ICS
点击此处添加中国标准文献分类号

T/CPPC

团　　体　　标　　准

T/CPPC ××××—××××

监管服务平台数据安全检测技术要求

Supervision Service Platform Data&information Security Test 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监管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监管平台的安全防护总体技术要求。

监管服务平台数据安全检测技术要求

1 概述

监管服务平台属于车联网“云、管、端”架构体系的“云”平台，其按照不同分层可分为基础设施层、数据层、计算层以及服务层，本检测技术规范主要围绕平台的分层结构，对相应的分层资源的安全防护情况进行具体检测评估。

基础设施层重点检测评估网络资源、主机(服务器)资源、存储资源；应用层重点检测评估平台站点安全、移动应用 APP 安全；数据层主要从数据传输、数据存储、数据使用以及数据共享等几个重点环节进行安全检测评估。。

2 检测技术规范

2.1 基础设施层

资源类别	安全措施分类	具体检测技术规范
网络资源	网络结构安全	a)应根据运营平台服务的类型以及功能的不同划分不同的子网、网段或安全组，并为各子网、网段合理分配易于管理和控制的地址段。
		b)应避免将平台重要业务网段部署在网络边界且直连外部系统，重要网段与其他网段之间采取可靠的技术隔离措施。
	访问控制	a）应在网络边界部署访问控制设备并启用访问控制功能，或通过云安全组设置访问控制策略。
		b）应能根据网络会话状态信息为数据流量提供明确的允许/拒绝访问的能力。
		c)应根据平台实际业务情况，合理限制网络最大流量以及最大连接数。
	网络入侵防御	a）平台应具备 DDOS 网络攻击防护能力，应能持续对大流量攻击进行识别、告警和清洗阻断。
		b)应在平台网络边界处持续检测如端口扫描、木马后门、拒绝服务及 IP 碎片等攻击行为。
		c）当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目标、攻击时间等基本事件信息，在发生严重入侵事件时应及时告警。
		d）应在平台网络边界处对恶意代码进行持续监测与清除防御。
	安全审计	a)应对平台系统网络中的网络设备运营状况、网络流量、用户行为等进行日志记录。
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功以及其他与审计相关信息。
		c)应对审计记录进行保护，在有效期内避免受到未授权的删除、修改或覆盖等。
	网络设备安全	a）应对登录网络设备的用户进行身份鉴别。

		b）网络设备用户的标识应唯一。
		c）身份鉴别信息应不易被仿冒，口令应具备复杂度要求并定期更换。
主机(服务器)资源	身份鉴别	a）应对登录运营平台服务器的用户进行身份标识和鉴别。
		b）服务器身份鉴别信息应不易被仿冒，口令应具备复杂度要求并定期更换。

		c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自由退出等措施。
		d）应采用双因素(2FA)或多因素(MFA)鉴别技术对登录服务器用户进行身份鉴别。
	访问控制	a）宜通过企业堡垒机统一管理管控服务器，对服务器访问用户进行授权控制。
		b）应根据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。
		c）应关闭服务器不使用的服务端口，减小攻击面。
	主机入侵防御	a）应安装防恶意代码软件，并及时更新恶意代码软件版本和恶意代码库。
		b）服务器操作系统应遵循最小安装原则，仅安装需要的组件和应用程序，并保持系统补丁能够及时更新。
		c)应能检测到对平台服务器的入侵行为，并记录攻击源IP、攻击类型、攻击目标、攻击时间等基本事件信息，在发生严重入侵事件时应及时告警。
	安全审计	a）审计范围应覆盖到服务器及堡垒机上的每个用户。
		b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件。
		c）审计记录应包括事件的日期、时间、类型、主体标识、主体标识和结果等。
		d）应保护审计记录，在有效期内避免受到未授权的删除、修改或覆盖等。
存储资源	存储数据保护	a）应采取如加密、单独存储等技术措施，实现存储的平台重要数据和敏感数据的保密性。
		b）应能检测到平台系统管理数据、鉴别信息及重要业务数据在存储过程中完整性受到破坏，并能采取必要的恢复措施。
	备份与恢复	a）应对运营平台相关的关键数据（如业务数据、系统配置数据等）有必要的容灾备份。
		b）应提供本地数据备份与恢复功能，完全数据备份至少每天一次。
		c）应提供异地数据备份功能，利用安全通信网络将关键数据定时传送至备份存储资源。
		d）分布式存储要保证数据副本在不同的物理机上或者不同的存储上。

2.2 应用层

应用类别	安全措施分类	具体检测技术规范

平台应用	应用环境安全保护	a）平台应用应部署 WAF、网页防篡改等应用安全防护措施，阻止 web 类攻击以及避免相关数据和页面被篡改和破坏。
		b）应对平台通信过程中的敏感信息进行加密传输，避免应用数据篡改、泄露。
		c）应能够对平台应用服务水平持续监控，并在指标降低到相应阈值时及时告警。
	身份鉴别	a）应采用一种或一种以上组合的鉴别技术来进行身份鉴别，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被仿冒。
		b）平台应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。
	访问控制	a）平台应提基于用户账号权限的访问控制功能，依据对应的安全策略控制用户对业务应用的访问。
		b）应严格限制平台应用之间的相互调用权限，依据相应安全策略要求控制应用对其他应用用户数据或特定指令等资源的访问与调用。
	安全审计	a）平台系统应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件(如业务应用关键操作、重要行为等)进行审计。
		b）审计记录的内容应包括事件的日期、时间、类型、主体标识、描述和结果等。
		c)应对审计记录进行保护，在有效期内避免受到未授权的删除、修改或覆盖等。
移动应用 APP	APP 基础安全保护	a）APP 应用不存在非授权收集或泄露个人敏感信息、非授权数据外传等恶意行为。采集用户数 据、敏感信息时，应告知用户采集目的和范围，取得授权同意，并提供关闭数据采集的功能。
		b）APP 的登录如采用账号密码机制，应至少使用包括数字、大小写字母、长度不少于 8 位的强复杂度口令。
		c）APP 端侧应采用加密等安全措施存储个人敏感信息，避免明文存储。
		d）APP 应用对外传输个人敏感信息时，应采用数据加密传输方式。
		e）APP 应用应对个人敏感信息进行脱敏等防护后写入应用日志，并对日志文件进行安全存储。
	代码安全保护	a）应用软件(APP)安装包应采用代码签名认证机制。
		b）APP 发布后不应包含调试功能及调试信息且在非调试场景或调试模式下，应用软件日志不应包含调试输出。

		c）建议采用相关安全机制（例如：混淆、加壳等），防止被逆向分析。
	运行安全保护	a）APP 软件应保证其稳定运行，避免出现功能失效等现象，且能处理可预知的错误操作，不应影响程序的正常工作。
		b）APP 软件的运行对终端设备的资源不应长时间固定或无限制占用。
		c）软件应支持更新升级，至少采取一种安全机制，保证升级的时效性和准确性；

2.3 数据层

数据活动	安全措施分类	具体检测技术规范
数据传输	传输保密性	a）应采用加密或其他有效措施实现运营平台的敏感数据或个人隐私数据传输的保密性。
	传输完整性保护	a）平台系统应能够检测到敏感数据在传输过程中的完整性被破坏，并能采取必要的恢复措施。
	通信合法性	a）营运车辆与运营平台的车云通信应采用基于PKI的机制对车辆和云平台进行双向认证，确保通信双方的合法性。
数据存储	存储数据安全保护	具体检测条目同 2.1 章节“存储资源”部分所述规范。
数据使用	数据系统展示安全	a）运营平台系统应依据数据使用目的及脱敏等级要求，针对平台敏感数据或个人隐私等数据在系统页面展示时进行脱敏处理。
		b）对数据的脱敏操作应当由后台应用完成，而不是由前端页面处理。
		c）在不影响系统页面查看的情况下，应采用明水印技术，防止重要数据的截图和拍照。
	数据下载导出安全	a）运营平台如提供数据下载、导出等功能，应默认需针对敏感数据以及用户个人信息进行脱敏处理。
	访问控制权限	a）应统一管理和维护运营平台账号、角色对应权限，基于最小必要原则进行访问控制授权，且应实现系统不同账号权责分离。
		b）数据的导出、下载应配备相应的审批流程。
数据共享	安全评估	a）应对数据共享的第三方进行数据安全能力及技术方案评估。
	共享通道安全	a）与三方共享数据应通过安全可信方式进行数据传输，如采用专线、VPN 或 HTTPS 等加密传输通道。
		b）共享数据双方应对接口、服务调用有一定的认证措施。

	安全监控	a）应对平台共享数据接口进行技术监控，如调用量、调用频率、调用来源等。

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