国 际 电 信 联 盟

ITU-T X.1371

(05/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务（2） – 智能交通系统（ITS）安全

联网车辆面临的安全威胁

ITU-T X.1371 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	**X.1370–X.1389**
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1371 建议书

联网车辆面临的安全威胁

摘要

X.1371建议书描述联网车辆和车辆生态系统面临的安全威胁。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1371	2020-05-29	17	11.1002/1000/14090

关键词

联网车辆、安全威胁

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1371建议书

联网车辆面临的安全威胁

1 范围

本建议书描述联网车辆面临的安全威胁。未来的ITU-T建议书可以参考本建议书，以确保这些ITU-T建议书始终考虑到智能交通系统（ITS）的安全问题。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 可用性（availability） [b-ITU-T X.800]：经授权实体一旦需要即可访问和使用的属性。

3.1.2 机密性（confidentiality）[b-ITU-T X.800]：不向未经授权个人、实体或过程提供或披露信息的属性。

3.1.3 完整性（integrity）[b-ISO/IEC 27000]：准确性和完整性。

3.1.4 威胁（threat）[b-ISO/IEC 27000]：有害事件的潜在原因，此原因能够对某个系统或组织造成伤害。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

3G 第三代
4G 第四代
5G 第五代
ADAS 高级驾驶员辅助系统
CAN 控制器局域网
CAM 协同感知消息
C-V2X 基于蜂窝的车辆对万物

DENM 分散式环境通知消息
DRM 数字权限管理
DSRC 专用短程通信
ECU 电子控制单元
GNSS 全球卫星导航系统
ICT 信息通信技术
ID 标识符
IT 信息技术
ITS 智能交通系统
IVN 车联网
JTAG 联合测试行动组
LIN 本地互联网络
MOST 面向媒质的系统传输
OBD 车载诊断系统
ODR 操作数据记录器
OEM 原始设备制造商
OTA 空中下载技术
RF 射频
RSU 路边单元
SD 安全数字
SQL 结构化查询语言
USB 通用串行总线
V2D 车辆对漫游设备
V2I 车辆对基础设施
V2P 车辆对行人
V2V 车辆对车辆
V2X 车联网
VIN 车辆识别号
Wi-Fi 无线上网

5 惯例

无。

6 联网车辆（车辆生态系统）模型

图1显示了联网车辆及其生态系统的概念。该模型是车辆生态系统的一个概念性表示，不知具体的物理实现和技术，认识到这些将随着时间的推移而变化。该模型可能无法涵盖一个车辆生态系统中用到的所有技术或系统，但可以用作识别与确定安全威胁的一个基础。

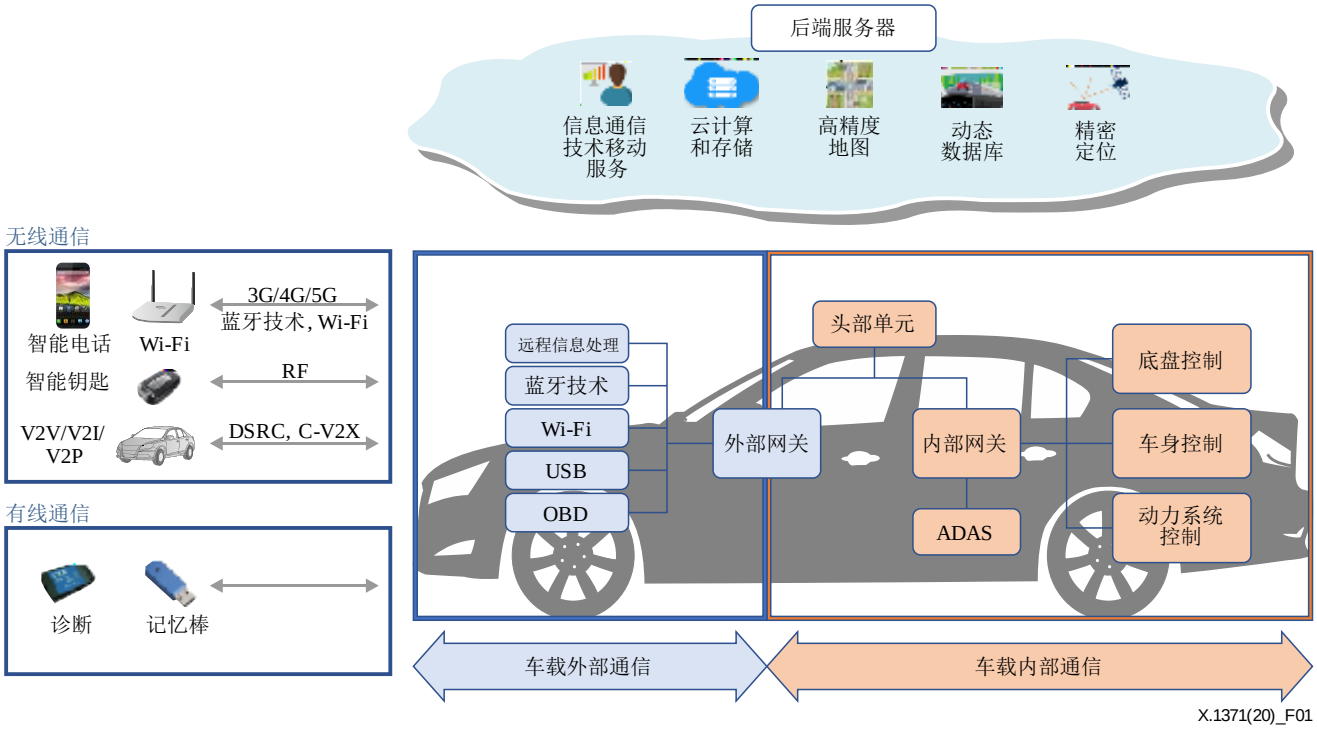

图1 – 联网车辆（车辆生态系统）概念

如今，通信技术在车辆中起着重要的作用。车辆通信可分为车辆外部和车辆内部通信。车辆的内部网络称为车载网络（IVN），包括传感器和电子控制单元（ECU）等车辆部件。这些传感器和电子控制单元用在若干领域中，如底盘控制、车身控制和车辆动力系统控制。此外，这些部件用在高级驾驶员辅助系统（ADAS）中，它在驾驶过程中为驾驶员提供支持，例如保持驾驶车道和巡航控制功能。头部单元是汽车信息娱乐系统的一个组成部分，它让用户可以控制车辆的信息和娱乐媒体，例如音频和视频。

车辆的外部通信称为V2X，意为“车联网”（“车辆对万物”），其中的“万物”指的是与车辆的安全与高效运作有关的任何事物。特别是，V2X被用作有关通信模式的一个通用术语，例如车辆对车辆（V2V）、车辆对基础设施（V2I）、车辆对漫游设备（V2D）和车辆对行人（V2P）。V2X技术包括专用的短距离通信（DSRC）和基于蜂窝的V2X （C-V2X）。基础设施包括路边单元（RSu）和后端设施，例如交通管理和监控系统。RSU可以通过有线或无线网络连接到后端设施。图II-1显示了后端服务器中的各种功能。它包括信息通信技术（ICT）移动服务、云存储、高清地图、有关周边环境的动态数据库以及车辆的精确定位。

在图1中，外部和内部网关在解决车载通信的复杂问题方面发挥着重要作用。内部网关处理车内领域的数据。外部网关通过V2X通信技术负责车辆与智能电话等外部设备和其它车辆之间的通信。外部通信可分为有线和无线通信。有线通信可以使用车载诊断II（OBD II）端口与诊断设备和车辆软件/固件更新程序进行通信。无线通信信道包括蜂窝通信技术、Wi-Fi和蓝牙，以将车辆与诸如智能电话等移动设备连接起来。

7 联网车辆或车辆生态系统面临的威胁以及与威胁相关的潜在信息

7.1 联网车辆或车辆生态系统面临的威胁

7.1.1 车辆在后端服务器方面面临的威胁

近年来，车辆连接的多样化显著提高，特别是对位于车辆后端的各种服务器（称为“后端服务器”）的连通性要求很高。后端服务器包括原始设备制造商（OEM）提供的服务器、供应商提供的服务器和信息通信技术服务提供的服务器，其目的是从远程后端支持车辆生态系统。

7.1.1.1 用作攻击车辆或提取数据手段的后端服务器

在车辆生态系统中，后端服务器主要从车辆上收集数据、存储数据，并向车辆发送信息。应对后端服务器的以下威胁进行处置，以防止它被未经授权的实体破坏：

– 内部人员滥用权限：滥用内部人员在后端服务器上的管理权限可能会泄露服务器的数据，向车辆发送虚假信息等。

– 从外部未经授权地访问后端服务器：如果在后端服务器中仍存在后门或已知漏洞，则可以从外部利用该漏洞，通过诸如结构化查询语言（SQL）注入和恶意软件注入等攻击方法来攻击后端服务器。如果攻击者获得服务器的管理权限，则亦应考虑上一条目描述的相同损害。

– 未经授权的物理访问：有若干种方法可以物理地访问后端服务器，例如使用通用串行总线（USB）闪盘或使用伪造的员工身份标识（ID）进入服务器大楼。在这种情况下，对车辆相关数据及其信息处理设施的损害和干扰甚至会更大。

7.1.1.2 后端服务器的服务中断

对后端服务器的攻击会导致服务器发生故障，并中断其与车辆的交互以及车辆所依赖之服务的提供。攻击可能会对车辆相关服务的可用性造成严重的有害影响，例如有关车辆和基础设施的认证管理。

7.1.1.3 后端服务器上保存的数据丢失或损坏

如第7.1.1.1节所述，如果后端服务器因内部人员滥用权限、未经授权的外部访问或未经授权的物理访问而遭到破坏，后端服务器可能会出现丢失或泄漏的情况。此外，还有以下其它威胁：

– 云中的信息丢失：如果存储在第三方云服务提供商的系统中，则车辆识别号（VIN）或驾驶员个人信息等敏感信息可能会被泄露和破坏。

– 不经意的数据共享导致的信息泄露：如果服务器因管理员的错误配置而位于不安全的周界中，则数据可能会被不经意地共享或泄露。

7.1.2 车辆在通信信道方面面临的威胁

车辆通信包括外部通信，如V2V、V2I、V2D和V2P通信，以及车载通信，如控制器局域网（CAN）、本地互联网（LIN）、面向媒体的系统传输（MOST）和FlexRay。这些通信中使用的信道可能是欺骗、窃听、或消息操纵等的攻击目标。

7.1.2.1 欺骗消息

可能会出现使用模仿的欺骗消息。在V2X通信和全球卫星导航系统（GNSS）中使用的消息的情况下，由于模仿攻击，车辆可能接收到无效消息。此外，如果在特定道路上有许多车辆，则可能实施女巫（Sybil）攻击，以欺骗其它车辆。

注 – 例如，当一辆车通过使用多个车辆标识符来模拟多辆车时，就会发生女巫攻击。

7.1.2.2 对车载代码或数据未经授权的操纵、删除或其它修改

如果车辆存在漏洞或弱点，则可以通过车辆的通信信道进行非法远程访问或恶意软件入侵攻击。因此，通信信道可能会导致许多安全威胁，如下所述：

– 代码注入，例如，已被篡改的软件二进制可能被注入到通信流中；

– 操纵车辆持有的数据或代码；

– 覆盖车辆持有的数据或代码；

– 擦除/删除车辆持有的数据或代码。

7.1.2.3 使用不可信或不可靠的消息和会话劫持或重放攻击

通过通信信道可能收到来自不可靠或不可信来源的消息。通过通信信道可能实施人在其中攻击和会话劫持。例如，对车辆中通信网关的攻击允许攻击者利用软件的已知漏洞，通过重放攻击来降级电子控制单元的软件或网关的固件，当中重复有效的数据传输是出于恶意。

7.1.2.4 信息披露

通过窃听通信或允许未经授权访问敏感文件或文件夹，信息很容易被泄露。也就是说，通信信道上交换的信息可能通过恶意拦截、干扰辐射和监控通信而被窃听。为此，攻击者可以获得对文件的未经授权的访问权限。

7.1.2.5 拒绝服务攻击

攻击者可以经通信信道向车辆信息系统发送大量垃圾数据来实施拒绝服务攻击，从而使车辆功能大部分被中断。另一方面，在列队或车对车通信的情况下，攻击者可以阻止向其它车辆发送必要数据，从而使其它车辆因缺乏数据而失去控制。这被称为“黑洞攻击”。

7.1.2.6 非特权用户的特权访问

通过通信信道的非法访问，非特权用户可能获得特权访问，例如对系统的根访问。这被称为“未经授权的权限升级”，一旦升级成功，攻击者就可做任何普通用户没法做的事情。

7.1.2.7 嵌入在通信媒质中的病毒

在发现车辆系统中的漏洞后，病毒或恶意软件可以通过通信信道注入车辆系统。病毒可能变成具有特权访问权限的管理员，并可能在车辆中实施任何预期的攻击。例如，如果病毒未经授权对目标车辆系统中的任何文件和信息进行加密，即所谓的“勒索病毒”（ransomware），则车辆系统将失去其功能。

7.1.2.8 含有恶意内容的消息

车辆收到的消息（例如诊断消息或来自其它车辆的消息）或者在车辆内传输的消息可能包含恶意内容。在IVN的情况下，攻击者可以通过病毒注入（见第7.1.2.7节）的方式来修改电子控制单元（ECU）的软件，并通过模仿成一名成员来加入车载网络。

邻近车辆可能收到恶意V2X消息，如协作感知消息（CAM）和分散式环境通知消息（DENM）。V2X通信是基于广播的，因此，大量恶意V2X消息可能会对整个车载网络（包括车辆本身中的IVN）造成有害影响。

也可能收到恶意诊断消息。攻击者可以记录诊断消息，并将其用于重放攻击。此外，甚至车辆的控制消息也可以通过重放攻击来接收。

专有消息通常由原始设备制造商或部件、系统或功能供应商来发送。然而，也可能从攻击者那里收到旨在破坏车辆系统的恶意专有消息。

7.1.3 车辆在更新程序方面面临的威胁

更新车辆系统有两种方式，例如通过OBD端口、安全数字（SD）卡或USB闪盘等便携式设备的的有线更新以及通过无线（OTA）方式的无线更新。要更新的软件可以是车辆的固件或配置数据。大多数电子问题和软件缺陷可以通过电子方式进行更新和解决，而无需物理访问，例如通过OBD测试仪。此外，OTA（无线）更新有助于缩短更新周期，从而最大限度地减少软件的已知漏洞暴露于可能的攻击下。

7.1.3.1 更新程序的误用或损坏

无论是使用OTA更新还是本地或物理更新，更新过程都可能面临使用伪造系统更新程序或受损固件的威胁。

虽然更新过程是完整的，但软件可能在更新过程之前被操纵。软件提供商为更新创建或准备软件，并将软件交付给需要更新的目标系统。因此，软件在投入使用前可能会受到被操纵和破坏的严重威胁。

特别是软件更新过程中使用的密钥和证书等加密材料可能会受到损害，因此可能会导致无效的软件更新。

7.1.3.2 拒绝合法更新

针对更新服务器或网络的拒绝服务攻击可能是软件更新过程中的一种攻击，这种攻击旨在阻止关键软件更新的推出或客户特定功能的开启，也可能是拒绝合法更新。

7.1.4 车辆在不经意人类行为方面面临的威胁

人类行为能在不经意间带来未知的威胁。默认情况下，这些威胁包括未经授权或无意中的软件修改。偶然的错误包括配置违规、编程错误以及因用户或操作者错误而导致的数据损坏。

7.1.4.1 合法行动者对设备或系统的错误配置

一个合法用户可能采取无意识间引发网络攻击。也就是说，在无意的安装、修理或使用期间，一个合法用户可能会异常改变车辆系统的设置。在管理或使用系统或设备包括软件更新时也可能会发生错误。

7.1.4.2 合法行动者无意中为网络攻击提供的便利

一个合法用户（例如所有者、操作者或维护工程师）可能是一个无辜的受害者，并被诱骗采取某种行动以非故意地加载恶意代码（恶意软件）或者发起攻击。此外，合法用户常会出现不遵循已确定之安全程序的现象。

7.1.5 车辆在外部连通与连接方面面临的威胁

为获得各种便利服务，车辆可以配备与后端服务器通信的部件，并可经无线连接与道路用户启用的所有设备进行通信。除了各便利功能，还有安全方面的益处，例如自动紧急呼叫功能和V2X通信支持的那些功能。然而，车辆越多连接到外部实体以增强连通性，就面临越多威胁和漏洞，因为攻击面会因额外的接口而扩大。

7.1.5.1 车辆功能连通性的操纵

操纵车辆功能连通性会导致网络攻击。这种威胁可在以下车辆要素中予以考虑：

– 操纵设计用于远程操作系统的功能：遥控钥匙、汽车防盗锁和充电桩；

– 操纵车辆远程信息处理：例如，远程解锁货物；

– 通过与短距离无线系统或传感器的接口进行操纵。

7.1.5.2 托管的第三方软件

可以连接到IVN的现代车辆信息娱乐系统可以安装第三方应用程序。第三方应用程序可能被破坏或软件安全性差，并被用作攻击车辆系统的方法。

7.1.5.3 连接到外部接口的设备

连接功能带来外部接口，连接到外部接口的设备可被用作攻击手段，来攻击带有以下易受攻击接口的车辆系统：

– 外部接口，如USB端口：用来通过代码注入进行攻击；

– 受病毒感染的媒质：病毒可以通过受感染的媒质来攻击车载系统；

– 诊断访问：利用通过OBD端口上的蓝牙软件狗访问的诊断功能来查看车辆状态，并操纵车辆软件中包含的车辆参数。

7.2 与威胁相关的潜在信息

7.2.1 攻击的潜在目标或动机

当车辆与车辆生态系统中的许多系统或服务实现电子连接时，车辆可能成为潜在网络攻击的目标。此外，攻击者通常不仅通过让世界知道其攻击技能，而且通过让原始设备制造商知道其攻击技能，来寻求经济利益。这些攻击可能对第7.2.1.1至7.2.1.7节所述车辆系统产生影响。

7.2.1.1 提取车辆数据或代码

提取的目标为敏感数据或证书数据，因为它们包含以下可获得经济收益的有用信息：

– 车辆的版权或专有软件。

– 所有者的私人信息，例如个人身份、支付账户信息、地址簿信息、位置信息和车辆电子标识。

– 密钥等。

7.2.1.2 操纵车辆数据或代码

通过操纵车辆数据或代码，攻击者能够模仿或否认正当权益所有方的行为。可以确定以下操纵方法：

– 非法/未经授权更改车辆的电子标识；

– 身份欺诈：如果用户在与收费系统和制造商后端系统通信时想要显示另一个身份；

– 规避监控系统的行动：黑客攻击、篡改或拦截消息，例如，操作数据记录器（ODR）跟踪器数据或运行次数；
– 操纵数据以篡改车辆行驶数据，例如里程、行驶速度、行驶方向和车辆参考时间；
– 未经授权更改系统诊断数据；
– 固件版本欺诈：使用尚无补丁的旧版本固件替换有漏洞补丁的最新固件，以防止某此漏洞。

7.2.1.3 擦除数据或代码

可能会出现未经授权删除或操纵系统事件日志的情况。这种篡改通常使分析数据变得不可能，或者使搜索攻击原因变得困难。

7.2.1.4 引入恶意软件

通过使用多种攻击方法将恶意软件引入车辆系统是攻击者活动的第一步。有各种攻击接口可引入恶意软件，例如使用外部接口和受感染的物理模块。

7.2.1.5 引入新的软件或覆盖现有软件

引入新软件或利用恶意软件覆盖现有软件，这种软件的篡改可能会对车辆控制系统或信息系统中的软件产生严重的网络安全影响。

7.2.1.6 中断系统或操作

针对车辆系统的拒绝服务攻击可通过在CAN总线上发送大量消息或通过高消息率在电子控制单元上引发故障而在内部网络上被触发。

7.2.1.7 操纵车辆参数

操纵车辆参数可对车辆系统产生很大影响，例如未经授权访问并篡改：
– 车辆关键功能的配置参数，例如制动数据或气囊展开阈值；
– 充电参数，例如充电电压、充电功率、电池温度等。

7.2.2 潜在漏洞

7.2.2.1 易受攻击的加密技术

加密技术可能会受到破坏或应用得不充分。密钥和/或证书，包括密码等凭证，可能被利用。例如，如果使用弱密钥和/或密钥长时间没有很好地更新，则密码系统可能会被暴力攻击而损坏。加密技术使用不充分也可能导致密钥和/或证书的泄露。此外，使用已损坏和过时的加密技术会增加信息泄露的风险。

7.2.2.2 受损的车辆零部件或供应品

车辆生态系统中所用的硬件或软件的设计可能被未达到抵御攻击的标准要求。车辆中的零部件或供应品可能遭到破坏，而使车辆受到攻击。

7.2.2.3 软件或硬件开发中的漏洞

软件缺陷的存在可能是潜在可利用漏洞的基础。如果软件未经测试以验证已知的坏代码或错误是否存在并降低未知的坏代码或错误存在的风险，则这一点显得尤其正确。

使用开发其余部分（例如调试端口、联合测试行动组（JTAG）端口、微处理器、开发证书和开发人员密码）也可能促成对电子控制单元的访问或者使攻击者获得更高的权限。

7.2.2.4 网络设计中的漏洞

如果在不必要的通信端口开放的情况下允许网络访问，则诸如未经授权的访问之类的攻击可能会增加。

此外，使用不受保护的网关或接入点（如卡车拖车网关）规避保护并获得对其它网段的访问，可能会导致恶意行为，例如发送任意的CAN总线消息。

7.2.2.5 数据的物理丢失

车辆生态系统中使用的敏感数据可能会因交通事故或盗窃事件中的物理损坏而丢失或泄露。也可能会发生因数字权限管理（DRM）而造成数据丢失的情况，例如删除用户数据。

此外，敏感数据的完整性可能会因信息技术（IT）部件的磨损而丢失，从而导致潜在的级联问题（例如，在密钥更改的情况下）。

7.2.2.6 数据的不经意传输

当车辆的用户发生变动时，私人或敏感数据可能被泄露（例如，车辆被出售或被不同用户用作租用车辆）。

7.2.2.7 系统的物理操纵

物理操纵系统，如原始设备制造商硬件，可能导致攻击。例如，如果将未经授权的硬件添加到车辆上，可能导致“人在其中”的攻击。

附录I

与威胁有关的漏洞或攻击方法示例

（此附录不构成本建议书不可分割的组成部分）

本附录提供了[b-UNECE GRVA]表1中提到的、与威胁有关的漏洞或攻击方法示例。

注 – 表I.1最左栏包含的数字，是[b-UNECE GRVA]中使用的数字。

表I.1 – 与威胁有关的漏洞或攻击方法示例列表

漏洞/威胁的高级和低级描述			漏洞或攻击方法示例	
4.3.1车辆在后端服务器方面面临的威胁	1	用作攻击车辆或提取数据手段的后端服务器	1.1	员工滥用权限（内部人员攻击）。
			1.2	未经授权地通过互联网访问服务器（例如通过后门、未打补丁的系统软件漏洞、SQL攻击或其它方式促成）。
			1.3	未经授权地物理访问服务器（例如通过USB棒或连接服务器的其它媒质促成）。
	2	后端服务器的服务被中断，影响车辆的运作	2.1	对后端服务器的攻击导致其发生故障，例如阻止其与车辆的交互以及车辆所依赖之服务的提供。
	3	后端服务器上保存的数据被丢失或损坏（“数据泄露”）	3.1	员工滥用权限（内部人员攻击）。
			3.2	丢失云中的信息。如果数据存储在第三方云服务提供商中，则可能会因攻击或事故而丢失敏感数据。
			3.3	未经授权地通过互联网接入服务器（例如通过后门、未打补丁的系统软件漏洞、SQL攻击或其它方式促成）。
			3.4	未经授权地物理访问服务器（例如通过USB棒或连接服务器的其它媒质促成）。
			3.5	不经意的数据共享导致的信息泄露（管理错误、将数据存储在位于车库的服务器中）。
4.3.2车辆在通信信道方面面临的威胁	4	欺骗车辆接收的消息或数据	4.1	通过模仿来欺骗消息（例如，列队期间的802.11p V2X、GNSS消息等）。
			4.2	女巫（Sybil）攻击（以欺骗其它车辆，仿佛路上有许多车辆）。
	5	利用通信信道对车载代码/数据进行未经授权的操纵、删除或其它修改	5.1	通信信道许可代码注入，例如，被篡改的软件二进制可能被注入到通信流中。
			5.2	通信信道许可操纵车辆持有的数据/代码。
			5.3	通信信道许可覆盖车辆持有的数据/代码。
			5.4	通信信道许可擦除车辆持有的数据/代码。
			5.5	通信信道许可在车辆中引入数据/代码（写数据/代码）。
	6		6.1	接受来自不可靠或不可信来源的消息。

表I.1 – 与威胁有关的漏洞或攻击方法示例列表

漏洞/威胁的高级和低级描述			漏洞或攻击方法示例	
		通信信道许可接受不可信/不可靠的消息或易遭受会话劫持/重放攻击	6.2	人在其中攻击和会话劫持。
			6.3	重放攻击，例如针对通信网关的攻击允许攻击者降级电子控制单元的软件或网关的固件。
	7	信息易被披露。例如，通过窃听通信或允许未经授权的访问敏感文件或文件夹。	7.1	拦截信息/干扰辐射/监控通信。
			7.2	获得对文件或数据的未经授权访问。
	8	通过通信信道中断车辆功能实施拒绝服务攻击	8.1	向车辆信息系统发送大量垃圾数据，使之无法以正常方式提供服务。
			8.2	黑洞攻击，以破坏车辆之间的通信，使攻击者能够阻断车辆之间的消息。
	9	非特权用户能够特权访问车辆系统	9.1	非特权用户能够获得特权访问，例如根访问。
	10	嵌入在通信媒质中的病毒能够感染车辆系统	10.1	嵌入在通信媒质中的病毒感染车辆系统。
	11	车辆接收的消息（例如X2V或诊断消息）或车辆内传送的消息含有恶意内容	11.1	恶意的内部（例如CAN）消息。
			11.2	恶意的V2X消息，例如基础设施到车辆或车辆到车辆的消息（如CAM、DENM）。
			11.3	恶意的诊断消息。
			11.4	恶意的专有消息（例如那些通常由原始设备制造商或部件/系统/功能供应商发送的消息）。
4.3.3车辆在更新程序方面面临的威胁	12	更新程序的误用或损坏	12.1	破坏软件无线更新过程。这包括篡改系统更新程序或固件。
			12.2	破坏本地/物理软件更新过程。这包括篡改系统更新程序或固件。
			12.3	在更新过程之前软件被操纵（并因此被损坏），尽管更新过程是完整的。
			12.4	破坏软件提供商的密钥，导致无效的更新。
	13	可能拒绝合法更新	13.1	针对更新服务器或网络的拒绝服务攻击，阻止关键软件更新的推出和/或客户特定功能的开启。
4.3.4车辆在不经意人类行为方面面临的威胁	14	合法行动者对设备或系统的错误配置，例如设备或系统的所有者或维护团体。	14.1	安装/修理/使用期间维护团体或所有者对设备的错误配置导致意想不到的后果。
			14.2	设备和系统的错误使用或管理（包括OTA更新）。
	15	合法行动者能够采取行动，这些行动会无意中为网络攻击提供便利。	15.1	无辜的受害者（例如所有者、操作者或维护工程师）被诱骗采取某种行动以非故意地加载恶意软件或者发起一次攻击。
			15.2	未遵循已确定的安全程序。

表I.1 – 与威胁有关的漏洞或攻击方法示例列表

漏洞/威胁的高级和低级描述			漏洞或攻击方法示例	
4.3.5车辆在外部连通与连接方面面临的威胁	16	操纵车辆功能的连通性而促成网络攻击，这可包括远程信息处理、系统许可远程操作、系统使用短距离无线通信。	16.1	操纵设计用于远程操作系统的功能，例如遥控钥匙、汽车防盗锁和充电桩。
			16.2	操纵车辆远程信息处理（例如操纵敏感货物的温度测量、远程打开货舱门）。
			16.3	干扰短距离无线系统或传感器。
	17	托管的第三方软件，例如娱乐应用程序，被当作一种攻击车辆系统的手段。	17.1	破坏应用程序或者软件安全性差的那些应用程序，被用作攻击车辆系统的一种方法。
	18	连接到外部接口的设备，例如USB接口、OBD端口，被当作一种攻击车辆系统的手段。	18.1	外部接口，例如USB或其它端口，被用作一个攻击点，例如通过代码注入进行攻击。
			18.2	连接至车辆系统的、受病毒感染的媒质。
			18.3	诊断访问（例如OBD端口上的软件狗）被用来促成一次攻击，例如（直接地或间接地）操纵车辆参数。
4.3.6攻击的潜在目标或动机	19	提取车辆数据/代码	19.1	从车辆系统提取版权或专有软件（产品剽窃）。
			19.2	未经授权访问所有者的私人信息，例如个人身份、支付账户信息、地址簿信息、位置信息和车辆电子标识符等。
			19.3	提取密钥。
	20	操纵车辆数据/代码	20.1	非法/未经授权更改车辆的电子标识符。
			20.2	身份欺诈：例如，如果用户在与收费系统和制造商后端系统通信时想要显示另一个身份。
			20.3	规避监控系统的行动（例如，黑客攻击/篡改/阻断消息，如ODR跟踪器数据或运行次数）。
			20.4	操纵数据以篡改车辆行驶数据（例如，里程、行驶速度、行驶方向等）。
			20.5	未经授权更改系统诊断数据。
	21	擦除数据/代码	21.1	未经授权删除/操纵系统事件日志。
	22	引入恶意软件	22.2	引入恶意软件或恶意软件行为。
	23	引入新的软件或覆盖现有软件	23.1	篡改车辆控制系统或信息系统中的软件。
	24	中断系统或操作	24.1	拒绝服务，例如，这可通过在CAN总线上发送大量消息或通过高消息率在电子控制单元上引发故障而在内部网络上来触发。
	25	操纵车辆参数	25.1	未经授权访问并篡改车辆关键功能的配置参数，例如制动数据或气囊展开阈值等。
			25.2	未经授权访问并篡改充电参数，例如充电电压、充电功率、电池温度等。

表I.1 – 与威胁有关的漏洞或攻击方法示例列表

漏洞/威胁的高级和低级描述			漏洞或攻击方法示例	
4.3.7若得不到充分保护或加固而可能被利用的潜在漏洞	26	加密技术可能遭到损害或未被充分应用	26.1	短密钥和密钥长时间不更新使攻击者可能破坏密码系统。
			26.2	保护敏感系统的加密算法应用得不充分。
			26.3	使用已弃用或将弃用的加密算法。
	27	零部件或供应品可能受损而使车辆遭到攻击	27.1	硬件或软件设计不当使攻击可能得逞，或者设计得未达到抵御攻击的标准要求。
	28	软件或硬件开发中存在的漏洞	28.1	软件缺陷。软件缺陷的存在可能是潜在可利用漏洞的基础。如果软件未经测试以验证已知的坏代码/错误不存在并降低未知的坏代码/错误存在的风险，则这一点显得尤其正确。
			28.2	使用开发其余部分（例如调试端口、JTAG端口、微处理器、开发证书、开发人员密码等）可能促成对电子控制单元的访问或者使攻击者获得更高的权限。
	29	网络设计中引入的漏洞	29.1	开放多余的互联网端口，为访问网络系统提供了可能。
			29.2	规避网络隔离以获得控制。特定的例子是使用不受保护的网关或接入点（如卡车拖车网关）来规避保护并获得对其它网段的访问，以实施恶意行为，例如发送任意的CAN总线消息。
	30	可能发生数据的物理丢失	30.1	第三方造成的损坏。敏感数据可能会因交通事故或盗窃事件中的物理损坏而丢失或泄露。
			30.2	因数字权限管理（DRM）冲突而造成的丢失。用户数据可能会因DRM问题而被删除。
			30.3	敏感数据（的完整性）可能会因信息技术部件的磨损而丢失，从而导致潜在的级联问题（例如，在密钥更改的情况下）。
	31	可能发生数据的不经意传输	31.1	信息泄露。当汽车更换用户时，私人或敏感数据可能被泄露（例如，被出售或被新租用者用作租用车辆）。
	32	物理操纵系统可能导致的攻击	32.1	操纵原始设备制造商硬件，例如添加到车辆上的未经授权硬件，造成“人在其中”的攻击。

参考书目

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

[b-ISO/IEC 27000] ISO/IEC 27000：2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-UNECE GRVA] UNECE GRVA-01-17 (2017), *Draft Recommendation on cyber security of the Task Force on Cyber Security and Over-the-air Issues of UNECE WP.29 GRVA*. Available [viewed 2020-08-07] at: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦