ICS 35.040
CCS L80

DB50

重　庆　市　地　方　标　准

DB 50/T 1176—2021

智慧交通 物联网数据服务平台 运维管理通用要求

2021－11－30 发布　　2022－03－01 实施

重庆市市场监督管理局　　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。

本文件由重庆市经济和信息化委员会提出并归口。

本文件起草单位：重庆市城投金卡信息产业（集团）股份有限公司、中国电子技术标准化研究院、重庆市公安局、重庆市公安局交通管理局。

本文件主要起草人：张鹏、彭滨鸿、张璋、赵明、宋鸿、许汝峰、张伟、刘立国、胡芮嘉、易佳、廖汝秋、刘玉印、李春雨、钟添翼、徐龙、辜继东、郑儒和、代绪丰、耿力、宋继伟、刘倩颖、王思翔。

智慧交通　物联网数据服务平台　运维管理通用要求

1　范围

本文件规定了智慧交通物联网数据服务平台运维管理通用要求，包括接入管理、采集设备运维管理与软件系统运维管理三部分内容。

本文件适用于物联网数据服务平台中运维管理的设计、选型和验收。

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 31454-2015 公路收费车道图像抓拍与处理

DB 50/T 526-2013 机动车射频识别 标签产品规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

图像抓拍　video　capture

利用视频数字化技术将车道摄像机的视频信号转换为静态数字化图像的技术称为图像抓拍。

[来源：GB/T 31454-2015，3.2]

3.2

射频识别 radio frequency　identification

在频谱的射频部分，利用电磁耦合或感应耦合，通过各种调制和编码方案，与射频标签交互通信唯一读取射频标签身份的技术。

[来源：DB 50/T 526-2013，3.1]

3.3

读写器 reader/writer

一种用于从射频标签获取数据和向射频标签写入数据的电子设备，通常具有冲突仲裁、差错控制、信道编码、信道解码、信源编码、信源译码和交换源端数据等过程。

[来源：DB 50/T 526-2013，3.6]

3.4

角色　role

承载一个或多个权限的载体。

3.5

实例 instance

服务的一种具体表示，包含一种或多种资源。

3.6

租户 client

对一组物理和虚拟资源进行共享访问的一个或多个云服务用户。

3.7

节点 node

物联网数据服务平台中的一种计算或存储实体。

4 缩略语

下列缩略语适用于本文件。

API:应用程序编程接口（Application Programming Interface）

DOS: 拒绝服务攻击(Denial of Service)

DDOS: 分布式拒绝服务攻击(Distributed Denial of Service)

JDK:JAVA开发工具（JAVA Development Kit）

SSH:安全外壳（Secure Shell）

5 接入管理

5.1 接入流程

接入管理是为规范设备、网络及系统的接入安全工作，保障设备、网络和系统的安全运行。接入流程如图1所示，流程说明如下：

a）在设备、网络及系统进行前期规划时，由业务需求部门提出建设需求，建设部门按照本文件制定相应的建设方案，并提交方案给负责信息安全的部门和负责运维的部门进行评审；

b）由负责信息安全的部门和负责运维的部门根据相关要求对建设方案进行评审，评审通过后报相关负责人审批，如审批不通过则驳回申请，由申请提出部门修改后重新提出；

c）审批通过后，由建设部门组织，负责信息安全的部门和负责运维的部门等其他相关部门配合完成入网实施工作。在配套网络安全技术设施未建成的情况下，设备、网络和系统不能入网运行；

d）建设完成后，由建设部门组织，业务需求部门、负责信息安全的部门和负责运维的部门配合进行初验，如验收不通过则驳回验收申请，由申请提出部门修改后重新提出，如果某设备、网络或系统由于实际的技术原因暂时无法达到本文件的相关技术要求，应按照相关部门要求进行整改完成后方能初验；

e）相关设备、网络、系统的维护工作根据职责分工由相应的技术部门负责。

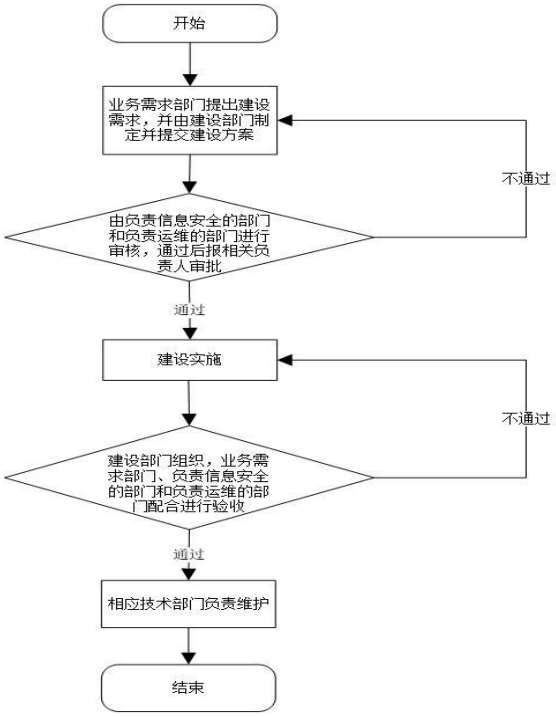

图1 接入流程

5.2 设备、网络和系统接入要求

设备、网络和系统接入要求如下：

a）应具备安全方面的功能和措施；

b）应提供产品安全功能和配套安全措施方面的详细描述；

c）对于拓扑结构设计，应满足基本的网络安全技术要求；

d）对于与外部网络的边界，应部署防火墙实施安全防护；

e）应具备统一的网络接口，以便进行两个网络间的高效、安全互联；

f）对于与互联网等高风险网络的网络边界，应部署双层异构防火墙进行安全保护；

g）对于向用户提供互联网访问服务的重要业务系统，应部署防DOS设备；

h）对于重要的业务系统、支撑系统，应在核心网段部署网络入侵检测设备；

i）在建立防火墙和入侵检测系统时，宜避免引入单点故障，并且应消除旁路路径；

j）对于在易遭受蠕虫病毒攻击的设备，宜增加病毒流量过滤设备；

k）电子邮箱系统应配套垃圾邮件和病毒邮件防护设备或软件；

l）应支持部署统一的防病毒软件。如不能支持，应特别说明并保障其能够实现定期升级病毒库的功能；

m）对涉及机密的数据，应采用密钥长度至少为128位的加密算法进行保护，选用的加密算法应符合国家密码相关规定并通过安全管理部门审核；

n）系统在申请初验时，申请部门应向服务和端口管理责任部门提供服务和端口检查和审核相关表格，并提供以下信息，作为入网服务与端口审核的依据；

具体文档应包含以下内容：

1）开启的服务与端口的对应关系以及用途说明；

2）相关服务与端口关闭和开启的操作方法；

3）版本信息。

o）业务端口管理责任部门应在验收环节检查服务和端口的实际开启情况，确保与提供的声明一致；

p）系统中所涉及的硬件资源应具备开放的管理方式能接入第三方网管，软件应具备运维管理模块。

5.3 安全加固及补丁要求

安全加固及补丁要求如下：

a）应安装操作系统、数据库、中间件等第三方软件的安全补丁，保证不出现高风险漏洞；

b）应在安全补丁安装前完成兼容性测试。如果出现不能兼容的情况，供应商和集成商必须免费对现有程序、应用进行修改和升级，或者免费提供额外的安全措施，以保证安全性；

c）在系统验收前，应对系统进行安全加固，并提交加固报告，并按5.1中所提供的接入流程，进行安全验收。

5.4 帐号口令及日志审计要求

账号口令及日志审计要求如下：

a）应支持基于帐号的访问控制功能，并对口令文件提供妥善的保护；

b）应能保存帐号增删、权限更改和登陆信息等有关安全内容的日志。日志的保存期限应不小于2年。如果因系统限制无法满足该要求，应将日志定期导出，采用其他手段进行保存；

c）应建立密码规则控制，以保证密码规则的有效实施（如能自动拒绝创建不符合安全设置条件的帐号和口令）；

d）应保存对共享帐号的“增加，更改，删除”操作日志，系统管理员定期审阅日志，若有异常操作，可结合IP地址以及登录时间进行进一步调查；

e）应支持口令至少8位大小写的字母、数字以及特殊符号等字符组成；

f）配置更改、敏感数据更改、登录尝试失败、重要操作均应支持日志记录功能；

g）日志应支持实时导出，供应商和集成商应提供日志的标准格式和定义。

5.5 应用软件安全要求

应用软件安全要求如下：

a）应具备测试小组和测试机制，测试过程中应包括安全方面的测试，例如：DOS/DDOS检测、堆栈溢出检测、非法输入检测等；

b）应保证最终代码中不存在测试用、调试用的代码，也不存在任何后门；

c）应该提供必须的备份机制和备份工具，备份至少支持配置备份、数据备份，另外备份媒体至少支持硬盘备份。同时应提供备份恢复工具。

5.6 网络验收要求

网络验收要求如下：

a)要求选择的相应产品及其平台应该满足本文件的要求,如购买和验收任何信息系统相关产品，应该将相关要求条目加入技术规范书或者作为合同附件；

b）安全验收报告至少应包括以下内容：

1）网络拓扑结构；

2）防火墙、入侵监测系统、抗拒绝服务攻击系统部署情况；

3）加密技术使用情况；

4）账号口令、日志审计功能；

5）防病毒软件安装情况；

6）安全管理系统接入情况；

7）安全补丁装载情况及补丁管理机制；
8）安全加固及配置情况；
9）终端安全管理情况；
10）其他安全技术设施的配置；
11）暂时不能满足要求的安全技术设施情况说明。

5.7 审计和执行要求

审计和执行要求如下：

a）信息安全部门应对安全接入的执行情况进行管理和审查，对未能达到本文件相关要求的行为及时指正，并监督相关部门予以解决；

b）信息安全部门应根据本文件定期对设备、网络和系统进行检查。

6 采集设备运维管理

6.1 概述

采集设备运维管理是对射频识别读写器、摄像机等数据采集设备进行运维管理。

6.2 管理流程

采集设备运维管理基本流程见图2，流程说明如下：

a) 采集点数据回传例行检查；
b) 如出现设备数据未回传现象，系统进行故障派单处理；
c) 外场运维人员收到派单以后检查数据未回传原因；
d) 如外场运维人员检查前端设备故障，则进行修复并将检查结果与是否修复的情况反馈至系统中，修复后检查数据是否正常回传；
e) 如外场运维人员检查前端设备正常，则检查服务器原因；
f) 如服务器检查异常，则进行修复并将检查结果与是否修复的情况反馈至系统中，修复后检查数据是否正常回传；
g) 如服务器检查正常，则交回外场运维人员处理；
h) 如故障未解决，外场运维人员持续对未恢复的设备进行处理，直至故障修复；
i) 如故障已解决，则检查结束。

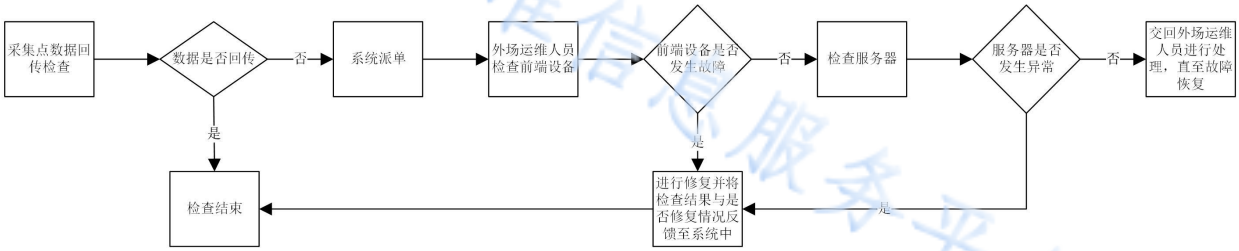

图2 采集设备运维管理流程图

7 软件系统运维管理

7.1 安装部署

安装部署功能要求如下：

a) 应提供图形化界面或自动安装脚本自动进行系统及服务组件的安装/卸载；
b) 应支持通过一种或多种方式进行服务部署，如模板、部署方案及自定义等方式；
c) 应支持集群部署时自动扫描或手动方式添加节点；
d) 宜支持安装前对软、硬件等进行配置和检测功能，如服务器、客户安装的操作系统等；
e) 应支持基于 X86 和非 X86 环境进行安装部署；
f) 应支持系统部署（安装/补丁/升级）失败给出修复方式，如重试、回退等方式；
g) 应支持安装/升级操作容错能力，不因个别节点的故障导致整个过程的失败；
h) 宜支持自动化打通集群内部节点无密 SSH 的能力；
i) 宜支持自动识别、格式化、挂载各类型磁盘的能力；
j) 应具备设置机房断电恢复后服务快速恢复运行的能力；
k) 应支持多集群多服务；
l) 应支持 JDK、数据库、Kerberos 认证等部件的预集成；
m) 应支持与第三方管理平台对接或提供开放 API，方便用户自定义服务组件接入；
n) 宜支持管理节点主备部署方式，主节点失效不影响对外功能；
o) 宜支持主备机自动切换，当主节点失效时，备节点主动接管主节点服务；
p) 应保证主备节点数据同步；
q) 应支持在集群不重启的情况下增加、删除节点；
r) 宜支持设置数据均衡，避免集群新增节点后将新数据均放到新节点；
s) 宜支持多种粒度的系统升级或补丁，同时不中断业务；
t) 宜支持服务器的大数据系统自动重装。

7.2 配置管理

配置管理功能要求如下：

a) 应支持图形化操作界面对系统的配置项进行管理，包括查看，修改，删除、自定义等；
b) 应提供特有配置参数的中英文命名和完整的解释；
c) 应支持多种方式对配置项进行管理，如：分类、分角色、分组等；
d) 应支持显示配置文件各配置项；
e) 应支持配置下的批量导入导出；
f) 应支持配置项或配置文件的上传、下载、更新；
g) 应支持滚动重启方式生效，不中断业务；
h) 应支持手动和自动方式推送配置项的更新给集群内相关节点；
i) 宜支持配置参数的历史版本、过期管理和回溯能力；
j) 应提供配置参数模板；
k) 应提供配置参数的默认值、阀值，针对可调参数应给出推荐值；
l) 宜支持角色组或实例组的管理，各个组下允许有不同的参数配置；
m) 应支持配置修改后同步到使用的客户端；
n) 应支持多种参数的配置能力，如部署路径、时钟同步、部署模式、安全模式、角色布局等参数；
o) 宜支持参数的相互影响识别，修改某参数对其它参数产生的影响给出提示或联动修改。

7.3 租户管理

租户管理功能要求如下：

a) 应支持以角色、用户、用户组的方式管理租户权限；

b） 应提供图形化界面管理角色、用户、用户组；
c） 应支持权限控制到服务内的资源，如表、目录、文件等资源；
d） 应支持租户管理，包括删除、创建等；

7.4 监控报警管理

监控报警管理功能要求如下：

a） 应支持对集群、主机、服务、实例等多维度运维对象监控；
b） 应支持对集群规模、资源使用情况、资源运行状态等进行监控；
c） 应支持对路由器、交换机、中间件、服务器、数据库等软硬件进行监控；
d） 应支持服务及服务组件监控指标的自定义；
e） 应支持监控项的定制功能，包括：展示方式，可视化的监控项等；
f） 应支持监控项的多种展示方式，包括：图形、表格、时间线等；
g） 应支持监控数据的导出、归档和清理等管理功能；
h） 应提供监控数据可视化报表的生成与导出功能，包括手动和自动两种方式；
i） 应支持图形化界面查看监控和报警，并支持按不同关键字查看；
j） 应支持报表能力，按照多维度提供资源统计报表，如：用户，租户，目录等；
k） 应支持数据汇聚和分析能力，给出数据的均值，最大值，最小值等；
l） 应支持与第三方管理系统对接，上传监控和报警等数据；
m） 应支持对不同级别报警信息设置处理优先级；
n） 应提供报警项定制功能，包括名称、级别、阈值等；
o） 应提供报警自动通知功能，如邮件、短信等方式；
p） 应支持故障自动检测并发送报警，故障恢复后报警能够自行消除；
q） 应支持故障修复后校验，以检查故障是否恢复成功。

7.5 服务管理

服务管理功能要求如下：

a） 应支持展示所有已安装服务及实例健康状态、运行状态等信息；
b） 应支持对服务、服务实例进行操作，如添加/卸载、启动/停止、强制停止、配置修改等；
c） 应支持服务进程挂起后自恢复的能力；
d） 应支持对服务进行升级，及升级失败后的自动回滚；
e） 应支持实时检查各服务进程的运行；
f） 应支持对服务配置的在线修改及同步；
g） 应支持可视化方式查看和下载指定节点服务角色的日志；
h） 应支持对分布式服务进行水平缩容/扩容的能力；
i） 应支持检测服务的可用性及发现问题时发送报警；
j） 应支持基于开源的大数据系统对开源组件原生 UI 的集成；
k） 应支持停止或重启某个服务时，上层服务联动一起停止或重启或给出提示；
l） 应支持通过各种策略（如分批，主备依次等）重启单个服务，同时不中断业务；
m） 应支持下载服务客户端；
n） 应支持服务和数据自动恢复到新增或者是更换之后的服务器。

7.6 日志管理

日志管理功能要求如下：

a） 应提供各类日志的收集与存储功能，如运行日志、操作日志等；
b） 应提供日志目录的管理功能，如更改日志存储空间、更改日志存储目录等；
c） 应提供图形化页面检索运行日志；
d） 应支持按照关键字段检索，如指定关键字、日志级别、服务、主机等；
e） 应提供日志的查询、过滤设置、导出等功能；
f） 应支持日志级别的设置功能；
g） 应支持操作审计能力。

7.7 日常管理

日常管理功能要求如下：

a） 应支持定期自动检查和手工检查；
b） 应支持对网络，服务器和操作系统的定期检查；
c） 应支持按照场景进行检查，如升级前检查；
d） 应支持输出检查报告；
e） 宜提供界面化的系统运行环境自动检查服务。