ICS
点击此处添加中国标准文献分类号

T/CPPC

团　　体　　标　　准

T/CPPC ××××—××××

营运车辆平台数据安全技术要求

Commercial Vehicles Platform Data&information Security Technology Requirement

点击此处添加与国际标准一致性程度的标识

文稿版次选择

××××－××－××发布　　××××－××－××实施

中国生产力促进中心协会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020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。

本文件由交通运输通信信息工程质量检测中心提出。

本文件由全国资产管理标准化技术委员会（SAC/TC 583）归口。

本文件起草单位：交通运输通信信息工程质量检测中心、长春吉大正元信息技术股份有限公司、北京诺君安信息技术股份有限公司，一汽解放，中寰卫星，T3出行，有为科技。

本文件主要起草人：×××、×××、×××。

本文件为首次发布。

引　　言

本标准针对营运车辆运营平台的数据的安全保护，从网络安全、应用安全、数据安全等方面规定了运营平台的安全防护总体技术要求。

营运车辆平台数据安全技术要求

1 范围

本标准适用于营运车辆的运营平台。

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 40856-2021 车载信息交互系统信息安全技术要求及试验方法

GB/T 22239信息安全技术信息系统安全等级保护基本要求

YD/T 3746-2020车联网信息服务 用户个人信息保护要求

YD/T 3751-2020车联网信息服务 数据安全技术要求

3 术语和定义

××××××界定的以及下列术语和定义适用于本文件。

3.1 车联网 Internet of Vehicle

简称IOV，是物联网在汽车行业领域的具体应用，车联网将物联网的范围限定到车与路、车与人、车与车以及车与传感设备上，各个车辆通过车载互联网设备经由无线网络、无线电等传播技术来实现车辆间、车辆与数据平台间的实时通信，汇总车辆的行驶信息、车辆周边的道路状况等动、静态信息，并将这些信息通过无线网络传输到信息中心进行加工、筛选、计算，再使用这些信息为车辆提供有效的引导、路况、信息共享、多媒体等综合网络服务，以满足车辆不同的功能需求。

3.2 IPS 入侵防御系统

IPS技术可以深度感知并检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对报文进行限流以保护网络带宽资源。

3.3 IDS 入侵检测系统

IDS是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。

3.4 PKI (Public Key Infrastructure)

中文叫做公开密钥基础设施，也就是利用公开密钥机制建立起来的基础设施，PKI指的是数字证书的制作和分发的一种机制。在这个机制的保障前提下，进行可信赖的网络通信。PKI的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

4 营运平台总体架构

营运车辆运营平台是基于企业车联网底层架构，利用互联网等信息通信技术，为企业营运业务开展提供基础能力支撑，帮助运营人员制定更为灵活高效的营运策略，同时也方便实现与政府监管机构营运车辆管理平台的数据对接。

4.1 运营平台架构

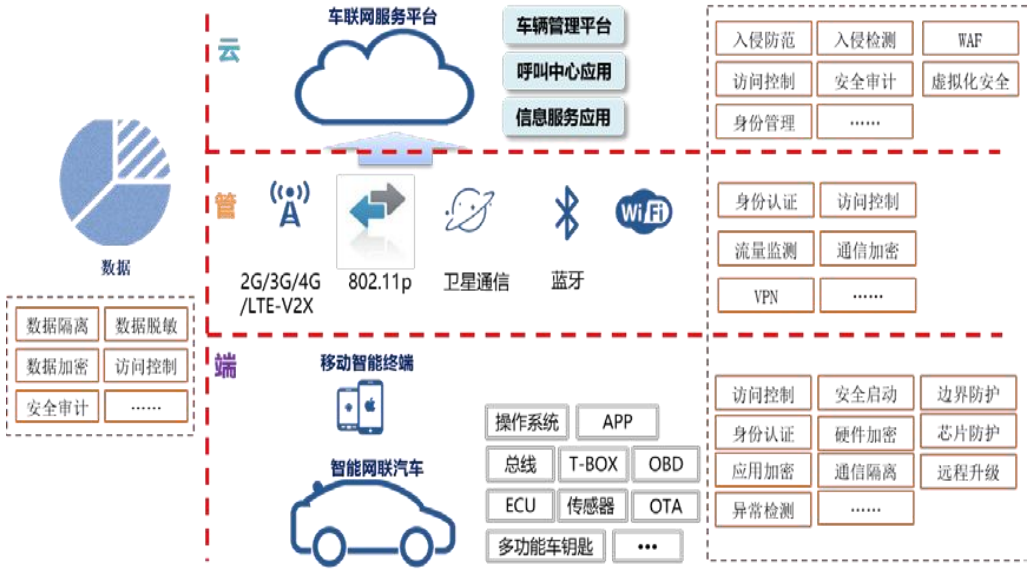

图 1 运营平台整体架构

如上图1示，运营平台仍旧架构于车联网“云、管、端”体系之上，其位于“云”端。

平台按照不同分层可包括基础设施层、应用层以及数据层。(如图2示)

基础设施是运营平台的底层基础资源（如服务器、网络、存储等），为平台提供底层运行支撑。

应用是运营平台所提供的各类应用场景服务，如各种web类服务、对外接口等，为平台实现各类运营管理提供基本支撑能力。

数据是运营平台所涉及的各类车联网营运数据，包括车端采集数据、三方交互数据等。涉及数据采集、传输、存储、使用及共享等全生命周期环节。

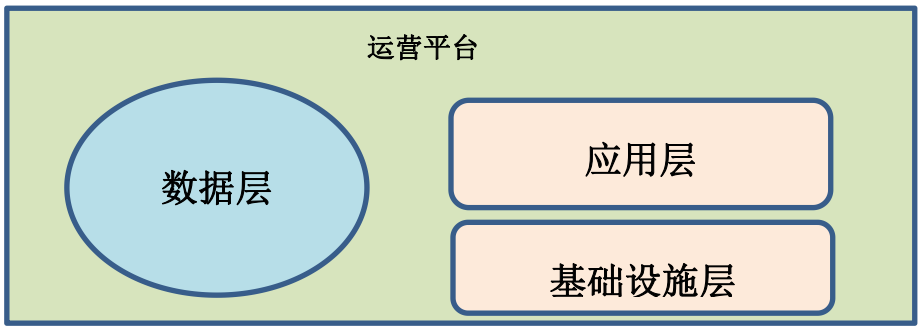

图2 运营平台分层

4.2 运营平台安全架构

图3 运营平台安全架构

运营平台的安全控制及合规模型以及新一代的自适应安全架构，与通用云平台安全相似，如图3示。

物理环境安全：在物理层，通过门禁系统、视频监控、环境监控、物理访问控制等措施实现云运行的物理环境、环境设施等层面的安全。

计算存储安全：通过对服务主机/设备进行安全配置和加固，部署主机防火墙、主机入侵检测，以及恶意代码防护、访问控制等技术手段对虚拟主机进行保护，确保主机能够持续提供稳定的服务。

可信计算：保证硬件、软件系统的行为/执行安全，包括安全的输入输出、内存安全、远程认证等服务。

网络安全：在网络层，基于完全域划分，通过防火墙、IPS、VLAN ACL 手段进行边界隔离和访问控制，通过 VPN 技术保障网络通信完整和用户的认证接入，在网络的重要区域部署入侵监测系统(IDS)以实现对网络攻击的实时监测和预警，部署流量监测和清洗设备以抵御 DDoS 攻击，部署恶意代码监测和防护系统以实现对恶意代码的防范。需要说明的是这里的网络包括了实体网络和虚拟网络，通过整体防御保障网络通信安全。

安全管理：根据 ISO27001、COBIT、ITIL 等标准及相关要求，制定覆盖安全设计与获取、安全开发和集成、安全风险管理、安全运维管理、安全事件管理、业务连续性管理等方面的安全管理制度、规范和流程，并配置相应的安全管理组织和人员，建立相应的技术支撑平台，保证系统得到有效管理。

信息安全：实现数据的保护，从数据隔离、数据加密、数据防泄露、剩余数据防护、文档权限管理、数据库防火墙、数据审计方面加强数据保护， 以及离线、备份数据的安全。

应用安全：保护应用的程序安全；通过 PKI 等机制对用户身份进行标识和鉴别，部署严格的访问控制策略；关键操作的多重授权等措施保护应用层安全；同时采用电子邮件防护、Web 应用防火墙、Web 网页防篡改、网站安全监控等应用安全防护解决方案确保特定应用的安全。

可信安全管理平台：包括建设并管理基于 PKI、身份管理等的安全基础支撑设施；管理平台综合利用成熟的安全控制措施，并构建良好的安全实现机制，保障系统的良好运转，以提供满足各层面需求的安全能力。

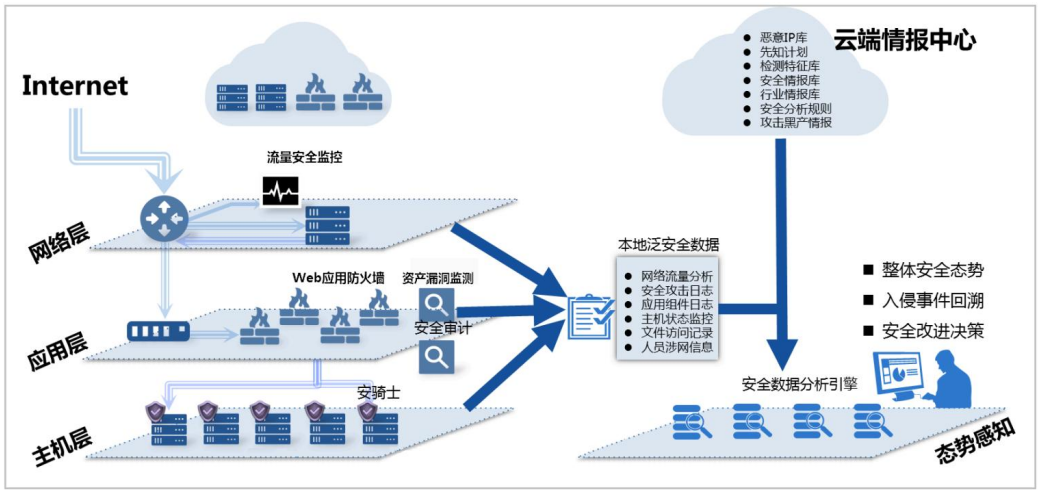

图4 典型运营平台安全拓扑

典型的运营平台安全架构拓扑如图4所示，平台基于等保三级安全技术要求，建设由外而内的纵深防御体系，包括DDOS安全防护、(云)防火墙、IPS/IDS、WAF、主机入侵检测(HIDS)、堡垒机、漏洞扫描、数据库审计、安全管理平台等安全系统措施。提升运营平台的整体安全防护水位，保障营运企业安全管理及业务安全稳定运营。

5 运营平台典型威胁

运营平台集合了地理信息服务和通信服务等现代计算机技术，为营运企业提供了全面的业务运营能力支撑。大多数运营平台是采用的公有云技术(基于企业自建私有云技术威胁及关注点类似)，平台直面云端的威胁，从威胁分类层面可以概括分为基础安全威胁、应用安全威胁以及数据安全威胁三大块，下面从这三方面威胁分别展开分析描述。

5.1 基础安全威胁

运营平台的底层基础设施基本组成为网络资源、主机资源及存储资源。各类基础设施资源面临的安全威胁不尽相同：

1.网络资源威胁

常见的网络威胁包括：

a）传统网络攻击如DDOS攻击等，可导致网络访问瘫痪，平台业务无法正常访问。

b）网络传输协议漏洞，如使用不安全的传输协议(如已过期的SSL协议、明文传输协议等)，可能进一步被利用导致业务系统的主机沦陷、通信劫持以及传输数据的泄露。

c）不合理的网络访问控制策略，无合理的平台业务系统的网络访问控制策略，会给予黑客或恶意用户更方便的入侵通道。

d）过多的端口暴露，非必要的网络端口暴露增加了平台的网络攻击面，给予黑客入侵更多的方式与可能性。

2.主机资源威胁

主机常见威胁包括：

a）恶意软件、病毒，通过在服务器主机植入恶意软件、病毒，可以实现黑客对主机的远程控制、主机文件加密勒索以及主机资源的恶意挖矿等，影响平台业务正常运行。

b）主机系统漏洞，利用服务器主机操作系统存在的漏洞，实现如虚机逃逸，进而控制运营平台的宿主机获取平台的核心接口、密钥、证书等关键信息，并可横向控制其他营运车辆。

c）缺失统一管控，主机的访问控制没有统一的隔离与管控，任意用户访问操作权限管控缺失，对主机管理带来极大安全威胁。

d）弱口令，弱口令是当下黑客最常见的入侵利用手段，如主机的管理密码存在弱口令将为主机的失陷埋下巨大隐患。

3.存储资源威胁

运营平台的存储一般分为结构化数据存储及非机构化数据存储。

对于结构化数据存储常见如数据库，潜在的安全威胁如弱口令、权限访问控制缺失、安全审计缺失、数据存储备份失效等。

对于非结构化数据存储常见如文件系统、公有云对象存储桶等，潜在的安全威胁如存储桶公有属性(public访问)滥用带来的敏感数据泄露、文件系统权限访问控制缺失等。

存储资源的安全威胁给平台业务运行带来的直接影响包括平台业务数据泄露、业务数据恶意操作等。

5.2 应用安全威胁

运营平台的应用系统整体上包括云端平台应用以及移动应用(APP)，两方面临的安全威胁如下分析：

1.平台应用

平台应用在车联网架构中是汽车以及手机之间的通讯中转站，广泛应用于车联网场景中，运营平台应用视各家企业运营模式不同，公开的暴露面威胁不一，但不论是互联网访问亦或是企业内网访问，作为平台应用自身面临的应用安全威胁如常见web类应用攻击，包括弱口令暴力破解、SQL注入攻击、逻辑漏洞、文件上传攻击、未授权访问等。一旦通过应用入侵成功，随之而来的风险包括敏感数据泄露、服务器失陷、横向其他车辆控制、管理后台失陷等。

2.移动应用

移动应用(App)是车联网运营平台的接入端，用户可以通过移动应用实现与运营平台以及与营运车辆的交互，如开车门、闪灯鸣笛等车控操作。在移动共享出行领域，手机app亦广泛应用于订单预约、取车还车等场景。

移动应用App因其易于获取且广泛使用的特点，往往会成为黑客的攻击入口，通过对App的破解、反编译等挖掘，获取密钥、证书等敏感信息，并分析通信接口，进一步入侵云平台和其他车辆。移动应用App常见的威胁包括反编译、二次打包、Activity劫持等。

5.3 数据安全威胁

运营平台作为整个车联网数据的处理中枢，涉及到各类数据，大致包括以下几大类数据：基础属性类数据(车辆基础属性、移动应用软件基础属性等)、车辆工况类数据、车控类数据、应用服务类数据以及可能涉及到司乘用户的个人信息。数据安全的威胁存在于数据生命周期的各个环节，对于运营平台而言，较高的数据安全威胁存在于数据传输、数据使用、数据共享及数据存储几个典型环节：

1.数据传输环节

车云通信、云云通信等典型传输环节，存在数据被截取、篡改致使数据的完整性及保密性遭到破坏的典型威胁。

2.数据使用环节

数据的分析、使用是运营平台典型的数据处理场景之一，如数据的提取、展示等业务活动，数据提取时如果未限制数据涉及人员范围、无有效的对于数据提取指令的审计则会存在较大的数据泄露的威胁，数据在运营平台使用展示时，如未对于敏感数据或用户隐私做相应的脱敏处理，账号权限的访问控制缺失或不合理则也会存在较大的数据泄露及数据滥用的风险。

3.数据共享环节

运营平台的业务可能会涉及到监管侧以及商业化的三方数据共享的场景，共享的数据可能会涉及到汽车数据以及个人信息等，特别是商业化的三方数据共享场景，如未对三方平台做事前严格的数据安全评估，三方平台自身数据安全防护能力不足，则可能会导致平台的数据及隐私泄露的风险。

4.数据存储环节

前面提到，运营平台的数据存储主要分为结构化数据及非结构化数据两类，其面临威胁同4.1章节“存储资源威胁”。

6 运营平台安全防护技术要求

对于运营平台的安全防护要求，整体遵从3.2章节的平台安全架构设计理念，基于管理加技术方向，建设由底层基础设施至上层应用的全面安全防护体系。

针对运营平台典型的三大类安全威胁（基础安全威胁、应用安全威胁、数据安全威胁），进一步详细阐明相关的防护技术要求。

6.1 基础安全防护

1.网络安全

运营平台的网络通信是所有信息服务的基础，对于传统网络边界应建设如DDOS防护能力以防范传统网络层的拒绝服务攻击以及IPS能力及时阻断网络流量攻击，另外需要加强 TCP/IP 协议各个层次的防范措施，对每个层次都实施加密技术，以保证网络的安全性服务。同时在车云网络通信过程中需采用基于PKI的认证机制对车辆和云平台进行双向认证，确保双方的合法性，从而保障整个信息接入与传输的安全。网络访问控制层面应按照业务系统实际情况做合理的区域隔离以及最小化开放端口管控，加强网络安全监测与审计，强化内部控制和安全保密策略，提高涉密人员的安全保护策略。同时还需要加强对网络信息的安全管理，实现信息传输的有效性和安全性。

2.主机安全

服务器主机是运营平台最基础的底层基础设施，所有服务器主机资源的访问控制应通过企业内部堡垒机统一运维管理，并针对主机的访问定期开展行为审计，及时发现并完善访问控制授权异常风险。针对主机系统漏洞问题，应定期更新漏洞列表，同时扩大漏洞收集途径，确保在第一时间内发现、解决并更新所有已知漏洞。另外一块非常重要的主机安全防护为主机的入侵检测能力，应为平台系统主机安装配置主机入侵检测防护软件(HIDS)，能够实时监测和阻断如恶意软件、病毒、反弹shell、恶意挖矿等安全威胁，保证主机系统平稳运行。

3.存储安全

针对运营平台的数据存储，常见安全防护技术措施包括：

a）存储加密，结构化数据如数据库，对于敏感数据或用户隐私信息，应采用一定安全等级的加密算法(常见加密算法如图5所示)，对相应的数据加密后落库安全存储，并通过如密钥管理系统(KMS)妥善保管加密密钥，确保数据存储的机密性。非结构化数据同样对于敏感、隐私信息，应对相应的文件或文件存储系统做加密后安全存储。

密码技术		国际标准	国内标准
加密	分组密码	AES、AES、3DES、IDEA	SM1(算法不公开)、SM4
	序列密码	RC4、A5	祖冲之序列密码(ZUC)
	非对称加密	RSA、Elgamal	SM2
认证	散列函数	MD5、SHA1、SHA-256、SHA-512	SM3
	数字签名	DSA、ECDSA	SM9

图5 常见密码技术

b）访问控制，对于平台结构化数据，应通过数据库堡垒机对平台数据的访问做严格的最小化账号访问控制授权。对于非结构化数据，则可以通过云平台对象存储后台，最小化授权子账号的访问与管理权限，确保数据的访问控制权限满足最小必要原则。

c）安全审计，应定期针对平台数据库以及文件系统的访问与操作进行安全审计，及时发现并治理高风险数据行为，同时可以设置高风险行为提醒和阻断策略，进一步降低数据安全风险。

d）备份与恢复，对于平台数据存储应考虑数据的备份与恢复机制，有条件企业应建立数据异地备份，并定期针对备份数据进行恢复演练，确保存储数据的完整性与可用性。

6.2 应用安全防护

1.应用站点安全

针对运营平台的应用站点（一般为web类站点），应采用WAF、RASP、网页防篡改等安全技术防护常见的应用安全攻击，保护应用程序安全，另外平台系统自身应配置登录强密码策略以及关键操作二次授权验证等措施保护应用层安全。

2.移动应用App安全

针对移动应用App的安全威胁，可通过采取移动应用App加固、代码混淆、以及移动应用App安全检测等技术来提升和保障移动应用的安全性。

6.3 数据安全防护

针对运营平台所涉及的风险较高的几个数据安全典型环节，分别建议安全防护措施如下：

1.数据传输安全

数据传输安全要求整体架构于5.1章节“网络安全”要求之上，采取安全通信协议及数据加密、签名等安全措施，保障平台数据传输过程的完整性与保密性。

2.数据使用安全

针对运营平台的数据提取、展示等使用场景，应采用数据脱敏、访问控制授权、安全审计等安全防护措施，以减缓平台数据使用过程中的滥用与泄露风险。

数据脱敏是数据使用过程中最常见的手段之一，平台系统应根据具体业务场景，依据数据使用目的以及脱敏等级要求，去选择相应的脱敏策略。常见脱敏方法策略如图6所示。

有条件的企业可建设平台的授权矩阵，按照最小必要原则建设和维护不同岗位的默认授权矩阵，进一步与账户生命周期管理系统相结合，实现访问控制授权线上化与自动化，减小授权的人工管理成本及账号权限风险。

脱敏方法	是否可逆	技术特点	主要技术	推荐处理对象	使用场景
遮盖脱敏	不可逆	不可见	*、#替换	数据构成规范	页面展示
哈希脱敏	不可逆	一一映射 结果长度固定	SHA散列 SM3散列 SM9标识	需要关联分析数据 登录密码、身份证存储	ETL处理流程 敏感数据交换 敏感数据存储
洗牌脱敏	不可逆	保留业务意义 脱敏后数据可用	数据重排 随机选择	无需关联、仅做统计的数据 (位置数据、设备信息)	数据运营分析 敏感数据存储
加密脱敏	可逆	可解密 内容不可见	AES加密 SM1加密	需要回源的数据	敏感数据存储 敏感数据传输
替换脱敏	部分可逆	保留数据业务意义 映射码表替换可逆	映射替换(凯撒密码) 随机替换	构成规则固定的数据	运营分析数据处理 敏感数据存储
变换脱敏	部分可逆	通过数学运算对数值型数据处理	取整 小数点位截取	数值类型的数据	敏感数据分析统计

图 6 常见脱敏方法策略

3.数据共享安全

针对运营平台两类典型的数据三方共享场景，基本安全防护要求为：

a）监管侧数据共享，原则上遵从监管要求的共享数据要求，建议仍遵从共享数据最小必要原则，并通过专线、VPN 等安全传输通道实现监管侧的数据共享。

b）商业化数据共享，事前应对三方进行全面的数据安全能力及资质评估，确保对方数据安全保护能力能够满足共享数据的安全保护要求。对于合作的共享数据需进行最小必要性评估并确保满足国家相关法律法规要求。数据共享技术宜采用隐私求交、联邦学习、多方安全计算、可信执行环境等隐私计算能力，确保共享数据的安全性。

4.数据存储安全

运营平台的数据存储安全技术要求同 5.1 章节“存储安全”所述安全防护要求。

参 考 文 献

[1] YD/T 3752-2020 车联网信息服务平台安全防护技术要求
[2] 车联网网络安全白皮书（2020年）
[3]
[4]
[5]

索　　引