四川省道路运输车辆主动安全智能防控系统行业监管平台 技术条件（试行）

1. 范围

本条件规定了道路运输车辆主动安全智能防控系统中行业监管平台的功能、性能及技术指标。

行业监管平台是行业管理部门对运输企业、营运车辆、运营商运用主动安全智能防控系统进行监督管理和考核的平台，各级行业管理平台、第三方监管平台应按照《道路运输车辆主动安全智能防控系统行业监管平台技术条件》进行建设、管理和维护。

1. 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 35658-2017 道路运输车辆卫星定位系统平台技术要求

JT/T 796-2011 道路运输车辆卫星定位系统平台技术要求

JT/T 1077-2016 道路运输车辆卫星定位系统车载视频平台技术要求

T/SCSDX 0001-2019.1 道路运输车辆主动安全智能防控系统技术规范 第1部分：企业监控平台

1. 组成结构

道路运输车辆主动安全智能防控系统主要包含主动安全智能防控终端、企业监控平台和行业监管平台，行业监管平台接收终端报警信息，必要时从企业监控平台获取报警附件，企业监控平台获取报警信息和报警附件。行业监管平台与系统其它组成部分的关系如图1所示。

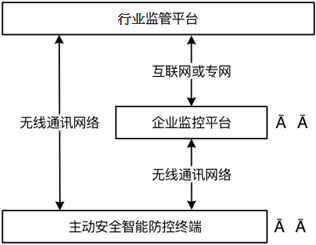


图 1 道路运输车辆主动安全智能防控系统架构

行业监管平台应满足以下要求：

卫星定位系统监管功能应满足GB/T 35658-2017标准中第5章功能要求；

视频监管系统监控功能应满足JT/T 1077-2016标准中第5章功能要求。

1. 功能描述
   1. 用户管理
      1. 用户设置

平台用户管理应具备管理员用户和普通用户两种类型用户的管理功能，同时应满足以下要求：

1. 管理员用户负责平台系统管理、设备管理以及用户管理和用户权限分配；
2. 普通用户可按照管理员分配的权限和管理范围操作系统。
   * 1. 日志管理

日志管理主要用于日志审计和操作跟踪，应满足如下要求：

1. 支持统计当前操作比较频繁的用户；
2. 支持按时间段和用户名查询用户操作；
3. 支持通过报表形式导出用户操作记录，应包含用户名、操作时间、操作内容、操作对象等。
   1. 接入管理

行业监管平台应对接入的主动安全车载终端、企业监控平台数据以及运营商进行管理，具体要求如下：

1. 应能够通过车载终端的MAC地址验证终端的有效性，记录终端校验信息；
2. 应能够记录车载终端上下线时间和运行时间；
3. 应能够对接入的企业监控平台进行管理，能够管理企业监控平台的接入码、用户名、密码、IP以及端口号等信息；
4. 应能够监控企业监控平台的连通性，能够记录平台异常断开信息。
   1. 静态信息管理
      1. 运输企业及车辆静态信息管理

平台应具备运输企业及车辆静态信息管理功能，具备要求如下：

1. 应能够存储运输企业静态信息，企业静态信息包含企业名称、业务范围、企业地址、企业联系人、下属车辆、下属驾驶员等；
2. 应能够存储车辆静态信息，车辆静态信息包含车牌号、车牌颜色、所属企业、车辆类型、终端型号等；
3. 应能够存储驾驶员静态信息，驾驶员静态信息包含驾驶员姓名、驾驶员身份证号、联系方式、驾驶证信息、从业资格证信息等；
4. 应能够定期获取运输企业、车辆、驾驶员等静态信息同步到终端静态信息中；
5. 支持通过名称企业名称、车牌号、驾驶员姓名等归属信息字段查询静态信息详情；
6. 支持车辆列表设置过滤条件，支持一键批量导出自动下载过滤后的列表数据。
   * 1. 终端静态信息管理

平台应具备终端静态信息管理功能，具体要求如下：

1. 应能够记录终端静态信息，终端静态信息包含终端品牌、MAC地址、终端型号、生产厂家、通讯类型等；
2. 应能够定期获取终端数据同步到终端静态信息中；
3. 支持终端号等终端信息字段查询终端信息详情；
4. 支持终端列表设置过滤条件，并支持一键批量导出自动下载过滤后的列表数据。
   * 1. 电子地图静态信息管理

平台应具备电子地图静态信息管理功能，具体要求如下：

1. 应能够记录电子地图静态信息，电子地图静态信息包含电子地图审图号、电子地图厂家等；
2. 应能够定期获取电子地图数据同步到电子地图静态信息中；
3. 支持电子地图厂家、电子地图审图号等终端信息字段查询终端信息详情；
4. 支持一键批量导出自动下载过滤后的列表数据。
   * 1. 运营商及平台静态信息管理

平台应具备运营商及平台静态信息管理功能，具体要求如下：

1. 应能够记录运营商静态信息，运营商信息包含公司名称、公司类型、公司联系人、联系人手机号、使用企业监控平台名称、所服务的运输企业、接入平台的车辆信息、接入平台的终端名称、地图审图号等；
2. 应能够定期获取运营商数据同步到运营商信息中；
3. 支持按照运营商名称等运营商信息查询功能；
4. 支持平台车辆列表设置过滤条件，并支持一键批量导出自动下载过滤后的列表数据；
   1. 动态信息管理
      1. 终端动态信息管理

平台应具备终端动态信息管理的功能，具体要求如下：

1. 应能够记录终端动态信息，终端动态信息包含终端报警记录、终端报警信息等；
2. 应能够定期获取终端动态数据同步到终端信息中；
3. 支持终端号等终端信息字段查询终端动态信息；
   * 1. 企业监控平台动态信息管理

平台应具备企业监控平台动态信息管理的功能，具体要求如下：

1. 应能够记录企业监控平台动态信息，企业监控平台动态信息包含车辆运行数据、终端报警数据、驾驶员驾驶记录、车辆上线率、平台连通率、数据合格率等；
2. 能够记录驾驶员IC卡动态信息，驾驶员IC动态信息包含驾驶员行驶记录、驾驶员记分记录等。
3. 平台能够定期获取企业监控平台动态数据同步到企业监控平台动态信息中；
4. 支持企业监控平台名称等信息字段查询企业监控平台动态信息；
   * 1. 电子地图动态信息管理

平台应具备电子地图动态信息管理的功能，具体要求如下：

1. 应能够记录电子地图的动态信息，电子地图动态信息包括电子地图状态、电子地图版本号、报警类型、报警信息等；
2. 平台能够定期获取电子地图动态数据同步至电子地图动态信息、IC卡登录登出信息中；
3. 支持电子地图版本号等电子地图信息字段查询终端动态信息。
   * 1. 统计分析

基于主动安全智能防控系统数据，对未来交通运输安全运行状况、趋势进行分析，以图表方式进行展现，具体要求如下：

1. 应能够支持实时按照不同报警类型、车辆类型、报警等级分别展示全省主动安全报警分布情况；
2. 应能够按照报警数量分类实时展示全省主动安全报警数据；
3. 应能够根据全省、地市、运输企业等单位展示全省主动安全报警趋势；
4. 应能够根据主动安全报警数量定期对地市和运输企业进行排名；
5. 应能够统计全省车辆入网情况，能够从全省、地市和企业等维度，分别展示总车辆数、入网车辆数以及入网率，同时能够输出未入网车辆列表，且支持报表导出。
6. 应具备企业管理平台报警处理率统计功能，可周期性展示统计结果，并根据处理率对企业进行排名，同时应能够展示处理率较低得企业。
   * 1. 考核管理

平台应具备考核指标统计功能，具体要求如下：

1. 应能够根据读取设备的信息，判别终端厂家、终端型号、终端MAC地址是否在备案终端清单内，结果可支持数据导出；
2. 应能够根据收到终端或企业监控平台的电子地图信息，与平台录入的备案地图信息对比，判别信息是否一致，结果可支持数据导出；
3. 应能够按照不同考核维度，对不同区域、不同运输企业、不同运营商、不同设备进行道路运输安装状态进行评估考核；
4. 支持下发普通通知通报，将通报信息下发到企业监管平台或同一平台的指定账户中，并根据考核结果自动生成通报所需的支撑数据表。
   * 1. 重要危险行为统计

平台应能够支持重要危险行为统计功能，具体要求如下：

1. 支持用户设置危险行为判定策略，用户应能够设置报警类型、触发频率、触发时间段等判定策略；
2. 触发重要危险报警时，应能够提醒监控人员；
3. 应能够将重要危险行为信息存储并与车辆进行关联；
4. 应能够动态展示重要危险行为数量最多的车辆。
   1. 接口管理

行业监管平台应能够连接企业监控平台、主动安全车载终端以及第三方监控平台，同时满足以下要求：

1. 支持主动安全智能防控系统按照JT/T 808-2011、JT/T 1078-2016第5章以及T/SCSDX 0001-2019第4章通讯协议直接连接行业监管平台；
2. 支持企业监控平台按照JT/T 809-2011、JT/T 1078-2016第6章以及T/SCSDX 0001-2019第5章通讯协议连接行业监管平台；
3. 支持第三方监测平台连接行业监管平台。
4. 性能要求
   1. 平台总体性能

平台总体性能应至少满足以下要求：

1. 支持平台7×24h不间断运行；
2. 在没有外部因素影响的情况下，故障恢复时间不超过120分钟；
   1. 车辆接入性能

平台车辆接入系统应满足以下要求：

1. 具有安全报警数据高并发处理能力：平均3000条/s、峰值5000条/s；
2. 平台能支持至少100,000台终端接入。
   1. 报警数据存储

报警相关数据存储及备份要求如下：

1. 报警信息数据在线存储时间不得少于183天；
2. 建立报警信息数据备份机制，每周对数据进行增量备份，每月对报警信息数据进行全量备份，备份报警数据时间不得小于1年，系统数据恢复时间不超过12h。
   1. 安全要求

平台部署环境安全应满足以下要求：

1. 数据库中关键数据加密存储，用户密码加密存储；
2. 采用日志对操作和接受及发送的数据记录，至少存储183天日志数据；
3. 采用备份平台，主平台出现问题能自动切换到备份平台；