ICS 35.020
L 09
备案号：36772-2013

DB11

北　京　市　地　方　标　准

DB11/T 948.12—2013

电梯运行安全监测信息管理系统技术规范 第12部分：系统信息安全规范

Technical specifications for lifts, escalators and moving walks operation safety monitoring information management system

Part 12: Specifications for system information security

2013 - 01 - 31 发布　　2013 - 05 - 01 实施

北京市质量技术监督局　　发布

目　　次

前　言

DB11/T 948《电梯运行安全监测信息管理系统技术规范》分为以下几个部分：

—— 第 1 部分：系统总体结构；

—— 第 2 部分：电梯基础信息与格式；

—— 第 3 部分：采集设备编码规则；

—— 第 4 部分：采集设备与平台的通信协议与数据格式；

—— 第 5 部分：传输网络要求；

—— 第 6 部分：监测数据存储要求；

—— 第 7 部分：图像子系统技术要求；

—— 第 8 部分：采集设备技术要求；

—— 第 9 部分：电梯运行数据格式与输出要求；

—— 第 10 部分：采集设备安装验收规范；

—— 第 11 部分：平台技术要求；

—— 第 12 部分：系统信息安全规范；

—— 第 13 部分：平台维护要求。

本部分为 DB11/T 948 的第 12 部分。

本部分由北京市质量技术监督局提出。

本部分由北京市质量技术监督局归口。

本部分由北京市质量技术监督局组织实施

本部分主要起草单位：北京市质量技术监督局、北京数字认证股份有限公司、北京市标准化研究所。

本部分主要起草人：王晓花、翟建军、彭海龙、李亮华、宋国建、邢磊、杨毅、李勇、陈凌、陈辉。

电梯运行安全监测信息管理系统技术规范
第 12 部分 系统信息安全

1 范围

本部分规定了电梯运行安全监测信息管理系统的信息安全技术要求。

本部分适用于电梯运行安全监测信息管理系统的规划，新建、改建、扩建工程的设计和验收。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所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（包括所有的修改单）适用于本文件。

GB/T 20273信息安全技术 数据库管理系统安全技术要求

GB/T 22239信息安全技术 信息系统安全等级保护基本要求

GB/T 24856信息安全技术 信息系统等级保护安全设计技术要求

3 术语和定义

下列术语和定义适用于本部分。

3.1

电梯数据采集端 Lifts, escalators and moving walks data acquisition terminal

电梯数据采集端由传感器、采集器、摄像头、通信网关等设备组成，负责采集电梯运行监测数据和图像数据，将采集到的数据转换成平台要求的格式，经网络传送至数据汇聚层。

3.2

传输网络 transmission network

承载电梯运行安全监测信息管理系统数据传输的网络。

3.3

物理访问控制 physical Access Control

对机房、设备间等关键物理位置进出人员的管理与控制。

4 缩略语

下列缩略语适用于本部分：

VPN：虚拟专网（Virtual Private Network）

RAID：独立磁盘冗余阵列（redundant array of independent disks）

5 系统信息安全总体框架

电梯运行安全监测信息管理系统信息安全技术框架见图1。

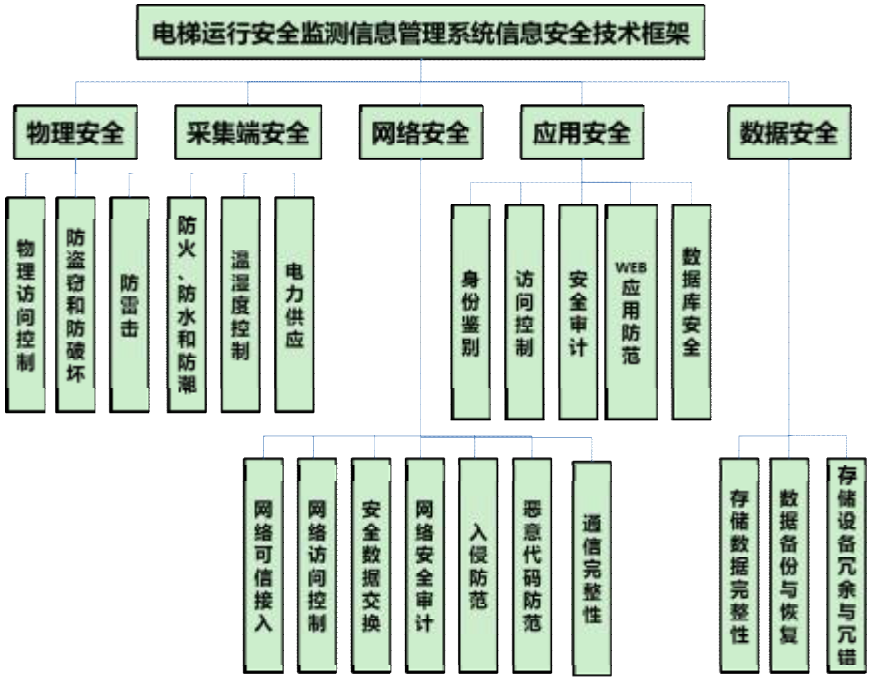

图 1 电梯运行安全监测信息管理系统信息安全技术框架图

6 物理安全

6.1 物理访问控制

6.1.1 区级平台、市级平台信息系统所在的机房应设置专人值守，控制、鉴别和记录进入人员；

6.1.2 进入市级平台信息系统所在机房的来访人员应经过相关负责部门的申请和审批流程，并且应限制和监控其活动范围。

6.2 防盗窃和防破坏

6.2.1 区级平台、市级平台信息系统的服务器、交换机等主要设备应放置在机房内；

6.2.2 设备或主要部件应固定，并设置明显的标记；

6.2.3 市级平台信息系统所在机房应安装防盗报警装置；

6.2.4 前端数据采集设备应具备防盗报警装置。

6.3 防雷击

6.3.1 信息系统机房、前端设备所在的建筑应安装避雷装置；

6.3.2 机房应设置交流电源地线。

6.4 防火、防水和防潮

6.4.1 市级平台信息系统机房应设置灭火设备和火灾自动报警系统；

6.4.2 水管安装，不应穿过机房屋顶和活动地板下；

6.4.3 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

6.4.4 应采取措施防止机房（包括信息系统机房和前端设备所在的机房）内水蒸气结露和地下积水的转移与渗透。

6.5 区级平台、市级平台信息系统机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6.6 电力供应

6.6.1 应在区级平台、市级平台的机房供电线路上配置稳压器和过电压防护设备；

6.6.2 市级平台机房应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

7 电梯数据采集端安全

7.1 应采用本系列标准第 3 部分规定的采集设备编码+MAC 地址绑定的方式，实现电梯数据采集设备的身份认证。

8 网络安全

8.1 传输网络结构

电梯运行安全监测信息管理系统传输网络结构如图2。

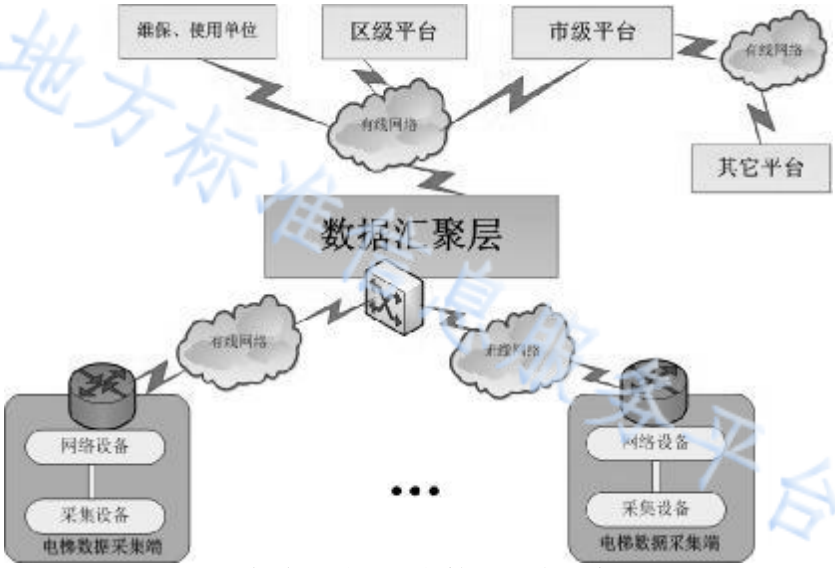

图 2 电梯运行安全监测信息管理系统传输网络结构图

8.2 应启用端口绑定等方式对接入系统传输网络的用户、设备进行网络层的可信接入认证机制，保证接入市级平台、区级平台等信息系统用户、设备的真实可靠。

8.3 网络访问控制

8.3.1 应在应用平台信息系统应用服务器、数据库服务器所在的网络边界部署防火墙等访问控制设备，根据安全策略提供明确的允许/拒绝访问，控制粒度为网段级；

8.3.2 对访问应用平台网络区域的终端，应采用“MAC+端口绑定”等技术方式来防止地址欺骗；

8.3.3 应对应用服务器、数据库服务器之间的安全边界开启访问控制策略，控制粒度为端口级；

8.4 数据汇聚层向区、市级应用平台上报数据、区级平台与市级平台数据交换时，应对文件类型及格式进行限定。

8.5 网络安全审计

8.5.1 应对应用平台信息系统应用服务器、数据库服务器所处的网络区域接入交换机旁路部署网络安全审计设备，对网络流量、用户行为等进行日志记录；

8.5.2 审计记录应包括事件的日期、事件、用户名、IP 地址、事件类型、事件是否成功等；

8.5.3 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保持 60 天；

8.5.4 应定期对审计记录进行分析，以便及时发现异常行为。

8.6 入侵防范

8.6.1 应在应用平台政务外网边界、互联网边界部署相关设备监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击和网络蠕虫攻击等；

8.6.2 当检测到攻击行为时，应能够记录攻击源 IP、攻击类型、攻击目的、攻击事件，发生严重入侵事件时应提供报警。

8.7 恶意代码防范

8.7.1 应用平台部署在互联网时，应在应用平台信息系统网络边界处对恶意代码进行检测和清除，及时维护恶意代码库的升级和检测系统的更新；

8.7.2 数据汇聚层、应用平台中的服务器应安装防病毒软件，并及时更新软件版本和恶意代码库；

8.7.3 采用的防病毒产品应具有计算机信息系统安全专用产品销售许可证；

8.7.4 应制定《电梯运行安全监测管理信息平台计算机病毒防治管理制度》，针对平台管理人员进行计算机病毒防治管理培训。

8.8 在数据汇聚层与应用平台双方通信时，应采用校验码技术、特定的文件格式、特定协议或等同强度的技术手段等进行传输，保证通信过程中的数据完整性。

9 应用安全

9.1 身份鉴别

9.1.1 平台应提供对采集设备身份鉴别功能；

9.1.2 应对接入应用平台的采集端设备（“采集设备编码+MAC”与“应用平台中注册的可信设备识别码”比对等方案）进行可信检验，确保接入平台的采集设备真实可信，防止恶意非法终端接入；

9.1.3 针对登录应用平台的用户，应基于数字证书等严格的强身份认证措施，应用平台需提供专用的登录控制模块，或者将登录控制模块集成到统一的门户认证系统中，应对登录应用平台的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

9.1.4 应用平台应提供身份标识唯一和鉴别信息复杂度检查功能，保证应用平台中不存在重复用户身份标识；

9.1.5 应用平台的系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令不应相同；

9.1.6 应用平台应提供登录失败处理功能，可采取结束会话、限制非法登录或自动退出等措施；

9.1.7 在数据汇聚层与应用平台之间数据交换应采用服务器证书方式实现服务器的身份识别。

9.2 应用层访问控制

9.2.1 市级平台应提供统一的门户，门户应具有鉴权机制，依据登录人员的不同身份展现不同的界面；

9.2.2 应用平台应具备身份认证与授权管理系统，实现用户的统一身份认证及资源的统一授权管理；

9.2.3 通过外部网络对应用平台进行访问时应使用安全方式接入，宜对用户采用数字证书等强制认证方式，应根据维保部门、使用单位等用户和应用平台之间的访问规则，决定对系统中资源的访问，访问控制粒度应为单个用户；

9.2.4 应根据应用平台管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

9.2.5 应实现操作系统和数据库系统特权用户的权限分离；

9.2.6 应及时删除应用平台中多余的、过期的帐户，避免共享帐户的存在。

9.3 安全审计

9.3.1 区级平台、市级平台应具备直接相关系统安全审计功能；

9.3.2 针对平台管理员，审计内容应包括用户登录、修改配置、操作内容、操作结果等重要行为，以及系统资源的异常使用等；针对平台用户，审计内容应包括用户登录、操作内容等重要行为；

9.3.3 审计记录应至少包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；

9.3.4 应保证无法删除、修改或覆盖审计记录，市级平台审计记录至少保存 90 天，区级平台审计记录至少保存 60 天。

9.4 对维保单位、各使用单位等用户提供服务的 WEB 应用应能够抵抗 SQL 注入等应用层攻击，具备网页防篡改等应用层防护体系。

9.5 完整性保护

9.5.1 应规范采集设备与平台的通信协议与数据格式，协议中应具备数据完整性校验；

9.5.2　应采用 SSLVPN 技术确保应用平台远程接入用户的通信完整性。

10　数据安全

10.1　至少采用 RAID1 策略来存储数据。

10.2　数据备份与恢复

10.2.1　监测数据备份与恢复

10.2.1.1　监测数据应以数据库形式提供全系统备份与恢复。应用平台信息系统发生故障时，应能够实现监测数据的恢复；

10.2.1.2　数据汇聚层存储节点和应用层存储节点应提供数据本地备份与恢复功能。完全数据备份至少每月一次，增量备份至少每天一次；

10.2.1.3　可选用硬盘、磁带、光盘等作为数据备份介质；

10.2.1.4　应制定数据备份与恢复策略和计划，每年应至少进行 1 次数据恢复演练。

10.2.2　故障图像片段备份与恢复

10.2.2.1　故障图像片段应以文件形式提供备份与恢复机制，备份策略采用完全备份与增量备份结合的方式，完全数据备份至少每 2 个月 1 次，应用平台信息系统发生故障时，能够实现恢复；

10.2.2.2　可选用磁盘、磁带、光盘等作为数据备份介质；

10.2.2.3　应制定数据备份与恢复计划，每年可至少进行 1 次的数据恢复演练。

10.3　数据存储设备宜采用冗余设计。