入侵行为。

5.1.6 身份认证

防区布防模式下，佩戴经过授权的合法终端的人员进入系统实时监控区域，系统显示巡检事件并记录；佩戴未授权终端的人员进入实时监控区域，系统报警。

5.1.7 防区逻辑划分

管理平台可对防区进行逻辑划分，无需移动设备位置，即可灵活配置或调整防区的数量和范围，防区的最小粒度可达 20 米。

5.1.8 防区自动撤布防

管理平台可以防区为单位手动进行布防/撤防模式的切换，也可以定时定防区自动切换。

5.1.9 防区有效性验证

系统可通过终端设备可以对防区有效性进行验证。

5.1.10 存储和查询

管理平台具有数据存储、查询、备份功能

5.1.11 自诊断

系统具有自诊断功能。当系统中探测节点、智能探测线缆、智慧墙分站等设备发生故障时，管理平台可报警并记录。

5.1.12 系统冗余设计

系统前端探测器非连续损坏可由其它探测器自动弥补漏洞，不影响系统正常工作的能力。

5.1.13 事件管理

管理平台能够记录、显示、查询入侵事件、巡检事件的发生时间、结束时间、发生位置、结束位置。

5.2 安全性

a）设备使用的电源线，应符合 GB 16796-2009 中 5.4.8 的要求；

b）设备应具有保护接地端子，应符合 GB 16796-2009 中 5.4.5 的要求；

c）设备的抗电强度、绝缘电阻、泄漏电流应符合 GB 16796-2009 中 5.4.3、5.4.4 和 5.4.6 的要求。

6 试验方法

6.1 试验环境条件

除环境试验或有关标准中另有规定外，试验应在下列环境条件中进行

a） 环境温度:15-35℃

b） 相对湿度:45% -75%

c） 大气压力:86-106kPa

6.2 电源条件

除非有关标准另有规定，侧试用电源应符合以下要求:

交流供电电源:

a） 电压:误差应不大于 2%

b） 频率:50Hz，其误差应不大于 1%

C） 谐波失真系数:应不大于 5%

直流供电电源:

a） 电压:误差应不大于 2%;

b） 周期与随机偏移:ΔU/ U 不大于 0.1%

1） ΔU 为周期与随机偏移的峰到峰值

2） U 为直流供电电压的额定值

6.3 受试系统要求

a） 中心站设备一套包括：主机四台（含 2 台显示器）、交换机一台；

b） 构成周界安防区所必需的设备；

e） 构成系统的其他必要设备。

6.4 受试系统的连接

按图 2 接测试系统。

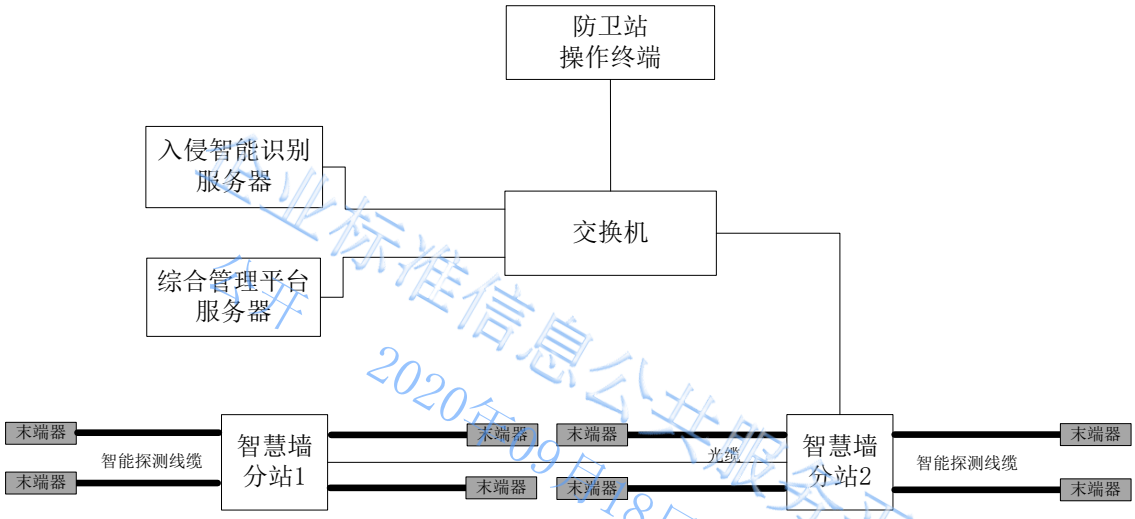

图 2 测试系统连接图

6.5 测试条件

6.5.1Web 服务器正常连接到入侵智能识别服务器。

6.5.2 在管理平台上检查 SmartWall 设备工作正常。

6.5.3 在无入侵情况下，管理平台无系统告警。

6.6 系统功能试验

6.6.1 入侵探测告警功能测试

测试条件	1. 正常天气条件：无风或微风、无雨/雪/雾 2. 入侵人员特征：160~180cm，50~80kg 3. 入侵人员速度：①快速跑入：5m/s；②慢速移动：0.1m/s 4. 闯入方式：入侵人员从系统探测区域外连续移动进入探测区域但不接触探测线缆
测试方法描述	1) 入侵人员快速闯入系统探测区域内，实时查看管理平台视图管理界面的报警提示，并对比报警位置、报警时间与实际闯入位置、闯入时间； 2) 入侵人员慢速闯入系统探测区域内，实时查看管理平台视图管理界面的报警提示，并对比报警位置、报警时间与实际闯入位置、闯入时间； 3) 调整系统参数，缩减或放大探测区域，入侵人员距离探测线缆不同距

	离报警
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 人员闯入时，管理平台发出报警提示； ② 报警位置与实际闯入位置误差 5m 以内； ③ 探测范围可跟随参数调整变化

6.6.2 多点入侵告警功能测试

测试条件	1. 正常天气条件：无风或微风、无雨/雪/雾 2. 人员特征：160~180cm，50~80kg 3. 闯入方式：两名入侵人员从系统探测区域外间隔 15 米以上同时连续移动进入探测区域
测试方法描述	1) 在布防模式下,两名入侵人员间隔 15 米以上同时闯入系统探测区域内，实时查看管理平台视图管理界面的报警提示，可同时显示并记录两点入侵行为，并对比报警位置、报警时间与实际闯入位置、闯入时间
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 两名入侵人员人员闯入时，管理平台视图管理界面的产生两处非法入侵告警；

6.6.3 身份认证功能测试

测试条件	1. 正常天气条件：无风或微风、无雨/雪/雾 2. 人员特征：160~180cm，50~80kg 3. 闯入方式：入侵人员佩戴巡检卡从系统探测区域外连续移动进入探测区域
测试方法描述	1) 在布防模式下,入侵人员佩戴授权巡检卡终端闯入系统探测区域内，实时查看管理平台视图管理界面，可显示记录为巡检事件，并可对比巡检位置、巡检时间与实际是否相符； 2) 在布防模式下,入侵人员佩戴未授权巡检卡终端闯入系统探测区域内，实时查看管理平台视图管理界面，显示记录为报警事件
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 佩戴授权巡检卡终端闯入显示为巡检事件； ② 佩戴未授权巡检卡终端显示为报警事件

6.6.4 事件管理功能测试

测试条件	1. 6.6.1-6.6.3 用例已执行，并产生入侵及巡检事件（告警）
测试方法描述	1) 人员闯入系统探测区，实时查看管理平台报警提示； 2) 可以通过管理平台调用历史事件，回放查看事件发生时间、结束时间、发生位置、结束位置等信息
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 综合平台视图管理界面，调用历史事件，显示人员轨迹与事件回放基本一致；

6.6.5 防区管理功能测试

测试条件	1. 系统管理平台正常工作
测试方法描述	1) 在管理平台中重新划分系统防区； 2) 在管理平台中对个别防区进行撤防布防模式切换； 3) 预设防区自动撤布防时间，通过修改系统时间模拟测试自动撤布防功能
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 管理平台可以逻辑划分防区； ② 管理平台可以设置系统布防/撤防模式； ③ 自动撤布防功能有效

6.6.6 存储和查询功能测试

测试条件	1、6.6.1-6.6.3 用例已执行，并产生入侵、巡检事件（告警）
测试方法描述	1) 登陆管理管理平台； 2) 进入事件管理模块，查看当前事件和历史事件界面，输入防区位置、或者入侵事件等关键字，查询；
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 历史事件显示； ② 查找结果与关键字符合；

6.6.7 自诊断功能测试

测试条件	1、系统正常工作
测试方法描述	(1) 系统正常的前提下，关闭一个正常的 CC； (2) 卸载被关闭的 CC 上的一条智能探测线缆；

	(3) 启动 CC； (4) 登陆管理平台，选择视图管理，勾选设备
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 关闭 CC 时查看管理平台，视图管理产生设备事件，显示设备事件明细中 CC 的与关闭 CC 的 sn 一致，设备异常； ② 卸载线缆后启动 CC，视图管理产生设备事件，显示设备事件明细中 CC 的与关闭 CC 的 sn 一致，CC 的 port 异常

6.6.8 冗余设计自修复功能测试

测试条件	1、正常天气条件：无风或微风、无雨/雪/雾 2、人员特征：160~180cm，50~80kg 3、闯入方式：入侵人员从系统探测区域外连续移动进入探测区域
测试方法描述	(1) 系统正常的前提下，关闭一个正常的 FN 探测节点； (2) 人员闯入系统探测区，实时查看管理平台报警提示
测试结果评判	测试结果同时满足以下条件则认定为合格： ① 人员闯入时，管理平台发出报警提示

6.7 安全性检验

对采用交流供电的设备，按 GB 16796-2009 中的相关规定进行试验，判断结果是否符合第 7 条的要求。

检验规则

7.1 检验分类

系统的检验分出厂检验及型式检验两种。

7.2 出厂检验

7.2.1 每套系统均需进行出厂检验，系统内检验合格的产品应给予产品合格证。

7.2.2 出厂检验一般由制造厂质检部门负责进行，必要时用户可提出参加。

7.2.3 出厂检验项目包括 5.1 功能要求和 5.2 安全性的检验内容。

7.2.4 出厂检验的各项性能和指标应符合本标准和相关标准的规定，否则按不合格处理。

7.3 型式检验

7.3.1 型式检验应由国家认可的产品质量检验机构进行检验，并应出示“检验报告”。

7.3.2 型式检验的项目为本标准中规定的 5.1 及 5.2 全部项目。

7.3.3 型式检验应在下列情况之一时进行；

1) 系统内产品采用的工艺有较大改变时；
2) 国家质量监督管理机构提出型式试验检验时；
3) 停产两年后恢复生产时；
4) 正常生产时每五年一次。

7.3.4 型式检验的样品应从出厂检验合格的产品中随机抽取，每次不得少于二套。

7.3.5 判定原则：有任何一项出现故障或某项通不过时，应立即停止检验，认真查找，提出改进措施，重新对该项进行检验，若再次出现故障或通不过时，应加倍抽样重新进行型式检验。

8 标志、包装、运输和贮存

8.1 智能探测线缆

8.1.1 标志

8.1.1.1 产品标志

智能探测线缆表面应用激光打标印制产品标志。应包括下列主要内容：

1) 产品名称及型号；
2) 产品合格证；
3) 制造厂名或注册商标。

印字必须清晰耐擦、印字间隔不超过 1m。

8.1.1.2 包装箱标志

储运标志应符合 GB/T 191-2008 的规定；收发货标志应符合 GB 6388-1986 的规定，一般应包括以下内容：

1) 制造厂名及厂址；
2) 产品型号名称和规格；
3) 生产日期。

8.1.2 包装

包装要求：

1) 线缆应成卷或成盘交货，其弯曲半径不得小于外径的 10 倍。线缆两端必须密封，成卷线缆应妥善包装。
2) 成盘包装的线缆必须整齐地绕在线缆盘上。线缆盘上应标明线缆盘正确的旋转方向。
3) 每卷或每盘线缆上应附标签，标明 8.1.1.2 规定的内容。

8.1.3 运输

1) 装箱产品在避免雨雪直接淋袭的条件下，能适应飞机、轮船、火车、汽车等运输方式。
2) 运输中应有遮蓬，注意防日晒、防雨水、防尘埃、防机械损伤；应避免酸、碱及其它腐蚀性气体的腐蚀；避免强烈颠簸震动与撞击。
3) 运输中应防止严重弯曲。

8.1.4 贮存

包装后的产品应能在温度为-40℃～+60℃，相对湿度不大于 90%，无急剧温度变化，周围空气中没有酸性和其他有害电子产品气体的环境中贮存一年以上（电池除外）。

8.2 智慧墙分站

8.2.1 包装要求

产品包装应采用符合防护包装类型，具有防雨、防潮、防尘、防振能力。符合相关标准的要求。

8.2.2 包装标志

包装贮运标志应符合 GB/T 191-2008 的规定，包装箱外标识应有：

4) 制造厂名及厂址；
5) 产品型号名称和规格；
6) 生产日期。

8.2.3 装箱文件

1) 产品合格证；
2) 使用说明书；
3) 相关方要求的其他附件清单；

8.2.4 运输要求

产品包装后能适用于汽车、火车、轮船、飞机等方式运输，运输中应遮蓬、防雨、文明装卸。

8.2.5 存储要求

产品使用前应放在原包装箱内，仓库内不允许有有害气体、易燃、易爆及有腐蚀性的化学物品，并且应无强烈的机械振动、冲击和强磁场作用。不允许露天存放。产品应能在温度为-40℃～+60℃，相对湿度不大于 90%的环境中贮存 12 个月以上。