ICS 35.030
CCS L 80

DB4403

深 圳 市 地 方 标 准

DB4403/T 426—2024

智能网联汽车网络安全技术要求

Technical requirements for network security of intelligent connected vehicles

2024-01-22 发布　　2024-02-01 实施

深圳市市场监督管理局　　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。

本文件由深圳市政务服务数据管理局提出并归口。

本文件起草单位：深圳市信息安全管理中心、杭州安恒信息技术股份有限公司、鹏城实验室、深圳市未来智能网联交通系统产业创新中心、同济大学、比亚迪汽车工业有限公司、深圳市智慧城市通信有限公司、深圳市腾讯计算机系统有限公司、深圳美团科技有限公司、深圳安途智行科技有限公司、北京轻舟智航科技有限公司。

本文件主要起草人：李苏、董安波、林宇群、穆端端、赵剑、轩豪男、束建钢、周亚超、蒋洪林、张雷、毕欣、赵贵权、马登辉、郑恬静、何淑婷、马鑫、苑广勇、倪平、曹阳、秦孟强、张晓超。

智能网联汽车网络安全技术要求

1 范围

本文件提出了智能网联汽车网络安全总体框架，规定了车载终端安全要求、通信安全要求、应用服务安全要求、数据安全要求、网络安全保障要求。

本文件适用于指导智能网联汽车相关生产方、运营方、服务提供方等对智能网联汽车网络安全的建设和实施。

注：在不引起混淆的情况下，本文件中的“汽车”“车”“车辆”均为“智能网联汽车”。

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 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39786—2021 信息安全技术信息系统密码应用基本要求

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 40861—2021 汽车信息安全通用技术要求

YD/T 3751—2020 车联网信息服务数据安全技术要求

DB4403/T 271—2022 公共数据安全要求

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

智能网联汽车 intelligent connected vehicle

利用车载传感器、控制器、执行器、通信装置等，实现环境感知、智能决策和/或自动控制、协同控制、信息交互等功能的汽车的总称。

注1：环境感知、智能决策、自动控制以及协同控制等功能一般称为智能功能，其中协同控制功能一般需要网联功能支持。

注2：车辆利用通信技术实现与外界信息交互的功能称为网联功能，“外界”是指车辆自身范畴以外，例如穿戴设备等属于“外界”的范畴。

注3：具备智能功能的汽车称为智能汽车，具备网联功能的汽车称为网联汽车。

3.2

车载终端 on-board terminal

安装于智能网联汽车上，具有信息的采集、处理、存储、传输等功能的车载信息设备。

4 缩略语

下列缩略语适用于本文件。

C-V2X：蜂窝车联网（Cellular-V2X）

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

DSRC：专用短程通信（Dedicated Short Range Communications）

OBD：车载诊断系统（On-Board Diagnostic）

OBU：车载单元（On board Unit）

RFID：射频识别（Radio Frequency Identification）

TLS：安全传输层协议（Transport Layer Security）

USB：通用串行总线（Universal Serial Bus）

V2X：车对车、车对外界的信息交换（Vehicle to Everything）

Wi-Fi：无线保真技术（Wireless Fidelity）

3G：第三代移动通信系统（3rd Generation）

4G：第四代移动通信系统（4th Generation）

5G：第五代移动通信系统（5th Generation）

5 网络安全总体框架

智能网联汽车网络安全总体框架主要根据智能网联汽车的基本构成进行划分，分为车载终端安全要求、通信安全要求、数据安全要求、应用服务安全要求和网络安全保障要求，智能网联汽车网络安全总体框架见图1。

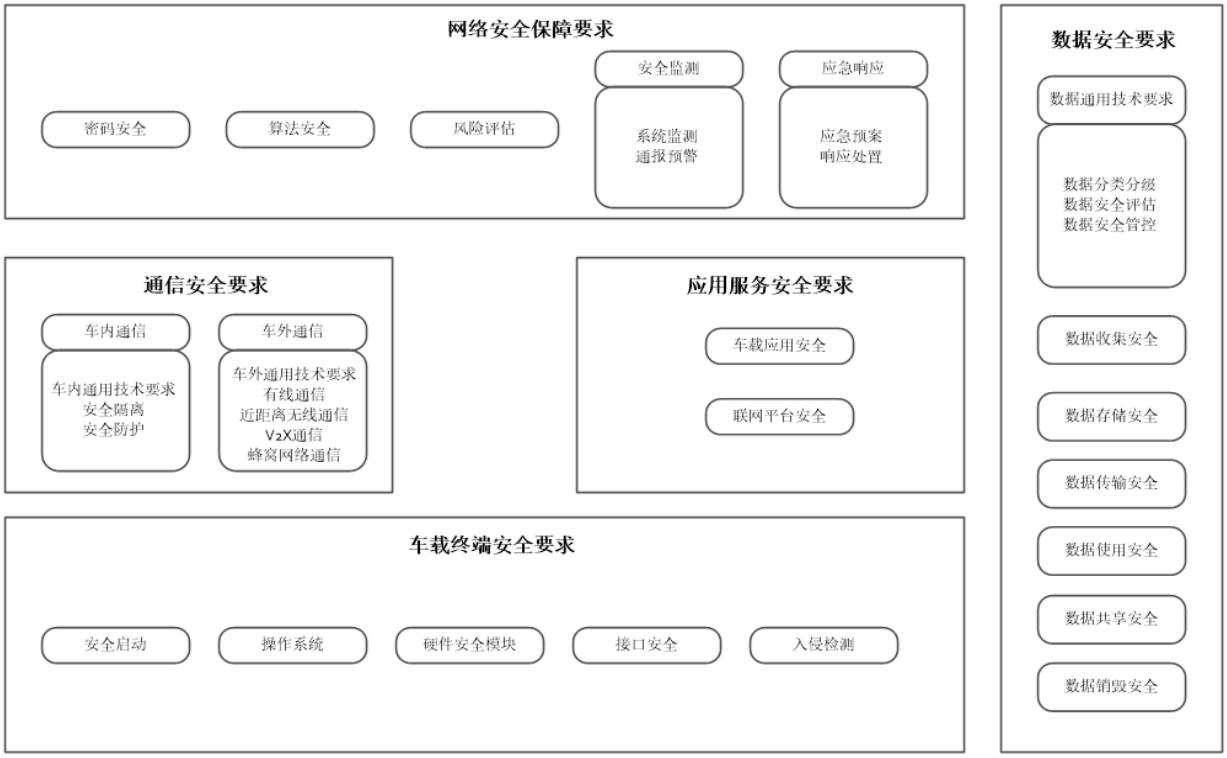

图1 智能网联汽车网络安全总体框架

6 车载终端安全要求

6.1 安全启动

支持安全芯片的车载设备应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。故障注入、侧信道攻击防护要求。

6.2 操作系统

操作系统安全要求如下：

a) 应具备权限管理机制和身份识别与鉴权，删除非必要账户，限制提权操作；
b) 应具备访问控制机制，依据安全策略控制用户账号、进程等主体对客体的访问；
c) 应仅允许必要端口对外开放，关闭不必要的端口、进程或服务；
d) 应对开发者调试接口进行管控，避免非授权访问；
e) 应具有内存保护机制以降低缓冲区溢出攻击等风险；
f) 不应存在未经处置的国家权威漏洞平台公开发布 6 个月及以上的高危安全漏洞；
g) 系统升级时，应建立升级设备与升级服务器或者离线升级设备之间的认证机制，认证机制宜采用双向认证机制；
h) 系统升级时，应对升级包进行完整性和合法性的验证，防止升级包被恶意篡改。

6.3 硬件安全模块

硬件安全模块安全要求如下：

a) 可通过密码学算法确认使用者身份，如通过外部授权（对称验证）或非对称验证等方式实现；
b) 应设置权限管理机制，确定权限类别、访问权限属性和权限范围。

6.4 接口安全

接口安全要求如下：

a) 硬件调试接口和硬件测试接口应禁用或采用安全访问控制措施；
b) 具备刷写功能的 OBD 诊断接口应具备身份鉴别功能；
c) 板载芯片及印制电路板不应存在对芯片内存进行访问或者更改芯片功能的隐蔽接口；
d) 不应存在隐藏的系统通信接口；
e) 应采用身份鉴别和访问控制措施实现对系统通信接口的访问；
f) 宜记录关键接口的操作日志。

6.5 入侵检测

车载核心设备具备入侵检测功能，其安全要求如下：

a) 应检测是否存在被 Dos/DDos 攻击、后门连入、异常来源用户访问以及其他异常连接信息；
b) 应检测是否存在被移植恶意程序所导致的系统资源异常消耗；
c) 应检测是否存在后门或可调式的应用，如 knockd、qconn 等，是否有其他未知、恶意进程存在；
d) 应检测是否被上传恶意文件，或文件篡改行为；
e) 应检测是否对系统关键配置的增删改进行监控，防止如域隔离策略被删除的情况；
f) 在检测到入侵行为时应进行告警、记录；
g) 可通过在线升级或离线升级方式，实现对特征库、规则文件等的升级；

h) 宜具备网络流量审计机制，对汽车内部正常通信流量和异常流量进行实时监测，并提供分析统计和告警；
i) 宜具有网络安全监测机制，对各种网络行为进行实时监测，发现报文异常、系统入侵、异常流量攻击等，并提供分析统计和警告等安全响应动作；
j) 应对智能网联汽车系统运行异常、配置异常、通信异常、越权访问、系统资源异常、流量异常、用户异常、文件未授权访问、文件未授权修改进行监测；
k) 应对智能网联汽车数据异常、数据伪造、数据窃取、日志异常进行监测；
l) 应识别来自蜂窝网络的非法连接请求，过滤恶意数据包。

7 通信安全要求

7.1 车内通信

7.1.1 车内通用技术要求

车内通信应符合GB/T 40861—2021中6.3.1.4规定的技术要求。

7.1.2 安全隔离

安全隔离要求如下：
a) 汽车内部网络的设计，应根据各个功能区域的重要程度、安全属性等因素，将车内网络划分为不同安全区域，各安全区域之间应进行网络隔离；
b) 各安全区域之间应建立安全的访问路径，防止非授权访问，宜采用边界访问控制机制对来访的报文进行控制（如采用报文过滤机制、报文过载控制机制和用户访问权限控制机制等）。

7.1.3 安全防护

报文安全防护要求如下：
a) 车内关键通信报文应保障汽车内部通信报文的完整性、真实性、合法性和机密性，防止报文被篡改和伪造；
b) 车内关键通信报文应具备防止重放攻击机制，如新鲜值机制保护报文的时效性；
c) 应具有密钥和证书的管理功能，对用于安全通信的密钥和证书进行全生命周期的管理；
d) 应对重要信息安全告警生成日志记录，应将日志进行权限访问限制，避免日志记录被篡改。

7.2 车外通信

7.2.1 车外通用技术要求

车外通信通用技术要求应符合GB/T 40861—2021中6.3.2规定的技术要求。

7.2.2 有线通信

有线通信是通过USB、OBD等介质接口与车内网络进行通信，其安全要求如下：
a) 应采取访问控制措施限制OBD接口对重要服务的访问请求，防止攻击者通过OBD接口对汽车总线网络进行攻击；
b) 宜采用身份认证来确保接入OBD接口的设备为合法授权的设备，防止黑客通过未授权的OBD设备攻击汽车总线网络；
c) 应对USB端口接入设备中的文件进行访问控制，只允许安装或执行指定签名的应用软件。

7.2.3 近距离无线通信

近距离无线通信是通过Wi-Fi、蓝牙、RFID等通信信道在车载网络中进行通信，其安全要求如下：

a) 应具备启用与关闭近距离无线连接的管理功能；
b) 应对请求连接的设备进行访问控制；
c) 已建立的短距离通信，应在相应的输出设备上有明确的连接状态显示；
d) 车载端的应用调用短距离无线连接功能时，车载端应明示用户，并提供配置能力和符合场景的配置方式；
e) 应使用安全协议进行通讯。

7.2.4 V2X 通信

V2X通信是OBU设备通过C-V2X、DSRC等通信信道在车载网络中进行通信，其安全要求如下：

a) 应具备符合标准的身份标识，并可以对所连接的通信节点的设备进行身份验证；
b) 应使用注册证书和假名证书相结合的方式，为 V2X 消息提供数字签名服务。其中，注册证书是车辆或者行人参与 V2X 直连通信的身份凭证；假名证书用来对 V2X 直连通信发送的消息进行数字签名；
c) 证书由云端管理系统进行统一分发，参与 V2X 直连通信的车辆或者行人按照流程向云端系统提供身份信息，在通过身份认证后可获得相应的注册证书，并进一步获得假名证书；
d) 云端管理系统和 V2X 通信设备均应申请支持显式证书、隐式证书等多种方式，具体采用的方式由云端管理系统和 V2X 通信设备协商确定；
e) OBU 设备应依据云端管理系统下发的安全策略使用安全服务，并保持与云端管理系统的同步更新；
f) OBU 设备宜具备向云端管理系统上报有恶意行为的 V2X 通信设备的能力；
g) OBU 设备应对所接收到的其它 V2X 通信设备发送的数据进行签名验证，并且只对通过验证的数据进行进一步的处理；未通过验证的消息将被丢弃；
h) OBU 设备应支持使用安全运行环境、安全单元或安全处理器等对敏感信息（如密钥、证书等）的保护；
i) 宜保护 V2V/V2I 通信终端的匿名性和隐私性，保证 V2X 设备不应被未经监管机构或用户授权的一方在该区域追踪。

7.2.5 蜂窝网络通信

蜂窝网络通信是通过3G、4G、5G等通信通道在车载网络中进行通信，其安全要求如下：

a) 与网络侧通信设备之间建立通信连接，宜充分使用通信技术提供的认证鉴权、加密解密等安全机制，平台侧应具备对接入请求进行二次鉴权的能力，确保接入真实可靠的网络和请求接入的合法性；
b) 与核心业务平台的通信信道，应与公网逻辑隔离；
c) 应采取技术措施，不应使用功能需求范围外的蜂窝网络通信功能。

8 应用服务安全要求

8.1 联网平台

联网平台安全要求如下：

a) 保障联网平台基础设备安全，对设备的物理端口、服务端口和系统资源等进行实时监控，出现问题及时上报和处理，确保系统的稳定性和可靠性；
b) 联网平台应进行安全域划分，并在边界部署防火墙或在核心交换机上配置防火墙模块、访问控制策略（如：IPS 入侵防御系统、ACL 访问控制列表等）实现访问控制；
c) 联网平台定期检测服务器的操作系统、数据库系统配置等，识别安全隐患，评测安全风险，提供改进措施；
d) 联网平台应对通信接口进行访问控制，防止非法终端接入、非法数据注入等；
e) 联网平台与客户端的通信应使用 TLS 1.2 及以上版本传输；
f) 联网平台应在边界部署 WEB 攻击防范设备，如 WEB 应用防火墙，实现对 WEB 攻击的检测和阻断，防止接口越权控制、SQL 注入、XSS 攻击、越权漏洞利用、暴力破解、文件上传漏洞利用、CSRF 等；
g) 联网平台本地存储的敏感数据应进行加密；
h) 联网平台应采用 IDS 对客户端传输的数据进行检测；
i) 联网平台宜对平台状态、行为、数据变化进行监控，检测异常行为并及时告警。

8.2 车载应用

车载应用安全要求如下：

a) 应对第三方应用的访问权限及资源进行访问控制，对控制外的应用安装应提示风险、控制访问权限；
b) 不应存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞；
c) 不应在代码中硬编码密码、密钥等内容；
d) 应符合GB/T 40856—2021中5.4.2规定的应用软件代码安全要求。

9 数据安全要求

9.1 数据通用技术要求

9.1.1 数据分类分级

数据分类分级要求如下：

a) 按 GB/T 35273—2020、DB4403/T 271—2022、YD/T 3751—2020 描述的要求，制定本组织的数据分类分级和安全保护制度，特别是智能网联汽车相关个人信息和重要数据的识别和保护策略；
b) 按 DB4403/T 271—2022 描述的内容形成数据资产清单，并明确数据资产类型、数据量、存放位置、数据关联系统、数据共享情况、数据出境情况等。

9.1.2 数据安全评估

数据安全评估要求如下：

a) 涉及处理敏感个人信息或者国家规定的重要数据、核心数据的机构，应定期开展风险评估，并向有关主管部门报送风险评估报告；
b) 涉及数据安全合规监管的相关机构，应定期开展数据安全合规性评估，并向有关主管部门报送合规性评估报告；

c） 个人敏感信息处理、个人信息自动化决策、委托处理、他人提供（含境外）、公开等对个人权益有重大影响的个人信息处理活动，应事先开展个人信息保护影响评估，评估记录至少保存三年。

9.1.3 数据安全管控

数据安全管控要求如下：

a） 针对不同的数据保护级别，依据数据保护策略实施相应级别的数据访问权限、数据防泄漏、数据接口管控；
b） 在适用于安全管控的终端层面及时对异常数据操作行为进行预警；
c） 宜在网络层面对异常数据操作行为及时定位和阻断；
d） 宜在硬件层面对可能造成数据泄露或异常的物理行为进行物理层面的阻断。

9.2 数据收集

数据收集安全要求如下：

a） 在平台收集之前，对收集设备及软件应使用身份鉴别技术进行双向身份认证，确保收集设备是用户所允许的，不应未经授权访问和非法使用用户个人信息；
b） 对不同等级的数据使用不同的收集标准，应对敏感数据设置高等级的收集要求；
c） 收集前应对数据类型进行确认，并确保不同类型数据收集的合法性和机密性，收集数据类型包括重要数据、个人信息和一般数据等；
d） 测绘地理信息、高精度定位等相关国家安全的重要数据，应向相关监管机构进行报备；
e） 与用户身份、位置信息等相关的个人信息，应通过显式的方式告知用户并获得用户明示同意，并说明数据收集所依据的国家法律法规及业务需求；
f） 可能影响人员及车辆安全的重要数据的收集，应进行签名并加盖时间戳；
g） 对用户数据的收集应在提供相应服务的同时进行。若业务需要事先收集相关数据，应向用户明示事先收集的目的和范围，并且在用户同意的情况下方可继续；
h） 收集用户使用行为等用户数据时，应提示用户并向用户提供关闭数据收集的功能；
i） 对于软件中非应用必需的数据收集，系统应进行适当的干预，比如娱乐导航等应用软件不能访问车机系统的敏感数据；
j） 收集的个人信息的类型应与业务功能有直接关联；
k） 自动收集个人信息的频率应是实现服务的业务功能所必需的最低频率；
l） 间接获取个人信息的数量应是实现服务的业务功能所必需的最少数量。

注：直接关联是指没有该等信息的参与，产品或服务的功能无法实现。

9.3 数据存储

数据存储安全要求如下：

a） 敏感数据应存储在安全存储区域，或为敏感数据设置适当的访问权限，只允许被授权的应用访问；
b） 存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅存储摘要信息；
c） 设备中的口令、密钥等敏感数据应以非明文方式存储；
d） 对被授权访问数据的人员应建立授权的访问控制策略，使其只能访问职责所需的信息，且仅具备完成职责所需的数据操作权限；

e) 应控制敏感数据（如输入的账号密码信息、指纹信息等）的使用范围和使用时间，保证敏感服务不被非法使用。若超出服务范围和使用时间则设备应退出敏感服务并返回到正常模式；
f) 未向用户明示或未经用户同意不应擅自修改用户数据；
g) 个人信息保存期限应为实现个人信息主体授权使用的目的所必需的最短时间，超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理；
h) 传输和存储个人敏感信息时，应采用加密等安全措施；
i) 应提供数据的备份与恢复功能，定期备份重要数据；
j) 车辆信息系统中的应用配置数据等应具有备份，应用异常时可使用备份数据恢复；
k) 应具备相关的灾难恢复机制，保证业务的持续性；
l) 数据的存储期限应满足保存六个月的要求。

9.4 数据传输

数据传输安全要求如下：
a) 车载终端上传数据到云端服务器，车辆身份标识应做匿名化处理，匿名后标识唯一，不重复；
b) 应采用校验技术或密码技术保证通信过程中重要数据的完整性；
c) 应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。

9.5 数据使用

数据使用安全要求如下：
a) 使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意；
b) 保障数据在授权范围内被访问、处理，防止数据被窃取、泄露、删除；
c) 根据数据使用过程中数据安全需求设立数据安全域，同一安全域应具有相同的访问控制和边界控制策略，保证数据的安全；
d) 在数据使用的过程中，应使用数据脱敏等技术防止隐私信息泄露；
e) 对数据使用的日志应进行管理和审计。

9.6 数据共享

数据共享安全要求如下：
a) 应对数据的共享行为进行授权和管理；
b) 敏感数据向第三方分享过程中，应采用数据去标识化技术，保障数据分享安全；
c) 有效管理数据共享行为，防范数据共享过程中被窃取或者泄露。

9.7 数据销毁

数据销毁安全要求如下：
a) 建立数据销毁与删除规程，明确数据销毁与删除场景、方式及审批机制，设置相关监督角色，应记录数据销毁与删除操作过程；
b) 委托数据合作方完成数据处理后，应及时销毁委托相关的数据，法律、法规另有规定或者双方另有约定的除外；
c) 根据要求、约定删除数据或完成数据处理后无需保留源数据的，应及时删除相关数据；
d) 当运营主体停止运营其产品或服务时，应及时停止收集相关数据并对所持数据进行删除或匿名化处理。

10 网络安全保障要求

10.1 密码安全

密码安全要求如下：

a) 用于车载设备中使用的密码产品和密码服务，应符合GB/T 39786—2021附录A的要求；
b) 用于车载设备中使用的密钥的全生命周期管理，应符合GB/T 39786—2021附录B的要求；
c) 应支持商用密码算法，包括但不限于SM2、SM3、SM4、SM9。

10.2 算法安全

算法安全要求如下：

a) 所使用的相关算法应采用国家或行业主管部门批准使用的，安全有效期内未被破解的算法；
b) 应采用具有足够强度的算法和足够长度的密钥进行密码运算，对称算法不低于128位，非对称算法不低于2048位；
c) 应使用安全区域或硬件安全模块保护密钥的安全性。

10.3 风险评估

风险评估要求如下：

a) 应建立智能网联汽车网络安全风险评估机制，包括确立评估标准、评估执行主体、评估内容、评估周期等；
b) 应识别和管理车型产品与供应商相关的风险；
c) 应确认车型的关键要素，对车型进行详细的风险评估，应处理及管理已识别的风险；
d) 应对风险评估的结果采取相应的处置措施保护车型不受风险评估中已识别的风险影响。若相应的处置措施与所识别的风险不相关或不充分，车辆制造商应确保实施其它适当的处置措施，并说明其采取措施的合理性。

10.4 安全监测

10.4.1 系统监测

系统监测要求如下：

a) 应支持违规或异常监测结果的分析、告警、汇总、统计、展示；
b) 宜支持根据分析结果进行风险计算；
c) 应支持异常行为回溯分析；
d) 宜具备展示攻击事件的能力，如相同事件名称攻击的目标排行、事件源地址攻击目标排行、事件目的地址的攻击源排行、相同车型受攻击的目标排行等。

10.4.2 通报预警

通报预警要求如下：

a) 应具备多渠道预警信息通报、信息上报、网络安全事件处置过程支持和跟踪、通报数据统计等功能；
b) 预警内容应包括预警级别及其事件性质、威胁方式、影响范围、涉及车型、影响程度、防范对策等信息等；
c) 应对当前告警和历史告警详细信息的展示，如告警名称、告警级别、告警类型、告警报送次数等。

10.5 应急响应

10.5.1 应急预案

应编制智能网联汽车网络安全平台的应急预案，预案满足以下要求：

a) 应明确有关各方的工作职责和沟通方式，说明重要资源的业务影响范围、恢复时间目标、恢复点目标，明确资源的物理位置、设备型号、软件资源、网络配置、车型等关键信息；
b) 应明确各类风险的诊断方法和流程，制定数据恢复流程和应急处置操作手册。

10.5.2 响应处置

应编制智能网联汽车网络安全平台的响应处置要求如下：

a) 应具备评估攻击对企业造成的影响或损害程度的机制，结合资产、漏洞、响应措施等已知信息，对攻击造成的影响进行评估；
b) 应具备对攻击方式、攻击路径、攻击源、攻击目标及攻击事件等进行拓展分析的机制；
c) 应具备对安全事件的追溯能力。

参 考 文 献

[1] GB/T 38628—2020 信息安全技术 汽车电子系统网络安全指南
[2] GB/T 40855—2021 电动汽车远程信息服务与管理系统信息安全技术要求
[3] GB/T 40857—2021 汽车网关信息安全技术要求及测试方法
[4] YDB 102—2012 通信网支持智能交通系统总体框架
[5] YDB 124—2013 车联网总体技术要求