国 际 电 信 联 盟

ITU-T H.551

国际电信联盟
电信标准化部门

(01/2022)

H 系列：视听及多媒体系统

车辆网关和智能交通
系统（ITS）– 车辆网关的体系结构

车载多媒体系统架构

ITU-T H.551 建议书

ITU-T H 系列建议书

视听及多媒体系统

可视电话系统的特性	H.100-H.199
视听业务的基础设施	
概述	H.200-H.219
传输多路复用和同步	H.220-H.229
系统概况	H.230-H.239
通信规程	H.240-H.259
活动图像编码	H.260-H.279
相关的系统问题	H.280-H.299
视听业务的系统和终端设备	H.300-H.349
视听和多媒体业务的号码簿业务体系结构	H.350-H.359
视听和多媒体业务的服务质量体系结构	H.360-H.369
远程临场、沉浸式环境、虚拟和扩展现实	H.420-H.439
多媒体的补充业务	H.450-H.499
移动性和协作程序	
移动性和协作、定义、协议和程序概述	H.500-H.509
H 系列多媒体系统和业务的移动性	H.510-H.519
移动多媒体协作应用和业务	H.520-H.529
移动多媒体应用和业务的安全性	H.530-H.539
移动多媒体协作应用和业务的安全性	H.540-H.549
车辆网关和智能交通系统（ITS）	
车辆网关的体系结构	**H.550-H.559**
车辆网络的接口	H.560-H.569
宽带、三网合一和先进的多媒体业务	
在 VDSL 上传送宽带多媒体业务	H.610-H.619
先进的多媒体服务和应用	H.620–H.629
内容交付和无处不在的传感器网络应用	H.640–H.649
IPTV 多媒体服务和 IPTV 应用	
一般问题	H.700–H.719
IPTV 终端设备	H.720–H.729
IPTV 中间件	H.730–H.739
IPTV 应用程序事件处理	H.740–H.749
IPTV 元数据	H.750–H.759
IPTV 多媒体应用框架	H.760–H.769
IPTV 业务发现至消费	H.770–H.779
数字标牌	H.780–H.789
电子医疗多媒体系统服务和应用	
个人健康系统	H.810–H.819
个人健康系统的互操作性认证测试（HRN、PAN、LAN 和 WAN）	H.820–H.859
多媒体电子医疗数据交换服务	H.860–H.869
安全聆听	H.870–H.879

欲了解更详细信息，请查阅 ITU-T 建议书目录。

ITU-T H.551建议书

车载多媒体系统架构

摘要

ITU-T H.551 建议书定义了车载多媒体系统（VMS）的配置、车载多媒体系统架构的参考模型以及车载多媒体系统多媒体应用的参考解决方案，并描述了 VMS 安全问题以及个人身份信息保护和隐私问题。

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 H.551	2022-01-28	16	11.1002/1000/14811

关键词

架构、车辆多媒体系统。

* 为了获取此建议书，输入网址：http://handle.itu.int/intheaddressfieldofyourwebbrowser，后接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、信息通信技术（ICT）领域工作的联合国专门机构。国际电联电信标准化部门（ITU-T）是国际电联的一个常设机构，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布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，而后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 ITU-T 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，也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的条款（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，才认为达到了本建议书的合规性要求。“应该”或“必须”等其他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声明的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的、有关已声明之知识产权的证据、有效性或适用性不表明任何意见。

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、有关受专利保护的知识产权/软件版权的通知。但需要提醒实施者注意的是，这可能并非最新的信息，因此特大力提倡他们查询 ITU-T 网站的相应可用 ITU-T 数据库：http：//www.itu.int/ITU-T/ipr/。

目录

页码

1 范围 1

2 参考文献 1

3 定义 1

3.1 他处定义的术语 1

3.2 本建议书中定义的术语 1

4 缩写和缩略语 2

5 惯例 4

6 背景 4

7 VMS特征和配置 4

7.1 VMS特征 4

7.2 VMS配置 4

7.3 VMS特征列表 5

8 VMS架构 7

8.1 VMS功能 7

8.2 VMS架构的决定因素 8

8.3 VMS架构的参考模型 8

9 VMS多媒体应用 9

9.1 VMSP参考模型 10

9.2 融合传输的参考协议栈 11

9.3 参考接收器模型 13

10 VMS安全 15

11 个人身份信息（PII）保护和隐私 15

附件A – VMS安全 16

A.1 概述 16

A.2 对VMS及其生态系统的假定威胁 16

A.3 基于已识别威胁的安全能力 18

附件B – 个人身份信息（PII）保护和隐私 22
B.1 信息源 22
B.2 PII保护的实施：一般注意事项 22
B.3 数据可见性和透明度 23
B.4 数据准确性和数据完整性 23
B.5 机密性 24
B.6 数据匿名化 24
B.7 数据可用性 24
参考文献 25

ITU-T H.551建议书

车载多媒体系统架构

1 范围

本建议书定义了车载多媒体系统（VMS）的特征和配置以及车载多媒体系统架构的参考模型，并定义了车载多媒体服务平台的参考模型、融合传输的参考协议栈以及用于 VMS 多媒体应用的车载设备的参考接收器模型。此外，亦描述了 VMS 安全问题以及个人身份信息保护和隐私问题。

2 参考文献

下列 ITU-T 建议书及其他参考文献含有通过本文的引用构成本建议书条款的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此，鼓励本建议书的用户了解使用最新版本的下列建议书和其他参考文献的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T F.749.3]ITU-T F.749.3建议书（2020年），车载多媒体网络的使用案例和要求

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 车载多媒体网络（VMN）[ITU-T F.749.3]：VMN 由车载多媒体服务平台（VMSP）、广播和通信网络以及车载多媒体系统（VMS）组成。

3.1.2 车载多媒体服务平台（VMSP）[ITU-T F.749.3]：VMSP 是一个云端平台，可为车内最终用户提供多媒体服务。

3.1.3 车载多媒体系统（VMS）[ITU-T F.749.3]：VMS 由车载多媒体系统输入（VM I/P）、车载多媒体单元（VMU）和车载多媒体系统输出（VM O/P）组成。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 VMS 核心功能：一种处理 VMS 的物理、功能和逻辑数据的功能。

3.2.2 VMS 关联功能：一种仅接收和显示来自其他系统或子系统的功能和逻辑数据的功能。

3.2.3 VMS 共享功能：一种用于其他系统或子系统共享物理、功能和逻辑数据和控制信息的功能。

4 缩写和缩略语

本建议书使用以下缩写和缩略语：

ADAS	高级驾驶员辅助系统
AM	调幅
ANC	主动噪声消除
APP	应用
AR	增强现实
AVM	全景监控
bCall	故障呼叫
BGS	背景扫描
CA	有条件访问
CDN	内容分发网络
CDR	融合数字广播
DAB	数字音频广播
DASH	超文本传输协议上的动态自适应流
DMS	驾驶员监控系统
DNT	不跟踪
DRM	数字版权管理
DTTB	数字地面电视广播
eCall	紧急呼叫
ECM	授权控制消息
ECU	电子控制单元
EMM	授权管理消息
FM	调频
GDPR	一般数据保护条例
HEO	高地球轨道
HLS	HTTP 直播流
HMI	人机界面
HTTP	超文本传输协议
HVAC	供暖、通风和空调
IAM	身份和访问管理
IBOC	带内同频道
iCall	信息呼叫

IP	互联网协议
LCD	液晶显示
LED	发光二极管
LEO	低地球轨道
MR	混合现实
NAT	网络地址转换
OBD	车载诊断
OEM	原始设备制造商
OLED	有机发光二极管
OS	操作系统
OTA	空中
PD	相位分集
PII	个人身份信息
PUF	物理不可克隆功能
RDS	无线电数据系统
RF	无线电频率
RVC	后视摄像头
TCP	传输控制协议
TMC	交通信息频道
UDP	用户数据报协议
V2I	车辆到基础设施
V2P	车到人
V2V	车到车
V2X	车到一切
VM	车载多媒体
VM I/P	车载多媒体系统输入
VM O/P	车载多媒体系统输出
VMN	车载多媒体网络
VMSP	车载多媒体服务平台
VMS	车载多媒体系统
VMU	车载多媒体单元
VR	虚拟现实

5 惯例

在本建议书中：

– 关键词“须”指必须严格遵守的要求，且如已表明遵守本文件则不得出现任何偏差。

– 关键词“不得”指必须严格遵守某项要求，且如已表明遵守本文件则不得出现任何偏差。

– 关键词“建议”指建议遵守某项要求，但并不强制遵守此要求。 因此，在表明遵守本建议书时，无需采用此类要求。

– 关键词“不建议”指不建议遵守某项要求，但不对此要求做出特定限制。因此，即使采用了此类要求，亦仍可表明遵守了本建议书。

6 背景

在本建议书中，车载多媒体系统（VMS）的特征和配置以及 VMS 架构的参考模型是按照[ITU-T F.749.3]中的要求定义的。此外，还定义了车载多媒体服务平台（VMSP）的参考模型、用于融合传输的参考协议栈以及用于 VMS 多媒体应用的车载设备的参考接收器模型。同时，亦定义了 VMS 安全问题、个人身份信息（PII）保护和隐私问题。

本建议书组织如下：

第 7 节定义了虚拟机的特征和配置。第 8 节定义了 VMS 架构的参考模型。第 9 节定义了 VMSP 的参考模型、异构网络上多媒体内容融合传输的参考协议栈以及车载设备的参考接收器模型。第 10 节阐述了 VMS 安全问题。第 11 节阐述了个人身份信息（PII）保护和隐私问题。

7 VMS 特征和配置

7.1 VMS 特征

基于以下原则确定 VMS 特征：

– 面向驾驶员和乘客的用户体验、娱乐和信息特征及应用。

– 市场、区域和国家的具体要求。

– 法律和强制性要求。

不过，VMS 特征并未描述车辆的整体网络架构或车辆中多个域的集成情况。

7.2 VMS 配置

VMS 配置基于以下原则：

– VMS配置定义了向驾驶员和乘客显示娱乐和信息的独立要求。

– 建议在特征和功能级别定义VMS配置。

– 建议VMS配置包含VMS中的硬件组件。

– 多种VMS配置是可能的。

– 建议VMS配置高度可变。建议考虑由原始设备制造商负责制造和售后的VMS插件产品。

不过，VMS 配置并未描述车辆的整体网络架构或车辆中多个域的集成情况。

7.2.1 决定因素

VMS 配置是基于以下决定因素确定的：

– 使用要求。
– 特征、功能要求。
– 接口要求。
– 成本要求。
– 基准要求。

7.3 VMS 特征列表

表 1 总结了 VMS 参考特征。

表1 – VMS参考特征

特征	子功能	可配置
人机界面（HMI）	显示技术	发光二极管（LED）/液晶显示器（LCD）/有机发光二极管（OLED）等。
	显示器数量	多个（前、中、后等）
	控制	传统控制：按钮/旋钮/触摸控制等。
		智能控制：语音控制、人脸识别、语音生物识别、手势、个性化、眼球运动控制、触觉灵活反馈触摸等。
	多屏互动	将信息推送到不同的屏幕
		视频文件同步或异步显示
		双导航显示
		显示界面的自由匹配
	系统语言	用户界面：法规要求的不同语言要求
	摄像机显示器	后视摄像头（RVC）/全景监控（AVM）
	控制和显示	供暖、通风和空调显示和控制
		驾驶员辅助控制和显示
广播	地面	模拟：调幅（AM）广播、调频（FM）广播、双调谐器和相位分集（PD）调频广播、背景扫描调频广播（BGS）、无线电数据系统（RGS）等。
		数字：数字音频广播（DAB）、数字地面电视广播（DTTB）、带内同频道（IBOC）技术、融合数字广播（CDR）等。
	卫星	卫星音频/视频服务（例如，卫星音频/视频流服务）
外部网络连接	蜂窝网络	3G/4G/5G
	卫星双向	低地球轨道（LEO）卫星双向通信网络
		高地球轨道（HEO）卫星双向通信网络
	车到一切（V2X）	车到车（V2V）、车到基础设施（V2I）、车到人（V2P）
	无线局域网	IEEE 802.11热点
车内移动连接		使用个人区域网络进行免提通话和音乐播放

表1 – VMS参考特征

特征	子功能	可配置
		使用IEEE 802.11局域网进行网上冲浪
		使用短距离通信网络的屏幕共享
		第三方车辆接口应用
远程信息处理配置	远程	远程监控、控制、车辆数据传输
	呼叫	紧急呼叫、故障呼叫、信息呼叫
在线应用商店/套件	应用商店	下载新功能
	主题市场	主题皮肤替换
空中（OTA）更新		OTA软件
媒体	声音	正常和高保真
	图像	不同格式
	视频	各种分辨率的普通视频、增强现实（AR）、虚拟现实（VR）、混合现实（MR）
媒体	声音	正常和高保真
	图像	不同格式
	视频	各种分辨率的普通视频、增强现实（AR）、虚拟现实（VR）、混合现实（MR）
导航	本地导航	
	云导航	来自远程信息处理盒（3G/4G/5G）调制解调器的数据/用户移动数据
	实时交通	交通信息频道（TMC）、传送协议专家组（TPEG）、实时交通中心等。
	服务	导航服务、实时天气预报服务等
	高级功能	智能旅行应用，如日历、规划器等
语音识别与合成	本地虚拟现实、云虚拟现实和合成	自然语言理解
		自动语音识别
		文本到语音
音频	音频质量	速度功能的音量调节
		声音算法
		主动噪声消除（ANC）
		个性化设置（声音模式和面部识别）
		最佳听音位置调整
		音质降低技术
	放大器配置	多通道集成放大器
		带扬声器的放大器
	声音配置	多扬声器配置高音扬声器（高音喇叭）/低音扬声器（低音喇叭）/全音域扬声器

表1 – VMS参考特征

特征	子功能	可配置
安全		身份和访问管理（IAM）、身份验证、授权和交易审计
		网络安全
		操作安全
		应用安全
		软件OTA安全
		硬件安全
		密码安全
隐私		一般数据保护注意事项
		个人信息保护
		数据可见性保护
		保密性、完整性和可用性
智能特征	驾驶员监控系统（DMS）	疲劳、表情和情绪识别
	健康	心跳监视器、血压监视器
	办公环境	电子邮件、视频电话会议、全息投影、手势识别、眼球运动控制、手写备忘录
	游戏	基于语音的互动问答游戏、全息互动游戏、冒险游戏
	社交	车载社交应用

注–安全和隐私功能对于配置为M1到M5的虚拟机而言必不可少，但对于配置为M0的虚拟机来说为可选配置。[ITU-T F.749.3]的附录一中给出了从M0到M5的VMS配置示例。

8 VMS 架构

本节定义了 VMS 功能的分类、决定因素和 VMS 架构的参考模型。

8.1 VMS 功能

一般来说，VMS 功能可以分为三类，即 VMS 核心功能、VMS 关联功能和 VMS 共享功能。

VMS 核心功能是处理 VMS 的物理、功能和逻辑数据的 VMS 功能。VMS 核心功能的例子包括调谐器、媒体处理、显示功能等。

VMS 关联功能指仅接收和显示来自其他系统或子系统的功能和逻辑数据的 VMS 功能。VMS 关联功能的示例包括来自后置车载摄像头的摄像头输入、由事故启动的 eCall 信息显示等。

VMS 共享功能指其他系统或子系统用来共享物理、功能和逻辑数据及控制信息的 VMS 功能。VMS 共享功能的示例包括通过车载多媒体单元（VMU）进行的暖通空调（HVAC）控制等。

8.2 VMS 架构的决定因素

以下是 VMS 架构的决定因素：

– 技术要求
– 操作系统、内存和硬件要求
– 特征、功能、子系统、逻辑和物理要求
– 接口要求
– 所需费用
– 使用要求
– 基准要求
– 标准合规性要求

8.3 VMS 架构的参考模型

VMS 架构是在接口、子系统和系统级别定义的。图 1 给出了 VMS 架构的参考模型。

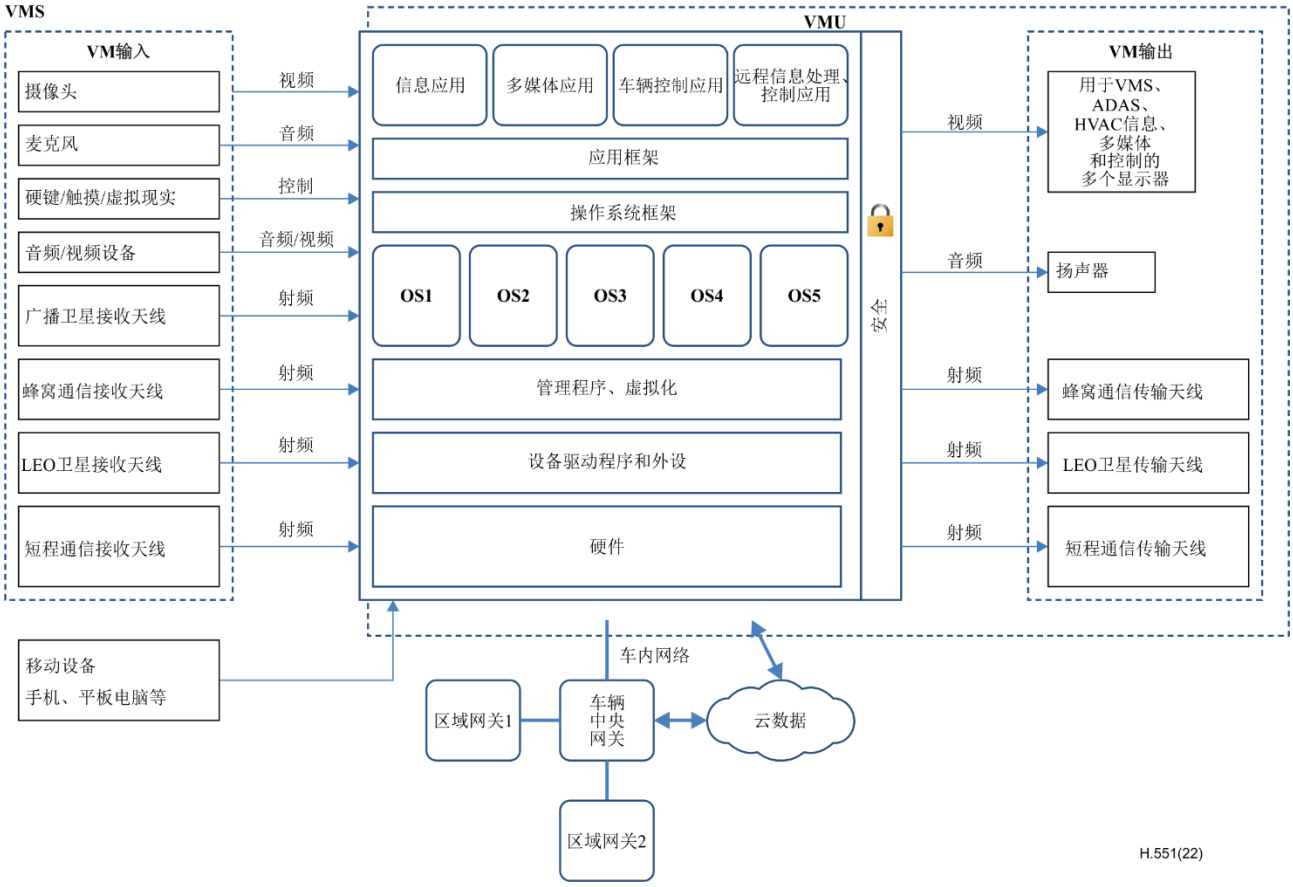

图1 – VMS架构的参考模型

8.3.1 应用

VMS 的应用包括：

– 信息应用，例如组合仪表、平视显示器、导航和天气。
– 多媒体应用，如媒体、导航、虚拟现实（VR）和人机界面（HMI）。
– 车辆控制应用，例如暖通空调（HVAC）和联网汽车。
– 远程信息处理应用，例如远程控制、诊断和数据访问。
– 显示应用，例如前/后显示屏应用。

8.3.2 应用框架

通过根据应用框架设计的用户界面工具，可以访问 VMS 特征和功能。

8.3.3 操作系统框架

操作系统框架处理系统服务。它可以是原始设备制造商和 VMS 开发人员的专有框架。

8.3.4 操作系统（OS）

根据处理负载、速度和精度要求，使用各种嵌入式操作系统和内核。

8.3.5 管理程序和虚拟化

管理程序和虚拟化技术用于由单个高功率处理器通过计算资源共享来支持多个操作系统和处理任务。

8.3.6 设备驱动程序和外设

设备驱动程序包括车辆网络接口驱动程序、音频和视频驱动程序、显示驱动程序、处理器间协议驱动程序和处理器内协议驱动程序。

8.3.7 硬件

硬件包括处理器、内存和其他组件。

8.3.8 云数据

云数据包括：

– 多媒体服务数据
– 远程信息服务的数据，即远程诊断服务、软件OTA更新服务、bCall / iCall服务和导航服务。

9 VMS 多媒体应用

图2描述了一个用于VMS多媒体应用的系统，该系统由云中的车载多媒体服务平台（VMSP）、异构网络和车载设备组成。融合传输方案用于提高多媒体内容在异构网络（即卫星广播网络和移动通信网络）上的传输效率。本节描述了VMSP参考模型（第9.1节）、异构网络上多媒体内容融合传输的参考协议栈（第9.2节）和车载设备的参考接收器模型（第9.3节）。

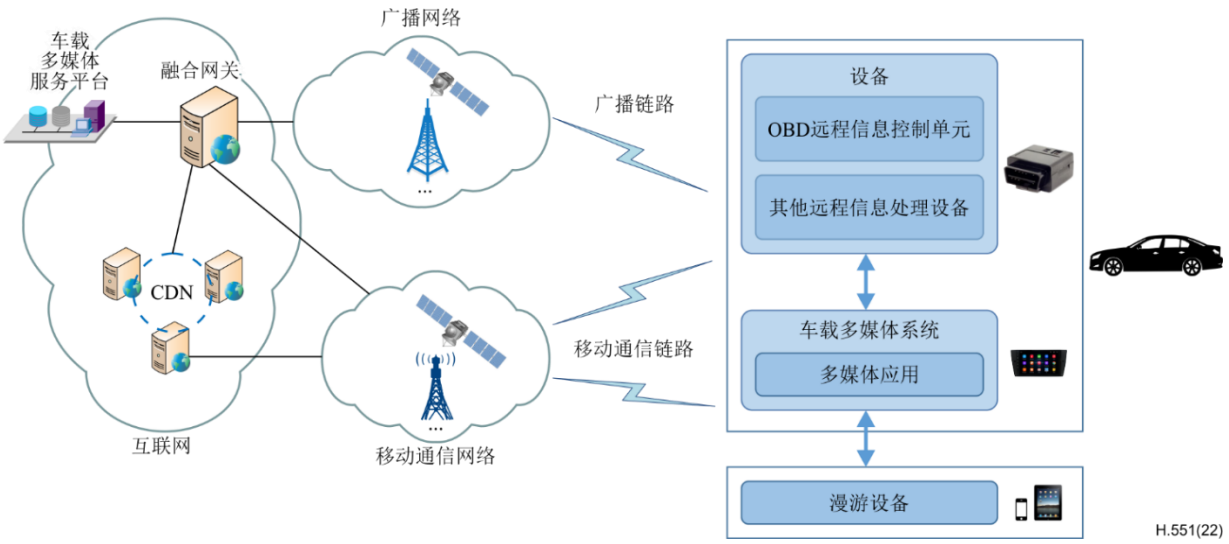

图2 – VMS多媒体应用的系统图

9.1 VMSP 参考模型

VMSP 由内容服务器、许可证服务器（可选）和条件接收服务器（可选）组成。其参考模型如图 3 所示。

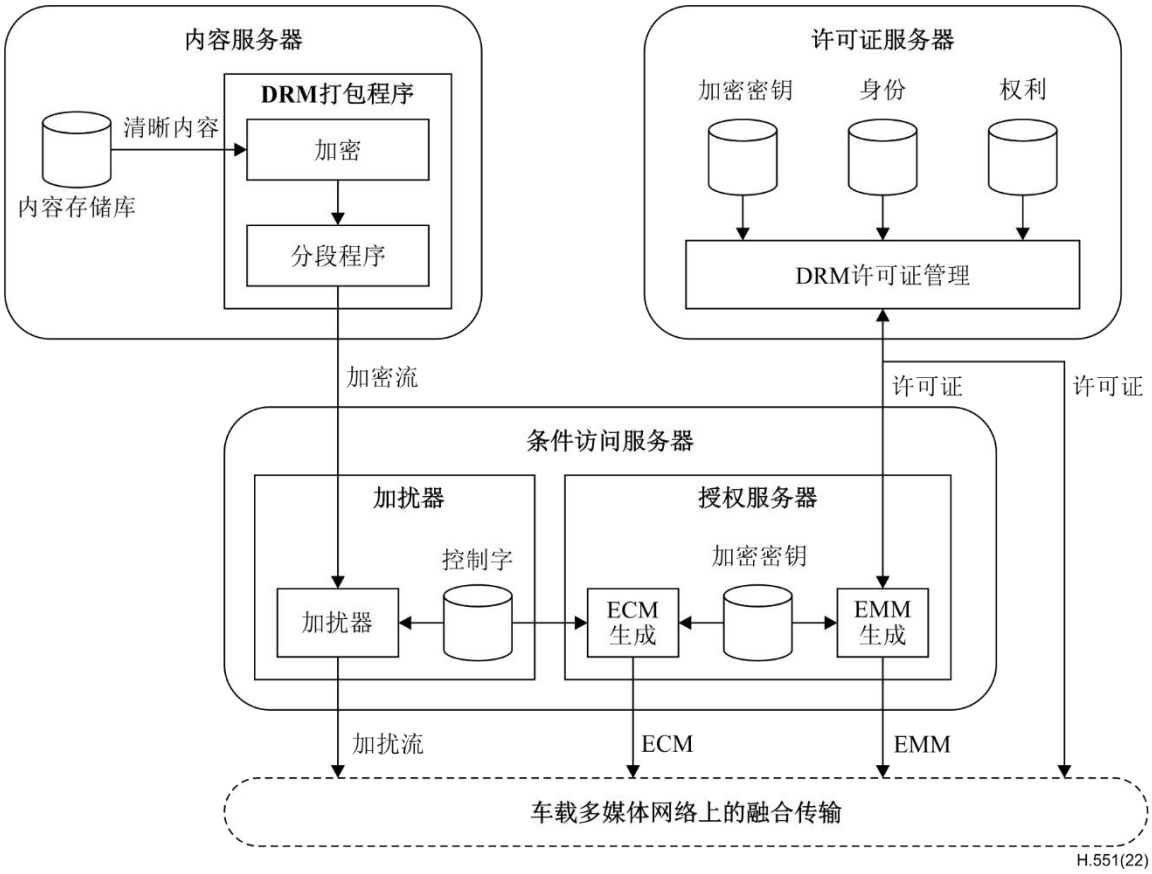

图3 – VMSP的参考模型

内容服务器由内容存储库和数字版权管理（DRM）打包程序组成。内容存储库用于存储内容提供商想要分发的清晰内容。请注意，内容存储库通常内置于 DRM 解决方案中，或者有时集成到与 DRM 服务器接口的内容管理系统中。DRM 打包程序对多媒体内容进行加密和打包，以便通过 VMN 传输。许可证服务器用于管理 DRM 许可证的创建、修改和撤销。DRM 许可证包含身份、权利规范和加密密钥。通常，DRM 客户端可以通过使用移动通信网络连接从许可证服务器获取其 DRM 许可证。VMN 流媒体的候选打包方案包括 MPEG-DASH [b-ISO/IEC 23009-1]和 HLS [b-IETF RFC 8216]。

条件接收（CA）服务器由加扰器和授权服务器组成。加扰器用于使用控制字对入站流进行加扰。授权服务器用于生成授权控制消息（ECM）和授权管理消息（EMM）。通常，出站的加扰流、ECM 和 EMM 通过卫星广播网络传送。但是，有以下两个例外：

1) 当用户开车到没有手机覆盖的地方时，不能通过任何移动通信网络获取DRM许可证。在这种情况下，DRM许可证可以集成到EMM中，并通过卫星网络交付给用户。因此，可以实现服务连续性。

2) 当运营商刚开始推出服务时，成千上万的新客户可能会试图在短时间内激活其设备。不过，在卫星广播网络中，为这些设备传送EMM所需的带宽可能不可用。在这种情况下，EMM可以暂时从卫星广播网络卸载到移动通信网络，因此可以保证运营商成功地推出服务。

9.2 融合传输的参考协议栈

广播通常被认为是在广阔的地理区域向大量人口传送线性节目的最具成本效益的方式。尽管 Ka 频段和 Ku 频段固定数字电视广播在全球取得了成功，但通过广播向车辆提供服务仍具有挑战性。例如，在城市环境中，由于接收器的移动和高层建筑的频繁信号阻塞，广播通信的可靠性相当成问题。虽然广播的城市覆盖问题可以通过地面中继器网络来解决，以填补服务中断缺口，但建设填补缺口的基础设施既昂贵又非常耗时。广播通信的另一个限制是它只能提供单向服务，因此无法容纳个性化服务或支持用户交互。

为了应对这些挑战，提出了一种通过 VMN 传输多媒体内容的融合传输方案，其中大部分媒体内容通过广播网络传送给大量用户，而移动通信网络仅用于恢复被广播网络丢弃的分组。来自 VMSP 的加扰流被发送到融合网关，在融合网关，媒体片段被进一步打包成有序分组，并通过卫星网络广播给所有用户。在终端，可以容易地检测到广播流的丢失情况或错误分组。这些丢失的分组通过移动通信网络上的重传来恢复。一旦媒体流无缝重组，终端不仅可以在驾驶舱显示器和扬声器播放这些媒体流，还可以作为本地信息娱乐中心，使用智能手机和平板电脑等个人设备与所有乘客无线共享这些媒体流。融合传输方案如图 4 所示。

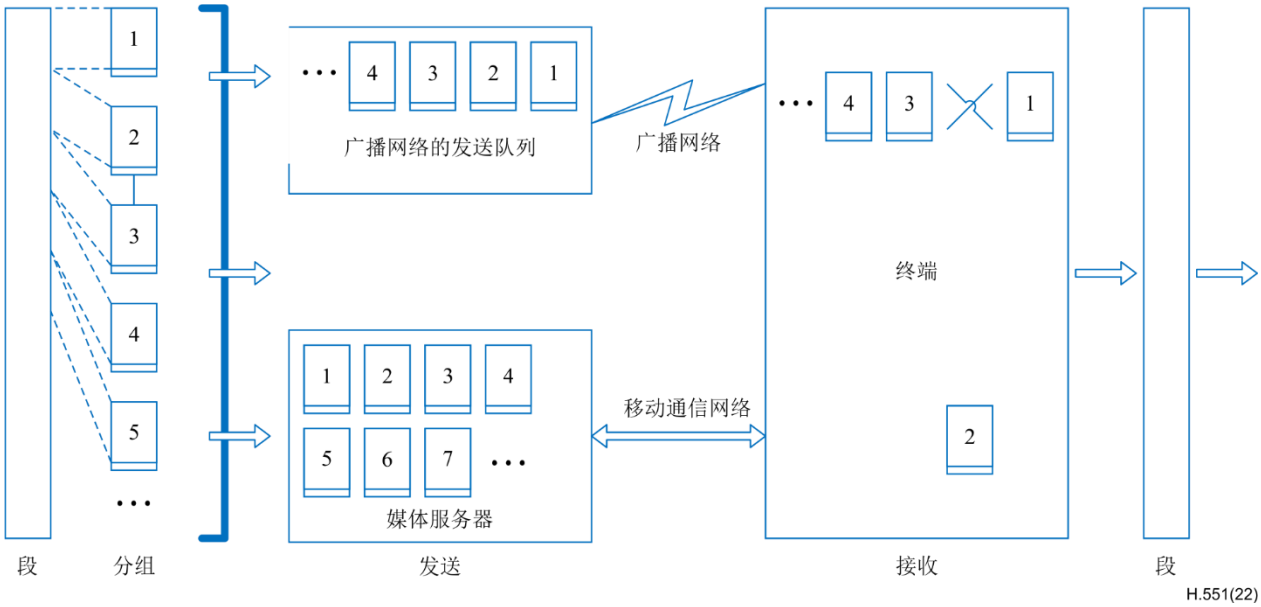

图4 – 融合传输的处理

融合传输方案充分利用了广播网络和移动通信网络的互补优势。因此，优化了 VMN 多媒体流服务的系统效率。

图 5 给出了 VMN 多媒体内容融合传输的参考协议栈。请注意，融合传输协议对底层物理层标准是不可知的，对上层标准是透明的。因此，可以保证对现有广播或移动通信基础设施的最小修改。

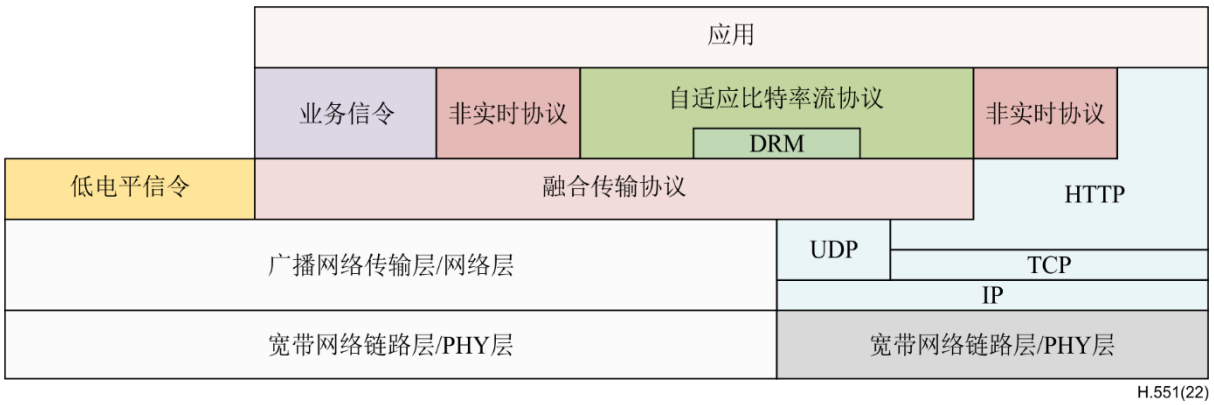

图5 – 融合传输的参考协议栈

一般假设是网络层协议可能基于两个版本的 IP 协议（IPv4 和 IPv6）。出于以下原因，建议选择 IPv6 [b-IETF RFC 8200]用于 VMS 和云平台之间的直接和安全连接：

– IETF明确建议其他标准开发组织（SDO）首选IPv6 [b-IAB]。因此，建议标准化工作采用IPv6。

– IPv4地址空间于2011年1月正式用尽，当时互联网号码分配机构（IANA）分配了其最后一个IPv4顶级地址空间（即/8）。因此，采用IPv6作为唯一的网络协议是保证网络服务和应用发展的唯一可行解决方案。

– 若干政府机构仅将向IPv6的过渡视为一项战略举措。其中一个例子是[b-USG OMB]，美国联邦政府以此提出了将国家机构的网络迁移至IPv6的具体截止日期和目标。

– 车载用户设备可能需要端到端的可达性，例如连接到任何应用和平台。这是一种无法采用网络地址转换（NAT）[b-IETF RFC 2663]结合私有IPv4寻址的情况。相反，IPv6完全支持用户设备始终可达的全局寻址方案。

虽然人们对 IPv4 更加熟悉，且 IPv6 的部署存在一定的新挑战，但 IPv6 的用户和流量增长速度远快于 IPv4。这意味着，综合考虑所有因素，行业的集体智慧选择了未来的 IPv6 [b-ETSI WP35]。

9.3 参考接收器模型

图 6 给出了车载设备的参考接收器模型，其中确定了以下功能：

– 广播连接和宽带连接，为接收器接收信令和数据提供连接。

– 融合传输协议/UDP/HTTP/TCP/IP栈和HTTP/TCP/IP栈，为接收方提供面向对象的传输协议，以接收多媒体流服务的自适应比特率流（如DASH或HLS）资源。

– 低级信令：通过广播网络传送的信令，使接收方能够建立基本服务列表，并引导发现每个多媒体服务的服务信令。

– 服务信令：与服务相关的信令，使接收方能够发现和访问多媒体流服务及其内容组件。

– 缓存：清单、初始化段和媒体段的临时存储和处理，其接收通过服务信令来实现。

– 自适应比特率流（即DASH/HLS）服务器：本地自适应比特率流服务器，用于将底层抽象为自适应比特率流客户端。对于自适应比特率流客户端，通过自适应比特率流服务器提供清单、初始化段和媒体段。

– 自适应比特率流客户端：一种消耗清单和段并与接收器中的其他组件进行通信的功能，以基于平台功能、用户偏好和用户交互来实现媒体体验的个性化。

– 应用：一种本地或下载的应用，利用广播或宽带传送的数据向最终用户提供丰富的交互式演示。

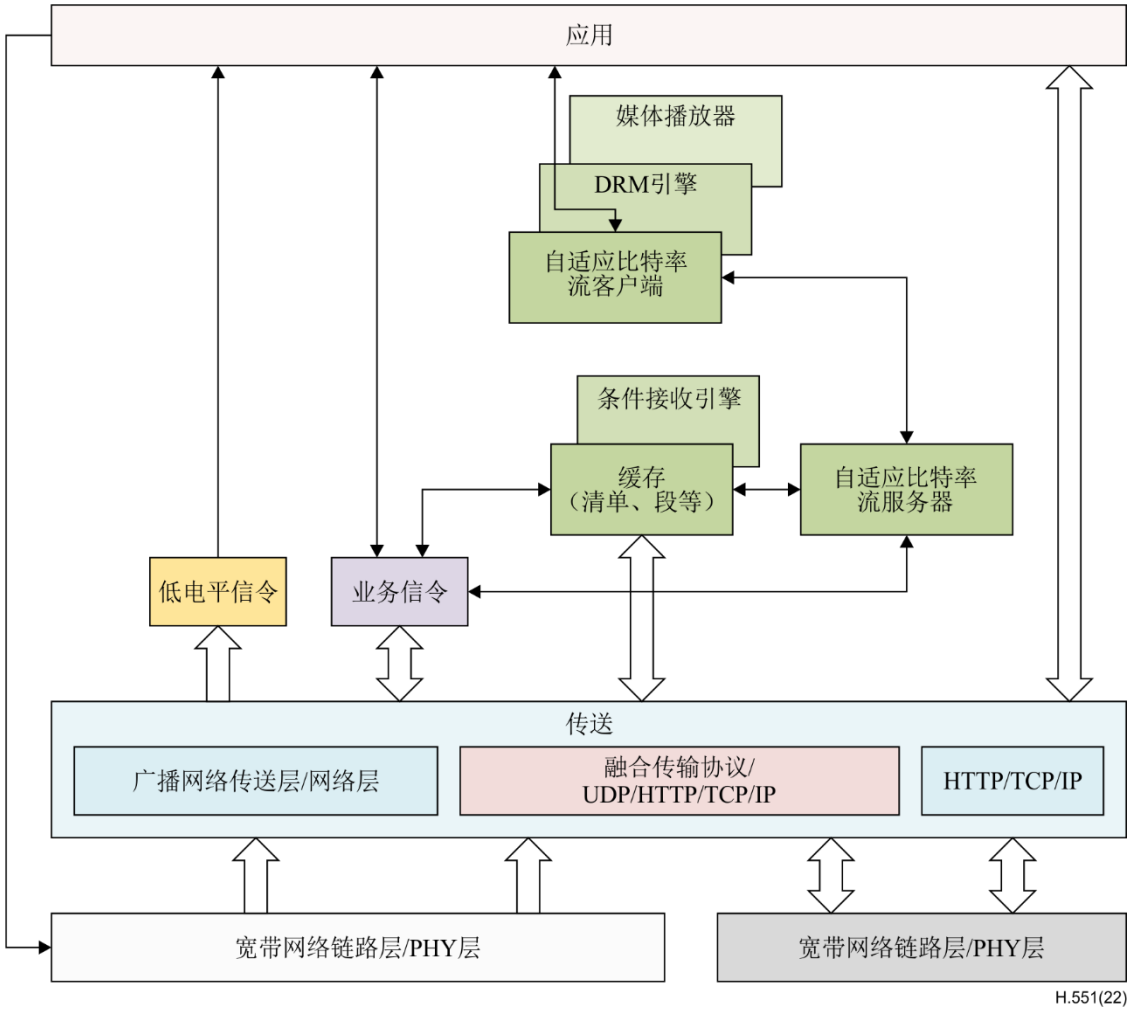

图6 – 车载设备的参考接收器模型

参考接收器的典型自举序列如下所示：

– 应用在低级信令中请求预配置的服务列表。服务列表被传送到应用，然后应用为选择多媒体流服务提供用户界面。用户选择多媒体流服务来消费。

– 应用使用在所选服务的服务列表中携带的服务信令入口点信息，向融合传输协议/UDP/HTTP/TCP/IP栈提供访问信息，以检索服务信令。服务信令被传递给应用。

– 通过使用服务信令，应用向融合传输协议/UDP/HTTP/TCP/IP栈提供访问信息，用于下载所选服务的自适应比特率流格式的媒体组件，这些组件被发送到高速缓存以进行存储、解扰并随后被转发到自适应比特率流服务器。

– 在选择服务时，应用激活自适应比特率流客户端，使得DASH/HLS客户端在媒体段可用性开始时间或之后从自适应比特率流服务器请求和接收媒体段。

– 在接收到媒体片段时，包括自适应比特率流客户端、DRM引擎和媒体播放器的复合功能对接收到的媒体片段进行解码，并将解码后的媒体返回给应用进行播放。

10 VMS 安全

建议将 VMS 和汽车安全中涉及的其他部件（通常是电子控制单元（ECU））之间的相互作用限制在第 8.1 节中提到的共享功能。

详情见附件 A。

11 个人身份信息（PII）保护和隐私

建议 VMS 在车辆联网时提供端到端保护，并提供更多交互式服务。需要保护更多用户数据和隐私相关信息，以确保存储在 VMS、车辆和 VMS 云或后端服务器中的用户数据的机密性和完整性。

详情见附件 B。

附件A

VMS安全

（此附件是本建议书不可分割的组成部分）

A.1 概述

建议将 VMS 和汽车安全中涉及的其他组件（通常是 ECU）之间的相互作用限制在第 8.1 节中提到的共享功能范围内。实际上，建议 VMS 不要对确保汽车所需安全性的其他组件的功能产生负面影响，尤其是在自动驾驶车辆的情况下。

关于 VMS 安全，第 A.2 节对 VMS 及其生态系统的假定威胁做了总结，第 A.3 节的参考资料介绍了针对威胁的安全能力方面的内容。

A.2 对 VMS 及其生态系统的假定威胁

A.2.1 对车载多媒体服务平台（VMSP）的威胁

近年来，车辆连通性的多样化显著增加，特别是对位于 VMSP 的各种服务器的连通性要求很高。在 VMS 的背景下，后端服务器被认为是一种 VMSP，其中包括原始设备制造商提供的服务器、供应商提供的服务器和信息通信技术（ICT）服务提供的服务器，以从远程后端支持车辆生态系统。可以确定与 VMSP 有关的下列威胁：

– VMSP的服务器被用作攻击车辆或提取数据的手段。

– VMSP提供的服务被中断。

– VMSP服务器上保存的数据丢失或泄露。

A.2.2 车辆在通信信道方面面临的威胁

车辆通信包括通过蜂窝、LEO 卫星、广播网络和短程网络进行的外部通信。上述通信中使用的信道可能成为欺骗、窃听、消息操纵等攻击的目标。根据通信信道可以识别以下威胁：

– 未经授权操纵、删除或修改车载代码/数据。

– VM接口可用于访问车辆内的其他（智能）基础设施（例如，与VMS无关的ECU）。

– 使用不可信/不可靠的消息和会话劫持/重放攻击。

– 由于VM应用可以通过无线方式进行更新，因此这些攻击也适用于VM。

– 信息披露。

见[ITU-T F.749.3]第 9 节。

– 拒绝服务攻击。

– VM本身可能无法访问车辆内的关键基础设施，但可以充当这些攻击的网关。

– 非特权用户的特权访问。

– 由于个性化用户帐户可以与VM应用相关联，因此非特权访问是可能的。通过VM进行的非特权访问可能无法提供对关键基础架构的直接访问（例如，根访问；进入制动系统），但也可以作为进入车辆基础设施的入口。

– 通信媒体中嵌入的恶意软件。

– 智能VM依赖于VMS和云中VMSP之间的数据传输。通过渗透这一通信信道，攻击者可能会使用从VMSP到VMS的消息/数据传输来部署恶意软件。

– 含有恶意内容的邮件。

智能VM依赖于VMS之间的数据传输，例如云中的VMSP。通过穿透这一通信信道，攻击者可能会改变从VMSP到VMS的消息/数据传输，以访问目标智能车辆内的VMS和/或ECU。

A.2.3 车辆在更新程序方面面临的威胁

为更新车载系统可以采用两种方法，即：通过车载诊断（OBD）端口、SD 卡或 u 盘等便携式设备的有线更新以及无线更新。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更新和解决，而无需物理访问，例如通过 OBD 测试仪。此外，无线更新有助于缩短更新周期，从而最大限度地减少软件已知漏洞的攻击风险。在更新过程中可以发现以下威胁：

– 更新程序的滥用或危害。

无论是使用空中更新还是本地/物理更新，更新过程都可能遇到使用编造的系统更新程序或受损固件的威胁。

尽管更新过程是完整的，但软件却有在更新过程之前被人操纵的可能。软件提供商为更新创建/准备其软件，并将软件交付给需要更新的目标系统。因此，可能存在严重的威胁，即软件在提供服务之前就可能被人操纵和破坏。

特别是在更新过程中，软件更新中使用的加密材料（如密钥和证书）可能会受到损害，因此可能会导致无效或恶意的软件更新。

– 拒绝服务和拒绝合法更新。

针对更新服务器或网络的拒绝服务攻击的目的是阻止关键软件更新的推出和/或解锁客户的特定功能，这是软件更新过程中的可能发生的一种攻击。此外，亦可能发生拒绝合法更新一类的攻击。

A.2.4 车辆在外部连通性与连接方面面临的威胁

为了提供各种便利的服务，车辆可以配备与 VMSP 服务器通信的组件，并且可以通过无线连接与道路用户启用的所有设备进行通信。除了便利功能，这亦具有安全优势，如自动紧急呼叫功能和 V2X 通信支持的功能。不过，由于额外的接口会导致攻击面扩大，为提高连通性连接到外部实体的车辆越多，出现的威胁和漏洞亦会越多。可识别到的与外部连通性和连接有关的威胁包括：

– 车辆功能连通性的操纵

VMS不提供对关键车辆功能的直接访问，但可以用作访问这些关键部件的网关，例如专用ECU。

– 托管的第三方软件

VMS应用可以包含在“托管的第三方软件”类别中。

– 连接到外部接口的设备

如[ITU-T F.749.3]中所述，连通性可以基于智能手机等引入设备。

A.3 基于已识别威胁的安全能力

A.3.1 身份和访问管理（IAM）、认证、授权和交易审计

VMS 服务涉及多个管理员和用户，这些服务可以在内部和外部访问和使用。之所以需要身份管理，不仅是为了保护身份，而且是为了在这样一个动态和开放的 VMS 基础设施中便于访问管理、认证、授权和交易审计过程的实现。

IAM 需要一个或多个通用信任模型来认证身份，开发人员、管理程序和其他系统组件则需要一个或多个通用信任模型来认证系统组件，如下载的软件模块、应用或数据集。

IAM 有助于服务和资源的机密性、完整性和可用性，因此在 VMS 中变得至关重要。此外，IAM 可以使用不同的认证机制或分布在不同的安全域中，实现 VMS 的单点登录和身份联合。

交易审计保护交易不受否认的影响，在安全事件后进行取证分析，并对攻击（入侵和内部攻击）起到威慑作用。交易审计不仅仅意味着简单的日志记录，还包括主动监控，以标记可疑活动。

A.3.2 接口安全

这一功能保护了向 VMS 开发人员和/或其他签约的 VMSP 供应商开放的接口，通过这些接口可以交付各种 VMS，并保护了基于这些接口的通信。可用于确保接口安全的机制包括但不限于：单边/相互认证、完整性校验和、端到端加密和数字签名。

A.3.3 网络安全

在 VMS 环境中，网络安全支持物理和虚拟网络隔离，并保护所有参与者之间的通信。它支持网络安全域分区、网络边界访问控制（例如防火墙）、入侵检测和预防以及基于安全策略的网络流量隔离，并保护网络免受物理和虚拟网络环境中的攻击。

A.3.4 操作安全

这一功能为 VMS 和 VMSP 基础设施的日常运行和维护提供了安全保护。

这一操作安全功能包括：

– 定义一套安全策略和安全活动，如配置管理、补丁升级、安全评估、事件响应；

– 监测VMSP的安全措施及其有效性，并向受影响的VMS提交适当报告。

如果 VMSP 的安全措施或其有效性发生变化，所有下游 VMS 都将收到此类变化的警报。

这些报告和警报使授权的 VMS 能够看到与其 VMS 相关的适当事件、审计信息和配置数据。

A.3.5 软件和固件更新

安全的 OTA 更新需要符合基线安全标准。建议更新过程考虑操作因素（例如，更新时间和加密/解密过程）。多个原始设备制造商和第三方供应商的存在导致了车辆内不同的子系统接口。因此，针对这些原始设备制造商或供应商的任何漏洞或网络风险都可以有效地劫持合法的 OTA 软件更新，然后作为云数据发送到车辆上。

建议设计、实施和运行更新 VMS（ECU 和相关系统）软件和固件的机制。

在 VMS 服务的开发中，建议将 VMS 的软件和固件更新机制作为一项基本功能来设计和实现。回退软件和固件的机制亦建议通过设计来实现，以便在更新失败时使用。

在 VMS 服务的使用和支持中，在更新过程开始之前，软件/固件更新包由设备验证其数字签名、签名证书和签名证书链。

建议安全管理和适当操作用于更新完整性保护和机密性的密钥。当通过 OTA 进行更新时，建议通过加密通信信道进行更新。

建议使用 OTA 的更新要么完全成功，要么以可恢复的方式失败。在更新失败的情况下，建议设备回退到上次已知的良好配置，并且建议不要禁用设备与更新服务器的连接。

A.3.6 应用安全

此类安全功能通常用于提高“VMS 应用”的安全性，且为此通常会发现、修复和防范 VMS 及其生态系统中的安全漏洞。在设计、开发、部署、升级和维护等应用生命周期的不同阶段，将使用不同的技术来暴露此类安全漏洞。

A.3.7 事件管理

事件管理提供事件监控、预测、警报和响应。为了了解整个基础设施中的 VMS 是否按预期运行，持续监控是必要的（例如，监控在 VMSP 使用的服务器的实时性能）。这使得系统能够捕获服务安全状态，识别异常情况，并提供安全系统过载、漏洞、服务中断等的早期警告。安全事件发生后，系统会自动或在管理员的干预下识别问题并对事件做出快速响应。系统会记录并分析已关闭事件的潜在模式，并在随后对其加以主动应对。

A.3.8 密码系统

这一功能确保了在 VMS 及其生态系统中使用和交换的数据的机密性和完整性。这是以特定形式存储和传输数据的基本方法，以便只有数据的目标用户才能读取和处理数据。这一功能不仅可以保护 VMS 数据不被窃取或篡改，还可以用于用户身份认证等。

作为实现密码系统的一个范例，在[b-ITU-T X.1197 Amd1]中给出了选择用于 IPTV 系统的密码原语的指南，并且可以应用于车辆系统中的多媒体流，前提是这些多媒体流与非车载 IPTV 系统中的多媒体流具有相同的重要性/关键性。同样，对于具有 5G 连通性的车辆，[b-ITU-T X.1811]提供了如何实现[b-ITU-T X.1197 Amd1]的基线安全级别的进一步指导，其中包括但不限于多媒体流。

此外，利用基于强认证加密的 DRM 解决方案，将仅允许信息娱乐系统消费合法的、受版权保护的内容，且信息娱乐和辅助驾驶系统将仅考虑合法的视距外部多媒体流，因此允许交通在没有任何中断的情况下进行。

A.3.9 硬件安全

这一功能旨在消除 VMS 硬件固有的漏洞和安全弱点，并为硬件级实施提供安全环境。应特别指出，在硬件中实现许多基本的加密功能变得至关重要，例如加密密钥管理、加密/解密的执行以及数字签名和强认证的提供，且这对确保 VMS 中的安全性非常重要。为此，考虑到可能的威胁和攻击，有必要从硬件设计阶段即安全地设计和验证相关硬件的操作。

例如，为了确保 VMS 架构中的 ECU 级安全性，建议实施的每个 ECU 都受到 HSM 和 PUF 的保护，后者是硬件安全模块的典型组件。

A.3.10 一般安全能力

注 – 以下安全功能对于本建议书是可选的。但是，这些功能可以有效地用于提高VMS的安全性。

– 安全评估和审计

这一功能支持VMS的安全评估。它使授权方能够验证VMS是否符合适用的安全要求。安全评估或安全审计可以由VMS、VSMP或第三方执行，安全认证可以由授权的第三方执行。

实施适当的安全标准，以使VMS和VMSP之间相互了解安全级别。

– 信任模型

公共信任模型对于任何系统都是必要的，在这些系统中，多个提供商合作来提供可信任的服务。

由于VMS的高度多利益主体性质，VMS环境将需要包含一个整体信任模型。这种信任模型将能够创建信任实体的岛和/或联盟，使得系统的不同元素将能够认证其他实体和组件的身份和授权权限。每个信任岛或联盟将基于一个或多个可信机构（例如，公钥基础设施（PKI）证书机构）。

– 数据隔离和保护

a) 数据隔离

数据隔离可以在逻辑上或物理上实现，具体取决于所需的隔离粒度和VMS软件和硬件的具体部署。

b) 数据保护

数据保护确保保存在VMSP的VMS数据和派生数据得到适当保护，以便只能在VMS授权的情况下进行访问或更改。这种保护可以包括访问控制列表、完整性验证、纠错/数据恢复、加密和其他适当机制的某种组合。

当VMSP为VMS提供存储加密时，这一功能可以是客户端加密（例如，在CSP应用中）或服务器端加密。

– 安全协调

由于不同的VMS意味着不同的安全控制实现，这种安全功能协调的事异构安全机制，以避免保护冲突。

在VMS生态系统中扮演不同角色的各方对物理或虚拟资源和服务拥有不同程度的控制，其中包括安全控制。

对于每一方，都会有各种安全机制，期中包括VMS管理程序隔离、IAM。

网络保护等。安全协调依赖于不同安全机制的互操作性和协调性。

– 供应链安全

一个VMSP使用几个供应商来建立其服务。其中一些将是VMS行业参与者，而另一些将是传统的信息技术（IT）设备或服务供应商，例如与VMS没有直接关系的硬件制造商。这一功能能够通过安全活动在VMSP和供应链的所有参与者之间建立信任关系。这些供应链安全活动包括：识别和收集有关VMSP获得的用于提供VMS的组件和服务的信息，以及实施供应链安全政策。

例如，VMSP典型的供应链安全活动可能包括：

a) 确认供应链参与者的背景信息；

b) 验证VMSP使用的硬件、软件和服务；

c) 检查VMSP购买的硬件和软件，确保其在运输途中不被篡改；

d) 提供验证VMS软件来源的机制，例如软件供应商提供的代码。

这一功能是持续的，以覆盖正在进行的系统演进和更新。

– 安全的开发环境和程序

这一功能是为了避免在开发过程中给VMS及其生态系统带来不安全性。开发环境包括与系统开发相关的人员、过程、技术和设施。建议VMS服务开发人员评估各项VMS开发工作中的风险，并建立安全的开发环境，同时考虑：

a) 在环境中工作的人员；

b) 应用开发方法以及软件和数据处理流程；

c) 外包产品和服务的使用；

d) 物理和网络环境；

e) 与其他开发和运营工作共存。

VMS服务开发人员还需要确定开发环境和相关程序，以降低风险。建议将这些程序传播给参与开发工作的个人。

附件B

个人身份信息（PII）保护和隐私

（此附件是本建议书不可分割的组成部分）

建议VMS在车辆联网时提供端到端保护，并提供更多交互式服务。需要保护更多用户数据和隐私相关信息，以确保存储在VMS、车辆和VMS云或后端服务器中的用户数据的机密性和完整性。

根据美国国家标准和技术研究所（NIST）的说法，个人身份信息（PII）是“允许通过直接或间接方式合理推断信息适用的个人身份的任何信息表示”[b-NIST SP 800-79-2]。

“隐私”一词没有单一的定义。隐私的含义取决于法律、政治、社会、文化和社会技术背景。

通常，信息隐私可以定义如下：

1) 如果个人受到保护，免受未经授权的他人的渗透、干扰或对其数据的访问，那么个人拥有信息隐私。

PII 保护是确保隐私的一个方面。

VMS 可以存储 PII，也可以作为车主、司机和/或其他乘客访问 PII 的网关。

B.1 信息源

VMS 包括多个信息输入源，例如：

– 传感器（运动探测器、位置探测器等）
– 摄像头（个性化、特征识别等）
– 麦克风 – 音频（可能进一步用于录音和语音识别、语音生物识别等。）
– 网络通信协议标识符，如IP地址、MAC地址等。
– u盘、安全数字卡、外置硬盘等媒体来源。
– 第三方应用、支付网关、服务、设备、配件等。

基于车辆架构、区域、立法和认证要求，VMS 存储信息并与车辆或云中的其他系统共享信息。

B.2 PII 保护的实施：一般注意事项

个人数据（例如，数据、文本、音频、视频或图像）以及除预期客户或任何最终用户（如远程云、商店或进程）之外的用户可能使用 VMS 请求的任何内容都将受到保护。

需要就与每个客户、最终用户和第三方相关的个人数据的数据共享达成一致。任何此类客户协议或任何其他管理 VMS 服务使用的相关协议均应基于以下标准：

– 基于用户在服务和兴趣方面所做选择的个性化访问。
– VMS旨在根据隐私法规要求允许其使用。
– VMS软件、硬件和网络设计使其只允许经过身份认证的访问。
– VMS PII和隐私保护是为只有一个用户的私家车和有多个用户的共享车辆设计的。

B.3 数据可见性和透明度

建议实施众所周知、经过严格审查的安全标准。建议避免使用专有加密算法。

推荐采用众所周知的进程。

建议向用户通知通过 VMS 存储/访问的数据。由于透明度提高了用户的接受度，建议用户通知包括关于数据类型、收集目的、数据处理实体的身份和数据存储期限的信息。

B.3.1 默认隐私

建议用户能够控制数据下载的限制，以及能够选择加入/选择退出数据下载和存储。选择退出策略更能保护隐私，且更符合默认隐私原则。因此，建议采用选择退出策略。

建议 VMS 确定满足数据隐私要求和设置的用例列表。

对于特定的用例，应用可能会使用多个资源。例如，在位置服务的情况下，蓝牙、全球定位系统、众包无线热点或基站位置可用于确定用户的大致位置。建议 VMS 为用户提供关闭特定跟踪的可能性。全局设置控制可以通过为所有应用定义隐私策略来实现这一点；或者，使用者可以在单个应用级别上控制数据访问。亦可使用像 PRICON posit 方法这样的隐私控制，以将两种方法结合起来。VMS 的另一个选项可能是网络浏览器已经使用的“不跟踪”（DNT）信号。DNT 信号是一个 HTTP 标头字段，说明在服务跟踪用户活动或通过跨站点跟踪用户方面的用户偏好。

应用或控件可以请求仅在应用正在使用时接收用户数据，或者允许随时接收用户数据（例如位置数据）。使用者可以选择不允许这种访问，并且建议使用者能够在设置中随时改变其选择。如果应用于同样在欧盟内运营的服务，那么通用数据保护条例（GDPR）要求用户能够做出明智的隐私决定。如果决策者意识到数据泄露（谁获得何种数据，出于何种目的，在什么条件下）或拒绝（哪些特定功能受到限制）的后果，便有可能做出明智的隐私决定。

如果应用已被授予对某些数据的访问权限，并且要在后台模式下使用这些数据，那么需要提醒用户相关权限已获批准，并允许用户更改应用的访问权限。

建议采用稳固的 VMS 架构，以防止应用访问用户未明确授予访问权限的信息。

B.4 数据准确性和数据完整性

建议 VMS 以特定方式维护数据的所有方面，如数据上传、下载、通信和删除。

端到端安全性 – 全生命周期保护。建议进行定期代码审查和严格安全测试。此外，建议实施广播级、数据库级和接收器级的保护策略。

建议提供软件安全保证，以防止使用、控制和保护的数据和资源的丢失、不准确、变更、不可用或滥用。

建议允许用户验证 PII 的准确性及其处理的合法性。

完整性意味着数据的一致性、准确性和可信度会随着时间的推移而得到保持。因此，建议建立防范信息遭到不当修改或破坏的机制。建议采取适当的措施来确保信息的不可否认性和真实性。

在设置中，建议用户能够看到其允许哪些应用访问某些信息，以及能够授予或撤销任何未来的访问权限。

此外，建议 VMS 操作系统提供限制，以防止可信数据管理解决方案安装的应用和帐户与用户安装的应用和帐户之间的数据移动。

如果用户的个人身份信息不准确，或者用户认为对其个人身份信息的处理违反了适用的法律，那么用户可以要求对其个人身份信息进行更正、修改或删除。

应实施系统、应用和程序来保护用户个人身份信息，以最大限度地降低信息被盗、损坏、丢失或遭到未经授权访问或使用的风险。

建议检测 VMS 或云中对 PII 的任何未经授权的更改，并通知用户。

B.5 机密性

机密性包括保留对访问和披露的授权限制，其中包括保护个人隐私和专有信息的手段。

B.5.1 机密性影响级别

建议对 PII 进行评估，以确定其机密性影响级别，以适用适当的保障措施。不建议对存储或创建的所有 PII 数据平等对待。

根据可识别性、数据敏感性和法规保护义务，建议将机密性影响级别评估为低、中或高。

B.5.2 机密性保护

建议通过以下措施实现机密性保护：

– 实施访问控制机制，使用密码从VMS访问数据。

– 高影响机密性PII的多层访问。

– 移动电话、笔记本电脑和个人数字设备的多级访问控制。

– 传输前加密PII。详细措施在第A.3.8节（密码系统）中有所描述。

此外，建议在部署新需求之前进行风险评估。建议实施持续的风险监控机制，以评估 VMS 的变化或识别与 VMS 相关的新风险。

B.6 数据匿名化

数据匿名化是为了保护 PII 数据主体而不可逆转地改变分类数据的过程。

通过对 VMS 环境中处理的数据进行匿名化，可以实现广泛的数据分析和数据共享。

B.7 数据可用性

可用性要求确保及时可靠地获取和使用信息。

建议授权用户对使用位置信息的系统服务进行详细控制，这包括用户能够关闭内部应用收集的信息中包含的位置信息、导航搜索历史以及蓝牙和无线接入信息。如果用户登录到 OEM 云，在默认情况下，功能上必需的应用将被授予对 OEM 云的访问权限。建议用户在设置中控制每个应用对云的访问。

如果通过远程信息处理来远程访问 PII，那么建议连接的服务使用多级身份认证进行操作。

由于以加密格式（例如，使用同态加密）执行各种数据处理（计算、统计处理等）可以获得数据，因此可以对 VMS 中的数据执行类似的数据处理。

参考文献

b-ITU-T X.1197 Amd1] Recommendation ITU-T X.1197 Amd.1 (2019), *Guidelines on Criteria for Selecting Cryptographic Algorithms for IPTV Service and Content Protection, Amendment 1*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2020), *Security Guidelines for Applying Quantum-Safe Algorithms in 5G Systems*.

[b-ETSI WP35] ETSI White Paper 35 (2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020, *IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

[b-IETF RFC 8200] IETF RFC 8200 (July 2017), *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IETF RFC 8216] IETF RFC 8216 (2017), *HTTP Live Streaming*.

[b-ISO/IEC 23009-1] ISO/IEC 23009-1:2019, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

[b-IAB] Internet Architecture Board (IAB) statement on IPv6 address exhaustion (November 2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [Online].

[b-NIST SP 800-79-2] NIST Special Publication 800-79-2 (2015), *Guidelines for the Authorization of Personal Identity Verification Card Issues (PCI) and Derived PIV Credential Issuers (DPCI)*.

[b-USG OMB] US Office of Management and Budget (November 2020), *Memorandum for heads of executive departments and agencies*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [Online].

ITU-T 系列建议书

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

瑞士印刷
2022年，日内瓦