ICS 43.020
T40/49

中华人民共和国国家标准

GB/T XXXXX.X—XXXX

汽车信息安全通用技术要求

General cybersecurity technical requirements for road vehicles

（征求意见稿）

××××-××-××发布　　××××-××-××实施

国家市场监督管理总局
国家标准化管理委员会　　发布

目　次

前　　言

本标准按照 GB/T　1.1-2009 给出的规则起草。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国汽车标准化技术委员会(SAC/TC 114)归口。

本标准主要起草单位：

本标准主要起草人：

引　　言

随着智能化和网联化快速发展，汽车从相对孤立的电子机械系统逐渐演变成能与外界实时通信的智能系统。汽车网联化有利于促进行业技术升级，但同时也为汽车行业带来大量信息安全问题。

传统通信行业的信息安全问题主要造成财产损失，但是汽车作为载人和载物的移动工具，当其发生信息安全问题时，不仅造成财产损失，还将严重威胁人身和公共安全。鉴于汽车与传统通信设施所面临信息安全风险的诱因和危害有很大差异，为了更好地指导汽车行业健康发展，有必要对汽车信息安全制定专门标准。

本标准编写思路如图1所示，主要明确保护对象和规范技术要求，管理要求将由其他标准配合制定。其中技术要求分为原则性要求、系统性防御策略要求和保护维度要求，原则性要求和系统性防御策略要求是基础技术要求，保护维度要求是从八个维度针对子保护对象制定的具体技术要求。八个维度如下所示：

a） 真实性维度；
b） 保密性维度；
c） 完整性维度；
d） 可用性维度；
e） 访问可控性维度；
f） 抗抵赖性维度；
g） 可核查性维度；
h） 可预防性维度。

注：为了更好理解保护对象在不同维度的技术要求，在附录A中列举了保护对象所面临的典型的安全威胁。

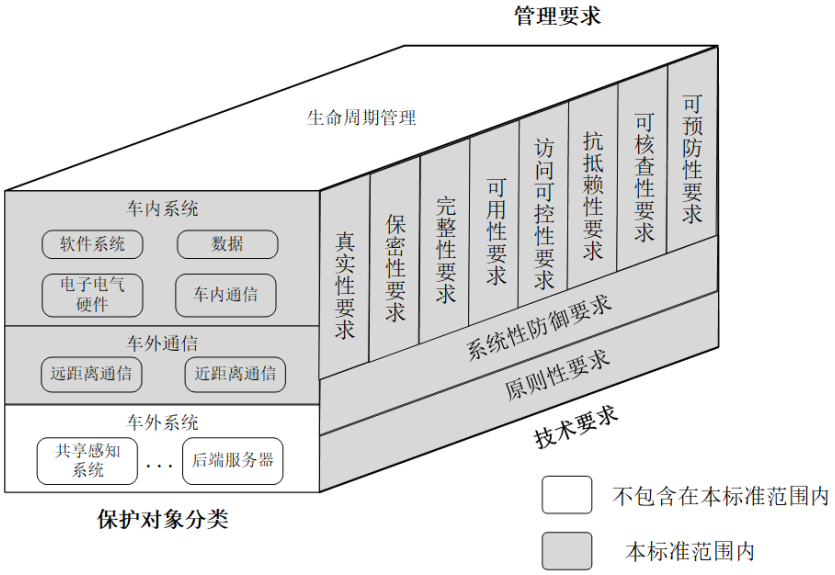

图1　标准框架

汽车信息安全通用技术要求

1 范围

本标准规定了汽车信息安全的保护对象和技术要求。

本标准适用于M类、N类汽车整车及其电子电气零部件。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 29246-2017 信息技术 安全技术信息安全管理体系 概述和词汇

GB/T 34590.3-2017 道路车辆 功能安全 第三部分：概念阶段

3 术语和定义

GB/T 29246-2017界定的以及下列术语和定义适用于本文件。下面定义中列出了标准的出处，所以导语内容不全

3.1

汽车信息安全 road vehicle cybersecurity

汽车及其功能被保护，以使其电子电气组件不受威胁的状态。

3.2

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的特性。

[GB/T 29246-2017，定义2.12]

3.3

完整性 integrity

准确和完备的特性。

[GB/T 29246-2017，定义2.40]

3.4

可用性 availability

根据授权实体的要求可访问和可使用的特性。

[GB/T 29246-2017，定义2.9]

3.5

真实性 authenticity

一个实体是其所声称实体的这种特性。

[GB/T 29246-2017，定义2.8]

3.6

访问可控性 access controllability

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特性。

3.7

抗抵赖 non-repudiation

证明所声称事态或行为的发生及其源头的能力。

[GB/T 29246-2017，定义2.54]

3.8

可核查性 accountability

确保可从一个实体的行为唯一地追溯到该实体的特性。

3.9

可预防性 preventability

对信息异常行为和攻击行为，具备识别、侦测，以及相应的安全响应能力。

3.10

拒绝服务 denial of service（DoS）

阻止对系统资源的授权访问或延迟系统的运行和功能，从而导致授权用户的可用性受损。

3.11

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

通过损害或者控制多个系统对攻击目标系统的带宽和资源进行泛洪攻击，从而阻止对目标系统资源的授权访问或延迟其运行和功能，从而导致授权用户的可用性受损。

3.12

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。

3.13

凭证 credential

身份的代表。

注1：凭证的生成通常是用来促进对其所代表的身份中的身份信息进行数据鉴别。

注2：由凭证表示的身份信息可以印在纸上或存储在物理令牌中，通常以这种方式来维护信息的有效性。

3.14

根密钥 derivation key

用来生成派生秘钥的顶层秘钥。

3.15

安全重要参数 security important parameter

与安全相关的信息，包含秘密和私有密码秘钥、口令之类的鉴别数据、证书或其他密码相关参数的信息。

3.16

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
[GB/T 29246-2017,定义2.1]

4 缩略语

TLS	传输层安全协议 （Transport Layer Security）
TPM	可信赖平台模块 （Trusted Platform Module）
HSM	硬件安全模块 （Hardware Secure Module）
TEE	可信执行环境 （Trusted Execution Environments）
OBD	车载诊断 （On-Board Diagnostics）
IMSI	国际移动用户识别码 （International Mobile Subscriber Identity）

5 保护对象

5.1 总则

汽车作为保护对象可划分为三类子保护对象：车内系统、车外通信和车外系统，如图1所示。
注：本标准不涉及车外系统。

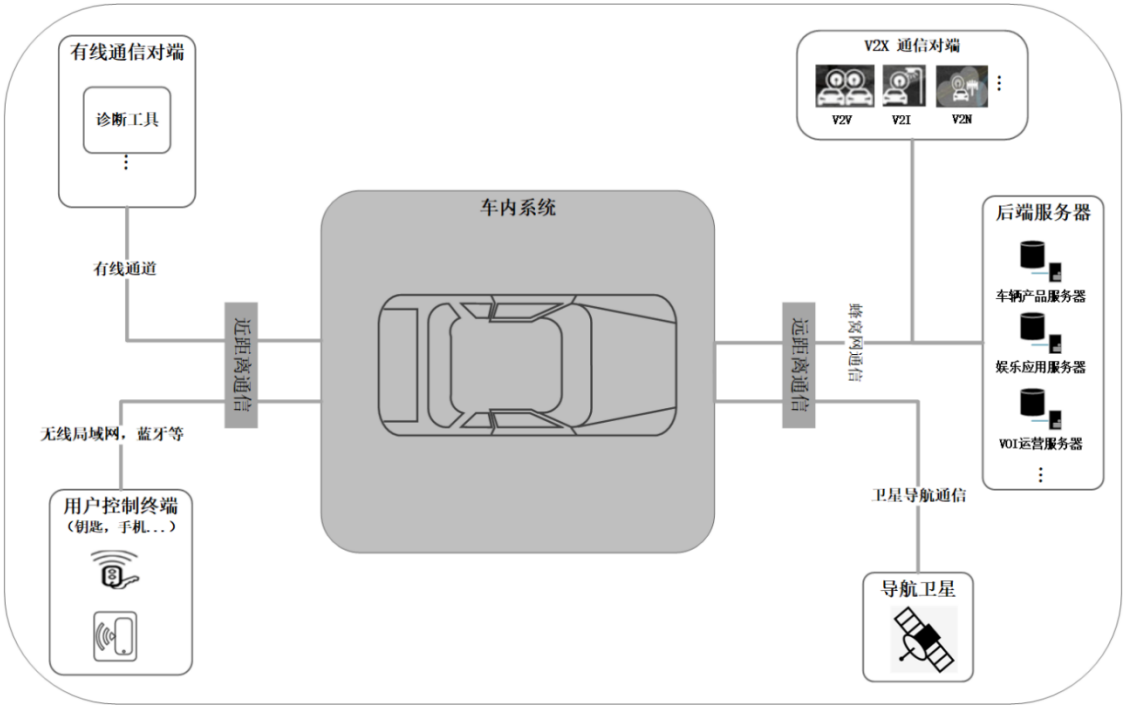

图1　保护对象模型

5.2　车内系统

车内系统分为如下子保护对象：

a）　软件系统；

b）　电子电气硬件；

c）　车内数据；

d）　车内通信。

注：车内通信即车内零部件之间的通信，包括但不限于CAN通信，LIN通信，以太网通信等。

5.3　车外通信

车外通信分为如下子保护对象：

a）　车外远距离通信；

b）　车外近距离通信。

注1：车外通信即整车与车外终端的通信。

注2：车外远距离通信如蜂窝移动通信、卫星导航等。

注3：车外近距离通信如OBD、蓝牙、近场无线通信和Wifi等。

6　技术要求

6.1　原则性要求

6.1.1　业务适用性原则

产品的信息安全设计应充分考虑业务或者功能环境的实际需求，功能或者业务的正常使用不应受到信息安全设计的影响。

6.1.2 软件无后门原则

软件系统不应留有后门。

6.1.3 功能最小化原则

无用的软件组件、协议端口和ECU硬件调试口应禁用或者移除，不宜暴露器件的管脚信息。

6.1.4 最小化授权原则

产品的访问和信息处理活动应只授予必要的权限。

6.1.5 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，且权限应相互分离和单独授予。

示例：用户要进行某项保护对象的操作，同时具有登录系统的合法身份和该保护对象的操作权限。

6.1.6 默认设置原则

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。

6.2 系统性防御策略要求

6.2.1 总则

产品应至少采用一种如下的系统性防御策略：

a) 纵深防御；
b) 主动防御；
c) 系统的韧性。

注：系统性防御策略，是基于构建系统的整体信息安全防护考虑，所采取的整体防御策略，避免因各个信息安全防护措施相互孤立而造成整体防护能力不足的问题。

6.2.2 纵深防御要求

纵深防御要求符合以下要求：

a) 根据保护对象所处的环境条件和信息安全管理的要求，应对保护对象实施由外到里或由里到外，层层设防的防护措施。
b) 各层次的安全措施应相互依托，形成系统化的防护机制，从而提高系统的整体抗攻击能力。

6.2.3 主动防御要求

主动防御应采用包括不限于情报分享、入侵检测技术、信息安全策略动态调整和各信息安全模块之间的协同措施，使信息系统在发生异常行为时降低其所面临的风险。

6.2.4 系统的韧性要求

信息安全设计应综合考虑可靠性、功能安全等多个方面的工程设计，以提高系统的生存能力和自愈能力。

6.3 保护维度技术要求

6.3.1 车内系统的保护要求

6.3.1.1 软件系统的保护要求

6.3.1.1.1 真实性要求

软件系统符合以下真实性要求：

a) 在软件、固件和配置文件的升级、加载和安装时，应验证提供方的身份真实性和来源的合法性。
b) 软件系统应验证登录用户身份的真实性和合法性。

6.3.1.1.2 保密性要求

重要软件系统应防止被逆向分析，宜采用代码混淆或加壳等措施。

6.3.1.1.3 完整性要求

软件系统符合以下完整性要求：

a) 软件、固件和配置文件的升级、加载和安装时，应验证其完整性。
b) 软件系统启动和运行时，应验证其完整性。

6.3.1.1.4 可用性要求

当软件系统设计为符合GB/T 34590.3-2017中ASIL C和 D级时，其应支持防DoS/DDoS攻击。。

6.3.1.1.5 访问可控性要求

软件系统符合以下访问可控性要求：

a) 应具备访问权限控制的管理机制。
b) 应验证对各软件资源和数据资产的访问、操作和使用的权限。
c) 应验证软件、固件和配置文件的升级、加载和安装的权限。

6.3.1.1.6 抗抵赖性要求

软件系统应具有在请求的情况下为数据原发者或接收者提供数据原发证据和数据接收证据的功能。

6.3.1.1.7 可核查性要求

软件系统符合以下可核查性要求：

a) 应对包括不限于用户活动和操作指令的重要信息安全事件进行记录，记录内容宜包含事件的时间、用户、事件类型、事件成功情况的信息。
b) 应保护审计日志不被非法篡改、删除和伪造。

6.3.1.1.8 可预防性要求

软件系统应具备对自身受到信息安全攻击的感知能力，当受到信息安全攻击时，宜进行日志记录、信息安全告警或攻击阻止的响应。

6.3.1.2 电子电气硬件保护要求

6.3.1.2.1 保密性要求

电子电气硬件符合如下保密性要求：

a） 印制电路板上关键信号的线路应在内层走线。

示例：可能泄露敏感数据的数据总线、串行总线等关键信号。

b） 应去除印制电路板上具有标识作用的丝印设计。

6.3.1.2.2 完整性要求

对关键ECU的封装（外壳、封条等）应采用完整性保护。

示例：使用揭开时能留迹象的封条。

6.3.1.2.3 访问可控性要求

不必要的调试接口应被移除或者禁止。

6.3.1.3 车内数据保护要求

6.3.1.3.1.1 保密性要求

安全重要参数应符合如下保密性要求：

a） 不应以明文方式传输。

b） 应存储在安全的环境中。

示例：TPM 芯片，HSM 或者 TEE 等。

6.3.1.3.1.2 完整性要求

安全重要参数应支持完整性校验。

6.3.1.3.1.3 可用性要求

安全重要参数应防止丢失和被误删除，宜采用备份或专用安全空间存储等措施。

6.3.1.4 车内通信的保护要求

6.3.1.4.1 真实性要求

车内通信应验证通信双方身份的真实性

6.3.1.4.2 保密性要求

车内通信数据应进行加密。

6.3.1.4.3 完整性要求

车内通信数据应采用完整性保护。

6.3.1.4.4 可用性要求

车内通信应具备通信流量控制能力。

示例：当受到恶意软件感染或者服务拒绝攻击而造成车内通信流量异常时，仍然有能力提供可接受的通信。

6.3.1.4.5 访问可控性要求

车内通信应符合如下访问可控性要求：

a） 应将车内网络划分为不同的信息安全区域，每个信息安全区域之间宜进行网络隔离。
b） 信息安全区域间应采用边界访问控制机制对来访的报文进行控制。

示例：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。

6.3.1.4.6 可核查性要求

车内通信应具备日志记录的能力。

示例：记录流量过载、高频率的收到异常报文等现象。

6.3.1.4.7 可预防性要求

车内通信应对异常报文具有感知能力，当感知到异常报文时，宜具有告警或者其他安全响应的能力。

示例：接收到高频率的重放报文或者被篡改过的报文等异常现象。

6.3.2 车外通信的保护要求

6.3.2.1 车外远距离通信的保护要求

6.3.2.1.1 真实性要求

车外远距离通信符合如下真实性要求：

a） 应开启 3G、4G、5G 通信网络层的双向认证功能。
b） 蜂窝移动通信网络层之上应支持独立的双向认证机制。

6.3.2.1.2 保密性要求

车外远距离通信符合如下保密性要求：

a） 应具备 3G、4G、5G 通信网络层的加密功能。
b） 蜂窝移动通信网络层之上应支持独立的加密机制，应采用 TLS1.2 版本及以上的安全协议进行加密。

6.3.2.1.3 完整性要求

车外远距离通信符合如下完整性要求：

a） 应具备 3G、4G、5G 通信网络层的完整性保护功能。
b） 蜂窝移动通信网络层之上应支持独立的完整性机制，应采用 TLS1.2 版本及以上安全协议进行完整性保护。

6.3.2.1.4 可用性要求

车外远距离通信符合如下可用性要求：

a） 与外部通信的部件应支持防 DoS/DDoS 攻击。
b） 应支持抗无线干扰。

6.3.2.1.5 访问可控性要求

车外远距离通信应具备对通信报文进行访问控制的能力。

示例：白名单访问控制、报文过滤、防通信流量过载机制等。

6.3.2.1.6 抗抵赖性要求

车外远距离通信应确保蜂窝移动通信网络层通信ID（如：国际移动用户识别码IMSI等）的唯一性。

6.3.2.1.7 可预防性要求

车外远距离通信应具备对通信报文的安全监控能力和攻击行为的感知能力，当受到信息安全攻击时，宜进行报文清洗、流量控制或阻止攻击行为的响应。

6.3.2.2 近距离通信保护要求

6.3.2.2.1 真实性要求

车外近距离通信应开启身份认证功能。

6.3.2.2.2 保密性要求

车外近距离通信应开启加密功能。

6.3.2.2.3 完整性要求

车外近距离通信应开启完整性保护功能。

6.3.2.2.4 可用性要求

与外部通信的部件应支持防DoS/DDoS攻击。

6.3.2.2.5 可核查性要求

车外近距离通信应具备记录近距离通信信息安全相关的事件，记录的内容宜包含来访用户ID和通信时间。

附 录 A
（资料性附录）
信息安全威胁

A.1 车内系统信息安全威胁示例

A.1.1 软件系统的信息安全威胁示例

表A.1列举了软件系统可能面临的信息安全威胁：

表A.1 软件系统的信息安全威胁

编号	威胁描述
1	用户通过越权方式访问软件系统，包含两个方面： a） 普通用户能够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； b） 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），访问了不应访问的资源。
2	用户利用用户身份认证不充分或者默认账号密码未修改等问题，从而非法访问车内软件系统。
3	软件系统中存在不安全的远程访问或者控制组件，如 Telnet、FTP、TFTP 以及其他不需要强认证和未加密传输的远程控制组件，攻击者利用这些不安全的软件组件进行远程非法访问车内系统。
4	软件系统中存在未移除或者禁止的功能业务未用的组件和协议端口，攻击者发现并利用这些隐藏的服务和端口攻击系统。
5	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，或者让车辆在不恰当的时间和地点进行停车升级软件。
6	攻击者通过重放合法的升级软件包，让汽车反复升级软件，干扰车辆正常工作。
7	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。
8	车辆的软件系统没有足够完备的信息安全日志或者其他事件记录系统，导致对攻击和异常行为不感知，也为事后的信息安全事故的调查、取证和追溯等方面带来困难。
9	软件系统缺乏可信的启动机制，导致系统运行被篡改过或者不完整的软件。
10	软件系统的访问认证机制缺乏防暴力破解措施，攻击者利用暴力方式直接破解访问的账号和密码。
11	软件系统尤其是数据库，对接收到的输入命令没有做格式的合法性校验，导致出现注入攻击。
12	软件系统存在“后门”，即存在绕过正常认证机制直接进入到系统的隐秘通道，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 等方式无需采用正常认证即可直接进入系统，或者软件存在隐藏的访问账号和远程访问通道等，攻击者一旦获得这些“后门”，就可以非法进入车内软件系统。
13	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，无法获知自身所面临的异常信息处理行为，导致用户或者后台服务器无法及时采取应对措施。

A.1.2 硬件的信息安全威胁示例

表A.2列举了电子电气硬件可能面临的信息安全威胁：

表A.2　电子电气硬件的信息安全威胁

编号	威胁描述
1	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。比如通过 OS 内存泄密，在各种应用在执行认证时，直接访问接触到安全重要参数，从而导致泄密。
2	攻击者针对芯片的信息安全存储的攻击，企图窃取安全重要参数，例如，实施侧信道攻击、故障注入攻击等物理攻击，以及穷举暴力攻击和信息安全协议攻击等逻辑攻击方式
3	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者伪造软件的远程证明凭证等。
4	攻击者直接接入硬件调试接口，如 JTAG、串口或者能访问硬件的管脚 PIN，对 ECU 和芯片进行非法调试。
5	攻击者通过攻击物理设备或利用物理泄露进行攻击，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.1.3　车内数据的信息安全威胁示例

表A.3列举了车内数据可能面临的信息安全威胁：

表A.3　车内数据的信息安全威胁

编号	威胁描述
1	车内系统对安全重要参数的存储，如通信密钥、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者直接写死在代码中而导致加密密钥泄密问题。
2	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通道非法窃取和篡改数据。
3	车内各类软件涉及安全重要参数的使用时，因保护不当而导致泄露，比如缓存中存在加密密钥和认证凭证、信息安全日志或者其他记录文件记录了密钥和长期 ID 等信息。
4	车内系统的参数配置因缺乏有效的保护，比如发动机配置参数、控制算法的建模参数和感知系统的配置参数等，导致攻击者通过修改这些配置参数，进行车辆操纵。
5	车辆共享同样的安全重要参数，例如所有车辆使用同样的 root 口令，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.1.4　车内通信的信息安全威胁示例

表A.4列举了车内通信可能面临的信息安全威胁：

表A.4　车内通信的信息安全威胁

编号	威胁描述
1	由于车内网络未采用分区分域信息安全隔离方式，攻击者一旦攻破某个单元，就可以利用攻破的点，对整个车内系统发起跨越式攻击。
2	车内网络连接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，就可以通过篡改消息和伪造消息，对车辆进行操纵。
3	车内网络系统缺乏防 DDoS 或者流控措施，某些信息单元被攻击者操纵或者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。
4	攻击者截取合法报文，不断的进行重复发送，进行重放攻击。

5	通过 OBD 接口接入总线方式或者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.2 车外通信的信息安全威胁示例

A.2.1 车外远距离通信的信息安全威胁示例

表A.5列举了车外远距离通信可能面临的信息安全威胁：

表A.5 车外远距离通信的信息安全威胁

编号	威胁描述
1	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 消息或者卫星导航信息；伪造车辆 ID，采用女巫攻击方式，伪造出众多虚假车辆，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。
2	利用通信通道对车通信实施 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。
3	通过架设无线干扰器，干扰 V2X 或者卫星导航信号，造成车辆无法正常通信
4	车辆与车外系统之间的通信加密密钥被窃取或者采用明文方式通信，导致通信内容存在泄漏的风险。
5	车辆与车外系统之间通信通道的完整性保护密钥被窃取或者未采用完整性保护措施，导致通信内容被非法篡改。
6	采用中间人攻击方式，向车辆或者车外系统发送伪造的服务拒绝响应消息，干扰正常通信。
7	攻击者利用车的通信信道对车实施网络嗅探，例如 IP 端口扫描、ping 扫描、TCP syn 扫描等针对 IP 通信的嗅探。
8	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，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。
9	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。

A.2.2 车外近距离通信的信息安全威胁示例

表A.6列举了车外近距离通信可能面临的信息安全威胁：

表A.6 车外近距离通信的信息安全威胁

编号	威胁描述
1	利用门禁的无线通信信道，伪造门禁控制命令，例如采取无线中继放大器进行中间人攻击方式，分别向车钥匙和门禁系统发生伪造信号，骗取正确的应答信号，从而打开门禁甚至启动引擎。
2	通过无线通信信道破解车钥匙，例如通过暴力破解方式，反复向门禁系统发送控制信息，或者通过监听通信信道进行前向预测攻击、重放攻击、字典式攻击。
3	伪造近距离通信报文，比如伪造胎压管理系统 TPMS 的近距离通信消息，向相关 ECU 发送错误的胎压检测信息等。
4	攻击者通过各类接触式的通信接口，如 OBD 接口、充电桩接口、USB 接口等，入侵车内系统，包括植入恶意软件、修改车内的关键控制系统的参数配置、窃取车内数据、非法访问文件、注入非法数据等行为
5	针对车内的无线局域通信，如蓝牙和 WIFI，发起包括伪造 AP 和暴力破解方案的攻击，试图利用无线局域网非法接入车载系统

参 考 文 献

[1] ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model

[2] ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts

[3] ISO/IEC 27039:2015 Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)