国际电信联盟
电信标准化部门

建议书

ITU-T X.1381 (03/2023)

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

基于以太网的车载网络的安全指南

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
万维网安全（1）	X.1140–X.1149
应用安全（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.1350–X.1369
智能交通系统（ITS）安全	**X.1370–X.1399**
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
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
网络防御	X.1590–X.1599
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
数据保护	X.1770–X.1789
IMT-2020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.1381建议书

基于以太网的车载网络的安全指南

摘要

ITU-T X.1381建议书为基于以太网的车载网络（IVN）提供了安全指南。当前的电气和电子（E/E）架构趋势是将以太网与控制器局域网（CAN）、本地互联网络（LIN）、面向媒体的系统传输（MOST）和FlexRay等传统车载网络集成。过去，以太网仅被视为车辆与外部环境之间的连接。在以太网上实现基于互联网协议的连接的标准协议（例如，基于互联网协议或通用测量和校准协议的诊断通信），被用于外部环境和车辆之间的通信。这些用例通常不需要满足严苛的实时要求。然而，使用以太网通信的车载应用，需要高时间敏感性和可靠性等特性。

目前车载通信技术的发展需要增加网络带宽。与以太网相比，传统IVN不足以满足当前车载应用的带宽要求。因此，无论现在和将来，基于以太网的IVN都是E/E架构的骨干。

然而，从普通计算机网络得出的对策不适用于汽车应用，因为它们不是针对汽车需求和能力而设计的。

为了满足这一需求，本建议书提供的汽车以太网技术安全指南，包括一个汽车以太网参考模型和基于以太网的IVN的威胁和脆弱性分析，以及该IVN的安全要求和使用案例。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1381	2023-03-03	17	11.1002/1000/15107

关键词

汽车以太网安全、智能交通系统（ITS）安全。

* 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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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他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，国际电联未收到实施本建议书可能需要的受专利/软件版权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，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2023

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

ITU-T X.1381建议书

基于以太网的车载网络的安全指南

1 范围

本建议书分析了分布式云的安全威胁，提供了分布式云的安全指南。

本建议书提供了基于以太网的车载网络（IVN）的安全指南，涉及网络安全的以下方面：

1) 安全威胁分析；

2) 安全要求；以及

3) 使用案例，

网络安全表明相关的技术通信架构是或可以成为网络物理系统的组成部分（例如，集成在嵌入式系统中的以太网通信协议栈）。

1.1 应用性陈述

一般网络，尤其是以太网上的网络用于通信服务。因此，本建议书的安全语境侧重于通信安全，不一定是指具有以太网连接的计算节点的信息安全。

因此，从安全工程的角度来看，本建议书的安全指南涵盖了汽车应用中使用的基于以太网的网络工程，因而相关的分层通信架构及其分层协议栈，是这种安全考虑的要点。

1.2 在整个时间范围内验证安全导则

车载以太网所需通信架构的安全性正在发生根本性变化，其主要原因在于

1) 网络拓扑可能发生了变化（受不断演进的分布式计算架构的驱动，利用该通信网络推进车辆自动化）；

2) 分层协议体系结构：现用以太网和非以太网协议栈可以改变、得到扩展等；

3) 协议的演进：当前使用的信息通信技术（ICT）协议（为IEEE、IETF、ITU-T、ETSI、3GPP等标准开发组织所有）仍然受到持续的维护活动和扩展的制约，体现在协议分析（如用于汽车应用的IEEE时间敏感网络（TSN）[b-IEEE 1722-2016]）或协议版本控制中；

注 – 此外，与协议规范相关的安全考虑也可能更新。

1) 通信安全背景下安全手段和解决方案的演变。

因此，预计今后将对本建议书进行修订。

本建议书特别关注第一组用例给出的初始安全导则，主要涉及第一代基于以太网的IVN，将在本建议书发布时，形成当前最佳的安全做法和安全导则。

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。ITU-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。

[ITU-T X.1371]　ITU-T X.1371建议书（2020年），联网汽车的安全威胁。

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　可核查性（accountability）[b-ITU-T X.800]：实体的一种属性，用于确保实体的行动可被唯一地追溯至该实体。

3.1.2　认证（authentication）[b-ITU-T X.1252]：验证的正式过程，如果成功，将为某实体产生一个经认证的身份。

注 – 在身份管理情境中使用术语认证是指实体认证。

3.1.3　真实性（authenticity）[b-ITU-T X.641]：保护相互验证和数据来源验证。

3.1.4　授权（authorization）[b-ITU-T X.800]：授予权限，包括授予基于访问权限进行访问的权限。

3.1.5　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。

3.1.6　机密性（confidentiality）[b-ITU-T X.800]：使信息不泄漏给未授权的个人、实体或过程的特性。

3.1.7　数据完整性（data integrity）[b-ITU-T X.800]：未经授权不更改或销毁数据的属性。

3.1.8　防火墙（firewall）[b-ITU-T X.1039]：放置在由专用设备或若干组件和技术组合而成的网络环境之间的一种安全屏障，从一个网络环境到另一个网络环境的所有通信都通过该屏障，反之亦然，只有本地安全策略定义的授权通信才获准通过。

3.1.9　安全网关（security gateway）[b-ITU-T X.1039]：网络之间、网络内子组之间，或者不同安全域内的软件应用之间的连接点，旨在根据给定的安全策略来保护网络。

3.1.10　车载网关（VG）[b-ITU-T F.749.1]：车载网关（VG）是一种支持车内设备与另一设备通信的装置，另一设备的物理位置既可位于车内亦可设在车外（如路边台站、云端服务器等。）。VG提供标准化的接口和协议、跨异构网络的通信、基于应用需求和网络服务质量（QoS）的优化网络选择、网络通信的仲裁和集成、安全性和交换网络连接，以保持服务连续性。

注1 – 中央网关这一术语（如本建议书所述）通常与抽象车载网络（IVN）的车辆网关同义，或与更详细的IVN架构中的车辆边界网关同义。

注2 – 车辆智能交通系统（ITS）网关这一术语基本上与车辆网关同义。

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　电气和电子架构（E/E架构）：耦合的双平面车辆架构，包括：1) 电能或电力分配网络平面；以及2) 信息处理和通信网络架构平面。

注 – 有时添加于E/E的第三个标签是指车辆推进技术，如E3；第三个E表示电动汽车。

3.2.2　车辆边界网关：位于车辆内部网络域和车辆外部网络域边界的车辆网关。因此，所有车辆到万物（V2X）的通信流量，都通过此类车辆网关选路。

注1 – 术语“车辆网关”也包含这一含义，因此对于只部署了一个车辆网关的车载网络（IVN）架构或许足够了。然而，IVN也可以将车辆网关仅用于内部互连和互通目的。这种网络环境可能需要更详细的网关类型区分。

注2 – 特定网关类型支持的具体互通功能通常由扩展网关名称表示，例如，表示在网络分层结构中的位置（如接入或核心网络层面）、网间互通的边界或互连类型（如安全域）、具体网络接口或通信技术。

注3 – 通信控制单元被理解为属于车辆边界网关（功能）类别的技术部件。

注4 – V2X通信涵盖所有流量类型，例如来自远程信息处理、ITS或诊断服务的流量。

3.2.3 面向区域的电气和电子架构：按传感器、执行器和计算节点在网络子域中的位置（注2）对车载组件（注1）进行分组的电气和电子（E/E）架构。每个子域，即所谓区域（注3），都有一个与区域相关的车辆计算节点（称为汽车应用中的区域控制器），连接到所有内部子域的车载组件。每个区域的区域控制器再与一个卓越的高性能车载计算节点互连。因此，从分布式计算架构的角度来看，在区域和整个车载网络（IVN）域之间存在一个由此产生的处理层级。

注1 – 在IVN环境中确定计算和网络组件的范围。

注2 – “位置”被理解为物理或虚拟IVN拓扑层级的网络位置。

注3 – 这里的区域概念主要与E/E架构环境中的网络域概念相关。这种区域不一定包括其他与安全相关的ITU-T建议书（如[b-ITU-T Y.2770]）所用的安全区域、信任区域或非军事区域的概念。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

ADAS 高级驾驶员辅助系统

ARP 地址解析协议

AUTOSAR 汽车开放系统体系结构

AVB 音频视频桥接

CAN 控制器局域网

CGW 中央网关

CPU 中央处理器

CRC 循环冗余校验

DHCP 动态主机配置协议

DoIP 网络协议诊断通信

DoS 拒绝服务

DTLS 数据报传输层安全

ECU 电子控制单元

E/E 电气和电子

FDB 转发数据库

FIB 转发信息库

HSM 硬件安全模块

ICMP	互联网控制消息协议
ICT	信息通信技术
ID	标识符
IDS	入侵检测系统
IP	互联网协议
IPsec	网际协议安全性
IPv4	互联网协议第4版
IPv6	互联网协议第6版
ITS	智能交通系统
IVN	车载网络
LIN	本地互联网络
MAC	媒质访问控制
MACsec	媒质访问控制安全
MCU	微控制器单元
MOST	面向媒质的系统传输
MPU	多点控制单元
OBD	车载诊断系统
OEM	原始设备制造商
PDU	协议数据单元
PVID	端口VLAN ID
QoS	服务质量
SecOC	安全车载通信
SR	安全建议
TARA	威胁分析和风险评估
TCP	传输控制协议
TLS	传输层安全
TP	传输协议
TSN	时间敏感网络
UDP	用户数据报协议
UDS	统一诊断服务
V2X	车辆到万物
VG	车辆网关
VID	VLAN标识符
VLAN	虚拟局域网

5 习惯用法

本建议书提供了一个安全要求列表，标记为[SR-x]，其中x是一个数字。此类安全要求使用以下短语，其含义规定如下。

短语“建议”或“应”表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

短语“作为选择可以”表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。相反，这意味着供应商可以选择提供该特性，并且仍然声称符合该建议。

6 基于以太网的汽车和不断发展的车载架构概述

汽车以太网是一种物理网络，用于通过有线网络连接车内部件。汽车以太网也用作整个车载以太网的名称，包括该网络域中使用的所有协议层和协议。它旨在满足汽车市场的需求，包括满足电气要求(电磁干扰/射频干扰发射和敏感性）、带宽需求、延迟要求、同步和网管要求。随着自动驾驶汽车和高级驾驶员辅助系统（ADAS）技术益发受到关注，现代汽车通常配备的多个摄像头、车载诊断系统（OBD）和信息娱乐系统，都需要高带宽。此外，随着功能的增加，车载互连计算节点（例如电子控制单元（ECU））的数量也在增长，导致线束和车辆质量增大，从而降低了车辆性能和燃油效率。面向区域的E/E架构是特定车载计算和网络架构的突出示例，其中的以太网也用于最高网络层级，用于整个架构中所有区域（所谓骨干网）的互连。当控制器局域网（CAN）、本地互连网络（LIN）、面向媒质的系统传输（MOST）或FlexRay等传统IVN与以太网集成时，可以利用标准化的以太网电缆显著减轻质量并降低成本。此外，高带宽还可以减少控制系统的数量和复杂性。

然而，并不是每个IVN域，如动力系统、车身和底盘，都会变为汽车以太网。以车身为例，这意味着只需少量数据和带宽的车身，不需要使用额外资源和努力来改变网络协议。

图1显示了一个包含传统IVN协议的混合IVN，例如CAN和汽车以太网。带宽需求低的通信仍然可以使用传统的IVN协议，而自动或ADAS功能等带宽需求高的通信，可以改为基于以太网的IVN。

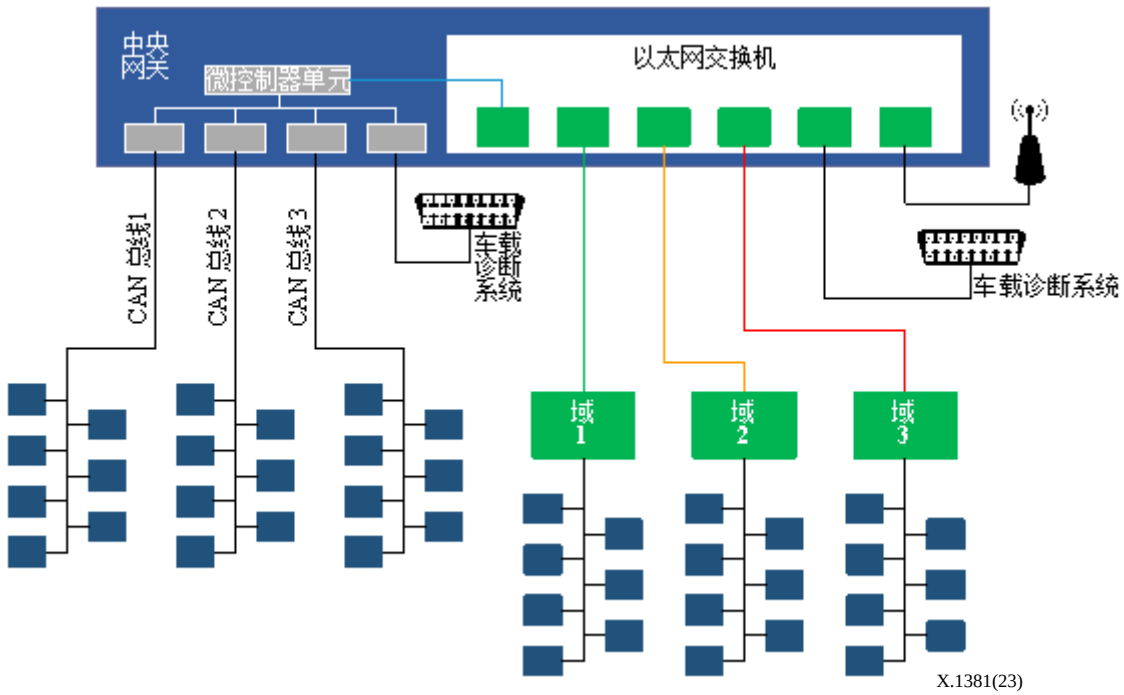


图 1 – 基于传统协议和汽车以太网的典型车载网络的现行异构性

众所周知，基于以太网的IVN有望随着时间的推移发展演变。这种网络演进通常伴随着通信架构（如通信拓扑、分层协议栈等）的变化，并最有可能影响相关的通信安全架构。

过去曾探讨过基于CAN/FlexRay/LIN和有时基于MOST的传统E/E架构的安全概念，而且某些建议的机制已进入标准化程序。以太网及其相关的上层协议不仅简单，而且能够更快地取代传统的汽车总线系统；并可能改变现行E/E架构的基本概念。

以太网的采用是提高车内安全性的大好契机，因为以太网已经解决了汽车应用中诸多苛刻的安全性问题，包括所谓运营商级ICT业务（如基于以太网的城域网、基于以太网的地面无线接入网）以及传统的信息技术业务（如作为专用企业局域网基线连接的以太网）。然而，它也带来了包括汽车或嵌入式系统局限性在内的巨大挑战，而应对这些挑战是目前起码获得与现行安全增强性E/E架构同等的安全性的保障。

6.1 车载电气和电子计算和网络架构

以往的E/E架构考虑将中央网关（CGW；在该类IVN中亦称VG或车辆ITS网关）用于车内通信和不同子域之间的互连，从而通过这类VG的路由传送实现端到端的连接。

注1 – 本文中的“路由”是通用流量路由功能，而不是IP路由等其他路由传送。当前基于以太网的IVN不使用IP路由器实体，仅使用IP类网关。IP和以太网的这种用途使它们类似于交换IP网络（用于基于IP的通信服务）。从通信安全的角度来看，这一点至关重要，因为它减少了与IP相关的安全目标（例如，将不会有IP路由协议带来的安全威胁）。

针对性的基于以太网的通信，可望满足高实时性和可靠通信的要求，并且受益于成熟、广泛使用和经过验证的通信技术和工艺。

注2 – [b-IEEE 802.1]，尤其是[b-IEEE 802.1CB]，可实现可靠的通信，其中包括一个包含第2层冗余功能（R-Tag）的环形架构。

特别是CAN、FlexRay、LIN和MOST原生用于车载通信；CAN最受欢迎。CGW、一般的VG和具体的车辆边界网关，是车内网络和通信架构中的关键网络和安全元素。附录II和III提供了一些可能有益于通信安全的补充信息。

远程访问车辆（例如使用车间连接进行诊断或使用各种V2X通信选项）在过去是无法实现的。车载ECU通过一条或多条本地汽车优化现场总线相互连接。

生产后的合法访问只能通过直接和基于电缆的物理连接实现。因此，短距离点对点连接，专用于需要通过CAN协议连接到OBD端口的诊断服务。原始设备制造商（OEM）意识到，诊断功能和不提供任何安全功能的本地CAN协议面临更高的安全风险。[b-Autosar 654]关注CAN消息的真实性和完整性，而适用的安全概念主要采用消息认证码。

目前的研发成果使从外部设备到车辆的基于以太网的通信成为可能。通常，车内专用ECU可用作某种外部通信的接入点。如果需要，ECU通过公共汽车网络将相关信息路由到其他ECU，或者通过基于以太网的连接将流量转发至CGW，以便路由到其他共附的ECU。

6.2 未来与现用电气和电子架构安全性的比较

由于出现了一系列涉及车载组件的不同误用案例，现行的E/E架构已有既定的安全机制。就通信系统而言，主要CAN网络的认证机制已经发布和标准化，并将部分施用于未来几代车辆。汽车开放系统架构（AUTOSAR）针对车内通信的真实性和完整性，规定了一个安全的车载通信模块。请注意，认证机制不仅涉及传输消息的真实性，还要确保通信伙伴的真实性。

此外，CAN作为物理层总线技术，仅通过广播传输消息。

注1 – 因此，总线拓扑等共享物理介质通信的基本性质，与交换式以太网网络的设计方法相反。

因此，每个参与者都能够读取通过CAN总线传输的所有信息流。不同的基于总线的网络域以及其他子域，会将安全相关的流量与其他类型的流量（如信息娱乐或休闲）分开。网络域之间的通信只能通过CGW进行，而CGW通常通过策略规则（例如与过滤器相关的规则）的实施机制，防范泛洪攻击并确保网络的可用性。

注2 – 车辆网关（如CGW）提供一组网络功能，其中一个特定子集与通信安全相关。因此，得到实施的不仅有特指安全性，还有特指非安全性的策略规则（例如用于VLAN互通、IP转发或设置TSN驱动的QoS动作）。

以太网是应用广泛的网络通信既定标准，用于常见的机器类通信（如计算机）网络，覆盖多种规模的区域网络（如小型、本地、大都市）以及用于移动通信的陆地无线电接入网络。鉴于这一历史和网络背景，或许存在可供重用的网络安全模式。

由于它的普遍使用，基于以太网的通信（包括上层协议）遭受过多次攻击，但也存在针对不同用例的对策。例如，在互联网内，对（仅限）于基于传输控制协议（TCP）的传输服务，强烈建议使用传输层安全协议（TLS）来确保通信的真实性、完整性和机密性。还建议对基于用户数据报协议（UDP）的传输服务，使用补充传输安全协议数据报传输层安全协议（DTLS）。使用以太网作为车载通信的既定和普遍标准，可以重新使用互联网协议（IP）栈相关的安全机制。然而，从普通计算机网络获得的对策不适用于汽车应用，因为它们不是专门为其要求和能力而设计的。例如，它们或许无法提供实时保证，并且需要增强资源受限的嵌入式设备所无法提供的性能。因此，在发布时没有考虑基于以太网的时间敏感通信协议的安全机制集成。

出于安全考虑，车载通信的隔离至关重要。目前，原始设备制造商考虑使用网络虚拟化对以太网流量进行逻辑隔离，这涉及以太网中作为第2层虚拟专用网的虚拟局域网

（VLAN）。请注意，也可以通过其他方式实现车内流量隔离，例如通过第1层的VPN（物理分离以太网）或第3层的VPN（使用已知的用于以太网IP通信服务的VPN解决方案）。

VLAN是在普通计算机网络中为数据链路层提供逻辑隔离的成熟做法。VLAN通常用于将物理网络分成不同的逻辑网络。VLAN的车载应用主要基于VLAN支持业务量的优先排序的事实（例如，通过将VLAN优先级代码点直接映射到TSN业务量等级）。

注3 – 分级VLAN的安全考虑可能属于特定V2X互连模型的未来IVN范围，但超出了本版建议书的范围。因此，这里只做出单标记或基于端口的VLAN的假设。

一方面，广泛应用于车载通信的以太网标准提供了一些可能性；然而，另一方面还有一些特别需要注意的问题。除了缺少安全机制应用之外，不建议通过以太网将外部设备连接到车辆的特殊设备。

即使用户也有兴趣尝试通过插入其笔记本电脑或使用其智能手机，增强接入IVN的能力。将以太网交换机作为附加组件，可能会让经过专门培训的未授权人员获得有趣的攻击矢量。攻击者可以从互联网或已公布的普通以太网交换机漏洞实施已知的攻击。与通信安全的情况相似，也有针对普通以太网交换机的对策。然而，需要对汽车环境进行进一步的探索和研究。

表1在非常抽象的层面上显示了传统的、面向现场总线的IVN协议和基于以太网的协议之间的差异。每个比较目标的第一列是用符号表示的各自标准的成熟度，如差（–）、中性（0）、好（+）、最好（++）。请注意，表1有意做了简化；更严谨的协议评估需要将以太网与每个单独的现场总线或车辆总线通信技术进行比较。

表 1 – 车载传统和基于以太网的通信架构的比较

标准	面向现场总线的IVN协议（注 1）		基于以太网的IVN	
简单性	–	复杂、异构、多协议网关	++	与（大部分）第2层交换机非常同构
灵活性	–	难以扩展/适应新子网（子网内容易）	++	在新的子网或子网内部易于扩展/适应
性能	+	取决于总线类型	++	高达每秒几千兆比
实时	++	数十年久经考验	–	有能力但不以此为目的
与网络相关的物理材料的质量	–	每条总线单独布线	+	单一对绞线实现全部连接
成本（投资，而非运营）	–	小批量汽车专用生产	+	亦面向非汽车行业的全球量产
标准化程度	–	标准差异的巨大	+	几乎无差异的标准
物理层和数据链路层的连接模型（注2）	–	由于物理介质共用（“总线”），只有点对多点通信模式	+	以太网支持点对点和点对多点两种通信模式（注3）
消息完整性（注4）	+	循环冗余校验（CRC）+总线特定措施	+	CRC、块码
安全措施（注5）	–	几乎没有	0	附加（互联网协议第4版（IPv4）），互联网协议安全（IPSec）（互联网协议第6版（IPv6））

注 1 – 针对所列标准的评估反映了典型的协议设计，但并不适用于所有面向现场总线的通信技术，例如，CAN不提供支持实时通信的固有协议方法。

注2 – 此处假设：车载应用通常需要点对点或点对多点通信拓扑类型的通信服务。这种拓扑必须由逻辑连接拓扑提供服务，这意味着将链路层连接拓扑视为探讨的通信技术的共同“协议层”。

注3 – 车载以太网将仅在“交换模式”下部署和运行（主要由服务质量（QoS）目标驱动），这意味着仅在以太网物理媒介层支持点对点连接模式。物理媒介不是共享的，而每个以太网第1层端点都可以独享物理层资源。然而，也可直接通过数据链路层转发功能的本地以太网嵌入式组播和广播能力，或者间接通过上层协议（如IP及其组播、任播或广播类型的网络地址），支持点对多点通信拓扑结构。

注4 – 这里的安全相关完整性包括：a) 比特完整性；b) 数据完整性，即，协议数据单元（PDU）的单个比特的完整性范围或整个PDU本身（位于特定协议层）。

注5 – 评估安全措施的各项协议规范是否具有内在安全特性。

概述的比较标准涵盖基本网络工程和通信服务工程以及与安全具体相关的问题。

6.3 在汽车应用中使用以太网的通信服务

目前，汽车以太网主要用于诊断和传输多媒体流，例如来自ADAS摄像机传感器的视频数据。此外，这一于2010年代中期推出的技术，使车载计算节点（如ECU）通过以太网进行通信。

6.3.1 诊断

传统的车载诊断方法是将诊断工具连接到OBD-II端口，并通过统一诊断服务（UDS）协议与目标ECU通信。UDS是汽车行业精心制定的应用层协议，使诊断系统能与ECU通信，以诊断故障并对ECU进行相应的重新编程（参见[b-ISO 14229-5]）。

基于互联网协议的诊断通信（DoIP）以IP为基础（见[b-ISO 13400-2]）。DoIP支持通过以太网在车辆和外部测试设备之间传输UDS消息，并且可以远程检索车辆诊断数据，无需与车辆进行物理连接。DoIP将UDS消息封装在TCP数据包或UDP数据报中，如图2所示。

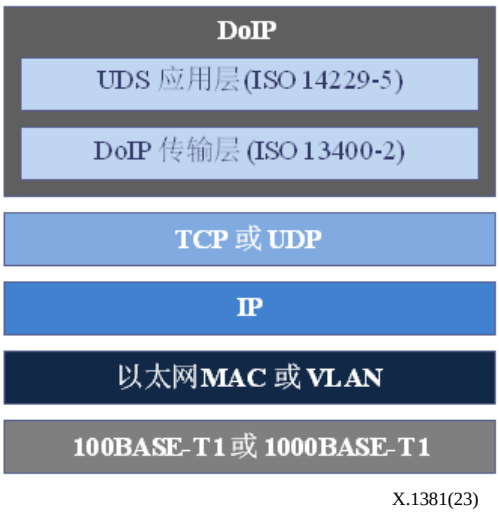


图 2 – 互联网协议诊断通信应用协议栈

DoIP本身无须考虑任何通信安全机制，通常也不会以任何方式对消息进行验证或加密。DoIP考虑的是非强制性的上层验证。

6.3.2 多媒体服务环境中的媒体流

对于ADAS，高度自动化和全自动驾驶的车辆必须配备大量传感器，如高清摄像头和连接功能，以获得感知车辆环境的充足信息。此外，许多车辆配备了使用或传输应用级媒体流（在以太网的情况下，不与物理媒体（子）层混合）的设备，用于信息娱乐系统、全景监视系统、泊车辅助系统、线路保持辅助系统、夜视等。在使用摄像头时，相对较大的媒体流（就通信流量而言）是以低延迟和高质量传输应用驱动的QoS目标生成的。如果使用CAN协议，由于协议设计的固有有效载荷范围有限，则不可能达到上述要求。

如采用IEEE音频视频桥接（AVB）框架，汽车以太网可以满足这些要求。

注 – 术语AVB表示一组[b-IEEE 802.1]标准，包括[b-IEEE 802.1Qav]、[b-IEEE 802.1AS]和[b-IEEE 802.1Qat]。因此，IEEE AVB任务组于2012年更名为TSN任务组，目前已将AVB标准包括在内。

AVB可以满足更普遍的TSN要求，开启了以单一网络处理信息娱乐、车身控制、驾驶辅助甚至安全攸关功能的可能性。

使用全景监控系统时，摄像机阵列提供车辆环境的同步360°环绕视图。该视频类媒体流可以被发送至驾驶员感知系统，即平视显示系统或视频导航系统。它还可以是通过AVB网络同步的附加传感器数据和相关ECU。

6.3.3 车载网络的骨干

现代汽车可能配备100多个ECU。一个ECU或车辆计算节点与以太网IVN拓扑的一个网络节点相关，具有一个或多个端节点（取决于每个计算节点的物理、逻辑或虚拟以太网连接接口的数量）。此外，ECU的数量还会进一步增加，致使ADAS和自动驾驶汽车开始向IVN提出更大IVN传输容量（俗称带宽）的要求。

此外，传统IVN协议使用的线束系统，是一沉重和巨大的成本因素。如果将以太网用作IVN骨干，则可以减少高达80%的车内连接成本和30%的车内布线质量。

如图1所示，基于以太网的IVN有多个域。传统的IVN协议被用于各域，而以太网用于域间通信，即核心网级别（相对于ICT网络），亦俗称骨干网级别的通信。

汽车以太网不同于总线系统的拓扑结构。没有连接到众多ECU、传感器和执行器的总线导线。相反，它们以点对点的方式与以太网交换机相连。如果通信消息必须从一个域发送到另一个域，它可以很容易地交由网络互通功能处理，即交给以太网交换机、VLAN网关、可能还有基于以太网的IVN中的IP路由器和IP网关提供的功能。相比之下，当与位于以太网的端点通信时，传统的车载现场总线协议需要网络，还可能需要通常位于网关的服务互通支持。

7 威胁分析

7.1 威胁分析采用的方法

本条款分析了车载以太网络环境下的安全威胁场景。[ITU-T X.1371]中描述了联网车辆中已识别的总体威胁。

为了获得安全概念，应制定安全目标。开展威胁分析和风险评估（TARA）以确定安全目标阶段的风险处理方法。为了开展TARA，应确定安全资产和安全目标，以及相关的威胁。如果根据已识别的安全资产、安全目标和威胁，通过影响评级和攻击可行性评级来确定相应风险的处理方法，则可以确定安全概念，更多信息请参见[b-ISO/SAE 21434]。根据[b-ISO/SAE 21434]的威胁分析方法可以识别安全资产和相关的安全目标，然后也可以在该条款中识别安全威胁。

影响评级、攻击可行性评级和风险决策的流程超出了本建议书的范围，需要进一步研究。

7.2 安全资产

安全资产指应受到保护的任何数据对象、功能或资源。考虑到基于以太网的IVN，表2列出了主要的安全资产。

表 2 – 安全资产

资产	描述
管理数据	管理数据包括两类（注1）： 配置数据，以具有以太网连接的网络元素或网络功能的功能性行为为特征，例如网关、以太网交换机、入侵检测系统（IDS）和防火墙等； 操作状态数据，不仅描述那些网络实体的实际行为，还描述使用通知[b-ITU-T M.3702]的所有管理服务，例如作为故障管理一部分的告警报告[b-ITU-T M.3703]。 管理实体和被管理实体之间的这两类管理数据流基本上都受到安全保护。然而，安全性影响，比如通过操纵配置数据产生的安全性影响通常应比对操作状态数据产生的影响高得多。另一方面，比如，对以太网网络元素发出的告警的有意抑制可能会恶化当前的故障情况
以太网通信相关的第2层协议数据单元	以太网流量由数据链路层流量构成，即传输到基于以太网的汽车IVN的以太网媒体访问控制（MAC）帧（作为第2层PDU）
日志生成的管理数据（注2）	可以审计安全事件的成功检测和相关信息
加密资料	对称和非对称方案的密钥和证书，包括密码等其他凭证
固件或软件映像	将在ECU等车辆计算节点上运行的已编译代码
注 1 – 参见以太网适用的网络管理框架，如[b-ITU-T M.3010，b-ITU-T X.703，b-ITU-T G.8013，b-ITU-T Y.1730]中描述的。以太网网络实体的管理数据以作为规范和管理数据建模语言的YANG [b-IETF RFC 6020]为基础。IEEE 802（作为以太网的技术所有者），即，本建议书的主要管理数据参考，为各种以太网实体提供基于YANG的管理数据模型。 注 2 – 本表不包括日志功能的管理[b-ITU-T M.3705]。这里的日志涉及由日志功能记录的管理信息流引起的系统事件（参见关于网络设备内部管理数据流的[b-ITU-T G.7710]）。 注 3 – 这种检测功能属于统计假设测试的范畴，主要是由事件描述中的不确定性或为明确识别这类事件的策略规则条件所产生的。因此，成功的检测仅提供固有的概率结果，包括除真阳性之外的假阳性。所以，应对检测质量的等级进行限定和量化，例如，通过估计预期的非真阳性比率。	

7.3 安全目标

根据表3列出的安全目标清单对安全资产（见第7.1条）进行了分析。

表 3 – 安全目标

安全资产	安全目标	说明
管理数据	完整性、机密性	不得操纵决定以太网网络元素（如车辆网关、以太网交换机、IDS和防火墙）功能性行为的数据

安全资产	安全目标	说明
以太网通信相关的第2层协议数据单元	机密性	禁止泄露传输到基于以太网的汽车IVN的特定层协议数据单元（（Lx）-PDU）
	可用性	只要满足明确定义的、与通信服务相关的限制条件，基于以太网的汽车IVN上的通信服务应是可能的
	真实性	基于以太网的汽车IVN上的通信应检测并拒绝其他部件的冒名顶替
	完整性	禁止操纵在基于以太网的汽车IVN上交换的通信数据
日志生成的管理数据	完整性	禁止在未检测的情况下操纵被记录下且可以被审计的安全事件的证据和信息。完整性包括位和数据的完整性，范围是被记录的信息
加密资料	机密性	禁止泄露机密和私钥，以及像密码这样的用户凭证
	完整性	禁止在未检测的情况下操纵密钥和证书
固件或软件映像	机密性	禁止向未经授权的实体泄露固件和软件的内容，例如与知识产权相关的编译代码和校准数据
	完整性	禁止操纵固件和软件映像，例如作为能力改变过程的主体的映像（如，通过空中固件、空中软件或一般的软件管理）

7.4 已识别的威胁

7.4.1 机密性威胁

– 未经授权暴露以太网通信流量（由以太网物理层（L1）或数据链路层（L2）PDU构成）

攻击者可以通过将负责外部通信的组件与以太网交换机连接来嗅探以太网通信流量。然后，攻击者通过嗅探以太网相关的PDU来分析通信流量信息。

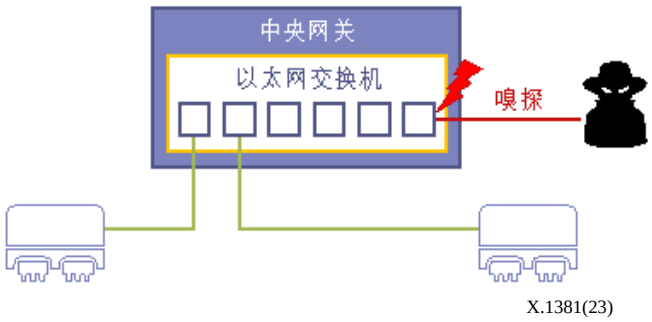


图 3 – 嗅探对机密性的威胁

– 未经授权暴露加密资料

攻击者可通过下列方式嗅探加密资料：

- 实际打开存储器外壳来获得加密资料；
- 从使用加密资料的各个组件的存储器中读取加密资料；
- 修改固件和改变控制流来暴露加密资料。

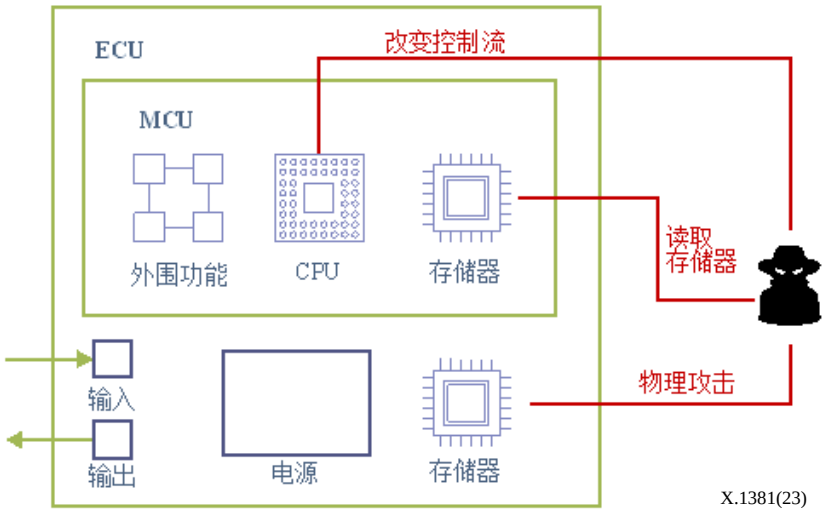


图 4 – 对加密资料机密性的威胁

7.4.2 完整性威胁

完整性的环境一般限于数据对象，此处给出了具体的安全用例。

– 操纵配置数据

攻击者可以操纵以太网交换机的配置数据。

– 操纵日志数据

攻击者可以从IDS、防火墙和无线广播系统中删除、修改日志数据，尤其是安全事件的审计日志。

– 操纵加密资料

攻击者可以自己更改有效的加密资料。

– 操纵固件

攻击者可以将固件更改为恶意固件。

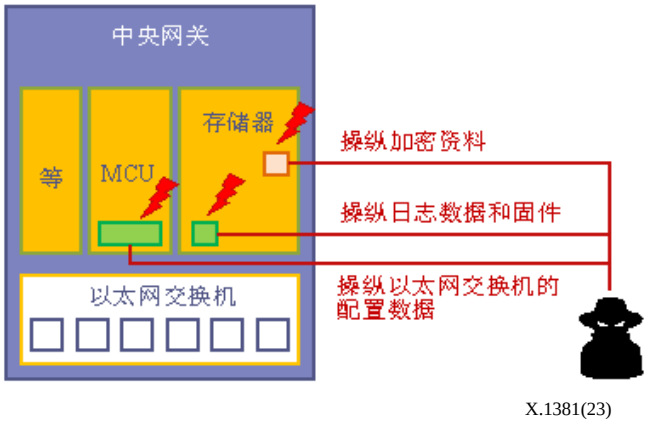


图 5 – 对通信中的数据单元完整性的威胁

7.4.3 可用性威胁

系统质量属性可用性在这里涉及以基于以太网通信为目标的通信服务可用性，这通常在网络和特定层的连接可用性要求中进行转换，也可能，例如，在路径冗余以太网IVN的情况下引起以太网路径的可用性。

– 针对可用性的威胁：基于以太网的IVN上的拒绝服务（DoS）攻击

攻击者可以发起DoS攻击，以阻止具体的ECU功能，包括CGW、车辆边界网关或连接控制单元。

如图6所示，攻击者可以使用众所周知的DoS攻击技术，例如针对IP传输协议的攻击，如TCP SYN flood或针对TCP的teardrop攻击，使特定的ECU和CGW对期望的计数器ECU不可用。此外，攻击者可以利用第2层广播风暴等攻击耗尽IVN的资源，使正常的以太网MAC帧（如第2层PDU）无法再交换。

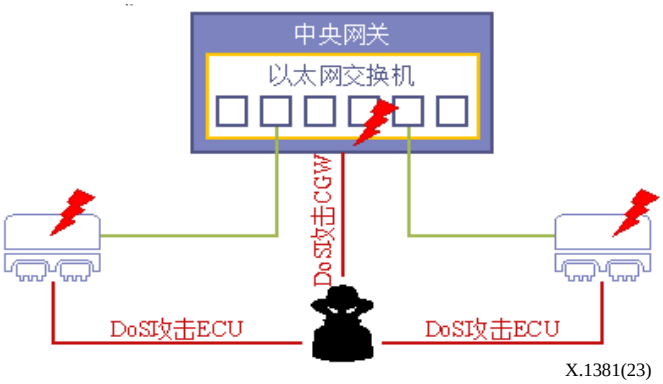


图6 – 可用性威胁

7.4.4 真实性威胁

– 车辆计算节点（如ECU）伪装

攻击者可以伪装ECU等有效组件，并向其他组件发送恶意消息。攻击者可以伪装成有效的通信端点（例如，由ECU托管）并发送恶意消息或获取传输的通信流量。在图7所示的示例中，正常情况是ECU A和B之间进行上层连接（例如，点对点IP传输连接），结果是ECU-A向ECU-B发送以太网流量（反之可能亦然）。攻击者使用地址解析协议（ARP）欺骗或IP欺骗等攻击方法伪装成ECU-A（例如，参见[b-IETF RFC 2827][b-IETF RFC 4953][b-IETF RFC 6575][b-IETF RFC 6959]），然后向ECU-B发送恶意消息。

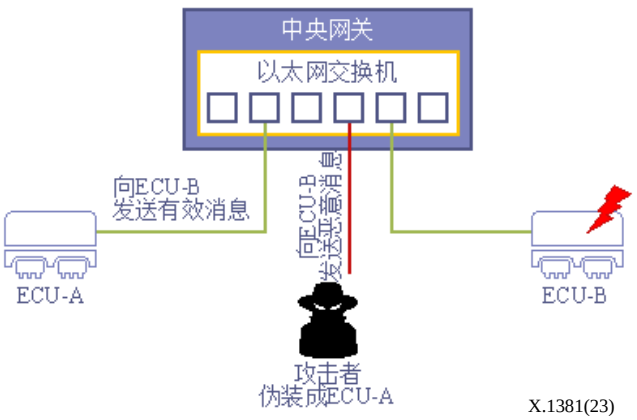


图7 – 真实性威胁

8 安全性要求

本条款描述了在基于以太网的IVN环境中应对已识别威胁的安全性要求。

8.1 机密性

– [SR-01]建议存储和使用加密资料的ECU使用硬件安全模块（HSM）等安全的存储器，以便安全地存储加密资料。

– [SR-02]建议部署例如由国际标准组织指定的众所周知的算法和协议。

– [SR-03]建议在以太网通信的消息中采用安全机制以防止窃听。

作为选择可以将具体针对各层的安全协议应用于相应的协议层，以对其和针对具体协议的PDU（全部或部分）进行加密，作为车辆中基于以太网的通信流量的一部分。这种通信安全协议例如，媒体访问控制安全（MACsec）、IPsec、TLS和DTLS。

– [SR-04]禁止未经授权的实体泄露敏感的加密资料。

当加密资料暴露给了未经授权的实体时，车辆的安全机制便不再安全。

– [SR-05]仅建议车辆中符合访问控制策略的经授权人员和设备在生产阶段处理加密资料。

– [SR-06]建议以太网交换机的MAC地址表进行静态配置。

预定义的ECU可以通过静态配置以太网交换机中的MAC地址表来访问车辆中的以太网。

动态MAC地址会导致欺骗和MAC泛洪等安全问题。当表中存储了大量MAC地址时，交换机可以将数据帧广播到所有网络端口。就车辆而言，可以静态配置MAC地址表以防止这些安全问题，因为已经指定了与交换机通信的ECU。

– [SR-07] 建议禁用以太网交换机中MAC地址表的动态学习功能。

停用MAC地址表的动态学习功能，可以防止会导致以太网消息传输到非预期目的地的MAC泛洪。

然而，如果对于车辆的操作或维护是必要的，则交换机不应仅在有限的时间内存储学习到的MAC地址。

– [SR-08] 建议使用以太网的IP主机功能（例如，由ECU托管）的IP网络接口获得由负责的网络管理功能分配的固定IP地址。

注 – 这里具体的网络管理功能是身份管理，包括网络地址管理。这种管理功能可以在基于以太网的IVN的不同生命周期和操作阶段期间执行，例如完全静态先验、静态和动态配置管理混合，这也取决于是否使用以太网和互联网层的网络操作协议。

该SR不仅适用于作为整体的单个ECU，还适用于以太网络中的每个分区或节点（例如，每台虚拟机）。

8.2 完整性

– [SR-09]建议保护以太网交换机的日志和配置数据，防止未经授权的修改和删除。

– [SR-10]建议只能由经授权的实体更新配置数据。

– [SR-11]建议ECU采用安全启动特征以及固件的完整性检查。

在执行之前或执行期间，应检查ECU的固件和存储在ECU存储器中的以太网交换机数据的完整性。固件的配置和输入参数的完整性检查可用于安全启动。

8.3 可用性

在这种情况下，可用性的含义与以太网域的网络可用性有关，即可用的通信服务。安全性攻击不仅会影响这些可用性目标，也会影响其他类型的非安全事件（如组件中断或通信故障）。

因此，可用性要求（在本条款中）实际上是对可用性目标有潜在影响的安全性要求。

– [SR-12] 建议在车辆的设计阶段考虑针对基于以太网的IVN的DoS攻击。

– [SR-13] 建议交换机通过以太网通信消息检测并防范DoS攻击。

为了将IVN中DoS攻击的风险降至最低，监控和控制ECU之间的流量至关重要。

– [SR-14]建议将安全关键功能与车辆中的其他网络隔离。

8.4 真实性

真实性指能够确保给定的信息不存在修改或伪造，且该信息的确由声明给出此信息的实体所产生。

– [SR-15] 建议为以太网通信消息提供防范假冒攻击的对策。

– [SR-16]建议IVN网络元素的物理以太网络接口（不用于生产车辆）使用默认配置值“禁用”来提供管理状态临时改变（启用、禁用）的能力。

注 – 这种与网络管理相关的要求显然意味着对以太网的相应细粒度管理数据模型的支持。

这一要求通过减少可用入口点的数量来限制攻击面。

– [SR-17]建议根据最小特权原则限制硬件或软件域中实现的访问通信接口。

– [SR-18]建议对ECU中的调试接口进行配置，以防止未经授权的实体。该要求涵盖了车辆计算节点本地调试接口以及基于IVN访问这种网络节点的远程调试接口。

表4展示了第7条中的已识别威胁与第8条中的安全性要求之间的对照关系。

表 4 – 安全性要求和威胁对照

威胁	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
未经授权暴露以太网通信消息	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
未经授权暴露加密资料	Y	Y	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	Y
操纵配置数据	Y	Y	–	–	–	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	Y
操纵日志数据	Y	Y	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y
操纵加密资料	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
基于以太网的IVN上的DoS攻击	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–
伪装ECU	–	Y	–	–	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y

每种已识别的威胁都可以通过满足标有Y的相应的安全性要求来解决。例如，第一种威胁（未经授权暴露以太网通信消息）的安全性要求是[SR-2]、[SR-3]和[SR-18]。

9 实施基于以太网的安全车载网络

9.1 提前考虑与实施相关的事项

本建议书提供了与实施相关的考虑因素，以便：

- 概述受技术限制因素驱动的安全问题；
- 说明典型的IVN技术架构中特定于实施的安全问题。

这种安全信息的价值本质上只与特定的技术观点紧密相关，因此未来可能会过时，例如，如果IVN技术系统架构发生变化。

然而，目前还没有任何对IVN适用的、可以用作特定于实施的安全问题讨论基线的非技术性参考模型和参考架构。因此，本建议书通过研究IVN技术系统示例（如第6条所述），至少提供了一些安全考虑。

9.2 汽车以太网相关的安全网关功能

监视和控制不同逻辑网络域（例如，VLAN、IPv4子网、IPv6前缀定义的子网；每个逻辑网络域通过其安全属性代表一个特定的安全域）之间的通信流对于尽可能地降低基于以太网的IVN中来自未经授权的访问和DoS攻击的风险是很重要的。使用具体的防火墙或一般的安全网关在IVN或在车载网络和外部网络的结合处根据预定规则允许或拒绝通信数据，以提高车辆安全级别。

如根据当前典型的车载E/E技术架构所知，建议使用以下技术组件来监控来自车辆或IVN外部的通信消息，以实现此类安全网关功能（如防火墙）。

– 以太网交换机。

注 1 – 逻辑以太网交换机组件代表网络节点类型，而不是端节点。有两种IVN实施选项。以太网交换机作为独立技术组件，或作为前端或端节点单片集成到车辆计算节点中。

– 车辆边界网关。

注 2 – 本地选择，因为该技术组件代表常规V2X通信流量的单一观察点。

– ECU：当ECU能够直接进行外部通信时。

注 3 – 车辆计算节点可以为车辆直接外部通信提供额外的通信接口（即，绕过车辆边界网关），例如用于诊断目的。

防火墙使用多种机制进行包过滤，包括静态包过滤，无状态或有状态包检测，浅度、中度甚至深度包检测。

注 4 – 为了无歧义，隐喻术语“浅度”、“深度”等需要与下列内容进行映射和关联：a) 协议层；以及b) PDU上下文类型的信息（参见[b-ITU-T Y.2770][b-ITU-T Y.2771]等），例如，就互联网业务而言，“浅度包检测”通常是L3、4头部检测。

特别是，静态包过滤机制基于预定义的策略规则。因此，根据车辆E/E架构和所应用的通信协议，建议具体的策略规则设置。此外，防火墙策略默认应用于白名单方法，这基本上阻止了所有未明确允许的通信。

防火墙的一个主要特征是防御DoS攻击。防火墙可以通过使用预先存储的值（如计数器）或应用频率过滤器来设置阈值，从而保护网络免受DoS攻击。

防火墙的另一个补充特征是日志功能（即，作为被管理实体的防火墙网络元素根据[b-ITU-T M.3705]提供日志管理综合功能）。一般来说，与安全相关的事件应该是日志服务的对象。因此，当安全事件发生时，防火墙、IDS或安全网关一般会记录信息，这不仅有助于

取证专家分析事件情况，而且可以通过阻挡记录等研究来提高防火墙策略的准确性。因此，在存储日志时，有必要使用加密机制来确保完整性。

9.3 安全的VLAN配置

配置安全的VLAN对于IVN的通信安全以满足[SR-14]和[SR-17]非常重要。OEM应作为VLAN规范的负责机构，因为VLAN配置取决于OEM选择的车辆E/E架构。

每个VLAN都有一个唯一的值，被称为“VLAN标识符（ID）”。根据VLAN规范，VLAN ID（VID）可以使用0到4094，但是不应使用表5中描述的预定义VLAN ID。VLAN ID 1也可用于使用双标签的攻击，因此交换机应该将VLAN ID 1更改为另一个VLAN ID。

表5 – 保留的VLAN ID

VID值 （十六进制）	含义/用途
0	空VID表示标签头部仅包含优先级信息；帧中没有VID。该VID值不应配置为端口VLAN ID（PVID）或VID集的成员，也不应配置在任何转发数据库（FDB）条目中，或用于任何管理操作。
1	用于在通过网桥端口进入时对帧进行分类的默认PVID值。管理人员可以更改端口的PVID值。
FFF	保留供实施使用。该VID值不应配置为PVID或VID的成员，也不应在标签头部中传输。该VID值可用于表示管理操作或FDB条目中VID的通配符匹配。

攻击者可以通过“VLAN跳跃”攻击，从另一个VLAN进行未经授权的访问来监控以太网流量。为了化解这种攻击，应将没有标记VLAN的帧配置为丢弃。但是，可能存在以下例外情况。对于时间同步，通过精确时间协议发送消息，该协议要求根据[b-IEEE 802.1AS]在没有VLAN标签的情况下传输帧。

本地VLAN中的攻击者可以使用默认的本地VLAN ID执行双标签攻击。攻击者向帧添加两个标签：第一个包含默认的本地VLAN ID；第二个包含攻击者的目标VLAN ID。当添加了标签的帧通过第一台交换机时，第一个标签被删除，第二个标签被转发到下一台交换机。然后，该交换机使用剩余的第二个标签将帧转发至目标VLAN。这样，攻击者就可以将消息发送到目标VLAN。因此，应更改默认的本地VLAN ID，以防止这种攻击。

9.4 汽车环境下以太网交换机的安全性

IEEE以太网桥，通常也称为“以太网交换机”，固有地提供转发信息库（FIB），作为转发和交换过程的本地手段。这种FIB包括一份MAC地址表。

注 1 – 本建议书使用了非常抽象的以太网交换机模型，仅关注可能受到安全性影响的网络功能。[b-IEEE Std 802.1Q]全面概述了以太网交换机的所有基本功能。

注 2 – 例如，[b-IEEE 802.1Q]规定了以太网MAC帧处理模型的（策略）规则，分为进入、转发和外出规则。比如，在VLAN情况下，这特别令人感兴趣。

典型的以太网交换机为要求灵活性的网络提供动态地址学习机制。当新的ECU连接到交换机端口时，以太网端节点的MAC地址条目被自动添加到MAC地址表中，以便它可以通过该交换机级与整个以太网络域中的其他ECU通信。

注 3 – 在端到端通信路径中可能有不止一台以太网交换机。

动态MAC地址学习功能有助于对网络进行未经授权的访问，因此应该被禁用。如果出于维护或诊断目的需要外部诊断设备，则可能需要此功能。在这种情况下，交换机应该支持限制动态获取的MAC地址的有效时间的能力。这两个建议显然是相互矛盾的，但它们实际上取决于车载以太网络的具体操作环境：有没有外部连接可以连接到，例如，DoIP以太网络域。这种网络操作环境依赖性可产生有条件的安全性建议，例如，在这里是启用了动态地址学习的有限的、受限的时间窗口等。

MAC地址欺骗是一种众所周知的计算机网络攻击方法，可以在车辆攻击场景中实施。为了保护IVN，如果使用了访问变体，则应保证使用基于端口的网络访问控制的连接设备具有身份验证和可靠性。这种控制会在授权访问网络之前对组件进行身份验证。仅当验证成功后，以太网交换机才与网络通信。

为了化解DoS攻击，交换机应防止广播风暴，并支持基于端口的数据包接收速率限制（参见[b-ITU-T Y.1222]中的以太网流量参数控制）。

为了交换机的安全性，应确保交换机配置管理数据的完整性，并且应只有通过用于更新的安全编程机制或安全管理协议才可能更新。

– 通常，在集成了自己的处理器的汽车应用中，操作和管理以太网交换机所需的安全功能如下：安全存储器

  安全存储器确保存储数据的机密性和完整性。密钥和MAC等数据应使用HSM等安全存储器进行保护。

– 安全启动

  安全启动在每个启动周期检查软件的完整性。初始启动时会生成软件映像的消息验证码并存储在安全存储器中。在下一次启动时，如果新生成的消息验证码与存储的消息验证码相同，则保障了软件的完整性。

– 安全的调试接口

  安全的调试接口防止未经授权访问调试接口。通常建议移除调试接口，这样任何调试实体都无法连接。然而，如果接口对于产品保证或维护是必要的，则应只允许经授权的实体访问。

– 安全的软件更新

  只有在软件的真实性得到保证的情况下，安全的软件更新才允许软件重新编程。软件供应商使用它们的私钥生成数字签名，并将数字签名和软件映像一起发送。当接收方使用供应商的公钥验证数字签名是由供应商生成的时，软件的真实性得到了保证。

附录I

通信端点位于AUTOSAR或非AUTOSAR计算节点中的基于以太网的部分车载网络协议的描述

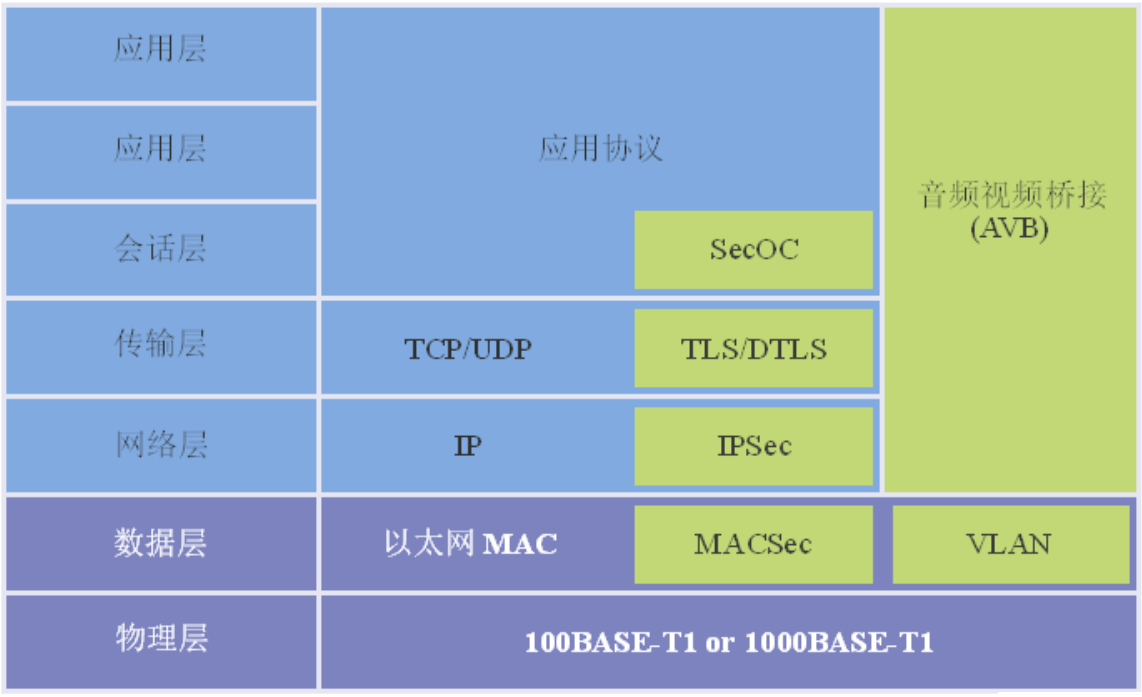
（此附录非本建议书不可分割的组成部分。）

基于以太网的网络存在许多通信协议，基于以太网的车载通信中使用的许多用例皆采用了其中的一种或多种。此外，IVN中的计算节点不仅可以通过基于AUTOSAR的软件架构系统（如AUTOSAR经典平台、AUTOSAR自适应平台）运行，还可以使用非基于AUTOSAR软件的通信架构。

因此，在以太网和互联网IVN工程的背景下，基本假设IVN由AUTOSAR和非AUTOSAR计算节点共同组成。

I.1 概述和范围

本附录简要说明了旨在用于基于以太网的车载通信的各项协议，如图I.1所示。



图I.1 – 以太网上基于互联网协议的和无互联网协议的通信业务，以及针对车载网络的特定层的相关安全协议

请注意，图I.1侧重于通信传输业务，而非会话和应用层协议。例如，基于AUTOSAR的可扩展的面向服务的IP中间件便不在本建议书的范围之内，它是一种会话和表示层协议，针对基于IP的、面向服务的通信业务。

I.2 AUTOSAR安全车载通信包括较低协议层安全协议

回想一下，AUTOSAR决定了其为软件架构，因而不包括部署架构。因此，对于后续如何将软件系统映射到处理器组件上（使用并发、并行、将AUTOSAR定义的通信栈替换为现成的商用栈等），有很多选择。

自AUTOSAR经典的4.0版本[b-Autosar 654]以来，以太网便一直是AUTOSAR标准的一部分。在AUTOSAR架构中，以太网通信栈与CAN、LIN和FLEXRay栈实例是并行的（在软件架构中）。

AUTOSAR PDU路由器负责AUTOSAR应用和通信端点相关网络接口之间的AUTOSAR PDU的计算节点内部路由。

注1 – 因此，AUTOSAR PDU路由器功能是重叠的，但不应与非AUTOSAR通信端点中已有的流量路由功能相混淆。

应用生成的报文被发送至PDU路由器，该路由器将报文发送至相应的接口或传输协议（TP）模块。每个接口/TP通过相关驱动将报文传输至网络接口。在以太网的情况下，PDU路由器向套接字适配模块（即基于TCP或UDP通信的第4层服务接入点）发送报文，并通过TCP/IP模块将报文传输至以太网接口。图I.2显示了AUTOSAR扩展通信栈中的控制和数据流。

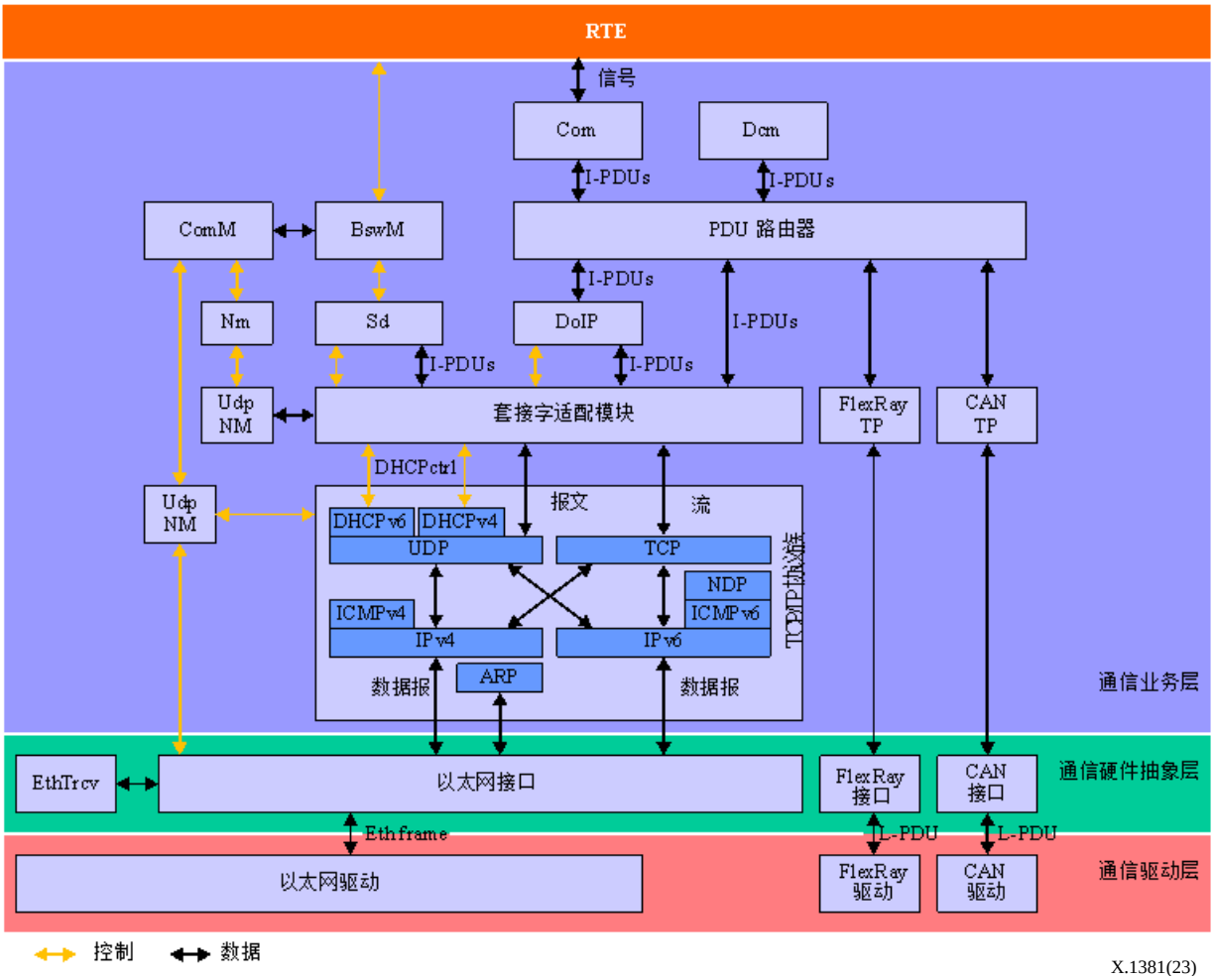


图 I.2 – AUTOSAR扩展通信栈（仅软件架构）（资料来源：[b-AUTOSAR 617]）

注 2 – AUTOSAR引入的PDU标记不同于ICT中使用的传统PDU语义（如[b-ITU-T X.200]中的规定）。AUTOSAR软件系统内部的I-PDU、N-PDU或L-PDU被映射为或在所使用的网络通信接口上表现为第x层PDU，通常记作（Lx）-PDU，具体取决于使用的特定协议栈。

I.2.1 安全车载通信

AUTOSAR的加密服务由加密业务层、安全硬件抽象层和加密驱动层提供，统称为加密栈。加密驱动层依赖于微控制器，提供可以访问硬件的接口。安全硬件抽象层提供了一个通

用接口，作为加密业务层和安全硬件层之间的中间件。通用接口在依赖于安全硬件的加密驱动层和作为上层业务的加密业务层之间提供了独立性。加密业务管理器（CSM）是加密业务层中包含的唯一模块。

安全车载通信（SecOC）是CSM的一项服务，提供了通信报文的完整性。

SecOC的目标是为PDU的软件层（或协议层）提供实用且高效利用资源的认证机制。由于应该最大限度地减少对现有系统的资源消耗，此类认证机制使用基于对称加密算法的报文认证码。

SecOC使用CSM生成验证报文认证码。CSM可以使用HSM加快对报文认证码的计算。

图I.3简要说明了SecOC的功能。

发送方通过向PDU添加包含报文认证码和新鲜度值的认证标签来生成安全PDU。新鲜度值可以为计数器值或时间戳。

接收方对接收到的安全PDU中的认证标签进行验证，即接收方根据接收到的安全PDU的数据生成报文认证码，并将其与接收到的报文认证码加以比对。

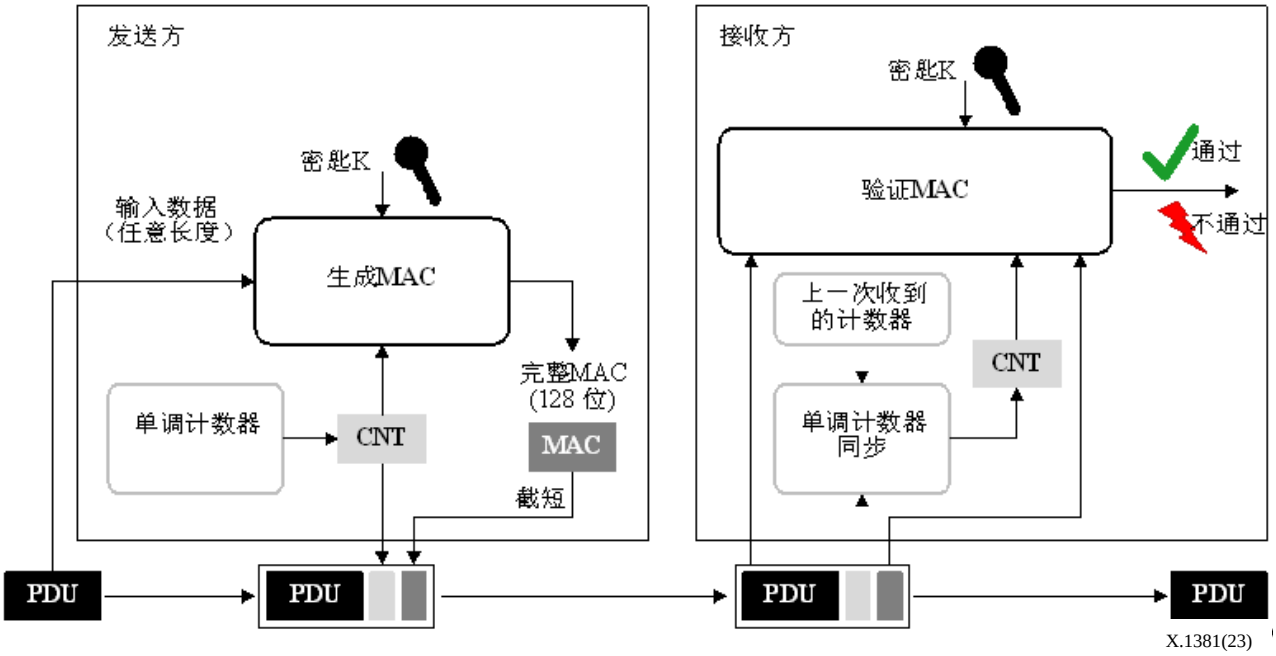


图 I.3 – 报文认证和新鲜度验证 [b-Autosar 654]

I.2.2 传输层安全

TLS通过可靠的TP（如TCP）提供端到端的安全通信业务。

AUTOSAR不支持低于TLS 1.2的TLS版本。

注 – 亦请见关于弃用TLS 1.0和TLS 1.1的[b-IETF RFC 8996]。

为在AUTOSAR中使用TLS，加密业务管理器允许执行TLS和IPsec子模块使用的加密作业和密钥操作。详细的要求和规范可查阅[b-AUTOSAR 617]。

I.2.3 数据报传输层安全

该议题供本建议书后续版本进一步研究。

I.2.4 互联网协议安全

IPsec基本上是IP网络的原生网络层安全协议，支持认证和加密。IPsec对于IPv4是可选的，但对于IPv6则是必需的。由于完全彻底的端到端IP连接有限（例如，由于IP拓扑隐藏网关或IP安全网关引起的中断），在ICT中部署IPsec（如有的话）通常仅限于小区域IP网络，但不能用于较大区域的IP网络。

但是，车载IP网络的类别属于（非常）小区域的网络，且受制于单一网络管理权限，这不应阻止仅限于车内IP网络域的IPsec的使用。

根据[b-AUTOSAR 617]，IPsec的隧道模式目前在AUTOSAR中不可用。只能使用传输模式。亦不支持IPv6和多播。详细的要求和规范可查阅[b-AUTOSAR 617]。

注 – 本建议书的此版本并未就IPsec协议提供针对特定IP版本的安全考量。

I.3 基于互联网协议的诊断通信

DoIP用于诊断目的，并无任何内嵌的安全措施。

DoIP是[b-ISO 13400-2]规定的基于IP的TP。DoIP可以通过以太网在车内UDS和外部测试设备之间传输报文。DoIP依赖于以下协议：

– DHCP；

– ICMP；

– 基于IP地址的MAC地址搜索（IPv4：ARP，IPv6：邻居发现协议）。

在UDP中，每个数据报仅包含一条DoIP报文。对基于TCP的数据，报头将数据流内各条单独的DoIP报文加以区分。

IANA注册的周知TCP端口13400应该用于从外部诊断设备到车载ECU的DoIP通信（诊断请求和诊断响应）。

DoIP不考虑任何通信安全机制。不以任何方式对报文进行认证或加密。因此，安全架构师在设计DoIP时，应考虑使用不同层的安全协议。

I.4 媒体访问控制安全

MACsec是[b-IEEE 802.1AE]标准安全协议，为数据链路层上的所有流量提供安全通信。MACsec支持以太网末端节点或交换节点间、以太网二层连接上的端到端安全或逐跳安全。MACsec包括认证和加密或解密，可识别和防范大多数的安全威胁，包括DoS攻击、入侵、中间人攻击、伪装攻击、被动搭线窃听和回放攻击。

附录II

具有以太网、IP或互联网连接的车载网关

（此附录非本建议书不可分割的组成部分）

II.1 动机

CGW、车载边界网关或VG常在车载通信安全架构中发挥关键作用，对于以太网和IP网络域及通信业务而言尤其如此。作为车载边界网关的CGW的网络拓扑位置说明并决定了其在车辆内部和外部网络域之间发挥着安全网关的作用。

此类网元类型的规范和标准化往往涉及明确的安全考量乃至安全指南和规范。

II.2 本附录的目的

本附录提供了安全相关的VG标准的不完全清单，这可能是有益的，因为它补充了本建议书范围内的通信安全信息。本建议书的后续版本可能会对本附录加以更新。

II.3 精选的带有安全信息的车载网关建议书

本条款列举了与安全相关的建议书，但并未对其特定的安全建议进行任何评估。

– [b-ITU-T F.749.1]：包括安全功能要求；

– [b-ITU-T F.749.2]：提供有关通信安全要求和高层安全要求的专门条款；

– [b-ITU-T H.550]：安全内容主要与VG的安全管理相关；

– [b-ITU-T H.560]：安全内容主要与用于外部通信的VG的通信接口相关。

附录III

车载智能交通系统安全

（此附录非本建议书不可分割的组成部分）

III.1 背景

ITS的概念包括车载通信架构，此架构涵盖了车辆内部通信系统以及与车辆外部通信系统和服务的互连。整个架构中最关键的网络和通信元素是位于车辆内部的ITS站，例如，请见[b-ETSI EN 302 665] [b-ETSI TR 101 607]。

ITS站代表着车载通信网络，它可能基于以太网，提供无IP或基于IP的通信业务。这样的ITS技术解决方案与本建议书的范围相匹配。

III.2 ITS车载网络

ITS规定的IVN架构由本建议书正文所述的相同网元组成：车载ITS网关；车载ITS主机；车载ITS路由器；车载ITS边界路由器或网关等。因此，ITS安全指南在很大程度上亦适用于本建议书，特别是当通信技术（即协议和协议栈）和通信架构相同时。

III.3 ITS安全

本建议书的目的并非评估ITS定义的安全。然而，ITS下开展的威胁、漏洞和风险分析、ITS安全指南、安全业务或安全架构可能是有益的补充阅读材料，在涉及通信安全的情况下尤其如此。更多信息和进一步的安全参引，请见[b-ETSI TS 102 731]。

参考文献

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

[b-ITU-T F.749.2] Recommendation ITU-T F.749.2 (2017), *Service requirements for vehicle gateways*.

[b-ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020), *Common equipment management function requirements*.

[b-ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.

[b-ITU-T H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

[b-ITU-T H.560] Recommendation ITU-T H.560 (2017), *Communications interface between external applications and a vehicle gateway platform*.

[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

[b-ITU-T M.3702] Recommendation ITU-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirement and analysis*.

[b-ITU-T M.3703] Recommendation ITU-T M.3703 (2010), *Common management services – Alarm management – Protocol neutral requirement and analysis*.

[b-ITU-T M.3705] Recommendation ITU-T M.3705 (2013), *Common management services – Log management – Protocol neutral requirements and analysis*.

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open systems interconnection – Basic reference model: The basic model*.

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework*.

[b-ITU-T X.703] Recommendation ITU-T X.703 (1997), *Information technology – Open distributed management architecture*.

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

[b-ITU-T X.1039] Recommendation ITU-T X.1039 (2016), *Technical security measures for implementation of ITU-T X.805 security dimensions*.

[b-ITU-T Y.1222] Recommendation ITU-T Y.1222 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[b-ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection*.

[b-Autosar 617] AUTOSAR 617 (2021), *Specification of TCP/IP stack*, AUTOSAR CP R21-11.

[b-Autosar 654] AUTOSAR 654 (2017), *Specification of secure onboard communication*, AUTOSAR CP Release 4.3.1.

[b-Autosar 970] AUTOSAR 970 (2019), *Requirements on IPsec Protocol*, AUTOSAR FO R19-11.

[b-ETSI EN 302 665] European Standard ETSI EN 302 665 V1.1.1 (2010), *Intelligent transport systems (ITS); Communications architecture*.

[b-ETSI TR 101 607] Technical Report ETSI TR 101 607 V1.2.1 (2020), *Intelligent transport systems (ITS); Cooperative ITS (C-ITS); Release 1*.

[b-ETSI TS 102 731] Technical Specification ETSI TS 102 731 V1.1.1 (2010), *Intelligent transport systems (ITS); Security; Security services and architecture*.

[b-IEEE 802.1] IEEE 802.1 (Internet). *Welcome to the IEEE 802.1 Working Group*. Available [viewed 2022-06-30]: https://1.ieee802.org/

[b-IEEE 802.1AE] IEEE 802.1AE-2018, *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) security*.

[b-IEEE 802.1AS] IEEE 802.1AS (Internet), *Standard for Local and metropolitan area networks – Timing and synchronization for time-sensitive applications in bridged local area networks.* Available [viewed 2022-06-30]: https://www.ieee802.org/1/pages/802.1as.html

[b-IEEE 802.1CB] IEEE 802.1CB-2017, *IEEE Standard for local and metropolitan area networks – Frame replication and elimination for reliability*.

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area network – Bridges and bridged networks*.

[b-IEEE 802.1Qat] IEEE 802.1Qat (Internet), *Standard for Local and metropolitan area networks – Virtual bridged local area networks - Amendment 9: Stream reservation protocol (SRP).* Available [viewed 2022-06-30]: https://www.ieee802.org/1/pages/802.1at.html

[b-IEEE 802.1Qav] IEEE 802.1Qav-2009, *IEEE Standard for Local and metropolitan area networks – Virtual bridged local area networks amendment 12: Forwarding and queuing enhancements for time-sensitive streams*.

[b-IEEE 1722-2016] IEEE 1722-2016, *Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks*.

[b-IETF RFC 2827] IETF RFC 2827 (1997), *Network ingress filtering: Defeating IP source address spoofing denial of service attacks*.

[b-IETF RFC 4953] IETF RFC 4953 (2007), *Defending TCP against spoofing attacks*.

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modeling language for the network configuration protocol (NETCONF)*.

[b-IETF RFC 6575] IETF RFC 6575 (2012), *Address resolution protocol (ARP) mediation for IP interworking of layer 2 VPNs*.

[b-IETF RFC 6959] IETF RFC 6959 (2013), *Source address validation improvement (SAVI) threat scope*.

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1*.

[b-ISO 13400-2] International Standard ISO 13400-2:2019, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Transport protocol and network layer services*.

[b-ISO 14229-5] International Standard ISO 14229-5:2022, *Road vehicles – Unified diagnostic services (UDS) – Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP)*.

[b-ISO/SAE 21434] International Standard ISO/SAE 21434:2021, *Road vehicles – Cybersecurity engineering*.

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
2023年，日内瓦