国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1373

(03/2017)

X系列：数据网、开放系统通信和安全性

安全应用和服务 – 智能交通系统 (ITS) 安全

智能交通系统通信设备的安全软件更新功能

ITU-T X.1373 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
报文处理系统	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
生物测定安全	X.1080–X.1099
安全应用和服务	
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	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	
计算网络安全	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	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI 相关建议书	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.1379**
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	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导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1373 建议书

智能交通系统通信设备的安全软件更新功能

摘要

随着智能交通系统 (ITS) 技术的改善，车辆对其他实体（如其他交通工具）、车辆对车辆(V2V)以及车辆对基础设施(V2I)的通信已经很普遍。由于诸如电子控制单元（ECU），电子收费系统（ETC）和汽车导航系统等车辆内的电气设备变得越来越复杂，为了错误修复、性能和安全改善以避免重大事故，这些电气设备内的软件模块需要适当更新。

为了实现上述要求，ITU-T X.1373建议书在软件更新服务器和有适当安全控制的车辆之间提供了安全软件更新程序。本建议书可以被车辆制造商和ITS相关的产业实际应用，作为一套最佳实践的标准化功能。

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.1373	2017-03-30	17	11.1002/1000/13197

关键词

通信设备、拒绝服务(DoS)攻击、嵌入式系统、硬件安全模块(HSM)、智能交通系统(ITS)、恶意软件、隐私、风险分析、车辆对车辆(V2V)、车辆对基础设施(V2I)、车辆对X(车辆/基础设施) (V2X)、无线通信。

* 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.1373 建议书

智能交通系统通信设备的安全软件更新功能

1 范围

在智能交通系统(ITS)通信环境中，车辆的电子设备的软件模块更新背景下，本建议书旨在为应用层的ITS通信设备提供安全软件更新程序，以预防诸如篡改或恶意入侵车辆内通信设备等威胁。这包括软件更新基本模型、软件更新的安全控制和更新软件模块的抽象数据格式规范。

与车载通信相关的程序不在本建议书的范围内。为了提供参考，本建议书中包括的车载程序是参考性的。

该程序旨在通过互联网和/或ITS专用网络在车辆对基础设施（V2I）通信下应用于ITS车辆内的通信设备。该过程提供了不包含合规要求的技术指南，可以被车辆制造商和ITS相关的产业实际应用，作为一套安全程序和安全控制。

2 参考文件

参考文献下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T X.509] ITU-T X.509 (2012)建议书 | ISO/IEC 9594-8:2014，信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架

[ITU-T X.1521] ITU-T X.1521 (2011)建议书，共同漏洞评分系统。

[ISO/IEC 15408-1] ISO/IEC 15408:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.*

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 威胁[ISO/IEC 27000]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 风险评估：风险分析方法为每个威胁计算的得分。

3.2.2 车载移动网关 (VMG)：一个为控制器区域网络(CAN)（车载公交）的电子控制单元(ECUs)及外部网络的外围智能交通系统（ITS）实体提供通信的模块。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

CA 认证机构
CAN 控制器区域网络
CD 光盘
CRSS 基于CVSS的风险评估系统
CVSS 通用缺陷评估系统
DoS 拒绝服务
DVD 数字多功能光盘
ECU 电子控制单元
ETC 电动收费系统
FT 故障树
GPS 全球定位系统
GUID 全球用户ID
HSM 硬件安全模块
HTTP 超文本传输协议
HTTPS 超文本传输协议安全
ID IDentifier
IT 信息技术
ITS 智能交通系统
LIN 本地互联网络
MAC 消息认证代码
MOST 面向媒体的系统传输
OBD 车载诊断
OEM 原始设备制造商
PC 个人电脑
RPM 每分钟转数
RSS 风险评估系统
SD 安全数字
SHA 安全散列算法

SSL 安全套接字层

TLS 传输层安全

TOE 评估目标

TPM 可信平台模块

TV TeleVision

UI 用户界面

URL 统一资源定位符

USB 通用串行总线

Usvr 更新服务器

V2V 车辆对车辆

V2X 车辆对X (车辆/基础设施)

VMG 车载移动网关

Wi-Fi 无线保真

XML 可扩展标识语言

5 排印惯例

无。

6 远程软件更新基本模型

为了考虑实际的安全架构，本节介绍了软件更新的常规架构的基本模型，其中提供了主要模块和典型软件更新过程的定义。

6.1 用于软件更新的ITS环境模块

图1提供了在ITS通信环境下，用于远程软件更新的车辆周围的主要模块的视图。这些主要模块是信息设备、电子控制单元 (ECUs)、车辆内的车载移动网关（VMG）、更新服务器（Usvr）以及车辆制造商和供应商的日志数据库。与车载通信（如在电子控制单元和车载移动网关）相关的程序不在本建议书的范围内。车载通信使用的模块（如“用户界面”和“电子控制单元”）在下文中以参考性的方式描述。

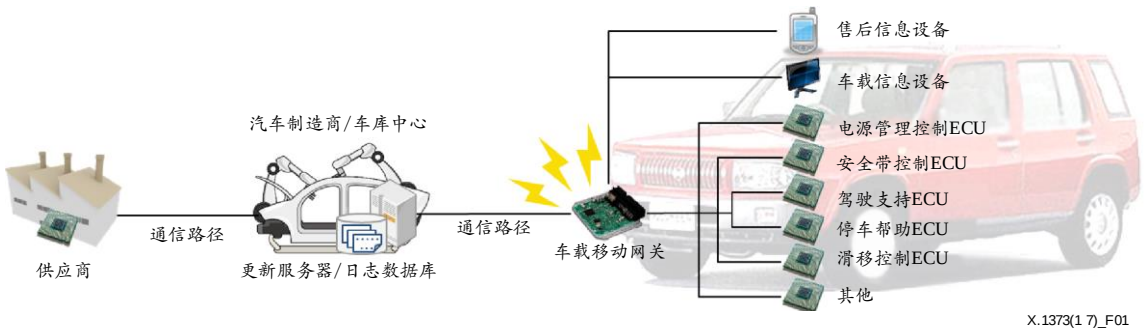


图1 – 车辆周围的基本模块

6.1.1 用户界面（参考性）

用户界面（UI）通常是车载或售后信息设备，即车辆内带有显示和输入的设备。这样的信息设备直接与车辆内的其他设备（如VMG或者ECU（见第6.1.2节））连接，以便能够获得和指示车辆的各种状态信息（如速度、每分钟转速(RPM)、燃油液面以及其他。）特别地，在本建议书中，用户界面用来通知车辆驾驶员更新的必要性。

6.1.2 电子控制单元（ECU）（参考性）

ECU是控制车辆内各种设备的计算机通用术语。在ECU出现的最早几年，其主要功能是点火正时、喷射、怠速调节和发动机限制器的控制，以提高燃料效率和减少气体排放。根据车辆的计算机化， ECU已经将其应用扩展出诸多功能，例如电源管理、安全带控制、驾驶支持、停车帮助、滑移控制、自动变速器等。近年来，车辆内的ECU数量已经从50增加到100，ECU对于安全控制和通信的重要性尤其在增长。然而，由于ECU的发展加入了复杂的软件实施，车辆内ECU的增长给汽车制造商带来了巨大的压力。

6.1.3 车载移动网关

车载移动网关（VMG）是分配给面向“更新服务器”（见第6.1.4节）的模块，以便车辆能进行软件更新。位于车辆内的软件连接管理实体（也被称作“中心网关”、“头单元”、“通信头单元”或者“车载网关（VG）”）在此环境中可以充当VMG的角色，其他任何设备也能够用于软件更新。蜂窝网络（移动网络）和固定网络，通过无线作为车载移动网关和外部ITS实体之间的通信路径。

6.1.4 更新服务器和日志数据库

更新服务器位于汽车制造商或者车库中心，用来从车辆的软件模块收集状态信息，以及将软件更新模块分配给车辆。同样地，在最近的大部分联网计算机（个人电脑（PCs）和智能手机）中，更新服务器的一个重要功能是完全管理和控制车辆内的软件。为了自动管理每辆车辆的这些软件状态，更新服务器应该与日志数据库（存储车辆上的这些软件状态信息作为证据）协同工作。注意，一个更新服务器不仅可以部署给汽车制造商，也可以给供应商或第三方。

6.1.5 供应商

车辆是由汽车供应商提供的数千个汽车零件构成的组件。车载通信设备和ECU由供应商提供，并由汽车制造商组装，组装时要考虑多种设备之间的依赖性。因此，以及通常情况下，车载通信设备的更新模块由对应的供应商而不是汽车制造商提前生产。经过汽车制造商仔细的检测和评估后，提供的更新模块由汽车制造商分配给车辆。

6.2 软件更新程序模型

6.2.1 基本更新程序

图2展示了软件更新程序的典型模型，由车载移动网关通过检查更新的存在来进行初始化。由于车载通信不在本建议书的范围内，图2中与车载通信相关的步骤仅作为参考性的示例，以便为安全更新程序的实施提供参考。

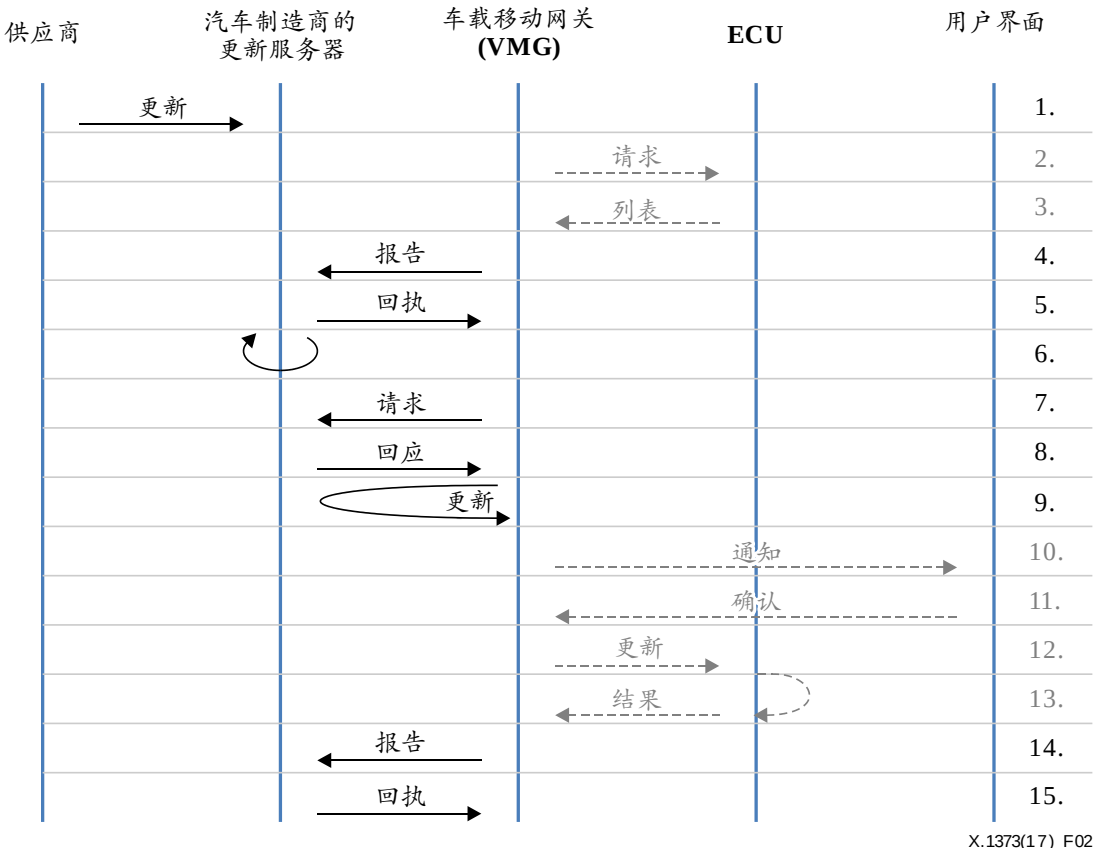


图2 – 软件更新过程的模型

更新程序的步骤如下所述，其中第2、3以及10-13斜体显示的步骤本质上是参考性的：

1) 过程的第一步，汽车组件供应商提供更新模块，该步骤与下列步骤异步发生。

2) *随着更新程序的开始，车载移动网关请求*ECU*提交他们的软件清单。*

3) *一个* ECU*检查它的软件状态，收集软件模块列表并报告给*VMG。

4) VMG将收集列表提交给更新服务器去检查车辆是否存在更新。

5) 更新服务器将提交列表的回执发送给VMG。

6) 根据列表，更新服务器检测车辆安装软件的状态，并且决定ECUs需要的软件更新。

7) 由于检测可能需要较长的时间，VMG周期性地检查车辆更新的必要性。

8) 如果有任何更新，更新服务器发送更新的统一资源定位符(URLs)获取；否则，它仅发回确认消息。

9) 如果车辆有任何更新，VMG 连接更新服务器为车辆下载更新模块。

10) *将更新应用到*ECU*之前，* VMG*通知驾驶员确认更新的应用。*

11) *驾驶员确认并接受应用更新。*

12) VMG 将更新文件传送至相应的ECUs，并请求他们应用更新（见第6.2.3节）。

13) 每个ECU 应用更新，并报告应用结果给车载移动网关。

14) 车载移动网关给更新服务器提交应用结果报告。

15) 最后，更新服务器将更新信息回执发回。如果更新应用失败或者其他更新被发现，更新服务器重试从步骤6到14的过程，直到应用程序成功。(见第 6.2.2节)

6.2.2 无限重试的考虑

根据步骤15提到的重试直到成功的描述，注意，在一些情况下，程序将永远不会成功，最终该描述会造成VMG重试无数次。 为了避免这种情况，重试的次数应该被限制为数字‘N’，该数字可以依据更新程序的策略来决定。如何定义更新的策略不在本建议书的范围内。

6.2.3 资源约束的考虑

至于车辆内的更新软件实际应用（6.2.1节中参考性的第12步），车辆内有模块没有足够的内存用于一次缓存整个更新模块。对于那些模块，应用通过流碎片化数据的流更新技术是必需的。

通常而言，车辆内的任何模块，无论属于何种更新系统，都应认真考虑设备的有限资源的约束，例如内存、存储器和网络吞吐量。

7 安全软件更新程序规范

本节明确更新服务器和带有安全功能的软件更新车辆（VMG）之间的实践步骤和应用消息格式。注意本建议书不明确消息保密功能。保密可以由较低层协议提供（例如传输文本协议安全（HTTPS）和安全隧道协议等。）

该过程需要考虑车辆安全性能的差异性。因此，在本建议书中，带有非对称加密算法的车辆应用数字签名方法 (第7.1.1节)，不带有非对称加密算法的车辆应用消息认证代码（MAC）方法(第7.1.2节) 来进行安全消息交换。

7.1 带有安全功能的一般消息格式

本节介绍带有安全功能的一般消息格式，包括消息发送者的认证方法和消息完整性的验证。至于完整性和认证技术，带有公钥算法的数字签名方法和/或带有共享密钥的消息认证代码可以被应用。在安全软件更新程序中，每条消息应该由下列所述方法中的一种构成。

7.1.1 数字签名方法

作为一种实施方法，依据[ITU-T X.509]的数字签名可以应用于通过硬件安全模块（HSM）（例如，TPM）的具有非对称加密能力的车辆之间的实体认证以及消息完整性的验证。

7.1.2 MAC 方法

由于共享密钥算法相对于公钥算法需要更少的处理负载，共享密钥算法适合具有低处理性能的设备。然而，在共享密钥算法中，发送者和接受者使用同一个密钥，因此大量设备使用同一个密钥。该操作需要一旦密钥泄露后，系统中的所有密钥都更新。除此之外，由于共享密钥本身不提供发送者认证，每条消息需要包括发送者设备ID，其预先假定设备中的ID没有被不适当地操纵。

7.2 协议定义和数据格式

应用数据格式只为软件更新传输消息，在前节描述的通用消息格式中包含。本节首先定义软件更新程序中的消息类型，然后介绍消息类型规范。消息的示例具有用于信息的扩展标记语言（XML）格式。

7.2.1 协议概述

依据第6节描述的软件更新程序模型，消息根据它们的目标被分类为几种类型，如图3所示。车载通信程序不在本建议书的范围内，在图中用灰色字体表示。

注 – 车载通信程序可以在 [b-ISO 14229]和[b-ISO 13440]中找到。

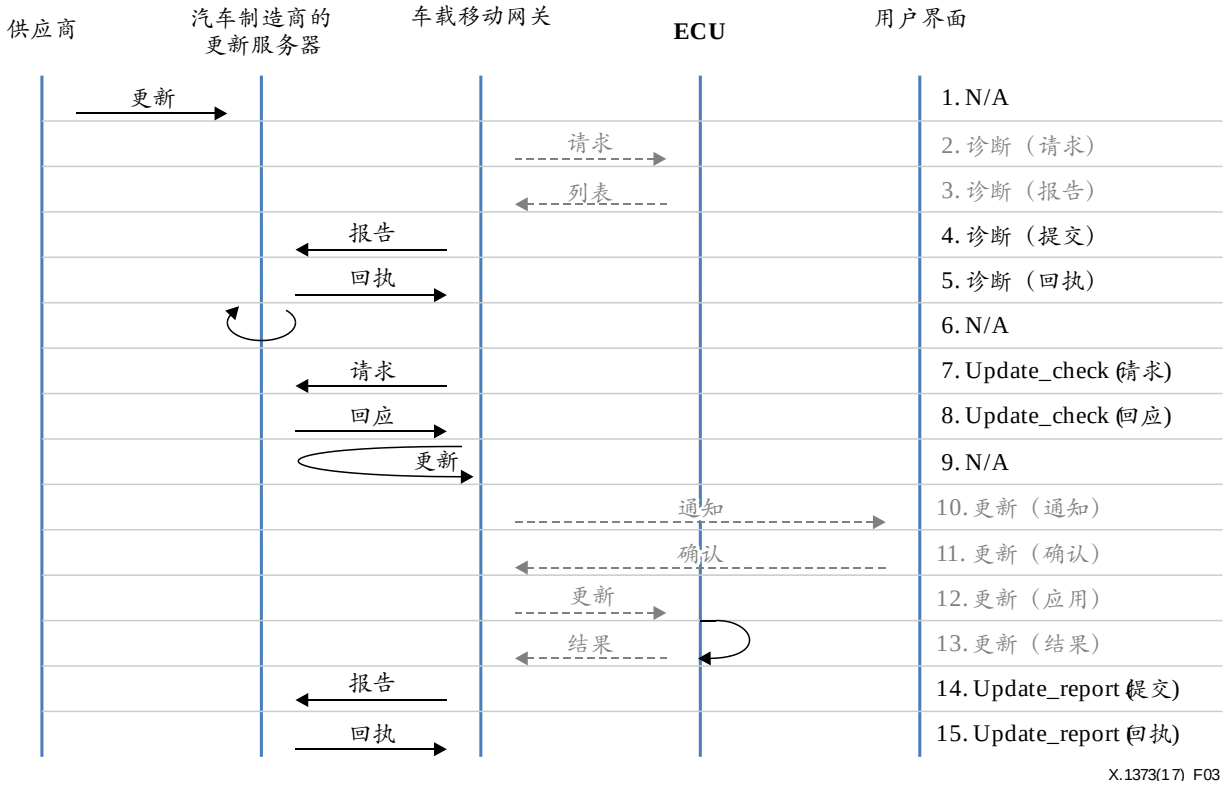


图3 – 消息种类定义

在步骤2、3、4和5中，因为消息的目的是请求和报告每个ECU的软件状态，消息被分类为“诊断”。以同样的方式，步骤 7 和 8 中的消息被分类为“update_check”。步骤10、11、 12和13为“更新”，消息用来确认和应用更新。最后，更新的结果通过步骤14 和15的“update_report”消息提交。消息的类型、子类型和代码见表1。

表1 – 消息类型

类型	子类型	来自	到	目的
诊断	请求	*VMG*	*ECU*	请求软件状态诊断
	报告	*ECU*	*VMG*	包括软件状态的诊断结果
	提交	VMG	Usvr	报告车辆内ECU结果
	回执	Usvr	VMG	诊断报告提交回执
update_check	请求	VMG	Usvr	更新模块请求
	回应	Usvr	VMG	提供的更新模块
更新	通知	*VMG*	*UI*	为驾驶员介绍更新的通知消息
	确认	*UI*	*VMG*	来自驾驶员的确认消息去应用更新
	应用	*VMG*	*ECU*	包括更新模块的请求消息
	结果	*ECU*	*VMG*	更新模块应用的结果
update_report	提交	VMG	Usvr	更新应用的报告
	回执	Usvr	VMG	报告回执
* Usvr：更新服务器 * UI：用户界面				

注 – 表1中，用灰色斜体表示不在本建议书范围内，仅提供信息的内容。

7.2.2 诊断消息

为了给车辆测定需要的更新模块，诊断消息在更新服务器和VMG间被用来将车辆上传的软件信息给更新服务器。

7.2.2.1 诊断（提交）消息

从车辆收集了诊断结果后， VMG提交软件信息清单给制造商（或者车库）的更新服务器。诊断（提交）消息包括车辆的身份信息（vid）以及从诊断（报告）消息中提取的软件信息清单。

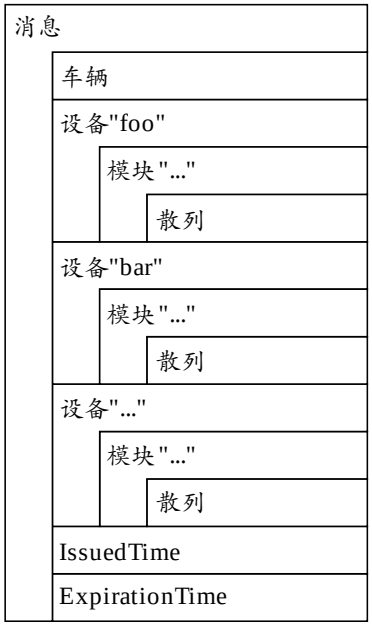


图4 – 诊断（提交）消息结构

表2 – 诊断（提交）消息元素

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“诊断”）
	子类型	消息子类型（总是“提交”）
	sessionid	会话标识（ID）是与诊断会话相关的随机全球用户ID（GUID）。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
车辆	-	车辆信息容器。它包括多个模块元素
	名称	车辆名称，如果有的话
	模型	汽车制造商提供的车辆模型名称
	modelid	车辆模型名称
	vehicleid	汽车制造商/供应商定义的车辆标识
	区域设置	车辆的区域信息

表2 – 诊断（提交）消息元素

元素	元素中的属性	描述
设备	-	设备信息容器。它包括多个模块元素
	名称	设备名称，如果有的话
	类型	设备类型名称，例如“电源管理ECU”“安全带控制ECU”等
	模型	设备的模型名称
	deviceid	汽车制造商/供应商定义的设备标识
	hwversion	该硬件模块版本
模块	-	模块信息容器，包括散列元素
	moduleid	模块标识是一种由汽车制造商/供应商提供的独特的标识
	版本	该软件模块版本
	nextversion	过程中模块更新的版本，主要用来在更新期间发送回应消息
散列	-	散列是散列值和散列算法信息的容器
	算法	散列功能算法（例：SHA-3、SHA-256等。）
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表3 – 诊断（提交）消息示例

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}" trustlevel="3">
<Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
01”>
<Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA}" version="1.3.23.0"
nextversion=""/>
<Hash algorithm="SHA-256">hash data here</Hash>
</Module>
<Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion=""/>
<Hash algorithm="SHA-256">hash data here</Hash>
</Module>
</Device>
<Device name="device2" type="ECU" model="model1" id="did0987234"hwversion=”HC-
02”>
<Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion=""/>
<Hash algorithm="SHA-256">hash data here</Hash>
</Module>
</Device>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.2.2 诊断（回执）消息

用诊断（提交）消息上传了车辆的软件信息后，更新服务器发回带有诊断（回执）消息的回执，以便车辆能识别该提交成功完成，继而车辆可以继续下一个状态（update_check）。

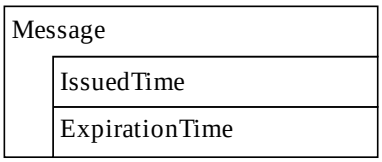


图5 – 诊断（回执）消息结构

表4 – 诊断（回执）消息元素

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“诊断”）
	子类型	消息子类型（总是“回执”）
	sessionid	会话标识是与诊断会话相关的随机GUID。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
	状态	确认报告以进行诊断（提交）
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表5 – 诊断（回执）消息示例

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="receipt"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{E313159C-2081-4A10-B61D-4F81D074D54F}" trustlevel="3"
status=”yes”>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3 update_check消息

当软件信息通过诊断消息上传至更新服务器后，更新服务器开始分析以决定车辆需要的更新模块，这可能需要花费较长时间。update_check消息被周期性地用来询问更新服务器的决定。update_check 消息有两种子类型：请求和回应，在 VMG和更新服务器之间进行转移。

7.2.3.1 update_check（请求）消息

update_check（请求）消息由VMG传输至更新服务器以检查更新的必要性。该消息包括待检测的模块信息，这与诊断（回执）消息非常相似。

图6 – update_check（请求）消息结构

表6 – update_check（请求）消息元素描述

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“update_check”）
	子类型	消息子类型（总是“请求”）
	sessionid	会话标识是与诊断会话相关的随机GUID。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
车辆	-	车辆信息容器。它包括多个模块元素
	名称	车辆名称，如果有的话
	模型	汽车制造商提供的车辆模型名称
	modelid	车辆模型名称
	vehicleid	汽车制造商/供应商定义的车辆标识
	区域设置	车辆的区域信息
设备	-	设备信息容器。它包括多个模块元素
	名称	设备名称，如果有的话
	类型	设备类型名称，例如“电源管理ECU”“安全带控制ECU”等

表6 – update_check（请求）消息元素描述

元素	元素中的属性	描述
	模型	设备的模型名称
	deviceid	汽车制造商/供应商定义的设备标识
	hwversion	该硬件模块版本
模块	-	模块信息容器，包括散列元素
	moduleid	模块标识是一种由汽车制造商/供应商提供的独特的标识
	版本	该软件模块版本
	nextversion	过程中模块更新的版本，主要用来在更新期间发送回应消息
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表7 – update_check（请求）消息示例

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="request"
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
<Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
01”>
<Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}" version="1.3.23.0"
nextversion=""/>
<Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion=""/>
</Device>
<Device name="device2" type="ECU" model="model1" id="did0987234"hwversion=”HC-
02”>
<Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion=""/>
</Device>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3.2 update_check（回应）消息

作为对update_check （请求）消息的回应，更新服务器发回检测结果。如果有车辆内任何模块所需要的更新， update_check（回应）消息下载URLs来获得更新模块。注意一个更新消息不包括更新模块本身的二进制文件，而VMG基于update_check（回应）消息中的资源信息使用另一个连接下载更新消息。

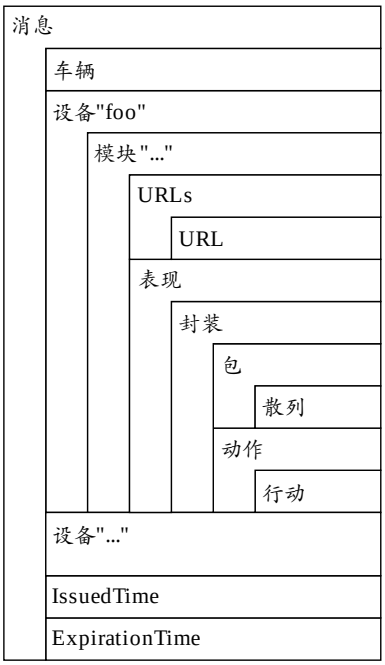


图7 – update_check（回应）消息结构

表8 – update_check（回应）消息元素描述

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“update_check”）
	子类型	消息子类型（总是“回应”）
	sessionid	会话标识是与诊断会话相关的随机GUID。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
车辆	-	车辆信息容器。它包括多个模块元素
	名称	车辆名称，如果有的话
	模型	汽车制造商提供的车辆模型名称
	modelid	车辆模型名称
	vehicleid	汽车制造商/供应商定义的车辆标识
	区域设置	车辆的区域信息

表8 – update_check（回应）消息元素描述

元素	元素中的属性	描述
设备	-	设备信息容器。它包括多个模块元素
	名称	设备名称，如果有的话
	类型	设备类型名称，例如“电源管理ECU”“安全带控制ECU”等
	模型	设备的模型名称
	deviceid	汽车制造商/供应商定义的设备标识
	hwversion	该硬件模块版本
模块	-	模块信息容器，包括散列元素
	moduleid	模块标识是一种由汽车制造商/供应商提供的独特的标识
	版本	该软件模块版本
	nextversion	过程中模块更新的版本，主要用来在更新期间发送回应消息
	状态	更新检测的状态。如果没有更新，将设置“noupdate”，如果该模块有任何更新，将设置“ok”
URLs	-	如果有任何更新的URL元素容器。当状态为ok时，该元素被包含于模块元素
URL	-	更新文件的URL。为了给第一个URL（服务器）备份，URL元素应至少被列出两次。URL元素的最大数量应该在考虑VMG 计算资源的前提下谨慎决定
	代码库	更新文件的位置
表现	-	描述需要被安装的模块，以及与那些文件一起需要采取的行动
	版本	该更新模块的特定新版本数量
封装	-	一套需要安装的文件。不包含属性。包含一个或多个包的子元素
包	-	该模块需要安装的单个文件
	名称	描述更新模块的文件名
	大小	包含更新模块的字节大小.
	描述	更新模块的描述
散列	-	散列值和它的散列算法的容器
	算法	散列功能的算法（例： SHA-3、SHA-256，等）
动作	-	当封装中所有需要的文件都成功下载后，安装模块需要执行的动作
行动	-	作为安装过程的一部分的单个执行的行动
	事件	当用固定字符表示的时候，该行动需执行。一个“预安装”、“安装”、“安装后”和“更新”
	参数	将要输入到安装过程的参数
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表9 – update_check（回应）消息的示例

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="response
" sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
<Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion="HB-
01">
<Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}" version="1.3.23.0"
nextversion="" status="ok">
<Urls>
<Url codebase="http://update1.server/this/is/an/example/url/"/>
<Url codebase="http://update2.server/this/is/an/example/url/"/>
<Url codebase="http://update3.server/this/is/an/example/url/"/>
</Urls>
<Manifest version="1.4.0">
<Packages>
<Package name="module1.bin" size="589" description="This update provides ...">
<Hash algorithm="SHA-256">hash data here</Hash>
</Package>
</Packages>
<Actions>
<Action arguments="--argument-for-installation" event="install"/>
</Actions>
</Manifest>
</Module>
<Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion="" status="noupdate">
</Module>
</Device>
<Device name="device2" type="ECU" model="model1" id="did0987234"hwversion="HC-
02">
<Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion="" status="noupdate">
</Module>
</Device>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.4 更新消息

车辆内进行的更新过程不在本建议书的范围内。没有更新消息的定义和规范。

7.2.5 update_report 消息

作为更新程序序列的最后一步，VMG将搜集的所有设备的更新应用报告提交给更新服务器，以方便后者能够从远程站点掌握和管理每一台车辆。VMG通过update_report （提交）消息将报告发送给更新服务器。最后，更新服务器发送报告（update_report（回执）消息)回执给VMG，使其可以识别整个更新过程的结束。

7.2.5.1 update_report（提交）消息

从设备收集了应用报告后，VMG发送update_report（提交）消息给更新服务器。该消息包括应用结果和软件（例：诊断（提交）消息）当前的状态。

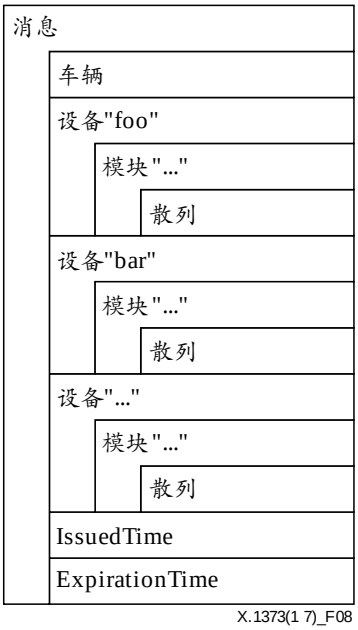


图8 – update_report（提交）消息结构

表10 – update_report（提交）消息元素述

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“update_report”）
	子类型	消息子类型（总是“提交”）
	sessionid	会话标识是与诊断会话相关的随机GUID。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
车辆	-	车辆信息容器。它包括多个模块元素
	名称	车辆名称，如果有的话
	模型	汽车制造商提供的车辆模型名称
	modelid	车辆模型名称
	vehicleid	汽车制造商/供应商定义的车辆标识
	区域设置	车辆的区域信息

表10 – update_report（提交）消息元素述

元素	元素中的属性	描述
设备	-	设备信息容器。它包括多个模块元素
	名称	设备名称，如果有的话
	类型	设备类型名称，例如“电源管理ECU”“安全带控制ECU”等
	模型	设备的模型名称
	deviceid	汽车制造商/供应商定义的设备标识
	hwversion	该硬件模块版本
模块	-	模块信息容器，包括散列元素
	moduleid	模块标识是一种由汽车制造商/供应商提供的独特的标识
	版本	该软件模块版本
	nextversion	过程中模块更新的版本，主要用来在更新期间发送回应消息
	状态	该模块的应用结果
散列	-	散列值和它的散列算法的容器
	算法	散列功能的算法（例： SHA-3、SHA-256，等）
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表11 – update_report（提交）消息示例

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="submit"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{3F7A6438-8306-447E-A1BB-99CED4C2B6AD}" trustlevel="3">
<Vehicle name="vehicleName" modelid="mid34987130" type="ECU" model="modelName"
vid="vid0987234" locale=”CH”/>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
01”>
<Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}" version="1.4.0"
nextversion="" status="ok">
<Hash algorithm="SHA-256">hash data here</ModuleHash>
</Module>
<Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion="" status="ok">
<Hash algorithm="SHA-256">hash data here</ModuleHash>
</Module>
</Device>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
02”>
<Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion="" status=”ok”>
<Hash algorithm="SHA-256">hash data here</ModuleHash>
</Module>
</Device>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.5.2 update_report（回执）消息

在该序列的结尾，更新服务器给VMG 发送update_report（回执）消息使其能识别整个更新程序的终止。update_report（回执）的消息格式基本与诊断（回执）消息相同。

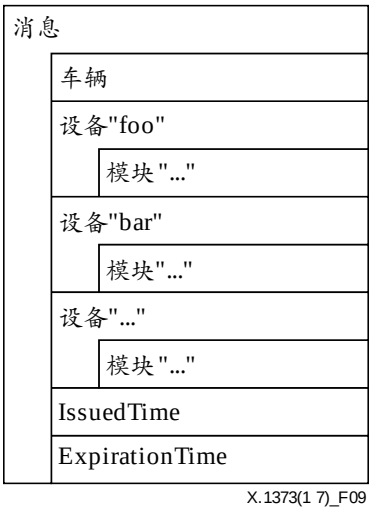


图9 – update_report（回执）消息结构

表12 – update_report（回执）消息元素

元素	元素中的属性	描述
消息	-	消息容器
	协议	总是 '1.0"
	版本	消息发送者的版本数量
	类型	消息类型（总是“update_report”）
	子类型	消息子类型（总是“回执”）
	sessionid	会话标识是与诊断会话相关的随机GUID。相同的会话标识应用于一组诊断请求、报告、提交和回执消息
	trustlevel	Trust level由生成此消息的设备的安全功能和安全要求来确定
	ownerid	拥有者标识由汽车制造商/供应商提供
	messageid	消息标识是与个人信息相关的随机GUID
车辆	-	车辆信息容器。它包括多个模块元素
	名称	车辆名称，如果有的话
	模型	汽车制造商提供的车辆模型名称
	modelid	车辆模型名称
	vehicleid	汽车制造商/供应商定义的车辆标识
	区域设置	车辆的区域信息
设备	-	设备信息容器。它包括多个模块元素
	名称	设备名称，如果有的话
	类型	设备类型名称，例如“电源管理ECU”“安全带控制ECU”等
	模型	设备的模型名称
	deviceid	汽车制造商/供应商定义的设备标识
	hwversion	该硬件模块版本
模块	-	模块信息容器，包括散列元素
	moduleid	模块标识是一种由汽车制造商/供应商提供的独特的标识
	版本	该软件模块版本
	nextversion	过程中模块更新的版本，主要用来在更新期间发送回应消息
	状态	该模块的确认报告
IssuedTime	-	生成该消息需要的时间
ExpirationTime	-	该消息的有效期

表13 – update_report（回执）消息示例

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="receipt"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{B5585708-6BDA-4B07-B2CB-5E9241F63271}" trustlevel="3">
<Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
01”>
<Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}" version="1.4.0"
nextversion="" status="ok"/>
<Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion="" status="ok"/>
</Device>
<Device name="device1" type="ECU" model="model1" id="did0987234"hwversion=”HB-
02”>
<Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion="" status="ok"/>
</Module>
</Device>
<IssuedTime "1903-07-01T00:00:00Z"/>
<ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

附录 I

风险分析方法论

（本附录不构成本建议书的一部分）

I.1 依据[b-JASO TP15002]的风险分析方法论

该附录提供与附录 II相关的详细信息。这些信息依据[b-JASO TP15002]中有关于汽车信息安全的指导。

信息安全在设计嵌入式系统时已经变得很重要。至今为止，多种IT系统的安全攻击示例已广为人知，评估风险的技术诀窍在IT系统设计中不断积累。在评估IT产品时所需要的基本安全概念在 [ISO/IEC 15408-1]中给出。关于评估， [ISO/IEC 15408-1]使用评估对象（TOE）这一术语。有一些资产是TOE的所有者可能赋值的实体。 [ISO/IEC 15408-1]旨在为TOE建立安全目标，其是对抗所识别的威胁和/或满足所识别的组织安全策略和/或假设的意图的声明。依据威胁发生的可能性以及威胁发生时对资产的影响，威胁会给资产带来风险。然而，[ISO/IEC 15408-1]没有明确如何进行威胁提取和风险分析。

就嵌入式系统而言，本附录根据[ISO/IEC 15408-1]的框架描述了威胁提取以及如何执行风险分析。这里，风险分析不依赖于安全设计中的技术诀窍。因此，在本建议书中，风险分析方法CRSS [b-JASO TP15002] 计算嵌入式系统的威胁风险等级。这种方法的特点如下：(1) 在系统模型定义步骤和威胁分析步骤中制定输出；(2) 我们使用之前步骤提供的信息来设置参数值。

[b-JASO TP15002]中的安全评估过程包括以下阶段：

阶段1：评估目标定义；

阶段2：威胁识别；

阶段3：风险分析。

每个阶段的解释如下。

I.1.1 阶段1：评估目标定义

威胁识别的目标在下个阶段明确。

下述4个步骤在阶段1中执行。

步骤1：共享意识建设

基于系统概述文档，以及为了使所有项目成员能就目标系统的生命周期和系统建设建立共识，准备诸如系统构造图、系统功能和系统使用数据的信息。

步骤2：评估目标模型图构建

构建一个“评估目标模型图”，来明确系统组件和系统组件间的信息流。

步骤3：模块功能概述定义

对于评估目标模型图中描述的每个组成模块，其能提供的功能以及其保护的资产都被明确了。这样，“模块功能概述”表被构建。

安全威胁可以这样描述：在评估目标系统中“哪些威胁代理存在，他们要对哪些资产执行何种不利的行动”。除了信息，哪些通常被视作需要保护的资产， 汽车嵌入式系统中的资产也包括嵌入式系统软件以及控制机械（如引擎或者刹车）的功能。

系统模型根据资产的性质，以及指定与这些资产相关的数据流的数据流图生成。

至于何种不利的行动将被执行（威胁），每个入口点可能发生的事情都会被研究，并且这也被视为可以对每种类型的资产发生的称为机密性，完整性或可用性的故障类型。例如，汽车IT 系统功能像预期一样正确地操作是很重要的，因此完整性或可用性的故障一定要被阻止。同样地，中心服务器和车载智能交通系统（ITS）设备间的信息交换受保护免于披露和修改是很重要的，因此机密性或者完整性故障一定要被阻止。表I.1展示了车辆应保护的信息和其他资产的示例。

表I.1 – 车辆应保护的信息和其他资产的示例（车辆信息安全）

应被保护的对象	描述
“基本控制”功能操作	“基本控制功能”的一致性和可用性，“基本控制功能”的执行环境，操作的通信
对于车辆来说独特的信息	对于汽车车身独特的信息（车辆ID、设备ID等），认证代码，以及诸如行驶历史和操作历史的累积信息
车辆状态信息	代表车辆状态的数据，例如：位置、行驶速度和目的地
用户信息	用户（驾驶员/乘客）的个人信息、认证信息、计费信息、使用历史和操作历史
软件	与车辆“基本控制功能”和“扩展功能”相关的软件。示例包括电子控制单元（ECU）的软件
内容	为了视频、音乐、地图等的应用的数据
配置信息	为硬件、软件等的行为设置数据

步骤4：生命周期目标范围的定义

“生命周期表”明确了构建的目标系统的整个生命周期。

威胁代理是指在车辆生命周期的任何时刻涉及的人员，包括其制造商，购买车辆的车主的使用是新的或二手的，以及其最终处置。这是因为汽车嵌入式系统的机密性信息不仅能在普通使用阶段存储和获取，也能在其他诸如生产、运输或者服务的阶段存储和获取。TOE生命周期详细说明见表I.2。

表I.2 – TOE生命周期

阶段	子阶段	概述	涉及人员
操作	运输	初始的设备制造商 （OEM）的工作人员将制造好的车辆运输给车辆经销商。他让运输业务经营者去做这项工作	· OEM的工作人员 · 运输业务经营者 · 车辆经销商的工作人员 · 第三方
	车辆交付	车辆经销商的工作人员将车辆交付给其拥有者	· 车辆经销商的工作人员 · 拥有者 · 第三方
	普通操作/使用	车辆拥有者或者用户使用车辆。服务器管理员作为提供软件的更新服务器的管理员参与其中。电信运营商参与其中提供通信网络	· 拥有者或用户 · 服务器管理员 · 电信运营商 · 第三方
	普通操作/使用 软件下载	通过更新服务器为软件更新做准备，车辆从更新服务器下载软件	· OEM的工作人员 · 供应商的工作人员 · 服务器管理员 · 电信运营商 · 第三方
	维护 （通过更新服务器的软件更新） 软件更新	停车时，软件更新被执行。服务器管理员作为更新服务器的管理员参与其中。电信运营商参与其中提供通信网络。供应商的工作人员作为使用通信网络的服务供应者	· OEM的工作人员 · 供应商的工作人员 · 服务器管理员 · 电信运营商 · 第三方
	维护 （通过车载诊断系统（OBD）连接器的软件更新）	车辆经销商的工作人员或者维修厂的工作人员在车辆检测时通过OBD连接器更新软件	· 车辆经销商的工作人员 · 维修厂的工作人员 · 拥有者或用户 · 第三方

I.1.2 阶段2：威胁识别

阶段1定义的设计TOE的安全问题被识别。

下列三个步骤在阶段2中执行。

步骤1：假设设置

为了明确被识别的威胁的范围，假设依据评估目标模型图、模块功能概述和生命周期表来定义。阶段2中识别的威胁的范围是有限的。TOE环境的假设被定义。带有“A”前缀的标识符被指派给每个已识别的威胁。这样，“假设表”被构建。

TOE在以下假设下操作：

A.Reliability_OfficeStaff （OEM 的工作人员/供应商的工作人员/车辆经销商的工作人员/维修厂的工作人员的可靠性）

OEM的工作人员或者供应商的工作人员不能物理地进入攻击目标车辆。此外，车辆经销商的工作人员/维修厂的工作人员不能在普通操作/使用阶段物理地进入车辆。

A.Reliability_ServiceProvider （服务器管理员/电信运营商的可靠性）

更新服务器的管理员/电信运营商不能物理地进入车辆。此外，更新服务器管理员/电信运营商不会故意地造成威胁。

A.Reliability_User （拥有者/用户的可靠性）

拥有者/用户，在维护阶段，不能物理地进入攻击目标车辆。

拥有者/用户，在维护阶段，不能物理地进入车辆。此外，拥有者/用户在普通操作/使用阶段经常会锁门。此外，拥有者/用户不允许未经允许的相关人员在普通操作/使用阶段进入车辆内部。

A.Operation_Server （评估目标外的服务器保护）

更新服务器恰当操作，意味着相关人员不会获取/操作存储在服务器的信息。

A.Control_OBD-Tool （评估目标外的测量设备等的保护）

测量设备恰当操作，意味着相关人员不会获取/操作存储在测量设备的信息。

步骤2：威胁识别

依据每个组件的评估目标模型图、模块功能概述和生命周期表，从哪里（入口点）、谁（威胁代理）、什么时间（生命周期阶段）、为什么（原因）和什么（不利行动）几个视角解释的威胁的身份见表I.3。带有前缀“T”的标识符被指派给每个已识别的威胁。这样，“威胁表”被构建。

通过将这些视角应用于在第I.1节描述的评估目标系统时所研究的系统模型、生命周期和不利行动，可以详尽地确定哪些威胁代理存在和他们对哪些资产及在哪些阶段将执行不利行动。

表I.3 – 威胁识别视角

视角	解释
哪里	识别攻击的入口点
谁	识别威胁代理
什么时间	识别攻击的生命周期阶段
为什么	识别攻击的原因
什么	识别不利行动

步骤3：机构的安全策略设置

机构的安全策略定义了由于除了威胁之外的其他原因而需要安全对策的要求。示例有在操作环境中的TOE的发展需要遵守的法律和行业指导。已被识别的涉及系统发展的法律或者公司条例应该被定义为TOE 的安全问题。带有前缀“O”的标识符被指派给每个安全策略。这样，“机构的安全策略表”被构建。

没有应用于TOE 的机构安全策略。

I.1.3 阶段3：风险分析

该步骤明确被识别的威胁的风险级别。

威胁表中的每个威胁的优先级被计算。

下述两个步骤在阶段3中被执行。

步骤1：风险评估

通常通过资产的价值和攻击成本推导得出威胁对IT系统造成的风险，这取决于威胁的执行方式。在有大量的攻击示例以及攻击方式成本能够达成共识时（包括诸如执行攻击所需的执行时间和执行他的人的特点等因素），这是一种有效的方法。在汽车嵌入式系统中，当一定数量的攻击示例已经在试验级别被识别，IT系统存在的各种攻击方式变量不可用。结果，测量攻击方式成本变得困难。

I.1.3.1 CRSS

基于CVSS的风险评估系统（CRSS）是一种威胁风险评估方法，依据[ITU-T X.1521]的通用缺陷评估系统（CVSS），即[ITU-T X.1521]的风险评估系统（RSS），用来评估[b-JASO TP15002]的IT系统缺陷的严重程度。 CVSS由三个度量指标组组成：基本组、时间组和环境组。每一组均含有一套度量指标。这些度量指标组的描述如下：

– 基本组：代表随时间和在用户环境中不断出现的漏洞的固有和根本特性。第6.5节具体讨论基本度量组。

– 时间组：代表随着时间但不随用户环境变化的漏洞的特性。

– 环境组：代表与特定用户环境有关的、独特的漏洞特性。

CRSS通过CVSS评估中的基本度量组评估风险评分。基本度量组捕获随时间在整个用户环境中出现的漏洞的特性。访问向量，访问复杂性和认证度量捕获缺陷是如何被访问的，以及是否需要额外条件来发现缺陷。

CRSS方法就机密性、完整性和可用性给每个资产指派资产值，然后从安装攻击的容易程度和影响程度计算风险得分。

安装攻击的容易程度来自反映威胁代理获得资产需要多近的距离以及他们为获取资产需要通过的障碍的多少的度量。安装攻击的容易程度分类示例见表I.4。

影响程度测量缺陷如果被发现将如何直接作用于资产，这里，影响被独立地定义为机密性、完整性和可用性的损失程度。例如，缺陷可能造成完整性和可用性的部分损失，但是机密性不会损失。影响程度的分类示例见表I.5。

表I.4 – 安装攻击的容易程度分类示例
（[b-JASO TP15002]的表D.2）

参数	考虑原则	分类	示例
参数向量（AV）： 攻击起源的分类	造成威胁的攻击的起源（哪里）分类	位置（L）	USB存储
		相邻网络（A）	Wi-Fi连接设备
		网络 （N）	移动线
获取复杂性 （AC）： 攻击条件的复杂性程度	攻击要求的技能和知识数量分类	高 （H）	攻击需要技能和知识
		中 （M）	攻击需要知识
		低（L）	攻击需要无（少量）技能和知识
认证（Au）： 攻击前需要的认证数量	资产和威胁代理之间的认证数量分类	多重 （M）	多重
		单个 （S）	单个
		无（N）	不需要

表I.5 – 影响程度的分类示例
（[b-JASO TP15002]的表D.3）

资产	分类	C: 机密性影响			I: 完整性影响			A: 可用性影响		
		无	部分	全部	无	部分	全部	无	部分	全部
移动通信功能	更新服务	Y					Y			Y
移动认证信息				Y			Y	Y		
软件获取功能		Y					Y			Y
软件				Y			Y	Y		
远程软件更新功能		Y					Y			Y
软件				Y			Y	Y		
GPS接收功能	信息处理	Y				Y			Y	
Wi-Fi连接功能		Y				Y			Y	
Wi-Fi认证信息			Y			Y		Y		
USB连接功能		Y				Y			Y	
CAN通信功能	车辆控制	Y					Y			Y
CAN网关功能		Y					Y			Y
根表				Y			Y	Y		
OBD连接功能		Y					Y			Y

以5W（哪里、谁、什么时间、为什么、什么）形式 描述的每个威胁，风险评分是可以计算的。

表 I.6 提供了风险评分评估的示例。

表I.6 – 风险评分评估示例
（[b-JASO TP15002]的表D.4）

#	威胁	AV	AC	Au	攻击的容易程度	C	I	A	影响程度	R风险值
1	T.control_fcn_Mobile_3rd_opearation_on_purpose of interfere-function	网络	中级	单独		不需要	大	大		
		1	0.61	0.56	6.83	0	0.66	0.66	9.20	7.95
2	T.vehicle_status_WiFi_dealer_main_purpose_forge	相邻网络	单独（S）	单独		小	小	无		
		0.646	0.71	0.56	5.14	0.275	0.275	0	4.94	4.14
3	T. info_transfer_USB_3rd_operation_pursuse_misop	位置	低	无		无	小	无		
		0.395	0.71	0.704	3.95	0	0.275	0	2.86	2.11

即使在像汽车嵌入式系统这样的缺乏累计的安全威胁的技术诀窍的系统， CRSS方法也能够分析性地从威胁的定义和评估系统来测量风险值。它还可以通过将功能作为资产处理的方式将诸如生命风险等因素考虑在风险评估内，并且为了评估，在完整性或可用性丧失具有严重后果的功能的情况下提高估计资产价值。

步骤2：识别威胁成因

对于风险评分大于特定值的每个威胁，通过故障树（FT）对原因进行逻辑分析。

I.2 使用MAC 算法的数据验证

MAC算法通过实现消息的完整性（认证）在密码和安全性中起到重要的作用。 ISO/IEC已经就MAC算法得出了很有意义的结论，例如[b-ISO/IEC 9797-1] （使用分组密码的机制）、[b-ISO/IEC 9797-2]（使用专用散列函数的机制）和 [b-ISO/IEC 9797-3] （使用通用散列函数的机制）。

考虑车辆内有限额实施资源，使用轻量级加密标准是合适的。 就此视角而言，有两种类型的MACs。第一种类型的MAC是使用[b-ISO/IEC 9797-1]和[b-ISO/IEC 29192-2]（轻量级分组密码）的基于分组密码的MAC 。第二种类型的MAC是使用[b-ISO/IEC 9797-2]和[b-ISO/IEC 29192-5] （轻量级散列功能）的基于散列功能的MAC。

为了给汽车安全选择可能的候选，MAC可能需要给出比现有的标准化MAC算法更明显的安全或性能优点。MAC的主要目标是在微控制器上实现紧凑和快速的软件实施，以及提供目标应用所需的足够的安全性。具体地，可以期望一种用于微控制器的非常有效的MAC算法。

附录 II

威胁、安全要求和安全控制

（本附录不构成为本建议书的一部分）

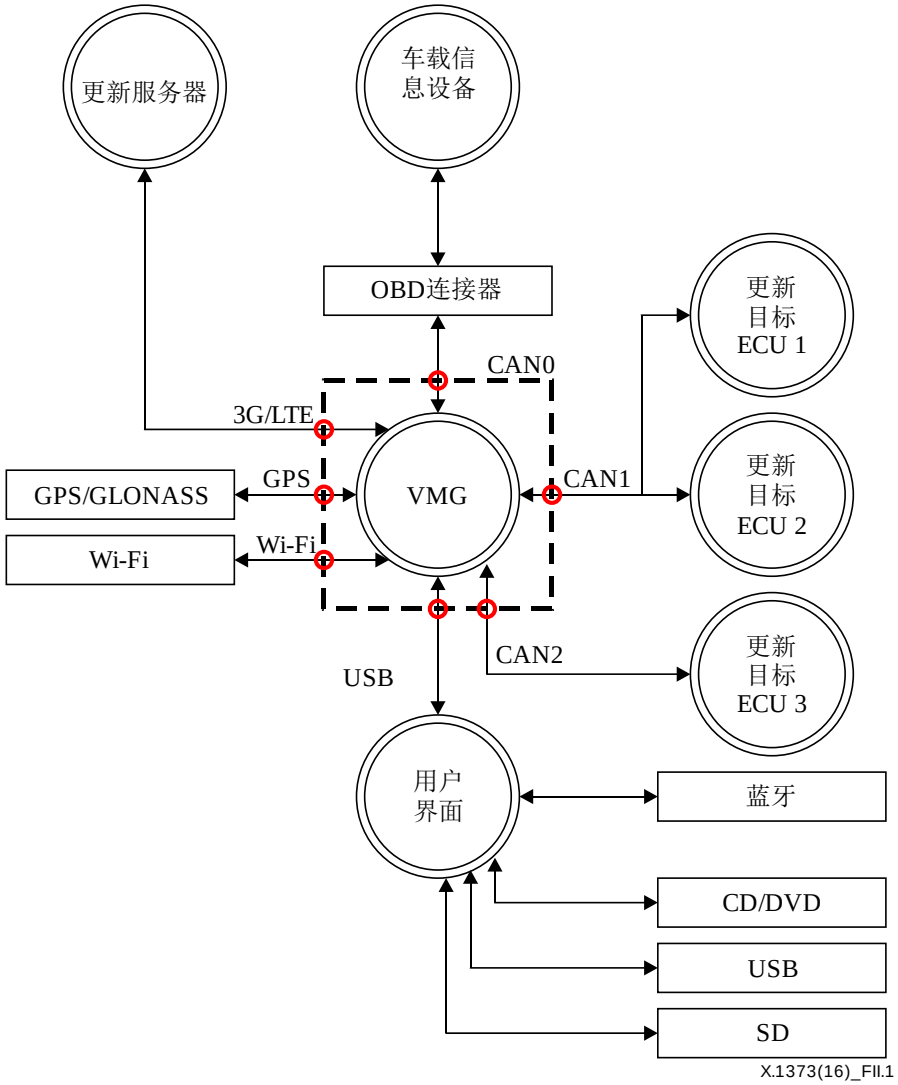
多种IT系统的安全攻击/威胁示例已广为人知，评估风险的技术诀窍在IT系统设计中不断积累。评估IT产品所需要的基本安全概念在 [ISO/IEC 15408-1]中给出。关于评估，[ISO/IEC 15408-1]使用评估对象（TOE）这一术语。有一些资产是TOE的所有者可能赋值的实体。 [ISO/IEC 15408-1]旨在为TOE建立安全目标，其是对抗所识别的威胁和/或满足所识别的组织安全策略和/或假设的意图的声明。依据威胁发生的可能性以及威胁发生时对资产的影响，威胁会给资产带来风险。然而，[ISO/IEC 15408-1]没有明确如何进行威胁提取和风险分析。另一方面，有很多已知的威胁识别和风险分析方法。在本节中，在给VMG（被认为是安全软件更新的主要组件）定义了评估目标（TOE）后，主要威胁识别进行，与主要威胁相关的安全要求也被考虑。 最后，高级别的安全控制为了满足安全要求而提供。

II.1 评估目标的定义

本节为VMG（在本建议书中被认为是安全软件更新的主要组件）定义了评估目标（TOE）。

作为外界接口的有：车载诊断（OBD）连接器、移动通信模块、全球定位系统/全球导航卫星系统（GPS/GLONASS）信号接收设备、无线保真（Wi-Fi）、电台 /电视 （TV）、蓝牙连接、CAN0/1连接器、带有光盘/数字多功能光盘（CD/DVD）的用户界面、通用串行总线（USB）连接器以及安全数字（SD）连接器。尽管该节中将控制器区域连接器（CAN）作为车载总线之一，但是相同的分析可以应用于其它类型的车载总线，例如面向媒体的系统传输（MOST），本地互连网络 LIN）和FlexRay等。

在图II.1中，评估目标（TOE）被定义为由虚线包围的区域，并且其作为车辆与外界的连接接口，实现了安全通信。



图II.1 – TOE模型

TOE的模块功能概述见表II.1。该表也提供了TOE中描述的功能与机密性（C）、完整性（I）和/或可用性（A）主要安全特征之间的关系，以便提供基于II.3节中的TOE的安全要求。

表II.1 – TOE模块功能概述

#	模块	功能		资产	C	I	A
1	车载移动网关	移动通信功能	它通过移动连接与服务器通信。 它使用认证信息给服务器认证	移动通信功能		Y	Y
				认证信息	Y	Y	
		软件获取功能	它通过移动连接或通过OBD连接器远程获取软件	软件获取功能		Y	Y
				软件信息	Y	Y	
		远程软件更新功能	它通过移动连接或通过OBD连接器远程更新软件。	远程软件更新功能		Y	Y
				更新所需的安全信息	Y	Y	

#	模块	功能		资产	C	I	A
			如果软件进行了远程更新，它使用安全信息来更新以认证服务器	软件信息	Y	Y	
		GPS接收功能	它从GPS卫星接收数据	GPS接收功能		Y	Y
		Wi-Fi连接功能	它通过Wi-Fi 连接器建立网络连接。 它通过Wi-Fi 连接器使用认证信息	Wi-Fi连接功能		Y	Y
				认证信息	Y	Y	
		USB连接功能	它通过USB电缆与用户界面进行通信	USB连接功能		Y	Y
		CAN通信功能	它向/从ECU发送/接收CAN数据	CAN通信功能		Y	Y
		CAN网关功能	路径表	CAN网关功能		Y	Y
				路径表	Y	Y	
		OBD连接功能	它通过OBD 在CAN发送数据	OBD连接功能		Y	Y

II.2 主要威胁识别

依据第II.1节的软件更新的TOE定义，本节根据[ISO / IEC 15408-1]的框架确定TOE中的主要威胁。

关于基于此TOE模型识别主要威胁的方法，本建议书采用附录I（参考性）中提供的风险分析方法。

表II.2 – 依据TOE模型的主要威胁

#	标记	谁	什么时间 (阶段)	为什么	哪里/什么
1	T.DoS-Functions-From-OBD-Device	第三方 维修厂的工作人员	普通操作 维护	有意地	对于VMG 的资产功能，它模拟 OBD 连接器连接设备，发送大量数据，并干扰该功能
2	T.Malfunction-Functions-From-OBD-Device	第三方 维修厂的工作人员	普通操作/维护 维护	有意地	对于VMG 的资产功能，它模拟 OBD 连接器连接设备，发送未授权的数据， 导致此功能的故障.

表II.2 – 依据TOE模型的主要威胁

#	标记	谁	什么时间 (阶段)	为什么	哪里/什么
3	T.MissDoS-Functions-From-OBD-Device	车辆经销商的工作人员 维修厂的工作人员	维护	意外地	对于VMG的资产功能， 它会错误地从OBD连接器连接设备发送大量数据或未授权的数据，并导致此功能的故障
4	T.DoS-Functions-From-ECU	第三方 维修厂的工作人员	普通操作/使用/维护 维护	有意地	对于VMG的资产功能，它使用与连接到CAN0-2的ECU固件相同的产品的逆向工程，将连接到CAN0-2的ECU固件更新为未经授权的固件; 这样，它从连接到CAN1-5的ECU发送大量数据，并干扰该功能
5	T.Malfunction-Functions-From-ECU	第三方 维修厂的工作人员	普通操作/使用/维护 维护	有意地	对于VMG的资产功能，它使用与连接到CAN1-5的ECU固件相同的产品的逆向工程，将连接到CAN1-5的ECU固件更新为未经授权的固件; 以这种方式，它从连接到CAN1-5的ECU发送未授权的数据，导致此功能的故障
6	T.DoS-Functions-From-Mobile-Device	第三方	普通操作/使用/维护	有意地	对于VMG的资产功能，它模拟服务器，从移动连接设备向VMG发送大量数据，并干扰此功能
7	T.Spoofing-Server_ToGet-Data	第三方	普通操作/使用 维护	有意地	对于VMG的资产信息，其通过截取通信信道或冒充移动连接设备来发送命令，以从移动连接设备获得VMG的资产信息。 以这种方式，它接收VMG的资产信息。
8	T.MissDoS-Functions-From-mobile-Device	服务器管理员	普通操作/使用/维护	意外地	对于VMG的资产功能，服务器通过误操作从移动连接设备发送大量数据或未经授权的数据，干扰该功能，并且导致该功能的故障

表II.2 – 依据TOE模型的主要威胁

#	标记	谁	什么时间 (阶段)	为什么	哪里/什么
9	T.Leaking-Mobile-Information-From-Mobile-Device	拥有者/用户 服务器管理员/车辆经销商的工作人员 服务器管理员	普通操作/使用/车辆交付 普通操作/使用/维护	意外地	对于VMG的资产信息，从移动连接设备，它通过误操作向VMG发送命令以获得VMG的保护资产（信息），并获得和泄漏VMG的保护资产（信息）
10	T.MissUpdate-Mobile-Information-From-Mobile-Device	拥有者/用户 服务器管理员/车辆经销商的工作人员 服务器管理员	普通操作/使用/ 车辆交付 普通操作/使用/维护	意外地	对于VMG的资产信息，从移动连接设备，通过误操作，它向VMG发送命令以更新VMG的保护资产（信息），并更新VMG的保护资产（信息）
11	T.Malfunction-Functions-From-mobile-Device	第三方	普通操作/使用/维护	有意地	对于VMG的资产功能，从移动连接设备，它模拟服务器，发送未授权的数据，并导致此功能的故障
12	T.Spoofing-Server_ToRewrite-Data	第三方	普通操作/使用	有意地	对于VMG的保护资产（信息），从移动连接设备，冒充移动连接设备，发送命令以重写VMG的保护资产（信息）和VMG的保护资产（信息）
13	T.DoS-Functions-From-Wi-Fi-Device	第三方	普通操作/使用/维护	有意地	对于Wi-Fi连接功能，它模拟Wi-Fi连接设备，发送大量的数据，并干扰该功能
14	T.Malfunction-Functions-From-Wi-Fi-Device	第三方	普通操作/使用/维护	有意地	对于Wi-Fi连接功能，它模拟Wi-Fi连接设备，发送未授权的数据，并导致此功能的故障
15	T.MissDoS-Functions-From-Wi-Fi-Device	拥有者/用户	普通操作/使用	意外地	对于Wi-Fi连接功能，由于Wi-Fi连接设备的误操作或Wi-Fi连接设备的恶意软件感染，它会发送大量的数据或未经授权的数据，干扰该功能，并导致此功能的故障

表II.2 – 依据TOE模型的主要威胁

#	标记	谁	什么时间 (阶段)	为什么	哪里/什么
16	T.Spoofing-Wi-Fi-Device_ToGet-Wi-Fi-Information	第三方	普通操作/使用/维护	有意地	对于Wi-Fi连接功能，模拟Wi-Fi连接设备，并发送命令以获得Wi-Fi连接认证信息，并且利用Wi-Fi连接认证信息
17	T.Spoofing-Wi-Fi-Device_ToRewrite-Wi-Fi-Information	第三方	普通操作/使用/维护	有意地	对于Wi-Fi连接功能，它模拟Wi-Fi连接设备，发送重写Wi-Fi连接认证信息的命令，并重写Wi-Fi连接认证信息
18	T.Leaking-Wi-Fi-Information-From-Wi-Fi-Device	车辆经销商的工作人员 拥有者/用户	车辆交付 普通操作/使用	意外地	对于Wi-Fi连接认证信息，它发送命令以获得Wi-Fi连接认证信息，并获取和泄漏Wi-Fi连接认证信息
19	T.MissUpdate-Wi-Fi-Information-From-Wi-Fi-Device	车辆经销商的工作人员 拥有者/用户	车辆交付 普通操作/使用	意外地	对于Wi-Fi连接认证信息，它发送重写Wi-Fi连接认证信息的命令，并重写Wi-Fi连接认证信息

II.3 TOE中的安全要求

基于II.2节中识别的威胁，在下边的子节中，安全要求的三个组件从TOE模型种抽取出来。每个安全要求来自第II.2节定义的威胁。在第II.3节中的每个安全要求中附加了可从表II.2获得的一组威胁ID（＃）。

II.3.1 TOE安全要求

II.3.1.1 通过CAN 通信对VMG 功能的SR.integrity /可用性保护

需要确保 VMG功能的完整性和可用性，以防止拒绝服务（DoS）和ECU通过CAN0-CAN2通信的故障攻击（见威胁4和5）。

描述

在CAN通信中，路径指定CAN标识符（ID）的唯一CAN数据。如果VMG收到了大量通信包和/或从CAN0-CAN2连接设备确认了不规则模型的接入，它不需要执行异常操作。

II.3.1.2 VMG数据的SR.confidentiality保护

VMG和服务器之间的通信内容需要在机密性方面受到保护，以保证第三方不能读取它们（见威胁7、16和17）。

II.3.1.3 通过移动通信对VMG 功能的SR.integrity /可用性保护

需要确保 VMG功能的完整性和可用性，以防止来自移动设备的通过移动通信的拒绝服务（DoS）和故障。（见威胁6、 7、 8、 9、10、11和12）。

描述

在与移动连接设备通信时，VMG需要确认通信方是否是认证过的移动连接设备。当收到通过移动通信的未授权/异常数据时，VMG需要防止冒充的服务器。 如果VMG从移动连接设备收到了大量通信包和/或从移动连接设备确认了不规则模型的接入，它不需要执行异常操作。此外，VMG需要确认从移动连接设备发送的命令之间的传输的一致性和频率。

II.3.1.4 VMG 功能的SR.FaultTolerance

VMG的功能需要延续它们的有目的性的操作，可能在由于攻击而不规则的情况下处于降低的水平（见威胁1、 2、3、4、5、6、8、11、15）。

II.3.1.5 通过OBD对VMG功能的 SR.integrity /可用性保护

需要确保 VMG功能的完整性和可用性，以防止来自OBD连接设备的通过OBD连接器的拒绝服务（DoS）和故障。（见威胁1、2和3）。

描述

就通过OBD连接器的CAN连接而言，只有特定的设备允许接入ECUs。当收到来自OBD连接器的未授权/异常数据时，VMG需要 防止冒充的OBD连接设备。如果VMG从OBD连接设备收到大量通信或未授权的命令，它不需要执行异常操作。

II.3.1.6 通过Wi-Fi 通信对VMG的SR.confidentiality /完整性/可用性的保护

当从 Wi-Fi 通信收到未授权/异常数据时（见威胁 13、14、15、16、17、18 和 19（，VMG 需要防止冒充的 Wi-Fi 通信设备。

描述

当与 Wi-Fi 设备通信时， VMG 需要确认该设备是否提前注册。如果 VMG 从 Wi-Fi 设备收到了大量通信包和/或从 Wi-Fi 设备确认了不规则模型的接入，它不需要执行异常操作。

II.3.2 IT视角下的操作环境安全要求

II.3.2.1 SRE.ECU保护

ECU 模块需要通过模块的模糊化来防止对 ECU 固件的分析。ECU 需要通过未经授权更换 ECU 来进行物理保护以防止攻击（见威胁 4 和 5）。

II.3.2.2 SRE.CAN通信保护

CAN 通信需要通过对 CAN 有效载荷数据的加扰操作（轻量级操作，例如比特翻转等）来分析 CAN 通信协议。 CAN 需要通过限制恶意第三方的 CAN 写入来进行物理保护以防止攻击（见威胁 4 和 5）。

II.3.2.3 SRE.Mobile通信网络保护

VMG 用来与服务器通信的移动通信网络需要被保护，以防止未授权设备的攻击。网络配置信息需要在机密性方面被保护。网络需要被监控以检测攻击（见威胁 6、7、11 和 12）。

II.3.2.4 SRE.Wireless通信保护

无线通信需要通过在通信包的有效载荷中存储仅有的最小数据，或者通过诸如比特翻转等轻量级操作对有效载荷数据进行加扰来保护，以防止无线通信协议的分析（参见威胁 7、12、16 和 17）。

II.3.3 就非IT操作/管理视角的操作环境安全要求

II.3.3.1 SREN.Caution

值得注意的是，对于车载系统的攻击是一种犯罪行为。此外，售卖产品以帮助犯罪需要被限制（见威胁 1、2、4、5、6、7、11、12、13、14、16 和 17）。

II.3.3.2 SREN.NetworkServicer

服务器管理员需要防止通过服务器的不恰当管理而导致储存的数据泄露或被篡改（见威胁 7 和 8）。

II.3.3.3 SREN.OBD工具保护

OBD 工具与车辆的连接需要被保护，通过安全管理以防止未授权的使用。此外，连接到车辆的工作操作方法需要在操作前被确认（见威胁 3）。

II.3.3.4 SREN.User

当用户使用车辆时，他们需要被告知要求的注意事项。

描述

当用户离开车辆时，需要对车辆上锁以防止第三方的入侵。当不被使用时，车辆应该被停在第三方不能轻易接近的地方。在使用车辆之前，用户需要确认没有未识别的设备。当将商业产品与作为维护接口的 OBD 连接器连接时，用户需要注意（见威胁 1、2、4、5、13、14、16 和 17）。

II.3.3.5 SREN.VirusScan

设备通过移动/ Wi-Fi 连接与系统连接时，需要定期进行扫描（见威胁 9、10、15、18 和 19）。

II.3.3.6 SREN.Wireless-Device保护

相关人士需要在操作前确认如何操作通过移动/ Wi-Fi 连接的设备。此外，相关人士注意防止通过 Wi-Fi 和命令导致的设备密码泄露（见威胁 9、10、12、13、14、16、17、18 和 19）。

II.3.3.7 SREN.Wireless-Display

用户使用 Wi-Fi/移动连接设备时，需要通过在设备的显示屏上做出选择，以确认是否发送 VMG 资产信息的“获取/写入”命令（见威胁 9、10、18 和 19）。

II.4 安全控制

基于第II.3节的安全要求，本节提供满足安全要求的安全控制，尤其从IT视角。

II.4.1 SC.Trusted 引导

作为对ECU中原始程序模块的分析（例如篡改）的对策，建议ECU通过在每个引导序列使用硬件安全模块（HSM）的引导安全保护机制来实现其软件的自检机制。

相应的安全要求

– 第II.3.2.1节的SRE.ECU保护。

II.4.2 SC.Message 验证

为防止篡改、窃取和重演的攻击，消息验证方法是一种保留实体的认证和消息的完整性的有效方法。

有两种合适的方法实现该目的：第一种是用数字签名（数字签名方法），第二种是用消息认证代码（MAC）。

同时，为了车辆内ECU的实际实施，设备的加密性能依据不同的车辆而改变。例如，对于豪华的车辆而言，可能其内部所有ECU都有HSMs；而对于普通车辆而言，其内部可能只有一部分ECU有HSMs。此外，加密性能的不同也取决于应用的HSMs 的类型。

因此，安全架构需要考虑不同车辆安全性能的不同。即，本建议书应用依据[ITU-T X.509] 的数字签名方法对带有不对称加密算法（例，可信平台模块（TPM）的车辆进行消息验证。另一方面，对没有不对称加密算法（例， HSM和智能卡）的车辆而言，本建议书应用 MAC来进行消息验证。对于包括消息验证的通信协议细节，见第7节。该安全控制是一种远程软件更新的基本措施，以验证本建议书中的消息。

相应的安全要求

– 第II.3.1.2节中VMG 数据的SR.confidentiality机密性保护；

– 第II.3.1.6节中通过Wi-Fi 通信对VMG 的SR.confidentiality机密性/完整性/可用性保护；

– 第II.3.2.3节中SRE.Mobile移动通信网络保护；

– 第II.3.2.4节中SRE.Wireless无线通信保护。

II.4.3 通信实体SC.Authentication

为了避免冒充改的通信实体（例，冒充的ECU、VMG和更新服务器），建议那些实体在每次通信开始时彼此认证。该安全控制应该在传输层实施，本建议书中定义的安全软件更新程序应该通过下层功能来保护。作为一种通信实体认证的具体对策，使用安全套接字层/传输层安全（SSL / TLS）的客户端和服务器认证在第三方认证中心（CA）下有效。

相应的安全要求

– 第II.3.1.6节中通过Wi-Fi 通信对VMG 的SR.confidentiality机密性/完整性/可用性保护；
– 第II.3.2.3节中SRE.Mobile移动通信网络保护；
– 第II.3.2.4节中SRE.Wireless无线通信保护。

II.4.4 SC.Message筛选

作为针对VMG的DoS攻击的示例，攻击者攻击ECU并且大量地向VMG发送伪造的消息以不适当地消耗它们的计算能力。为了降低这些DoS攻击造成的安全影响，消息筛选是一种有效的方法。 建议VMG根据发送者ID、消息类型、大小、频率等，或将这几项结合去筛选不相关消息。

相应的安全要求

– 第II.3.1.1节中通过CAN通信对VMG功能的SR.integrity完整性/可用性保护；
– 第II.3.1.3节中通过移动通信对VMG功能的SR.integrity完整性/可用性保护；
– 第II.3.1.5节中通过OBD对VMG功能的SR.integrity完整性/可用性保护。

II.4.5 VMG功能的SC.FaultTolerance

强烈建议VMG的供应商使用故障安全设计实施VMG软件，以便VMG可以在由于攻击而造成的不规则的情况下继续其预期操作。特别地，VMG监视操作状态，如果不相关的东西被检测到，就要采取一种能使其恢复到正常状态的措施（重启等）。如果不能恢复，它告知驾驶员该问题并且安全地暂停此操作。

相应的安全要求

– 第II.3.1.4节中VMG 功能的SR.FaultTolerance。

参考书目

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ISO/IEC 9797-1] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50375>

[b-ISO/IEC 9797-2] ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51618>

[b-ISO/IEC 9797-3] ISO/IEC 9797-3:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function.*
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51619>

[b-ISO/IEC 29192-2] ISO/IEC 29192-2:2012, *Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>

[b-ISO/IEC 29192-5] ISO/IEC 29192-5:2016, *Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions.*
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173>

[b-JASO TP15002] JASO TP15002:2015, *Guideline for automotive information security analysis.*

[b-FIPS-202] Federal Information Processing Standards Publication-202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. National Institute of Standards and Technology,
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

[b-ISO 14229] ISO 14229-1:2013, Road vehicles –Unified diagnostic services (UDS) – Part 1: Specification and requirements

[b-ISO 13400] Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition

ITU-T 系列建议书

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
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
2018年，日内瓦