ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 102-2022

车辆远程诊断信息安全技术要求及试验方法

Technical requirements and test methods for cybersecurity of vehicle remote diagnosis

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　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。

本文件由中国第一汽车集团有限公司智能网联开发院、启明信息技术股份有限公司联合提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：启明信息技术股份有限公司、中国第一汽车集团有限公司工程与生产物流部、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：辛明、李丹、董玮、李岩、刘宇航、赵沛时、魏利、陈有志、郭宏伟、吉岩、渠谨黛、谷淼、吴淼、李木犀、边泽宇。

本文件参与起草单位：中国汽车技术研究中心有限公司、吉林大学汽车仿真与控制国家重点实验室、中国汽车工程研究院股份有限公司、宇通客车股份有限公司、一汽奔腾轿车有限公司、长春吉大正元信息技术股份有限公司、一汽-大众汽车有限公司、中电信数智科技有限公司长春分公司、中电福富信息科技有限公司。

本文件参与起草人：李宝田、李杰、全代勇、杨品章、杨军涛、雷凯、苏日、王博、高深、李新坚。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

车辆远程诊断技术是传统车辆本地诊断技术的延伸，是汽车未来诊断技术的发展方向。车辆远程诊断技术也是传统车辆本地诊断技术与车联网技术的一种结合，因此，车辆远程诊断过程中所面临的车联网信息安全问题不容忽视，本文描述了车辆远程诊断的信息安全技术要求及参考试验方法，目的是希望在带来便利的同时，能够提高车辆远程诊断系统防范攻击的能力，实现相对安全可靠的车辆远程诊断。

车辆远程诊断信息安全技术要求及试验方法

1 范围

本文件规定了车辆诊断终端、远程诊断客户端和诊断服务平台的信息安全技术要求和试验方法。

本文件适用于车辆远程诊断产品或具有车辆远程诊断功能的车联网信息安全产品。

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 20275-2021 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 25069 信息安全技术 术语

GB/T 40650-2021 信息安全技术 可信计算规范 可信平台控制模块

GB/T 40855-2021 电动汽车远程服务与管理系统信息安全技术要求及试验方法

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 40857-2021 汽车网关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

3 术语和定义

GB/T 20275、GB/T 25056、GB/T 40650、GB/T 40855、GB/T 40856、GB/T 40857、GB/T 40861界定的以及下列术语和定义适用于本文件。

3.1

汽车信息安全 vehicle cybersecurity

汽车的电子电气系统、组件和功能被保护，使其资产不受威胁的状态。

3.2

远程诊断终端 vehicle diagnostic terminal

安装在汽车上，通过CAN、以太网等接口与车辆ECU进行诊断通信，获取车辆诊断数据，实现车辆诊断功能，同时可直接或间接实现远程通信功能的装置。

主要有两种安装方式：

a) 装置固定安装在车上，不可随意拆卸；

b) 装置是独立的设备，使用时插入车辆接口（如OBD接口），用后可以取下。

3.3

远程诊断客户端 remote diagnostic client

安装在电脑或手机端，通过远程诊断服务平台，与远程诊断终端进行通信，实现对车辆的远程诊断，

如故障分析，故障清除、ECU 配置刷写等。

3.4

远程诊断服务平台 remote diagnosis service platform

提供对远程诊断数据存储、计算、分析、处理、展示，监控的平台。

3.5

后门 backdoor

能够绕过系统认证等安全机制的管控而进入信息系统的通道。

3.6

访问控制 access control

确保对资产的访问是基于业务和安全要求进行授权和限制的手段。

3.7

拒绝服务 denial of service （DoS）

因阻止对系统资源的授权访问或延迟系统运行和功能实现而导致授权用户的可用性受损。

3.8

分布式拒绝服务攻击 distributed denial of service (DDoS)

通过损害或控制多个系统对攻击目标系统的带宽和资源进行攻击而实现拒绝服务。

3.9

可信验证 trusted verification

基于可信根对设备的目标程序进行完整性验证。

3.10

可信平台控制模块 trusted platform control module

集成在可信计算节点中防护部件组件，由硬件、软件及固件组成，与计算机部件的硬件、软件及固件并行连接，是用于建立和保障信任源点的一种基础核心模块，为可信计算节点提供主动度量、主动控制、可信验证、加密保护、可信报告、密码调用等功能。

4 缩略语

下列缩略语适用于本文件。

CAN：控制器局域网（Controller Area Network）；

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

DoIP：基于因特网协议的诊断通信（Diagnostic communication over Internet Protocol）；

DoS：拒绝服务（Denial of Service）；

ECU：电子控制单元（Electronic Control Unit）；

JTAG：联合测试工作组（Joint Test Action Group）；
OBD：车载诊断（On-Board Diagnostics）；
V2X：车辆与车外其它设备之间的无线通信（Vehicle to Everything）。

5 信息安全要求

5.1 总体结构图

车辆远程诊断信息安全总体结构见图 1。

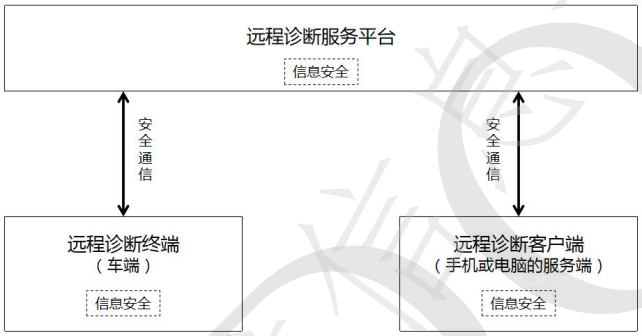

图 1 车辆远程诊断信息安全总体结构

5.2 原则性要求

5.2.1 业务适用性原则

车辆远程诊断产品的信息安全设计应结合车辆远程诊断的实际业务需求或环境需求，同时考虑对业务或功能的正常使用的影响。

5.2.2 软件无后门原则

车辆远程诊断产品的所有软件系统不应留有后门。

5.2.3 系统最小化原则

车辆远程诊断产品在产品正式交付前，无用的软件组件、协议端口和 ECU 硬件调试接口应禁用或移除；硬件器件的管脚信息不宜暴露。

5.2.4 授权最小化原则

车辆远程诊断产品的访问和信息处理活动只授予必要的用户必要的权限。

5.2.5 权限分离原则

重要保护对象的信息处理活动应具备两个或两个以上的权限，且各权限应相互分离和单独授予。

5.2.6 默认设置原则

车辆远程诊断产品应完成默认的信息安全设置，该设置对用户的信息安全设置诉求应做到最小化和最简单化。

5.3 远程诊断终端安全要求

5.3.1 硬件

远程诊断终端硬件安全要求如下：

a) 不应存在后门或隐蔽接口；

b) 调试接口应禁用或设置安全访问控制。

5.3.2 固件

对于固定在车上的诊断终端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。

5.3.3 数据存储

远程诊断终端数据存储要求如下：

a) 应保证所存储数据的保密性和完整性，宜支持 SM2、SM3、SM4、AES、RSA 等密码算法；

b) 远程诊断终端的安全重要参数在存储以及使用过程中，应只允许被授权的应用以授权方式读取、修改和删除。

5.3.4 软件系统

远程诊断终端软件系统要求如下：

a) 应具备判定和授予应用程序对系统资源的访问和操作权限的能力；

b) 宜进行可信验证。

5.3.5 网络端口传输

远程诊断终端网络端口传输安全要求如下：

a) 应通过对数据包的源地址、目的地址、源端口、目的端口和协议进行检查决定允许或拒绝数据进出；

b) 应具备根据会话状态信息为进出数据流判定允许或拒绝访问的能力；

c) 应基于应用协议和应用内容对进出网络端口的数据流实现访问控制；

d) 应关闭非业务相关的网络服务端口，并对业务相关的网络服务端口进行访问控制；

e) 宜对进入远程诊断终端的带有攻击行为特征的网络数据进行识别；

f) 宜采用专用网络或者虚拟专用网络通信，与公网隔离；

g) 宜具备更新扩展安全规则的能力。

5.3.6 日志

远程诊断终端日志功能要求如下：

a) 应记录远程诊断终端在远程服务过程中发生的信息安全相关事件，如检测受到网络攻击行为等；

b) 应使每个信息安全事件日志信息记录的内容包括但不限于：日期和时间（精确到秒）、车辆识别代号、事件类型；

c) 应保证所存储信息安全事件日志信息的完整性，日志应保持 180 天以上；

d) 远程诊断终端信息安全事件日志应只允许被授权的应用以授权的方式读取；

e) 应具有信息安全事件日志的上传机制，并使用安全通信协议将信息安全事件日志信息发送到平台。

5.3.7 系统安全

远程诊断终端不应存在由权威漏洞平台 6 个月内公布且未经处置的高危及以上的安全漏洞。

5.3.8 远程升级

若远程诊断终端具备远程升级功能，远程诊断终端应具有升级包校验机制，校验升级包的完整性以及来源真实性，升级失败应有安全的自动回退机制。

5.4 远程诊断客户端与诊断服务平台通信安全要求

5.4.1 一般要求

远程诊断客户端与远程诊断服务平台的通信应满足传输数据的保密性、完整性和可用性要求。在客户端登入平台之前，应和平台进行双向身份鉴别。

5.4.2 安全通信协议

安全通信协议要求如下：

a) 使用 TLS1.2 同等安全强度的协议或以上版本；
b) 不应允许降级，例如降到 TLS1.1 或 SSL3.0、SSL2.0；
c) 应禁用 TLS 会话重协商；
d) 应禁用 TLS 压缩；
e) 若使用基于非对称密钥的身份认证机制，宜使用 SM2、密钥长度不低于 2048 位的 RSA 或同级别以及更高级的密码算法，应具有对应的证书更新及撤销机制，证书的有效期宜不超过 10 年，证书更新过程应确保密钥安全性；
f) 若使用基于对称密钥的身份认证机制，宜使用 SM4、密钥长度不低于 128 位的 AES 或同级别以及更高级的密码算法，应具有对应的密钥更新机制，更新过程中应确保密钥安全性。

5.4.3 数据单元加密

对通信数据进行加密，加密要求如下：

a) 数据单元加密方式应采用 SM4、密钥长度不低于 128 位的 AES 或其他同等级别以及更高级的密码算法；
b) 加密数据单元的密钥应与安全通信协议所使用的密钥不同。

5.5 远程诊断终端与远程诊断服务平台通信安全要求

远程诊断终端到远程诊断服务平台的通信应满足双向身份鉴别和传输数据的保密性、完整性和可用性要求。

远程诊断终端与平台通信的数据应按 5.4.3 进行加密处理。

远程诊断终端到平台的安全通信协议应满足 5.4.2 的技术要求。

5.6 远程诊断服务平台安全要求

远程诊断服务平台应对远程诊断终端的信息安全进行监视管理，应能在远程诊断终端产生信息安全问题后，为信息安全应急响应提供远程诊断终端相关数据以及追溯手段。远程诊断服务平台应提供能通过网络攻击类型、车辆信息、日期等特征来筛选网络攻击行为的功能。

6 试验方法

6.1 概述

车辆远程诊断信息安全试验方法包括信息安全技术文档核查和试验样件信息安全功能验证。

6.2 远程诊断终端信息安全试验

6.2.1 硬件信息安全试验

应通过如下方法检测远程诊断终端的硬件信息安全并满足 5.3.1 要求：

a) 拆解被测样件设备外壳，取出 PCB 板，检查是否存在可非法对芯片进行访问或者更改芯片功能的隐蔽接口；

b) 根据远程诊断终端接口定义说明，检查是否存在暴露在 PCB 上的 JTAG 接口、USB 接口、UART 接口等调试接口，并使用测试工具尝试获取调试权限。

6.2.2 固件信息安全试验

6.2.2.1 硬件安全启动可信根防篡改试验

根据远程诊断终端安全启动可信根存储区域访问方法和地址范围说明，使用软件或硬件调试工具写入数据，重复多次验证是否可将数据写入该存储区域。

如未禁止写入则本试验失败。

6.2.2.2 硬件安全启动引导加载程序（Bootloader）校验试验

根据远程诊断终端安全启动可信根存储区域访问方法和地址范围说明，使用软件调试工具对该 Bootloader 的签名数据进行破坏，如成功破坏签名数据，则使用安全刷写工具对破坏签名后的 Bootloader 进行刷写，如成功写入到远程诊断终端内的指定区域，检测远程诊断终端芯片是否校验 Bootloader 签名，并在校验不成功时停止加载下一阶段系统镜像。

如最终能加载下一阶段系统镜像，则本试验失败。

6.2.2.3 软件安全启动 Bootloader 防篡改试验

根据远程诊断终端安全启动可信根存储区域访问方法和地址说明，尝试使用软件调试工具对 Bootloader 区域的存储数据进行篡改或替换破坏，检测远程诊断终端是否禁止将篡改或替换后的 Bootloader 写入到终端内的指定区域。如未禁止写入则本试验失败。

6.2.2.4 安全启动镜像校验试验

使用软件调试工具对系统镜像的签名数据进行破坏，将破坏签名后的系统镜像写入到远程诊断终端内的指定区域，检测远程诊断终端是否校验系统镜像签名，并在校验不成功时停止工作。如远程诊断终端仍能继续工作则本试验失败。

6.2.3 软件系统信息安全试验

6.2.3.1 软件系统访问控制试验

按照访问控制规则创建一个未添加访问控制权的软件应用程序，使用该未添加访问控制权的软件应用程序尝试访问受保护的软件应用程序资源，检测受保护的软件应用程序资源是否可被访问。如受保护的软件应用程序资源可被访问则本试验失败。

6.2.3.2 软件系统可信根存储区域试验

根据远程诊断终端安全启动可信根存储区域访问方法和地址范围说明，使用软件调试工具向软件系统可信根区域写入数据，重复多次验证是否可将数据写入该存储区域。如能写入则本试验失败。

6.2.4 数据存储信息安全试验

6.2.4.1 数据存储保密性试验

使用软件分析工具读取存储远程服务的数据区域内容，检测是否为密文存储。如非密文存储则本试验失败。

6.2.4.2 数据存储完整性试验

使用非授权的应用程序读取远程服务区域内容，检测是否可进行修改，若可修改，则检测修改后，终端是否依然可正常调用该数据。如终端可调用被修改的数据则本试验失败。

6.2.4.3 安全重要参数信息安全试验

使用非授权的应用程序读取系统数据区域的安全重要参数，测试是否可读取或使用。如能读取或使用则本试验失败。

6.2.5 网络端口传输信息安全试验

6.2.5.1 控制策略信息安全核查

核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。

6.2.5.2 数据流控制策略信息安全核查

核查是否采用会话认证等机制为进出数据流提供明确的允许或拒绝访问的能力。

6.2.5.3 访问控制策略试验

在被测样件设置符合标准规定的访问控制策略，检测设备向列表指定的源端口发送不符合策略规定的报文，并在列表指定的目的端口检测接收报文和日志。日志中应有该条记录。

6.2.5.4 冗余及非授权访问试验

使用网络扫描工具对远程诊断终端进行网络端口扫描：

a) 检测远程诊断终端是否开放非业务所需的冗余网络端口，如开放非业务所需端口则本试验失败；

b) 检测是否可针对开发的网络端口建立非授权访问控制连接，如能建立非授权访问连接则本试验失败。

6.2.5.5 安全扫描功能试验

将远程诊断终端接入测试网络，使用攻击案例对远程诊断终端实施攻击，检测远程诊断终端对攻击的识别率。识别率应不低于 95%。

6.2.5.6 专用网络认证机制试验

若远程诊断终端到平台采用专用网络或者虚拟专用网络进行通信，尝试在非授权网络条件下，将远程诊断终端连接到远程诊断服务平台，多次重复检测是否可建立通信。如可建立通信则本试验失败。

6.2.5.7 安全规则更新扩展能力核查

根据远程诊断终端安全规则更新扩展方案说明，核查远程诊断终端是否具备安全规则更新扩展的能力。

6.2.6 车远程升级功能信息安全试验

6.2.6.1 升级包完整性校验试验

使用软件调试工具破坏升级包的任意内容，将被破坏的升级包下载到远程诊断终端指定区域，并下发升级包升级指令，检测远程诊断终端加载升级包时是否进行完整性校验。如未进行完整性校验则本试验失败。

6.2.6.2 升级包来源真实性验证试验

将非授权签名的升级包下载到远程诊断终端指定区域，并下发升级包升级指令，检测远程诊断终端加载升级包是否进行授权校验。如未进行授权校验则本试验失败。

6.2.7 日志功能信息安全试验

6.2.7.1 日志功能信息安全核查

根据远程诊断终端安全事件日志记录规则说明，核查远程诊断终端日志信息记录的内容是否包括但不限于日期和时间、主体身份、事件类型、事件结果等组成部分。

6.2.7.2 日志功能保密性信息安全试验

根据远程诊断终端日志存储区域和地址范围说明，使用日志分析工具读取日志功能区域内容，检测是否为密文存储。如非密文存储则本试验失败。

6.2.7.3 日志功能完整性信息安全试验

根据远程诊断终端日志存储区域和地址范围说明，使用非授权的应用程序读取日志功能区域内容，检测是否可修改，若可修改，则检测修改后，是否依然可正常读取该日志。如可读取被修改的日志则本试验失败。

6.2.7.4 日志功能访问权限信息安全试验

根据远程诊断终端日志存储区域和地址范围说明，以非授权的用户应用程序访问审计信息存储区域，检测访问是否成功。如能访问则本试验失败。

6.2.7.5 日志上传信息安全试验

将远程诊断终端接入测试网络，使用攻击案例对远程诊断终端实施恶意攻击，核查攻击结束后，是否可在平台上检索到本次安全攻击事件日志。如无此事件日志则本试验失败。

6.2.8 系统信息安全试验

通过如下方法检测远程诊断终端系统信息安全：

a) 使用漏洞扫描工具对远程诊断终端进行漏洞检测，检测是否存在权威漏洞平台 6 个月前公布的高危及以上的安全漏洞；

b) 若存在高危及以上的安全漏洞，则检查厂商是否提供了该漏洞的处置方案。

如存在未处置的高危及以上的安全漏洞，则本试验失败。

6.3 远程诊断终端及远程诊断客户端与远程诊断服务平台通信安全试验

6.3.1 通信安全核查

6.3.1.1 协议版本核查

核查安全通信协议是否为 TLS1.2 或以上版本，是否允许降级，例如降到 TLS1.1 以下或 SSL3.0、

SSL2.0。

6.3.1.2 协议功能核查

核查安全通信协议是否禁用 TLS 会话重协商和 TLS 压缩功能。

6.3.1.3 安全算法核查

核查 TLS 协议的安全算法选择是否满足 5.4.2 的要求。

6.3.2 通信传输协议试验

使用网络抓包工具监听对外网络传输数据，分析数据包是否采用 TLS1.2 或以上版本协议。如未采用则本试验失败。

6.3.3 通信双向身份认证试验

在通信链路捕获通信流量包，分析捕获的数据报文，检测通信双方有无交换证书流量特征或者有无安全认证心跳包流量特征等双向认证方式。如无双向认证方式则本试验失败。

6.3.4 通信数据加密性试验

使用网络抓包工具监听网络传输数据，检测传输的数据是否为密文。如非密文传输则本试验失败。

6.3.5 通信数据完整性试验

对传输的数据进行破坏，检测数据破坏后，传输是否失败。如传输未失败则本试验失败。

6.3.6 通信中断安全试验

在传输数据的过程中，断电终止传输，恢复后检测功能是否正常并记录日志。如功能无法恢复或未在日志中记录，则本试验失败。

附 录 A
（资料性）
信息安全威胁示例

A.1 软件系统的信息安全威胁示例

软件系统的信息安全威胁示例如下：

a) 用户通过越权方式访问软件系统，包含两个方面：
   1） 普通用户通过非正常渠道篡改和提升其权限，从而访问权限外的数据和文件；
   2） 利用系统访问机制设置不恰当的漏洞（如没有对用户做最小权限设置），访问不应访问的资源。
b) 用户利用用户身份认证不充分或默认账号密码未修改等问题非法访问车内软件系统；
c) 攻击者发现并利用软件系统中未移除或禁止功能业务中未用的组件和协议端口等隐藏的服务和端口攻击系统；
d) 攻击者通过操纵软件升级的确认机制，让软件系统拒绝正常的软件升级或让车辆在不恰当的时间和地点停车进行软件升级；
e) 攻击者通重放合法的升级软件包让汽车反复升级软件以干扰车辆正常工作；
f) 车辆升级软件时没有进行来源合法性和软件包的完整性等可信环节的检查，导致非法软件安装到车辆中；
g) 车辆的软件系统没有足够完备的信息安全日志或其它事件记录系统，导致无法感知攻击和异常行为，给事后的信息安全事故调查、取证和追溯等带来困难；
h) 软件系统缺乏可信的启动机制，导致系统运行被篡改过的或不完整的软件；
i) 软件系统的访问认证机制缺乏防暴力破解措施，使攻击者可利用暴力方式破解访问的账号和密码；
j) 软件系统尤其是数据库对接收到的输入命令不校验格式的合法性，导致出现注入攻击；
k) 攻击者通过“后门”（如：组合键、鼠标特殊敲击、连接特定接口、使用特定客户端、使用特殊 URL、隐藏的访问账号、隐藏的远程访问通道等方式）非法进入车内软件系统；
l) 车辆软件系统缺乏预警与监控机制或预警与监控机制不充分，无法感知自身面临的异常处理行为，导致用户或后台服务器无法及时应对措施。

A.2 硬件的信息安全威胁示例

硬件的信息安全威胁示例如下：

a) 芯片缺乏独立的信息安全存储空间或可信计算空间去存储密钥、用户认证的生物特征信息等安全重要参数，从而导致泄密。例如，通过 OS 内存泄密；在各种应用执行认证时，可直接访问安全重要参数，从而导致泄密；
b) 攻击者对芯片的信息安全存储进行攻击以窃取安全重要参数。例如，实施侧信道攻击、故障注入攻击等物理攻击以及穷举暴力和信息安全协议等逻辑攻击方式；
c) 攻击者直接接入硬件调试接口。如 JTAG、串口或能访问硬件的管脚，对 ECU 和芯片进行非法调试；
d) 攻击基于芯片的软件系统可信启动机制，破坏软件启动前的可信环境和可信证明过程。例如，修改预存储的软件完整性校验值或伪造软件的远程证明凭证等；
e) 攻击者通过攻击物理设备或利用物理泄露进行攻击或对电子硬件实施物理注入攻击，包括入侵式攻击（如反向工程破解）、半入侵式注入攻击（如噪声注入、激光照射攻击等）和非入侵

式的侧通道攻击（通过电磁波、时序等分析密钥等）。

A.3 车内数据的信息安全威胁示例

车内数据的信息安全威胁示例如下：

a) 车内系统对安全重要的参数的存储（如通信私钥、车辆数字证书私钥、车辆长期 ID 等）缺乏有效的保护措施，导致安全重要参数的信息泄露。例如，采用明文存储、未采用专门的隔离区进行存储、加密安全重要参数的密钥采用固定密钥或直接写死在代码中而导致加密密钥泄密问题；

b) 车内系统对存储的车内数据缺乏有效的访问权限控制，导致攻击者通过各类通信信道非法窃取和篡改数据；

c) 车内各类软件涉及安全重要参数因使用时保护不当而发泄露。例如，缓存中存在加密密钥和认证凭证、信息安全日志或其它记录了密钥和长期 ID 等信息；

d) 车内系统的配置参数（如发动机配置参数、控制算法的建模参数和感知系统的配置参数等）缺乏有效的保护，导致攻击者通过修改这些配置参数操纵车辆；

e) 车辆共享同样的重要参数（如所有车辆使用同样的 root 口令或车辆软件对于外部输入数据检查及保护不足）导致代码注入攻击。

A.4 车内通信的信息安全威胁示例

车内通信的信息安全威胁示例如下：

a) 由于车内网络未采用分区域信息安全隔离方式，导致攻击者一旦攻破某个单元即可对整个车内系统发起跨越式攻击；

b) 车内网络缺乏对消息来源的真实性和完整性校验机制，导致攻击者一旦入侵了某个车内信息单元即可通过篡改消息和伪造消息操纵车辆；

c) 车内网络系统缺乏防 DDoS 或流控措施，发生某些单元被攻击者操纵或在功能故障后向车内总线发送大量的异常报文，导致车内通信系统拒绝服务；

d) 攻击者截取合法报文，导致不断地进行重复发送，进行重放攻击；

e) 通过 OBD 接口接入总线方式或植入恶意软件的方式，监听车总线的控制消息，破解不同运行状态的控制消息内容。

A.5 车外远距离通信的信息安全威胁示例

车外远距离通信的信息安全威胁示例如下：

a) 对汽车实现通信欺骗。例如，伪造基站或者路基通信设施身份、向车辆发送假冒的 V2X 消息或卫星导航信息；伪造车辆 ID、采用女巫攻击，伪造众多虚假车辆，影响车辆的正常行驶；伪造后端服务器身份、向汽车推送各种交互指令和伪造的软件升级包；

b) 利用通信通道对车辆实施 DoS/DDoS 攻击，造成车辆的信息处理功能中断。例如，发送各种通信协议的畸形报文、重放合法报文、大流量报文攻击等；

c) 通过架设无线干扰器来干扰 V2X 或卫星导航信号，造成车辆无法正常通信；

d) 车辆与车外系统之间的通信加密密钥被窃取或采用明文方式通信，导致通信内容存在泄漏的风险；

e) 车辆与车外系统之间通信信道的完整性保护密钥被窃取或未采用完整性保护措施，导致通信内容被非法篡改；

f) 采用中间人攻击方式向车辆或车外系统发送伪造的服务拒绝响应消息，干扰正常通信；

g) 攻击者利用车辆的通信信道对车辆实施网络嗅探。例如，IP 端口扫描、 ping 扫描、Tcp syn 扫描等针对 IP 通信的嗅探；

h) 车辆和各类后端服务器之间的通信缺乏端到端的信息安全保护机制，使得攻击者利用中间薄弱环节实施攻击，包括窃听、伪造身份通信、篡改通信内容等；

i) 针对车辆的证书发放系统的攻击。例如，恶意注入伪造的证书撤销列表 CRL 等。