

4. 门禁系统需求

4.1. 系统架构

- ◆ 服务端操作系统为 Linux，满载工作时 CPU 不超过 20%，具备来电自启动。
- ◆ 系统具备冗余机制，包括不限于服务器冗余、硬盘冗余等。
- ◆ 门禁系统需要满足腾讯的北向接口协议，腾讯可以远程对门禁系统进行授权和开关门禁。
接口应考虑安全性，具备白名单管理。
- ◆ 门禁系统需要集成 tblock 内的门禁，但是 tblock 的门禁和园区门禁授权必须分开
- ◆ 门禁需要开放接口以便和视频人脸识别系统对接，人脸识别系统在发现授权人员以后可以发送命令到门禁系统打开对应的门禁。
- ◆ 门禁系统需要配合巡检机器人厂家完成机器人和门禁的协同工作，使得巡检机器人可以向门禁系统发送命令，控制门的开启和关闭。
- ◆ 性能方面。对于 WEB 客户端，要支持不少于 10 个客户端并发访问，页面切换到数据完全呈现的时间不超过 2 秒，确保好的用户体验；在北向接口方面，要支持不少于 100 个客户端的并发访问，单请求响应时间小于 0.5 秒，接口访问成功率 100%，数据与告警准确率 100%，从北向接口获取的数据必须是最近 5 秒内设备的状态。

4.2. 功能需求

1) 系统界面

- ◆ 全中文界面，支持深色调和浅色调两种界面风格，便于投放大屏时与其它系统风格统一。
- ◆ 本子系统的主界面应为包含所有门禁设备在内的电子地图，直观显示每扇门的开关状态，开关位置需与现场位置、门牌号一致。在该界面上可直接点击任意门禁进入其工作状态界面，在工作状态界面上，应直观显示该门禁的实时进出情况，同时提供对历史进出记录的组合查询功能以及根据查询结果生成单门门禁报表的功能。

- ◆ 当门禁进出状态异常时，系统界面应自动切换到该门禁的工作状态界面，同时弹出告警信息窗口。
- ◆ 支持 B/S 架构，可开放写入接口。
- ◆ 系统需要分物理位置关系、通信关系两条线路来对系统功能进行展示。
 - 物理位置关系使得用户可以从园区、建筑、楼层、房间、tblock 模块、设备的关系链，一路往下点击追溯，每个层级会有不同的显示内容要求，最后定位到某个具体设备的相关信息，用户也可以点击路径链接进行跨路径跳转。具体见设施监控需求章节
 - 通信关系上，用户可以快速查看整体通信链路及运行状态、以及链路上的设备分布；用户能快速查看每一条通信链路的通信参数、通信状态；用户可以查看设备的通信参数、通信状态、并能直接跳转进指定设备监控页面中。
 - 对于物理位置关系及通信关系，厂家需要提供设备的模糊搜索功能，并提供类似树形结构的方式对设备进行管理。

2) 进出授权

- ◆ 进出卡：系统对人员进出权限的控制主要通过对进出卡的管理来实现，包括以下几个方面：
 - 进出卡中包含的用户信息应包括卡号、用户名、工号、部门、级别授权、授权进出区域、有效日期、授权进出时段、卡有效状态以及个人照片等信息。进出卡的设置信息应即时下载至门禁控制器中，保证门禁服务器故障时人员的进出不受影响。
 - 管理人员通过对进出卡的登记、注册、授权、变更、注销、挂失与解除挂失等操作实现对人员进出权限的控制。

3) 授权设定

- ◆ 区域授权：可以对已注册的进出卡设定其人员活动区域，按活动区域进行划分，即持卡人可以或不可以通过哪些门或通道。
- ◆ 级别授权：系统应允许用户将不同的区域和不同的进出时段按不同的级别进行划分与管理，可通过设定卡的级别来控制持卡人的进入区域权限以及进入该区域的时间段等。
- ◆ 组授权：系统应支持组授权功能，对于不同的组可以定义在哪些时间段内可以通过哪些区域；既可以按实际的区域进行划分，也可以按级别进行划分。
- ◆ 时间段授权设定：系统应提供自定义选项，允许以周为循环单位，从星期一到星期日、每天的 0 点到 24 点，允许用户根据实际情况进行选择；通过对时间段的设定，限制持卡人的出入时间。
- ◆ 有效日期授权：根据人员实际进出需求设定其进出卡有效期，分为“长期”、“自定义”两种选择，其中自定义选项包含起迄时间，精确到小时。
- ◆ 可通过刷任意门或使用加卡机对卡就行授权、且支持批量操作。

4) 告警功能

- ◆ 当出现异常情况时，系统具有报警告警功能。如：强行开门、门长时间不关、通信中断、设备被拆、用户卡失窃或无效的卡开门等，告警设定值可调，告警内容可透传至上层集成系统，管理平台会发出告警信号，实时显示案发地点，同时保存记录。以上各类非法操作均可通过设置与视频系统的联动逻辑，驱动最近的摄像机进行录像。
- ◆ 告警支持自定义打标功能，告警展示时可依据所打标签筛选展示。
- ◆ 具备告警屏蔽功能，系统应允许按照区域、子区域等多维颗粒度、告警接收对象等不同组合方式进行屏蔽，已屏蔽的设备必须支持在统一的界面显示，统一管理，以便及时恢复必要的告警。告警屏蔽规则应库化，可按需快速启用或停用。屏蔽的告警应当被产生、记录、并在指定的位置进行展示。

- ◆ 具有历史告警查询功能，调用方式至少包括：按时间、按设备、按机房、是否确认；并可多种方式混合查询；查询结果应可选择要显示哪些列、以及列的显示顺序。
- ◆ 其它：
 - 系统要能够主动发现底层设备的数据质量问题，并产生相应的告警。如：由于传感器中传感芯片故障而导致通信正常但数据长期不更新。再如：数据明显不在合理范围等。
 - 系统应当提供告警有效性的验证工具。比如提供模拟数据来验证告警策略的有效性。

5) 门禁封锁功能

- ◆ 在系统界面上可遥控所有门禁电锁的开关，当非法进入发生时，可通过授权对部分门禁进行封锁；
- ◆ 当某卡在某个门禁点连续非法刷卡的次数超过设定值时，该门禁将被自动封锁并告警。

6) 查询功能

- ◆ 系统应对每一门禁的工作状态、工作日志等内容提供简单、直接的查询方式，查询的结果可以输出及打印。
- ◆ 快速查询：系统应支持快速查询功能，一方面通过直接点击电子地图上的门禁图标进入其工作状态界面，在工作状态界面上点击查询选项弹出查询窗口；另一方面也可在管理界面上设置查询窗口，当管理人员输入门禁 ID 号、门禁名称等唯一性信息时，系统可自动弹出该门禁的查询窗口，便于管理人员随时查询。
- ◆ 可通过区间报警查询找到对应的门牌号-触发人员-触发时间等各参数的整体性报表。

7) 报表管理

- ◆ 系统应允许用户根据需要选择生成单项报表或组合报表：

- ◆ 单项报表指针对系统内某一项参量生成的报表。报表内容由用户根据报表模块提供的组合条件进行定制，包括参量选择、自定义报表时间段等，而报表格式则由系统根据参量特点自动选择。可生成单项报表的参量应不少于以下内容：
 - 指定时间段内指定门禁的记录报表，包括进出次数、非法刷卡次数、告警次数等（采用柱状图格式）。详细的事件记录可通过日志管理模块生成；
 - 指定时间段内指定人员的进出记录报表，包括进出机房次数、非法刷卡次数（尝试进入非授权区域）等（可指定时间段）。详细的进出记录可通过日志管理模块生成。
 - 组合报表指对系统内某些关键参量进行统计分析并组合生成的报表。报表内容由用户根据运营需要进行定制，报表格式可通过 Excel 导出。组合报表按时间段又可分为日报表、周报表和月报表等固定报表以及按时间段自定义生成的报表。
- ◆ 报表的生成分为自动和手动两种方式。通常日报表和周报表可设为自动生成，其他报表通过手工方式进行定制。

8) 日志管理

- ◆ 系统须提供基于数据库的日志功能。
- ◆ 系统日志应至少包括用户操作日志、系统运行状态日志、告警日志及通行日志（通行日志内容包括：进出时间、区域、进出卡号、进入方式等）。所有日志可以根据查询条件即时生成报表，并可打印输出。
- ◆ 系统日志原则上不可被任何人修改；除最高级用户外，系统日志也不能被删除。
- ◆ 系统日志的默认保存时间为三年。超过保存时间需要删除时，由最高级用户根据时间段进行删除。

9) 数据管理

- ◆ 数据的本地备份：系统应具备本地备份和恢复功能，系统能自动将历史数据、告警日志、数据库等数据备份到本地硬盘上并于必要时进行恢复。本地硬盘的容量应至少满足门禁系统数据保存三年的要求。

10) 联动控制

- ◆ 系统应支持与视频子系统的联动控制，比如门开启后自动联动摄像机进行录像等；
- ◆ 系统应支持与自控系统的联动控制，比如双路火警信号发生，满足触发条件时，门禁系统可即时联动控制所有门开启（消防系统中具体实现方案）；
- ◆ 双门互锁：当消防门打开时，应确保最近的机房入口门关闭（即实现互锁），如 D1 打开，要求系统能立即对该通道内可进入下一层空间的 D2 和 D3 执行关闭动作。

11) 系统维护

- ◆ 系统应支持在线维护，即系统运行时，支持实时的修改和维护。包括以下几个方面内容：
 - 设备的增减：门禁的增减可通过软件模块的增减实现，所有操作在线进行；
 - 参数及变量的修改维护：在线修改，即时完成，系统不用重启；
 - 显示界面的在线修改：可利用组态工具实现在线修改，即时完成，系统不用重启；
 - 基于远程的在线维护：系统应支持集中维护，可通过“上传”、“下载”等功能实现远程修改和维护，在不影响系统整体运行的前提下，保持系统的同步；
 - 系统在进行修改维护期间，各门禁控制器的正常工作不受影响。

4.3. 硬件产品要求

- 1) 门禁控制器、锁具、卡片等需满足腾讯南向硬件规格需求；卡片应支持加密功能，避免直接被手机 NFC 复制。
- 2) 访客系统