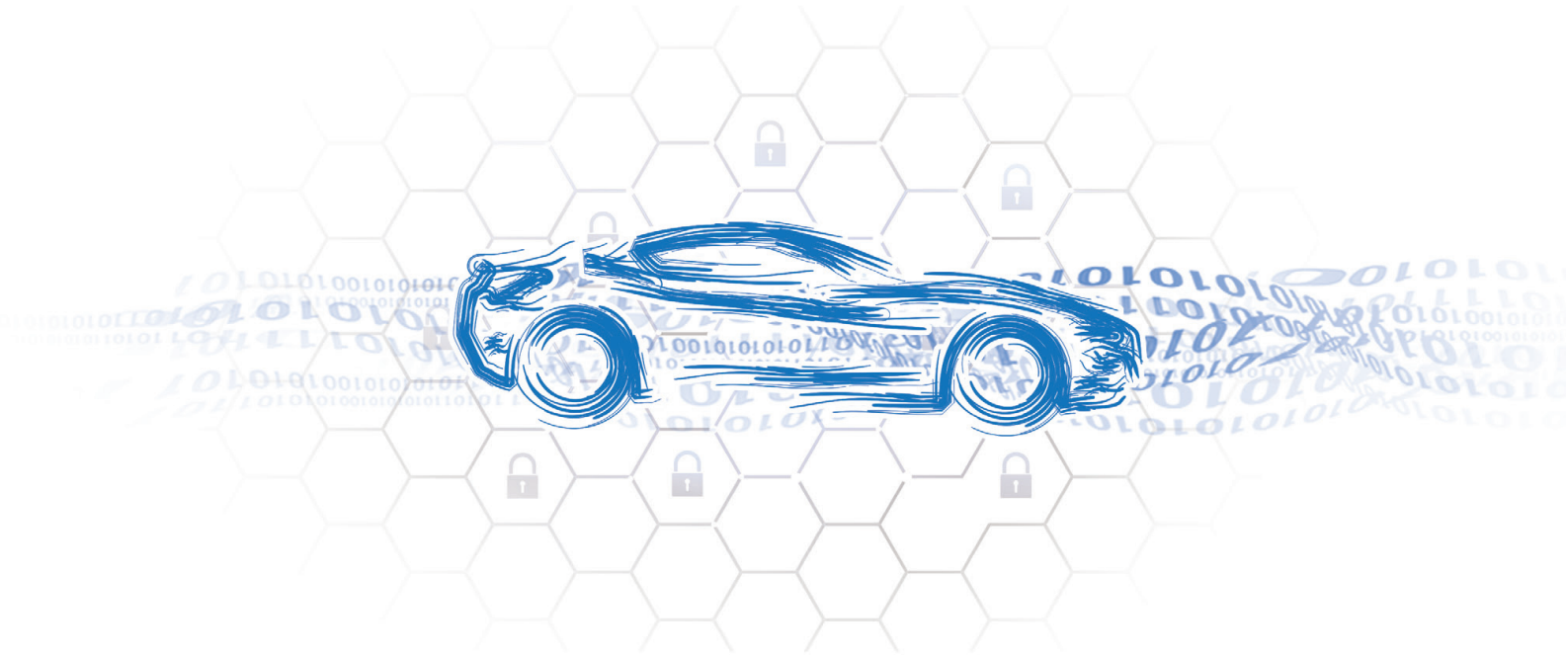
汽车电子网络安全标准化白皮书

（2018）



全国信息安全标准化技术委员会
信息安全评估标准工作组

2018年4月

汽车电子网络安全标准化白皮书

（2018）

全国信息安全标准化技术委员会
信 息 安 全 评 估 标 准 工 作 组

2018年4月

前言

随着信息技术、互联网与汽车产业的不断融合，汽车网络互联和智能化已成为汽车产业发展的必然趋势。汽车智能网联化使传统汽车技术延伸到新型传感、大数据、人工智能等新领域，实现了车内、车与人、车与车、车与路、车与服务平台等的全方位网络连接，提升汽车智能化水平，提高交通效率，改善汽车驾乘感受，构建汽车服务全新业态，未来将打通整个社会的智能交通生态系统，促进汽车产业、智能交通产业的深度融合与大发展。据Gartner预测，到2020年，我国联网汽车用户规模将突破5000万，届时90%的汽车将具备互联网接入功能，联网汽车将成为智能交通生态系统中的关键要素。

据统计，现代汽车中汽车电子系统的成本最高已占到整车成本的70%，可见汽车电子系统是汽车的核心构成，汽车联网其本质是汽车电子系统的联网。然而，以信息篡改、病毒入侵、恶意代码植入等手段对联网汽车进行网络攻击而引发的汽车网络安全问题也愈发严峻，在国际范围内引发极大关注。

习总书记曾在“4.19讲话”中表示“安全是发展的前提，发展是安全的保障，安全和发展要同步推进”。值此车联网产业发展的关键时期，本白皮书从汽车电子网络安全的视角阐述相关政策、法规、标准、产品、应用方面的最新进展和发展态势，归纳总结国内外汽车电子网络安全技术与标准的发展现状，探讨我国汽车电子网络安全面临的挑战和发展方向，希望与业内同仁共享成果，以期共同推动汽车电子乃至车联网网络安全标准化事业发展。

编写单位（排名不分先后）

中国电子技术标准化研究院
电子科技大学
中国汽车技术研究中心
东软集团股份有限公司
北京奇虎360科技有限公司
上海银基信息安全技术股份有限公司
中国汽车工程学会
北京航空航天大学
武汉大学
浙江吉利汽车研究院有限公司
北京新能源汽车股份有限公司
重庆长安汽车股份有限公司
国家信息技术安全研究中心
腾讯安全科恩实验室
广东为辰信息科技有限公司
惠州华阳通用电子有限公司
威马汽车技术有限公司
公安部第三研究所
全国汽车标准化技术委员会
全国智能运输系统标准化技术委员会
车载信息服务产业应用联盟
烽台科技（北京）有限公司
上海巍擎信息技术有限责任公司
北京工业大学

编写人员（排名不分先后）

杨建军　刘贤刚　范科峰　龚洁中　罗　蕾　王　兆　陈丽蓉
刘健皓　李京春　仇兆峰　刘经南（院士）　秦洪懋　刘建行
孙　航　王　建　董　威　陈静相　路　娜　何　文　汪向阳
雷　霆　郭　迟　崔竞松　刘金硕　王丽娜　唐　迪　王琪琳
李　允　罗建超　赵焕宇　姚相振　李　琳　周睿康　王秉政
朱新新　聂　森　张　屹　张颖奇　赵兴华　张军响　苗澎锋
庞春霖　龚亮华　魏钦志　陈家林　彭智俊　杨　震

目录 *CONTENTS*

第一章　导论…… 1

1.1 汽车电子的基本概念 …… 1

1.2 汽车电子的重要作用 …… 3

1.3 汽车的网络安全形势 …… 4

1.4 相关法律政策新要求 …… 6

1.5 汽车电子网络安全标准化工作的意义 …… 6

第二章　汽车电子网络安全政策和标准…… 9

2.1 网络安全法律政策 …… 9

2.1.1 国外情况 …… 9

2.1.2 国内情况 …… 11

2.2 国内外标准化情况 …… 14

ISO/TC22 …… 14

SAE…… 16

ITU–T…… 18

UN/WP.29 …… 20

ETSI ITS…… 21

TC114…… 22

TC260…… 24

TC268…… 26

CCSA …… 27

TIAA …… 28

CAICV…… 29

目录 *CONTENTS*

第三章　汽车电子网络安全技术研究 …… 31

3.1 威胁分析与风险评估技术研究 …… 31

3.1.1 威胁分析与风险评估过程 …… 31

3.1.2 安全风险归纳 …… 38

3.2 汽车电子系统网络安全生命周期研究 …… 39

3.3 汽车电子网络安全参考架构研究 …… 44

第四章　汽车电子网络安全标准化工作 …… 47

4.1 汽车电子网络安全标准体系 …… 47

4.2 下一步工作考虑 …… 50

缩略语 …… 54

参考文献 …… 57

附录A 汽车电子网络安全行业应用实践 …… 59

附录A1　EVITA：安全车辆入侵保护应用 …… 59

附录A2　PRESERVE：V2X安全通信系统 …… 64

附录A3　现代汽车网络安全最佳实践 …… 68

附录A4　日本汽车信息安全模型 …… 73

附录A5　AUTOSAR …… 74

附录B 汽车电子网络安全技术应用案例 …… 78

附录B1　T–BOX安全技术应用 …… 78

附录B2 车载信息娱乐系统安全技术应用 …… 80

附录B3 数字钥匙系统安全技术应用 …… 82

附录B4 车云网络通信安全PKI技术应用 …… 85

附录B5 车载系统FOTA安全技术应用 …… 87

第一章　导论

当前我国汽车工业已步入持续快速发展时期，2017年我国全年汽车销量2887.89万辆，连续九年居全球第一，并超过第二名的美国1164万辆。与此同时信息技术的迅猛发展和广泛应用，也促使智能网联汽车和车联网等新产品、新应用集中涌现，不断推动我国汽车产业向数字化、信息化、网络化、智能化方向快速发展。

经过数十年技术演进，目前发动机控制、底盘控制、车身电子控制等传统汽车电子控制技术已极为成熟，车辆信息服务系统、定位导航系统、电子娱乐系统等车载电子装置网络化、智能化发展不断深入，汽车电子的内涵和外延得到了不断扩展丰富。预测显示到2020年每辆汽车上各类电子装置将超过200个，在实现各类电子装置实时可靠传输数据、提供信息化服务的同时，汽车电子网络安全防护的理念、方法、技术、政策、标准等也必须跟上需求发展的步伐。如何建立更为安全可靠的汽车电子系统架构，满足开放式网络互联环境下的安全需求，部署有效措施防范安全风险，并形成切实可落地的标准，这一系列难点问题都值得我们加紧研究、持续关注。

1.1 汽车电子的基本概念

汽车电子（Automotive Electronics）是车体控制电子装置和车载服务电子装置的总称。其中前者和车上机械系统进行配合使用，包括发动机控制系统、底盘控制系统、车身电子控制系统等。后者则是在汽车环境下能够独立使用的电子装置，它和汽车本身的性能并无直接关系，主要包括车载信息娱乐系统及个人设备交互信息系统等。

汽车电子技术是伴随着汽车产品智能化、电动化、网联化及共享化的需求变化逐步完善起来的，同时不断与电子电气架构、车载网络、域控制及信息安全等技术相互融合促进，目前主要技术发展趋势表现在模块化、集中化、智能化和网络化四个方面。

（1）**模块化**主要是实现功能、软件、硬件或产品内部解耦，如AUTOSAR软件分层思想可实现应用层与底层软件的解耦，可更好的提升跨团队协作水平及跨产品或平台利用率，更快的响应市场需求。

（2）**集中化**是为了降低控制器数量及成本，通过提升计算及存储能力，将局部或全局功能更多的集中到一个控制器中，如域控制器技术将制动防抱死控制系统(ABS)、牵引力控制系统(TCS)和驱动防滑控制系统(ASR)综合在一起进行制动控制等。 根据博世电子电气架构路线发展规划定义，未来车辆将把部分本地计算转移到云端进行，本地和云端的作用将分别类比人的小脑和大脑。

（3）**智能化**是指车辆由开环控制向闭环控制转变，预先通过经验或智能算法将最佳（修正）运行数据输入车辆，并对车辆运行状态进行实时监控，使车辆自动调整到稳定状态。车辆ADAS系统如稳定性控制系统(VSC)、自适应巡航控制系统(ACC)，以及正在研发的无人驾驶系统，均属于汽车电子智能化发展过程中不同阶段的产物。

（4）**网络化**过去是指通过总线技术将车内众多的控制单元联结起来，实现信息共享，减少线束，提高可维护性。主流内网协议有LIN、CAN、MOST、FlexRay、Ethernet等，依据总线特性不同，分别应用于动力域、车身域、多媒体域和线控系统等。当前的网络化是指车载网络与移动互联网及后台的远程连接，实现了汽车电子单元资产由线下向线上的转移，但同时也增加内部资产在外网的暴露程度及车辆安全风险，能否有效解决网络安全问题已经成为影响汽车电子新产品、新技术落地推广的关键。

1.2 汽车电子的重要作用

近年来，汽车工业与电子技术深度融合，不断助推汽车产业转型升级，现代汽车的安全性、节能环保性和舒适性得到显著提升，主要表现在以下几个方面：

一是重视安全、环保和节能。汽车电子的应用是解决安全、环保、节能的主要技术手段，例如在节能方面，汽车厂商开始研究和应用电子模块控制的混合动力轿车、纯电动轿车等。

二是传感器性能不断提高、数量不断增加。传感器种类、数量不断增加，精度更高、可靠性更强、成本更低，特别在智能化方面发展迅速。

三是车用微处理器换代升级。随着汽车电子占整车比重不断提高，微控制单元（MCU）在汽车领域的应用将超过家电和通讯领域的使用数量，成为MCU最大应用领域。

四是数据总线技术应用日益普及。汽车内部网络的构成主要依靠总线传输技术，大量数据的快速交换、高可靠性及廉价性是对汽车电子网络系统的基本要求。

五是智能汽车及智能交通系统（ITS）广泛应用。以卫星通信、移动通信、计算机技术为依托进行车载电子产品的开发和应用，实现计算机、通讯和消费类电子产品“3C”整合。

六是车用嵌入式软件和硬件平台逐步替代传统设计开发模式。汽车电子产品的研发周期正在缩短，一般汽车发动机的更新周期为7年，而电子产品的更新周期通常在1至3年。

七是新技术在汽车电子产品中的深入应用。光纤在汽车信号传输中的应用，新的控制理论和方法的大量应用，蓝牙技术、基于无线射频等识别技术的应用等都是汽车电子技术的发展趋势。

多方预计全球汽车产业2020年开始迈入智能汽车时代，目前国内外普遍认为，先进驾驶辅助技术（ADAS）有望在2020年大规模应用推广，自

动驾驶技术也将在此之前示范运行，并有望在2025年进入市场推广阶段，相信快速发展的汽车电子技术将在产业转型升级中扮演越来越重要的角色。

1.3 汽车的网络安全形势

长期以来，汽车一直注重系统功能安全的可靠性，并在不断增强车辆主被动安全能力，并且有ISO26262标准为整车厂和零部件厂商提供功能安全开发的指导，而网络安全问题是随着汽车智能化的发展才逐渐被人们所关注，是新形势下的新问题。

现代汽车智能化的过程，是汽车产品由机械化向电子化及网联化转变的过程。汽车电子化完成了机械控制向硬线控制的转变，网联化实现了内网高价值资源与外部互联网连接，电子化和网联化共同支撑了当前汽车智能化进程，其推进速度快于网络安全防护理念、方法、技术、政策、标准的发展，现阶段汽车正面临巨大的网络安全风险，对功能安全的影响不断加剧。近年来，产、学、研各方力量极为关注汽车网络安全，面向智能网联汽车产品、云端主机和服务开展了大量安全研究工作。

表1-1 部分汽车网络安全研究和事件

序号	时间	研究和事件描述
1	2013年	Charlie Miller & Chris Valasek通过OBD接口破解了丰田普锐斯；
2	2014年	360公司破解了Tesla汽车远程控制功能；
3	2015年	宝马汽车ConnectedDrive功能存在漏洞，需要进行大规模的远程修复；
4	2015年	Samy Kamkar破解了通用安吉星OnStar系统；
5	2015年	360公司破解了比亚迪汽车云服务、遥控驾驶功能；
6	2015年	360公司破解了Tesla汽车毫米波雷达系统；

序号	时间	研究和事件描述
7	2015年	Charlie Miller & Chris Valasek远程破解了JEEP汽车，导致其召回140万辆汽车；
8	2016年	日产LEAF汽车API遭泄露，黑客可远程控制；
9	2016年	Troy Hunt发现了日产聆风手机App存在漏洞，全球停止NissanConnect服务；
10	2016年	腾讯科恩实验室实现了远程无接触式破解Tesla，可以在驻车状态和行驶状态下远程控制；
11	2017年	腾讯科恩实验室再次实现了远程无接触式破解Tesla。

在汽车网络安全领域，以腾讯和360公司为代表的互联网公司凭借在传统IT网络安全技术上的优势，对以特斯拉为代表的智能网联汽车开展了大量研究，常用的渗透路径可归纳为：首先通过车内开放式的网络连接端口进入车载服务电子系统，进而采用传统分析方法找出应用服务中的安全漏洞，获取多个车载系统权限；其次采用技术手段绕过部分ECU的固件完整性检测机制，刷新相应固件来获得向CAN总线读写数据的能力，掌握车体控制电子系统的命脉；最终通过将伪造的数据包注入到CAN总线，实现在驻车模式或行驶模式下对汽车的远程无物理接触式控制。由此可见，当前针对汽车的网络攻击实质上大多是针对汽车电子所构成系统的网络攻击。

这些研究成果引起了汽车生产厂商的极大关注，部分已经对在售的多款车型构成了影响。同时也表明，针对汽车的网络攻击能够通过突破车内网络或汽车电子组件实现敏感数据获取、车辆远程控制（或部分功能）等，影响汽车的功能安全，对驾乘车人的生命安全构成了威胁。安全是一切技术成型的基本要求，同功能安全一样，网络安全需得到相应的重视。客观上来说，网络安全问题已经成为影响传统汽车全面向智能网联汽车发展过渡的关键。

1.4 相关法律政策新要求

2017年6月1日起《中华人民共和国网络安全法》正式实施，明确要求包括车厂、车联网运营商在内的网络运营者须“履行网络安全保护义务，接受政府和社会的监督，承担社会责任”；“应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”；“网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展”。

“中国制造2025”已经将汽车网络安全列为关键基础问题进行研究，希望通过产学研用管共同努力，推动车联网整体架构、关键共性技术、标准规范、核心产品形成全链条的安全防护体系，助力智能网联汽车与智能交通的深度融合发展。国家政策法规、顶层战略都对车联网安全管理提出了更为明确的要求，对提升车联网产业整体网络安全具有重要意义。

1.5 汽车电子网络安全标准化工作的意义

2017年12月27日，工业和信息化部、国家标准化管理委员会联合发布了《国家车联网产业标准体系建设指南（总体要求）（征求意见稿）》（以下简称《建设指南》），明确提出了到2020年基本建成国家车联网产业标准体系的目标。《建设指南》将标准体系分为智能网联汽车、智能交通、信息通信、车辆智能管理、电子产品与服务五个重点领域，为打造自主可控、安全可靠、开放协同的车联网产业提供标准化支撑。

《建设指南》作为车联网标准化工作的顶层文件，是未来汽车电子快速健康发展的重要基础，是规范车联网电子产品与服务、智能网联汽车、信息通信、智能交通、车辆智能管理发展的关键核心。

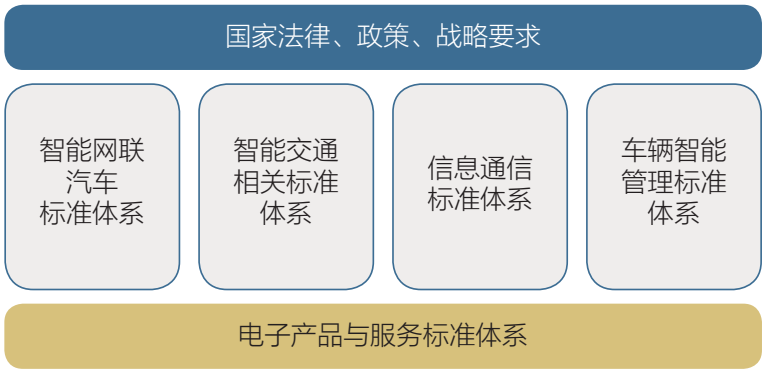


图1–1 车联网产业标准体系建设结构图

本白皮书所指的汽车电子范围不但包括电子产品与服务标准体系中所指向的车载服务电子装置，还包括车体控制电子装置，是包含基础元器件、软硬件设备、内部通信总线、车载操作系统及应用、外接终端设备等在内的广义电子概念，与五大重点领域标准体系均紧密相关，并且扮演着基础性功能落地实现的重要角色，是车联网产业发展不可缺失的底层支撑。

从全面保障车联网产业网络安全的角度来看，贯彻落实《建设指南》开展汽车电子网络安全标准化工作，是进一步夯实车联网产业健康发展的根基，是汽车行业切实落实《中华人民共和国网络安全法》的集中体现，对提升车联网产业网络安全防护水平，保障汽车电子网络安全具有重要意义。

第二章　汽车电子网络安全政策和标准

当前国内外在围绕汽车电子相关网络安全出台的法律政策方面，总体上呈现出一种以汽车联网、自动驾驶这些复杂应用场景为目标抓手，引导汽车产业链上各环节加强对网络安全保障投入的探索模式，国际标准化组织ISO和部分国家汽车行业组织及企业也均在积极研究并发布汽车网络安全相关政策、标准、指南等，为行业或企业提供可实施的规范。

2.1 网络安全法律政策

2.1.1 国外情况

（一）美国

美国2016年公布的《自动驾驶汽车政策》（《Preliminary Statement of Policy Concerning Automated Vehicles》）将高度自动驾驶汽车的安全部署任务分为四大部分：一是自动驾驶汽车性能指南；二是州政策模式；三是现行监管方式；四是监管新工具与权力。

2017年8月，美国交通部道路交通安全管理局（NHTSA）发布新版《联邦自动驾驶系统指南：安全愿景2.0》，要求汽车厂商采取措施应对网络威胁和网络漏洞，对车辆辅助系统进行网络安全评估。9月，美国众议院批准《自动驾驶法案（提案）》，赋予NHTSA专职负责自动驾驶网络安全的权力，要求其在法律出台的180天内制定自动驾驶网络安全细则。

（二）英国

英国要求汽车制造商承担起包括抵御网络攻击、对抗黑客在内的一系列网络安全责任。2017年8月，英国政府发布《智能网联汽车网络安全关

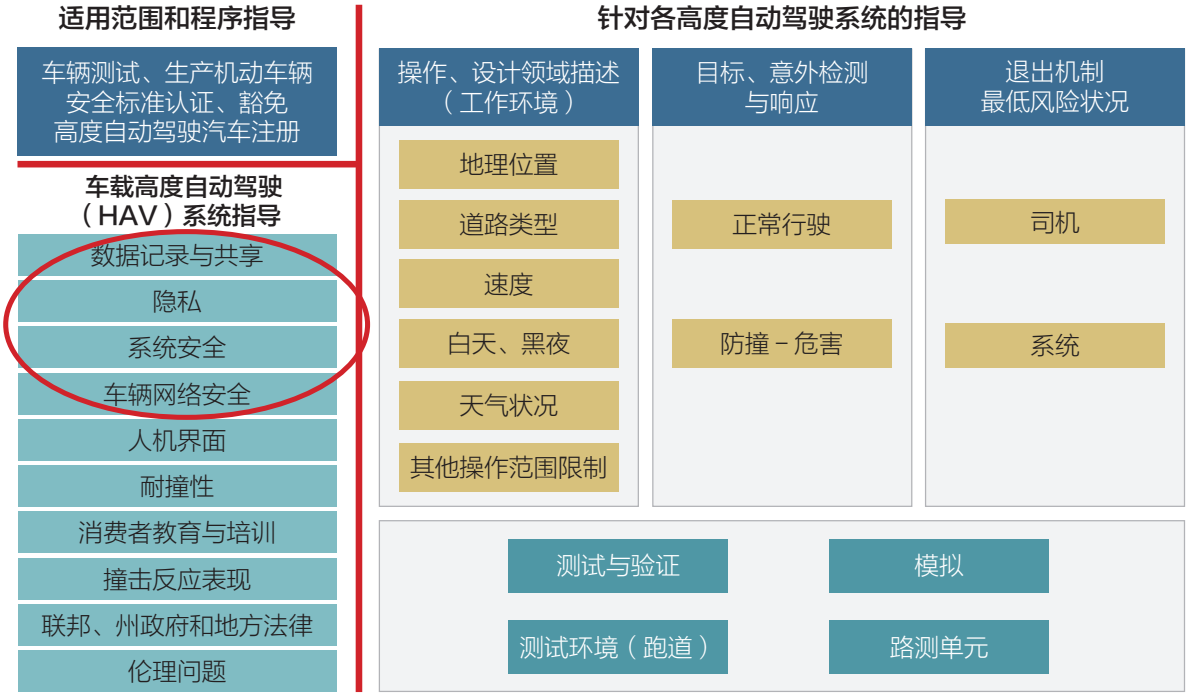


图2-1 自动驾驶车辆性能指导框架

键原则》（The Key Principles of Cyber Security for Connected and Automated Vehicles），提出8个大的方面关键原则，共29个细则。

1) 管理层推动：推进安全计划、方案安全设计等；

2) 安全风险管理与评估：风险评估与管理、风险识别、分类、优先排序、威胁处理等；

3) 产品售后服务与应急响应机制；

4) 整体安全性：安全分级管理、安全保证、安全可追溯可验证；

5) 系统设计：纵深防御与分段技术、边界防护、远程终端防护；

6) 软件安全管理：安全编码、配置管理、审计测试、代码共享；

7) 数据安全：存储安全、传输安全、个人数据管理、敏感数据；

8) 弹性设计：功能可用性保证、失效保护、功能恢复与响应。

其实质上将网络安全责任拓展到供应链上的每一个参与主体，包括第三方承包商，此外还要求将网络安全议题考虑在汽车全生命周期内，即便遭到网络攻击，也要保证车辆安全运行的基本功能。

（三）德国

德国作为传统汽车产业强国，对自动驾驶技术与产业发展持积极态度。2017年6月，德国通过颁布《道路交通法第八修正案》与《自动驾驶道德准则》成为自动驾驶领域立法的“先行者”。《道路交通法第八修正案》通过修订现有道路交通法案引入自动驾驶条款，旨在通过上位法的形式对自动驾驶的定义范围、驾驶人的责任与义务、驾驶数据的记录等进行原则性规定，为自动驾驶各方利益主体划定权利义务边界，提出政府监管的方向。作为德国首部自动驾驶相关法律，该法案为自动驾驶汽车在德国“上路”提供了法律依据，虽在主体责任划分、数据使用与信息安全等方面还有待修订完善，但在自动驾驶产业的立法进程中具有里程碑式意义。

《自动驾驶道德准则》作为全球第一个自动驾驶行业的道德准则，通过在道路安全与出行便利、个人保护与功利主义、人身权益与动物或财产权益、法律对技术的规制方式等方面确立优先原则，同时设立不允许自动驾驶厂商提前对极端情境的选择问题进行标准化设定或编程等准则，为自动驾驶所产生的道德和价值问题立下规矩。

2.1.2 国内情况

《中华人民共和国网络安全法》于2017年6月1日起正式实施，明确要求包括车联网运营商在内的网络运营者需履行网络安全保护义务。主要涉及以下方面要求：

- 应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行。
- 有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。
- 加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

为加快推动我国车联网发展，加强车联网产业的顶层设计，发挥技术标准的规范和促进作用，工业和信息化部、国家标准化管理委员会会同有关单位组织开展了《国家车联网产业标准体系建设指南》系列文件编制工作，内容包括总体要求、智能网联汽车、信息通信、电子产品和服务等部分。其中，《国家车联网产业标准体系建设指南（智能网联汽车）》部分已于2017年12月27日发布，《国家车联网产业标准体系建设指南（总体要求）》、《国家车联网产业标准体系建设指南（信息通信）》、《国家车联网产业标准体系建设指南（电子产品和服务）》三部分于2017年9月25日开始征集意见。

《国家车联网产业标准体系建设指南（总体要求）（征求意见稿）》提出了到2020年基本建成国家车联网产业标准体系的目标。该指南作为对车联网标准体系的顶层设计，分别给出了智能网联汽车标准体系、信息通信标准体系、电子产品与服务标准体系、智能交通相关标准体系、车辆智能管理标准体系的结构图，为车联网各个相关领域的标准体系建设提供了依据。

《国家车联网产业标准体系建设指南（智能网联汽车）》按照智能网联汽车的技术逻辑结构、产品物理结构相结合的构建方法，将标准体系框架定义为“基础”、“通用规范”、“产品与技术应用”、“相关标准”四个部分，并根据各具体标准在内容范围、技术等级上的共性和区别，对四部分做进一步细分，形成14个子类，规划提出99项领域标准项目，其中24项标准项目研究和制定工作已于近期启动。

在智能网联汽车标准体系的通用规范中，规划了信息安全类（编号204）的标准。在遵从信息安全通用要求的基础上，以保障车辆安全、稳定、可靠运行为核心，主要针对车辆及车载系统通信、数据、软硬件安全，从整车、系统、关键节点以及车辆与外界接口等方面提出风险评估、安全防护与测试评价要求，防范对车辆的攻击、侵入、干扰、破坏和非法使用以及意外事故。

图2-2 智能网联汽车标准体系框架

《国家车联网产业标准体系建设指南（信息通信）（征求意见稿）》的标准体系主要包括基础标准、通信协议和设备、业务与应用、网络与数据安全标准4大部分，其中网络与数据安全包括安全体系架构、通信安全、数据安全、网络安全防护、安全监控、应急管理等方面的标准。安全体系架构标准包括总体安全架构要求；通信安全标准包括车内通信、V2X通信安全要求、智能网关安全要求和测试方法等；数据安全标准包括数据安全及用户个人信息保护；网络安全防护标准包括信息服务平台安全防护与测评相关要求；安全监测标准包括车辆安全监测技术要求；应急管理标准包括车辆联网的应急管理要求。

《国家车联网产业标准体系建设指南（电子产品与服务）（征求意见稿）》的标准体系主要包括基础、汽车电子产品、网络设备、服务与平台、网络与信息安全等标准，标准体系的技术结构如下图所示。

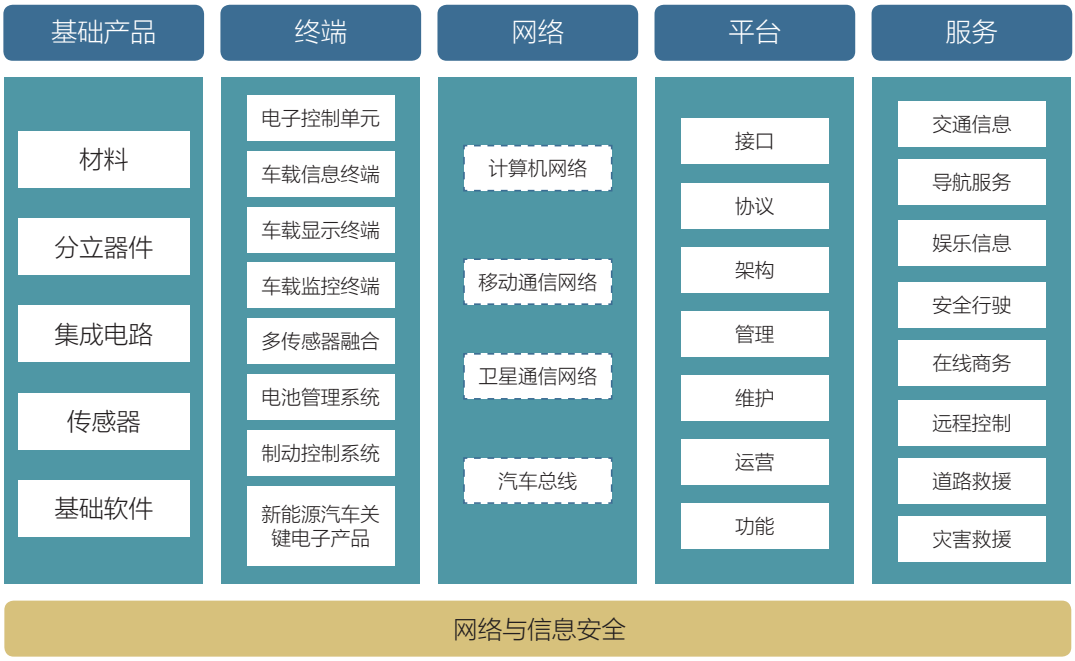


图2–3 车联网产业（电子产品和服务）标准体系技术结构图

网络与信息安全是贯穿电子产品和服务标准体系所涉及的基础产品、终端、网络、平台和服务等5大方面内容的共性要求。该标准体系提出汽车电子信息安全类标准包括车载系统安全、车载终端安全、移动应用软件和服务运营平台安全等。

2.2 国内外标准化情况

目前，我国已经着手研究建立汽车电子网络安全标准体系，促进汽车电子相关安全产品及服务体系的建设。在国家相关部门的指导下，国内有关标准化机构、汽车产业联盟自2016年下半年开始，纷纷启动开展了车联网、智能网联汽车相关标准体系的建设工作，截至目前已经取得阶段性成果。相关国际、国内标准化组织开展实施的相关标准制定情况如下。

ISO/TC22

国际标准化组织（International Organization for Standardization）简称

ISO，是负责除电工电子领域外的国际标准化工作的非政府性国际组织，成立于1947年，总部设在瑞士日内瓦，下设245个技术委员会。与汽车工业领域直接相关的技术委员会为TC22（道路车辆技术委员会）。ISO/TC22主要负责在1968年维也纳公约中所规定的道路车辆（包括挂车、摩托车、机动车、汽车列车、铰接车辆）及其装备的兼容性、互换性、安全性以及术语和性能评价试验规程（包括仪器的特性）的标准化工作，秘书处设在法国。

2016年，ISO/TC22道路车辆技术委员会成立SC32/WG11 Cybersecurity信息安全工作组，开展信息安全国际标准的制定工作。其运行方式以由美国SAE和ISO联合成立工作组的方式即ISO/SAE/JWG Automotive Security运行。工作组第一次会议于2016年10月在德国召开，基于SAE J3061，参考V字模型开发流程，讨论德国和美国SAE关于信息安全标准的立项建议，主要包括：信息安全相关的术语和定义；信息安全管理：包括企业组织层面和具体项目层面；威胁分析和风险评估（TARA）；信息安全概念阶段开发；架构层面和系统层面的威胁减轻措施和安全设计；软硬件层面的信息安全开发，包括信息安全的设计、集成、验证和确认；信息安全系统性的测试及其确认方法；信息安全开发过程中的支持流程，包括需求管理、可追溯性、变更管理和配置管理、监控和事件管理；信息安全事件在生产、运行、维护和报废阶段的预测、防止、探测、响应和恢复等。

2017年3月，ISO/TC22/SC32/WG11 Cybersecurity信息安全工作组第二次工作会议在美国召开，会议讨论了汽车信息安全国际标准的范围、对象、主要内容和框架、工作方式和计划。讨论确定标准范围：电子电气系统（Electricity and electronics system）、系统间的接口交互（Interface interactions of systems）、系统间的通信（System communication）。会议还讨论并确定了工作组的成果类型，且部分相关工作成果将作为联合国工作组（UN TFCS）的输入和参考。

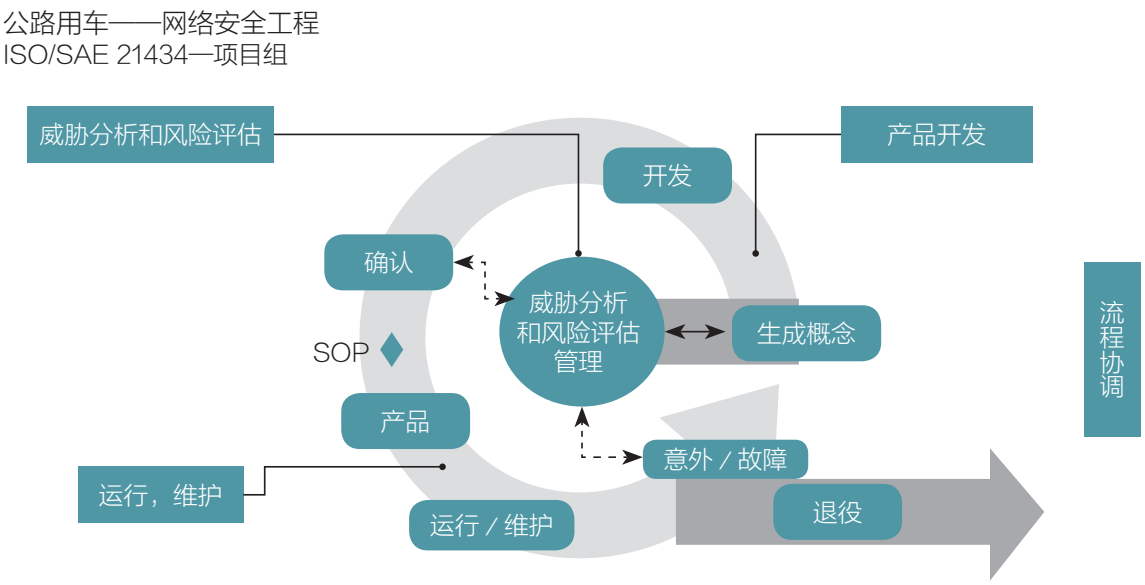


图2–4 ISO/SAE 21434内容框架

该汽车信息安全国际标准暂定编号为ISO/SAE AWI 21434，主要从风险评估管理、产品开发、运行/维护、流程审核等四个方面来保障汽车信息安全工程工作的开展。对应分设四个项目组（Project Groups）同步开展工作：威胁分析和风险评估管理（Risk Management）、产品开发（Product Development）、运行/维护（Operation, Maintenance and Other Process）、流程协调（Process Overview and Interdependencies）。目标是通过该标准设计、生产、测试的产品具备一定信息安全防护能力。

ISO/SAE 21434的工作计划为：1、2018年2月15日完成工作组草案，2、2018年9月完成委员会草案，3、2019年3月完成国际标准草案，4、2019年10月完成国际标准并发布。目前中国代表团在全国汽车标准化技术委员会（TC114）的组织下积极参与此项标准的制定，国内几家汽车信息安全企业、整车企业，也参与了该标准的制定。

SAE

SAE（国际自动化工程师学会）成立于1905年，是一个技术性学

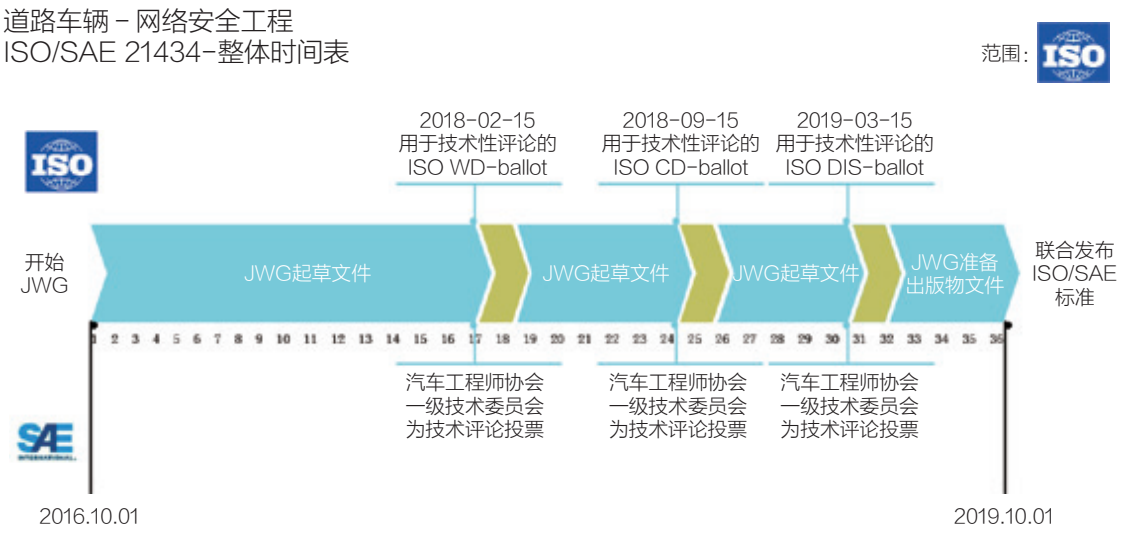


图2-5 ISO/SAE 21434时间计划

会，在全球拥有超过145,000名会员，包括航空航天、汽车和商用车辆行业的工程师和相关技术专家。其中，SAE的全球车辆标准工作组（Global Ground Vehicle Standards group）所属汽车电子系统安全委员会（Vehicle Electrical System Security Committee）负责汽车电子系统网络安全方面的标准化工作，作为第一个关于汽车电子系统网络安全的指南性文件，J3061对汽车电子系统的网络安全生命周期具有重要的应用意义，为开发具有网络安全要求的汽车电子系统提供了重要的过程依据。

J3061-1 Automotive Cybersecurity Integrity Levels

审查其他行业的现有分类方案和SAE提出的或可能正在其他组织中提出或使用的现有想法。确定使用现有方案或根据现有或提议的方法或想法（整合或合并思路）为汽车行业创建新的分类方案。威胁分析和风险评估方法，可以与分类方案一起使用，或者我们可以在网络安全完整性分类方案中将其映射到特定级别。这将需要审查现有的TARA方法并确定一个或一个定制的版本确定如何将ACSIL与安全相关的威胁与ISO 26262中的ASIL相关联。

J3061-2 Security Testing Methods

该文件是定义该主题的初始框架。该文件用作与软件和硬件测试相关的安全测试方法的详细分类。它是保持供应商不可知论的，并集中于发布时可用的测试类型。

J3061-3 Security Testing Tools

本文档是安全相关工具及其功能制造商的内部列表。这份清单并不是作为任何制造商的认可，而是市场上存在的例子和能力的清单。

J3101 Requirements for Hardware-Protected Security for Ground Vehicle Applications

为地面车辆的硬件定义一套通用的安全要求，以促进安全性增强的应用程序，提出对实现地面车辆应用硬件保护理想系统所需功能的期望，包括示例，但未明确详细说明实施要求。

J3138 Guidance for Securing the Data Link Connector (DLC)

车载诊断（OBD）法规要求轿车以及轻型和中型卡车提供数据链路连接器，以支持将诊断信息传送到车外设备。 立法诊断信息也需要及时传达给离线设备。 许多汽车制造商还通过该连接器提供增强型诊断信息和车辆系统/子系统。 一般来说，现有车辆使用两种通信方法：

a）开放访问通信总线。

b） 通过网关隔离的通信总线本文档提供了使用任一方法确保与任何车外设备通信的安全指南。

c）任何“混合”方法。

ITU–T

ITU-T的通信安全研究与标准制定工作很早就已经开展。但是在2000年以前，网络与信息安全并没有独立出来单独作为一个项目组来研究，而是在其它标准制定过程去发现有必要做相关安全标准时才开展相关工作，

相对来说网络与信息安全比较零散，并没有整体性的工作。为了适应日益严重的通信安全形势，ITU-T成立了专门的SG17来主要负责通信安全研究与标准制定工作。

在ITU-T SG17工作组已经开展了对智能交通，以及联网汽车安全的研究工作。目前已经正式发布的标准有X.1373，这个标准通过适当的安全控制措施，未远程更新服务器和车辆之间的提供软件安全的更新方案，并且定义了安全更新的流程和内容建议。

目前正在SG17组内正在制定的标准有：

X.itssec-2 该标准为V2X通信系统提供安全指导。V2X是本建议书中V2V（车辆到车辆），V2I（车辆到基础设施）和V2ND（车辆到漫游设备）和V2P（车辆到行人）通信模式的通用术语。

X.itssec-3 该标准重点从车载诊断II（OBD-II）端口连接和无线连接的角度确定车辆可访问外部设备的威胁和安全要求。

X.itssec-4 该标准主要集中在车载网络上的内部通信作为CAN通用IDS无法支持的部分，以保证利用各种高效光源来检测影响ECU通信的威胁重量检测模型，如基于签名的模型，基于熵的模型，基于自相似性的模型，基于危害的模型，本建议书将考虑使用IDS来保护连接的车辆。

X.itssec-5 该标准车辆边缘计算提供安全指导，它涵盖了车辆边缘计算的威胁分析，安全要求和使用案例。

X.mdcv是基于大数据分析的联网汽车的安全相关的异常行为检测机制，包括数据获得、数据分析等步骤。

X.srcd是V2X通讯数据分类的安全要求，它对V2X通信数据分为多种类型，定义起安全等级，并在此基础上提出安全要求。

X.stcv是联网汽车安全威胁，它首先详述联网汽车模型（汽车生态系统），然后确认对联网汽车（生态系统）高级别的威胁。

UN/WP.29

WP.29的前身为1952年6月6日成立的联合国/经济及社会理事会/欧洲经济委员会/内陆运输委员会/道路交通分委会/车辆结构工作组（UN/ECOSO/ECE/TRANS/SC.1/WP.29），旨在针对车辆结构性能的要求为各国政府实施《道路交通公约》制定建议或推荐要求。1998年，WP.29更名为“世界车辆法规协调论坛”，在继续制修订和实施ECE法规的同时，开始制定和实施全球技术法规（GTR），负责《1958年协定书》、《1998年协定书》以及与定期技术检查有关的《1997年协定书》三个汽车行业最具影响力的国际公约标准制修订与技术协调工作。在其范畴内制定的法规对联合国相关协定书签约国汽车行业具有强制性约束力，是目前世界各国实施汽车产品强制性认证、生产监管及运行管理的主要依据。

2014年12月，WP.29在其原有的智能交通ITS非正式工作组的基础上成立了智能交通与自动驾驶非正式工作组ITS/AD，并将汽车信息安全标准纳入协调范围。在后续的10次工作组会议上，各个国家和行业组织的代表对信息安全这一议题进行了热烈的讨论，并提出了关于网络安全和信息保护措施的指南草案“Guidelines on measures ensuring cyber security and data protection of connected vehicles and vehicles with automated driving technologies”。2016年12月，由英国和日本作为主席国，成立了专门的汽车信息安全标准任务组UN Task Force on Cyber security and OTA issues (CS/OTA)，围绕汽车网络安全、数据保护和软件升级OTA三部分开展国际法规及标准的制定工作，国际电信联盟（ITU—SG17）也全面与参与了该任务组的相关工作。我国各行业专家也在中国汽车技术研究中心（C-WP.29秘书处）的组织下参与了该任务组的部分工作，并有相关国际标准建议提案。2017年末，联合国ITS/AD工作组决定，以该任务组提交的研究报告为基础，制定汽车信息安全专用国际法规，标志着汽车信息安全标准即将成为联合国相关协定书签约国范畴内的强制性要求。

ETSI ITS

2008年12 月欧盟发布欧洲实施智能交通系统（Intelligent Transport System,简称ITS）行动计划，该计划是一个重要的ITS发展政策指导性文件。计划包括6个优先行动领域及实施阶段，其中合作系统作为智能交通发展中重要的阶段进行了规定，即在2011年到2013年对合作系统的研发进行评估，并对合作系统的部署应用策略进行评估。

欧盟采用授权法案（Mandate）的形式来推动标准的研究和制订。2009年10月6号，欧盟委员会通过法案M/453，授权欧洲标准化组织在法案规定的时间内制定一系列标准、技术规范和技术报告，支持将在欧盟广泛实施和部署可互操作的合作ITS系统。在法案中明确邀请欧洲通信标准化协会(European Telecommunications Standards Institute,简称ETSI)，欧洲标准化组织(Comité Européen de Normalisation（法文缩写：CEN）)，欧洲电子标准化组织(Comite Europeen de Normalisation Electrotechnique,简称CENELEC) 进行标准的制定工作，并给出了合作系统的定义、标准的工作内容、时间进度及与相关组织合作的内容。2010/40号指令要求加快了ITS部署，而车辆与交通基础设施的连接是优先领域。2013年，ETSI和CEN/ISO完成首版标准制订。第二版标准包已经进入微调阶段，主要是处理更为复杂的应用。

ETSI ITS安全构架包括几个不同的层次，一部分是安全应用层的服务，通过信息签署和认证，结合数据的加解密实现管理，即为安全服务处理，简称SA。第二部分是安全管理方面，即通过注册和认证建立起ITS网络服务，然后实施身份识别管理。第三部分是报告错误行为方面。最后一部分是HSM安全要求。

为实施更为安全的保护，ETSI ITS技术委员会制定了相应的技术规范（Technical Specification,简称TS），该技术规范主要包括安全架构、安全服务、安全管理、隐私保护等方面。主要是ITS安全架构与管理以及通讯

管理方面，不仅能够实现抽象层面的安全需求，同时可以最大程度上降低安全风险。其中安全服务方面，由系列标准ETSI TS 102 94x提供，通过该标准可实现加密认证的跟踪和机密性数据获取，另外还包括消息的内容和签名等。

TC114

全国汽车标准化技术委员会（简称汽标委）下属的智能网联汽车分技术委员会（编号为SAC/TC114/SC34）负责归口管理我国智能网联汽车领域的国家标准和行业标准，并成立了先进驾驶辅助系统（ADAS）标准工作组、信息安全、自动驾驶等工作组。《国家车联网产业标准体系建设指南（智能网联汽车）》明确了智能网联汽车标准体系建设的目标和原则，对智能网联汽车标准体系框架进行了分析和研究，并积极推进后续标准法规方面的各项事宜。信息安全标准体系（204）作为该方案的重要组成部分，支撑着整个智能网联汽车标准体系的整体架构。

2016年，汽标委先进驾驶辅助系统工作组率先组织行业内外汽车信息安全相关技术机构、企事业单位专家开展了国内汽车信息安全标准调研工作。2017年，汽标委正式成立汽车信息安全标准工作组，包括国内外整车、零部件、信息通信、电子、互联网在内的50余家成员单位，全面开展我国汽车信息安全国家及行业标准制定工作，并开展联合国、ISO等层面的国际汽车信息安全标准法规的制定与协调工作。汽车信息安全标准工作组在传统信息安全技术的要求的基础上，结合汽车设计、制造、使用过程中的特有的应用需求，并考虑与汽车功能安全的相关性，提出了“驾驶员或者车辆拥有者的个人隐私数据要保护；车辆运行信息向管理机构及用户有限度公开；车辆及驾驶员服务类信息要甄别、防范；车辆控制指令类信息甄别、确认、防范、处理”等标准制定应遵循的基本原则。并围绕基本原则的核心内容提出了“以驾驶任务为核心对信息进行分类；理清信息交

互的方式、渠道和节点；针对信息交互建立相应的防护措施；针对信息防护失效建立应急处理机制”的在标准中应体现的基本处理措施。

2018年1月22日-26日，全国汽车标准化技术委员会及下属智能网联汽车分标委（SAC/TC114/SC34）在杭州市召开智能网联汽车标准工作系列会议，集中推进包括汽车信息安全在内的智能网联汽车标准制定工作。

目前SAC/TC114/SC34已完成《汽车信息安全通用技术要求》、《车载网关信息安全技术要求》、《汽车信息交互系统信息安全技术要求》等3项汽车信息安全基础标准和《电动汽车远程管理与服务系统信息安全技术要求》、《电动汽车充电信息安全技术要求》等2项行业急需标准的预研工作，并向国家标准化管理委员会提交了推荐性国家标准立项申请。

为了更好的贯彻落实《国家车联网产业标准体系建设指南（智能网联汽车）》对于汽车信息安全标准制定工作的要求，全国汽车标准化技术委员会（TC114）智能网联汽车分标委（SC34）还拟定了汽车信息安全标准

图2-6 汽车信息安全标准子体系

的子体系框架，从评、防、测三个维度和基础、共性、系统部件、功能管理四个层面对汽车信息安全标准制定进行了全面梳理，并通过相关标准部分预留与其他信息安全标准体系的接口。

TC260

全国信息技术安全标准化技术委员会（信安标委）是国家标准化管理委员会的直属标准委员会，成立于2002年，编号为SAC/TC260，负责全国信息安全技术、安全机制、安全服务、安全管理、安全评估等领域标准化工作，并负责统一协调申报信息安全国家标准年度计划项目，组织国家标准的送审、报批工作。2016年8月，由中央网信办等部委联合印发《关于加强国家网络安全标准化工作的若干意见》。部署网络安全工作机制、标准体系、标准质量、标准宣贯、国际标准化、人才建设、资金保障等方面内容，明确网络安全国家标准统一归口协调管理。

2017年7月，信安标委立项首个关于汽车电子系统网络安全的国家标准制定项目——《信息安全技术 汽车电子系统网络安全指南》。汽车电子系统作为集电控技术、信息技术、网络技术和汽车技术于一体的复杂系统，汽车网络安全在根本上取决于汽车电子系统的网络安全防护能力。为此，信安标委将汽车电子纳入到重要的标准子体系中，并基本明确了各标

图2–7 信安标委的重要标准子体系

准子体系之间的关系，即针对“网络与系统”、“工控”、“物联网”等子体系，采用“二元化”结构，一方面等级保护子体系继续发展、完善，保证系统安全的基本要求，另一方面重要设施、系统要有更加专业的保护安全要求，重点防护。这可以作为在既有标准体系基础上发展汽车电子标准子体系的重要思路。

为了整合优势资源推进该标准的研制工作，成立了由中国电子技术标准化研究院、电子科技大学、东软集团等为代表的网络安全研究机构，联合中国一汽、上海汽车、长安汽车等汽车整车厂商组成标准编制工作组。《信息安全技术 汽车电子系统网络安全指南》的研究目标是提供一个网络安全过程框架及指南，以帮助组织识别和评估网络安全威胁，并将网络安全的设计融入到汽车电子系统的整个生命周期（从概念阶段到开发、生产、运行、服务和退役等阶段）的过程中，将网络安全控制性要素嵌入到每一个环节，并能够应对不断发展的汽车网络安全的威胁；指导组织从管理及流程的层面，消除/缓解汽车电子系统网络安全威胁，提升网络安全防御水平。本标准将为整车厂、零部件供应商、软件和芯片供应商、车联网网络运营者等汽车电子系统的产业链环节开展网络安全活动提供基于标准的指导和规范。

本标准主要的研究内容包括：

- 研究汽车电子系统在网络安全方面的领域特殊性，建立符合汽车电子需要的网络安全体系架构、安全等级要求以及网络安全过程框架；
- 研究汽车电子系统网络安全的生命周期，从全生命周期的角度，研究汽车电子系统在网络安全方面需要经历的阶段、过程活动、工作产品与相关要求，形成具有汽车电子领域针对性的方法论；
- 研究保障汽车电子系统网络安全的指导原则。

2017年7月，信安标委立项强制性国家标准项目《信息安全技术　网络产品和服务安全通用要求》（目前征求意见稿阶段），与车联网相关。

该标准针对网络产品和服务提出了恶意程序防范、缺陷漏洞管理、安全运行维护和用户信息保护等一般安全要求，以及对网络关键设备和网络安全专用产品的增强安全要求，包括安全功能要求和安全保障要求两大方面。旨在维护用户的合法权益，减少用户在使用网络产品和服务过程中的各种安全风险，提升用户对网络产品和服务在安全性、可控性方面的信心，保障国家网络安全。

另外，2017年4月，国家互联网信息办公室发布《个人信息和重要数据出境安全评估办法（征求意见稿）》，配套标准包括《信息安全技术　个人信息安全规范》（GB/T 35273-2017）、《信息安全技术　数据出境安全评估指南》（征求意见稿）（提出了个人信息和重要数据出境的安全评估流程、要点和方法）。这些法规与标准涉及联网汽车数据安全与隐私保护。当前，联网汽车数据收集手段存在差异，收集方式可划分为三类：一是汽车前装设备。如基于T-BOX、车机等设备，通过汽车CAN总线进行数据读取与收集；二是移动终端。如通过使用手机APP收集信息；三是汽车后装设备。如通过OBD等后装硬件收集信息。为保障汽车用户个人信息与企业数据资产安全，应从联网汽车数据收集、存储、使用、传输等角度进行安全规范，对整车厂和车联网运营者给出安全防护建议。

TC268

全国智能运输系统标准化技术委员会（SAC/TC268）于2003年9月成立，是国家标准委员会直管的在智能运输系统专业领域内，从事全国标准化工作的技术工作组织，负责全国智能运输系统标准化的技术归口工作。主要工作范围是：交通管理与控制、交通信息服务、城市交通智能化、营运车辆管理、电子收费与支付、智能驾驶、车路协同、交通通信和信息交换、交通数据管理与信息安全等。国际对口标准化组织是国际智能运输系统标准化技术委员（ISO/TC 204），通过车辆/车道警示和控制系统、合

作式智能交通等若干个工作组开展工作。截止目前，全国智能运输系统标准化技术委员会已发布《智能运输系统 自适应巡航控制系统 性能要求与检测方法》、《智能运输系统 车道偏离报警系统性能要求与检测方法》国家标准2项，在研《智能运输系统 换道决策辅助系统 性能要求与检测方法》等国家标准2项，交通行业标准4项。

CCSA

中国通信标准化协会 (英文译名为：China Communications Standards Association，缩写为：CCSA)。TC8的研究领域包括：面向公众服务的互联网的网络与信息安全标准，电信网与互联网结合中的网络与信息安全标准，特殊通信领域中的网络与信息安全标准。技术工作委员会下设四个工作组，即有线网络安全工作组（WG1）、无线网络安全工作组（WG2）、安全管理工作组（WG3）、安全基础工作组（WG4）。

国内CCSA TC8 WG2已经完成了《车路协同系统的安全研究》和《LTE-V2X安全研究》的研究，CCSA TC5 WG3已经开展了《基于公众LTE网络的车联网无线通信系统总体技术要求》的行标制定。CCSA TC8 WG2 提出适用于LTE-V2X的车联网通信安全总体技术要求。

《基于移动互联网的汽车用户数据应用与保护技术要求》，本标准主要规定互联网汽车数据在收集、存储、传输、使用、共享、交易、披露、出境及销毁等环节中应遵循的安全保护要求，建立相应的安全管理体系和技术防护措施。

《基于移动互联网的汽车用户数据应用与保护评估方法》本标准主要评估互联网汽车服务提供商在数据收集、存储、传输、使用、共享、交易、披露、出境及销毁等环节中的安全保护能力，可为第三方机构开展评估或企业自评估提供指导。

TIAA

车载信息服务产业应用联盟（TIAA，简称“车联”）于2010年在工业和信息化部、交通运输部、国家标准化管理委员会倡议、指导下成立，目前拥有整车、电子、软件、通信、服务五个技术领域的600余家成员单位。为结合汽车工业发展需求，为车联网网络安全保驾护航，在工业和信息化部、网信办、国密局等部委指导和支持下，于2016年11月4日成立了网络安全委员会。车联网络安全委员会立足电子信息技术与汽车、交通行业的深度融合，分析以信息终端为支点、信息通信为网络、大数据和云计算为支撑的车联网应用特点，面向民用、专用、军用三个领域，开展网络安全技术体系的分析和构建，确定核心技术标准，推动标准符合性认证、检测工作，构建安全、和谐的车载信息服务应用环境。

2017年2月，车联网络安全委员会发布了**《车联网网络安全白皮书》**。白皮书主要对国外车联网网络安全发展情况、国内车联网网络安全发展情况进行了介绍，重点对国外开展标准制定与技术研究的情况进行了分析，总结出当前我国车联网网络安全发展存在的主要问题，并就我国车联网网络安全面临的挑战与发展方向进行了分析，提出了加快推进相关政策法规、技术标准落地，有力推进顶层设计工作开展；推动汽车产业与信息安全产业跨界能力整合，加快建立车联网网络安全产品及服务体系；加快建立车联网网络安全产品评测体系，有效保障相关网络安全产品及服务质量；加强汽车产业信息安全人才队伍建设，提升汽车产业网络安全管理能力等方面的建议。

2017年2月，车联网络安全委员会发布了**《车联网网络安全防护指南细则（征求意见稿）》**（简称《指南细则》）。《指南细则》以《工业控制系统信息安全防护指南》、《中华人民共和国网络安全法》为基础，结合车联网的行业发展情况形成，并通过联盟广泛征求意见及讨论，于2017年6月发布了试行版。《指南细则》重点分析控制类应用场景、考虑数据

安全、资产安全、关键ECU（车机、T-BOX、网关等）、访问点等，从人、车、云的角度，以建立车联网一体化的防护体系为核心，针对物理安全风险、网络安全风险、系统安全风险、应用安全风险及管理安全风险等5大类风险，从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任等11个方面38个要点明确网络安全防护的要求。《指南细则》适用于车联网系统运营企业以及从事车联网系统相关产品规划、设计、建设、运维、评估的企事业单位，旨在为车联网行业提供网络安全防护方面的基本要求，提升网络安全防护能力。

CAICV

中国智能网联汽车产业创新联盟（CAICV），由中国汽车工程学会、中国汽车工业协会于2013年8月，组织汽车企业和科研院所、移动运营商、软硬件厂商共计30家单位，共同发起成立。自2015年8月开始，受工信部委托，组织汽车和相关产业40余家单位、近百位专家，编制完成“智能网联汽车技术路线图”，并根据“智能网联汽车技术路线图”研究的技术架构，设立了包括网络与信息安全在内的多个工作组。2016年7月14日，联盟信息安全工作委员会在长春成立，重点推进汽车信息安全标准体系建设，研究建立“端-管-云”三层面的汽车信息安全标准体系，开展适应中国国情的汽车信息安全管理标准、技术标准以及安全测试评估等研究，推动中国汽车信息安全保障体系的构建。

2017年6月12日，联盟组织中国汽车工程学会、北京航空航天大学、梆梆安全研究院共同编撰并发布了《智能网联汽车信息安全白皮书》。白皮书综合分析了国内外智能网联汽车安全产业现状与发展趋势，解析智能网联汽车所面临的安全威胁，提出智能网联汽车信息安全方法论，构建智

能网联汽车安全保障体系。并深入探讨智能网联汽车关键安全防护技术，绘制典型智能网联汽车攻击路径图，为智能网联汽车的安全发展提供科学决策依据，促进智能网联汽车产业的健康成长。

联盟依托中国汽车工程学会团体标准平台，自2017年起开始组织制定《智能网联汽车车载端信息安全技术要求》，并于2018年3月发布标准征求意见稿。该标准规定了智能网联汽车车载端的术语及定义，车载端安全架构和目标，以及安全架构内各部分的信息安全技术要求等内容。在不限定车载端具体产品结构的前提下，统一车载端安全防护中存在的各方面威胁，提出信息安全技术要求，适用于整车、零部件企业的智能网联汽车相关产品开发过程。

第三章　汽车电子网络安全技术研究

基于对车联网、汽车电子网络安全相关技术、标准的研究基础，编制成员单位同步开展了一些汽车电子网络安全问题的研究工作，系统化分析了汽车电子网络安全威胁与风险评估方法、汽车电子系统网络安全框架与生命周期、以及汽车电子网络安全参考架构等问题。

3.1威胁分析与风险评估技术研究

对整车或是零部件，开展威胁分析与风险评估，确定整车或是零部件中需要保护的资产、资产面临的威胁，并据此形成整车或是零部件的网络安全需求。

3.1.1 威胁分析与风险评估过程

在研究有关信息安全风险评估的国家标准以及国外有关汽车领域的威胁分析与风险评估方法的基础上，形成面向汽车电子网络安全的威胁分析与风险评估过程如图3-1所示，表3-1是对过程中相关活动的说明。

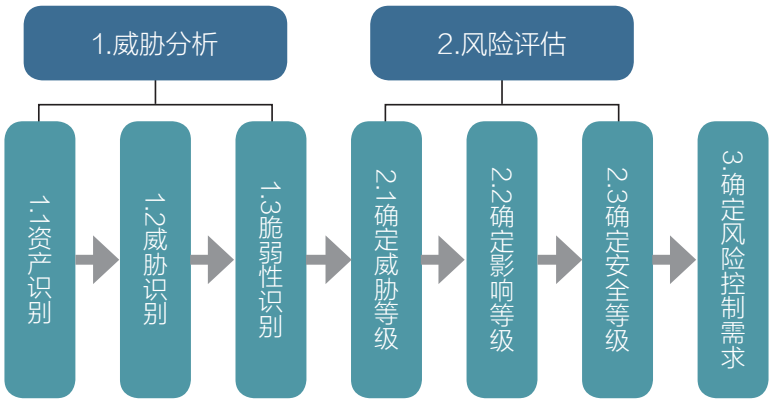


图3–1 面向汽车电子网络安全的威胁分析与风险评估过程

表3-1 面向汽车电子网络安全的威胁分析与风险评估活动说明

活动	活动说明
1 威胁分析	针对汽车电子系统的相关资产，分析其可能面临的各种威胁，以及可能被威胁利用的脆弱性
1.1 资产识别	对汽车电子系统需要保护的资产进行识别
1.2 威胁识别	对识别出的资产进行威胁识别，明确资产面临的具体威胁，并对威胁与安全属性进行映射
1.3 脆弱性识别	以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱点的严重程度进行评估
2 风险评估	用于确定每个“资产-威胁”对的网络安全等级
2.1 确定威胁等级	通过对威胁产生负面影响的可能性的分析与评估，明确威胁的等级
2.2 确定影响等级	针对威胁产生负面影响的严重程度进行分析和评估，明确威胁的影响等级
2.3 确定安全等级	综合威胁等级和影响等级的分析结果，确定针对每个“资产-威胁”对的安全等级，以反映风险水平的情况
3 确定风险控制需求	基于风险评估的结果，明确对汽车电子系统有关资产的安全需求，即需要采取的风险控制措施

（1）汽车电子系统资产识别

汽车电子系统需要保护的资产由内而外主要包括：车载电子组件，如ECU、传感器、执行器等，以及它们之间的连接；车载网关；车辆与外部环境连接的接口设备、外部感知部件等。

从资产的表现形式，可以分为数据、软件、硬件、服务等，而从需要保护的业务过程和活动、所关注信息的角度，资产类型可包括基于ECU的控制功能、与特定车辆相关的信息、车辆状态信息、用户信息、配置信息、特定的软件、内容等，如下表所示。

表3-2 汽车电子系统需保护的资产

需要保护的资产	描述
基于ECU的控制功能	控制功能的可获得性，控制功能的执行环境，操作所需要的通信
与特定车辆相关的信息	与具体车辆关联的信息（车辆ID，设备ID等），认证码，累积信息（运行的历史信息、操作的历史信息等）
车辆状态信息	表示车辆状态的数据（位置、速度、目的地等）
用户信息	个人信息、身份认证信息、账单信息、用户（车主和乘客）使用历史和操作历史等
软件	车辆相关的软件（固件、操作系统、应用软件等）
内容	用于应用（视频、音乐、地图等）的数据
配置信息	软硬件行为相关的设置数据

例如针对车载信息娱乐系统（业内通常简称其为“车机”），其需要保护的资产主要分为3个方面，即数据、软件和硬件：

- 车机数据资产：主要包括用户ID、密钥、系统配置数据、用户信息、与服务平台通信的数据、与CAN总线通信的数据等；
- 车机软件资产：主要包括启动加载软件、操作系统和应用软件；
- 车机需要保护的硬件接口：主要包括USB、3G/4G通信接口、WiFi、蓝牙、JTAG、串口、SIM和以太网接口等。

（2）威胁与脆弱性识别

可以通过对系统用例的分析，识别威胁与脆弱性。基于扩展的STRIDE方法（微软提出的结构化、定性的安全方法，以发现软件系统存在的威胁），将威胁的类型分为6大类（即仿冒、篡改、抵赖、信息泄露、拒绝服务、特权提升），并将它们与影响的安全属性（即真实性、完整性、机密性、可用性、时效性、防抵赖等）对应起来，如下表所示。

表3-3 威胁类型与安全属性对应关系

威胁类型	说明	影响的安全属性
仿冒	攻击者冒充某人或某事	真实性 时效性
篡改	攻击者改变传输过程或是存储的数据，也可能改变功能（通过软件、固件或是硬件实现的功能）	完整性
抵赖	攻击者的行为不能被追溯	防抵赖 时效性
信息泄露	攻击者访问传输过程或是存储的数据	机密性/隐私
拒绝服务	攻击者中断系统的合法操作	可用性
特权提升	攻击者执行未被授权的行为	授权

结合攻击者的动机与识别出的系统用例，分析对汽车电子系统可能的攻击。可结合攻击树方法对攻击场景进行分析，描绘出攻击路径，可以识别出针对具体资产的具体攻击手段（树中的叶子节点），并进一步识别系统资产可能被利用的脆弱性。图3-2展示了攻击树的主要结构：

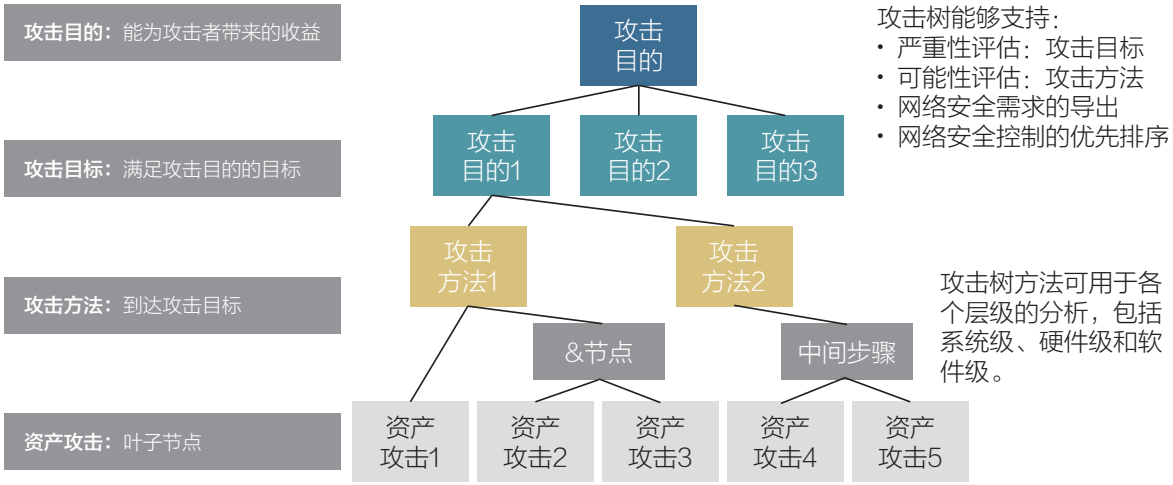


图3–2 攻击树结构

例如，车辆在与其他车辆进行通信时，可以接收来自其他车辆的危险告警信息，而攻击者可能对此发起“篡改告警消息”的攻击。以此为例进行攻击树分析，如下图所示。

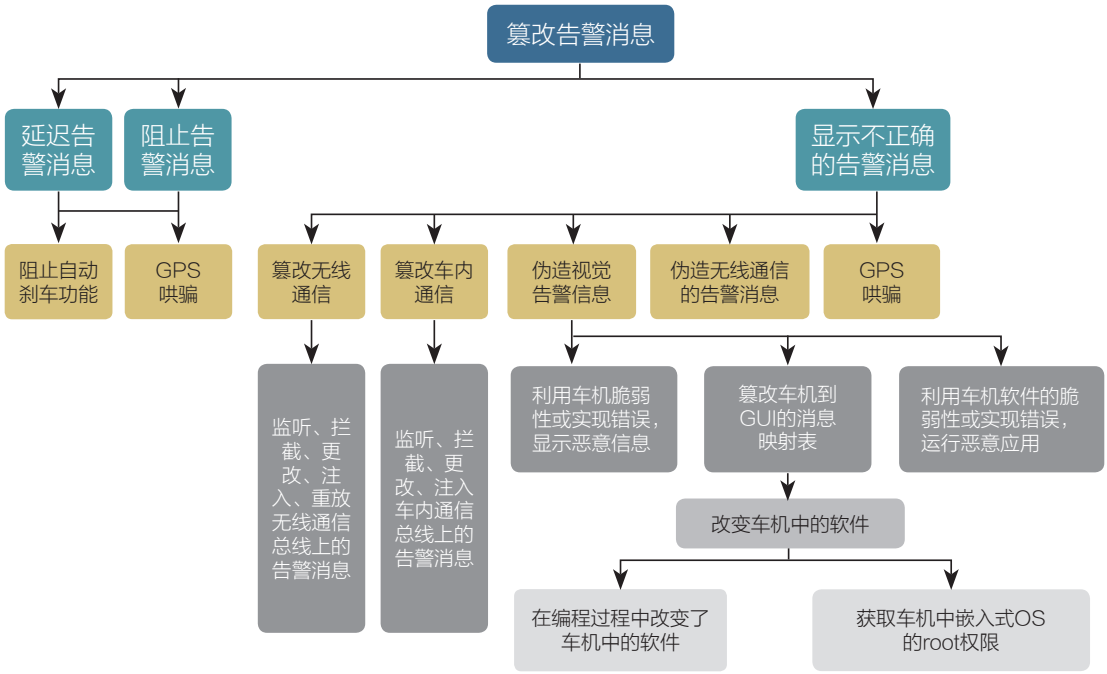


图3–3 攻击树实例

（3）风险评估

风险评估主要从威胁产生负面影响的严重程度以及攻击成功的可能性两个方面进行。威胁产生负面影响的严重程度从S0到S4一共分为5个由低到高的级别，具体可基于表3-4的方法进行分析。

表3-4 影响严重程度分级

分级	功能安全	隐私	经济	操作性
S0	无伤害	没有非授权的数据访问	没有经济损失	对操作性能没有影响
S1	轻微或中度的伤害	仅对匿名数据（无特定的车辆驾驶员数据）的非授权访问	低等级的经济损失	产生对驾驶员不明显的影响
S2	严重伤害（可能生还），或对多辆车的轻微或中度伤害	对车辆的标识或多个车辆的匿名数据的非授权访问	中度经济损失，或对多辆车的低等级经济损失	驾驶者能感知到性能的降低，或对多个车辆的不明显的影响

分级	功能安全	隐私	经济	操作性
S3	威胁生命（不确定是否能生还），或致命的伤害，或对多辆车的严重伤害	对驾驶者或车辆的跟踪标识，或对多个车辆的非授权访问	重大的经济损失，或对多个车辆的中度经济损失	对性能产生重大的影响，或对多辆车的显著性能影响
S4	威胁生命，或对多辆车的致命伤害	对多辆车的驾驶者或车辆的跟踪信息的非授权访问	对多辆车的重大经济损失	对多辆车的重大性能影响

而对于威胁等级（成功实施攻击的可能性），则可以从攻击者确定攻击系统和执行成功攻击所需的专业性要求、对系统的了解程度（关于被评估资产对象的知识）要求、时间机会窗口要求以及对专业设备的要求等方面进行分析，如表3-5所示。

表3-5 威胁等级（攻击成功可能性）相关因素分级

参数	值	解释
专业知识		
外行	0	相较于专家和熟手，不具备关于评估对象的特别的专业知识
熟手	1	具备有关信息安全领域的常识，并牵涉到相关的商业活动中
专家	2	熟悉信息安全相关的底层算法、协议、硬件、结构、安全行为、原理和概念等
专家团队	3	需要不同领域的专家联合行动，以完成特定步骤的攻击
关于被评估资产对象的知识		
公开的	0	通过互联网、书店以及不需要保密协议的共享信息所获得的知识
受限的	1	由开发者组织所控制的知识，以及与其他组织共享的知识
敏感的	2	在开发者组织中离散团队之间共享的知识，对这些知识的访问只限于特定团队的成员

关键的	3	仅被少数个体所知道的知识，对这些知识的访问受到严格的控制并需要承担个体责任
机会窗口		
关键的	0	被评估资产对象可通过公共的/不可信的网络被利用，其机会高且不受时间限制
高	1	被评估资产对象可被利用的机会高但时间有限，例如，在不接触到物理硬件的情况下，实施逻辑的或远程的访问
中	2	被评估资产对象可被利用的机会低，例如，有限的物理和/或逻辑的访问
低	3	被评估资产对象可被利用的机会非常低，例如，为了实施攻击，需要对被评估资产对象进行物理访问，以拆解车辆部件达到访问其内部的目的
设备需求		
标准的	0	对于攻击者已可用，不管是为了识别脆弱性还是发起攻击
专业的	1	对于攻击者尚不可用，但比较容易获得，比如通过购买适量的设备
定制的	2	需要特别定制生产的设备（例如非常复杂的软件），或者因为设备的专业性而被受控发布，其价格也非常贵
多个定制的	3	需要多个不同类型的定制设备以完成特定步骤的攻击

通过对上述攻击可能性相关因素的分析，将得到的值相加，再根据表3-6将和值映射为相应的威胁等级（P0~P4）。

表3-6 威胁等级（攻击成功可能性）的确定

相关参数的取值范围	攻击成功可能性	威胁等级
>9	很低	P0
7-9	低	P1
4-6	中等	P2

相关参数的取值范围	攻击成功可能性	威胁等级
2-3	高	P3
0-1	很高	P4

最后，再综合威胁影响严重程度分级和攻击成功可能性等级，确定被评估资产对象的安全风险水平（即安全等级R0~R4，R0为最低风险水平，R4为最高风险水平），确定方法如表3-7所示。

表3-7 安全等级确定矩阵

安全等级（R）	影响等级（S）					
威胁等级（P）		S0	S1	S2	S3	S4
	P0	R0	R0	R0	R0	R1
	P1	R0	R1	R1	R1	R2
	P2	R0	R1	R2	R2	R3
	P3	R0	R1	R2	R3	R3
	P4	R1	R2	R3	R3	R4

3.1.2 安全风险归纳

通过对近年来出现的各类汽车安全事件的搜集、分析和整理，结合我国汽车产业界发展中面临到的实际问题，我们从车内到车外，按照基础元器件、关键软硬件设备、内部通信总线、车载操作系统及应用、外接终端和云服务平台6个层面来归纳汽车电子领域当前面临的主要安全风险。

1. 基础元器件层面，汽车中大量使用的传感器、处理芯片等本身就可能存在设计上的缺陷或者漏洞，诸如信号干扰、缓冲区溢出、缺乏签名校验机制等，可能在遭受攻击时影响汽车正常行驶功能，构成严重安全威胁。

2. 关键软硬件设备层面，车体控制类ECU、T-BOX、车载网关这类关键设备在认证、鉴权、逆向信号分析等方面都可能存在较高安全风险，能够被攻击者操控利用，传统安全机制由于在复杂度和实时性方面不适用于汽车电子应用场景而无法直接部署应用。

3. 内部通信总线层面，从现代网络安全角度来看，CAN总线的消息机制设计极其不安全，缺乏必要的加密和访问控制机制，通信不认证，消息不校验，面临消息伪造、拒绝服务、重放攻击等一系列风险，需要进行安全加固。

4. 车载操作系统及应用层面，继承自传统IT操作系统的版本面临各种已知漏洞威胁，且易于被攻击者利用安装未知应用程序，窃取各类数据，甚至可能将风险传导至车体控制装置，对驾驶安全造成一定隐患。

5. 外接终端层面，一是外接终端安全水平的参差不齐决定了引入安全风险的不确定性，带来了更多的未知安全隐患；二是部分接入终端可能利用OBD接口直接读写车内总线，发送伪造控制信息，严重干扰汽车正常功能。

6. 云服务平台层面，可能存在传统操作系统漏洞及虚拟资源调度问题，还可能负责车辆控制和敏感数据的传输存储，但大部分平台目前访问控制策略偏弱，攻击者能够伪造凭证访问并获取大量数据，对车辆本身及用户数据隐私构成威胁，甚至能影响到部分可远程控制的车载功能。

3.2 汽车电子系统网络安全生命周期研究

汽车电子系统网络安全过程框架如图3-3所示，包含网络安全管理、生命周期各阶段的工程活动和支持过程，其中生命周期阶段包括概念设计阶段、产品开发阶段、产品生产、运行和服务阶段。

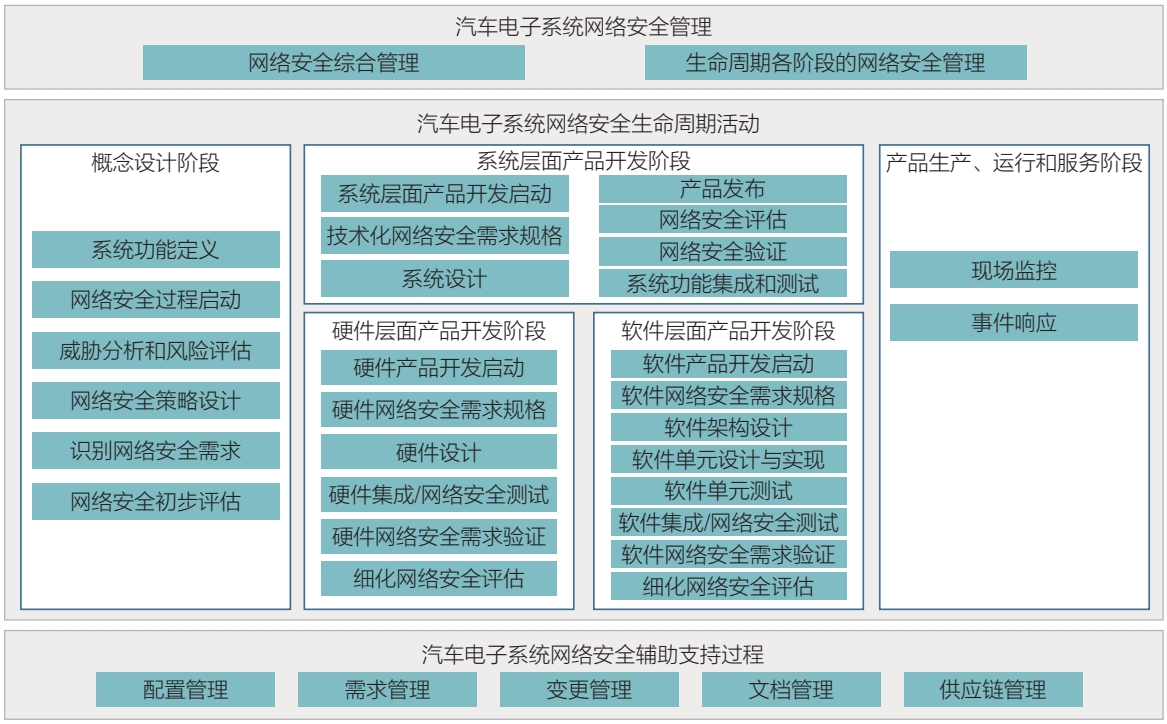


图3–3 汽车电子系统网络安全过程框架

汽车电子系统网络安全管理主要包括网络安全综合管理、以及在产品生命周期的各个阶段所实施的网络安全管理活动，如图3-4所示。

概念设计阶段主要包括系统功能定义、网络安全过程启动（计划）活动、威胁分析和风险评估、网络安全概念设计、识别网络安全需求、网络安全初步评估等环节的活动，如图3-5所示。

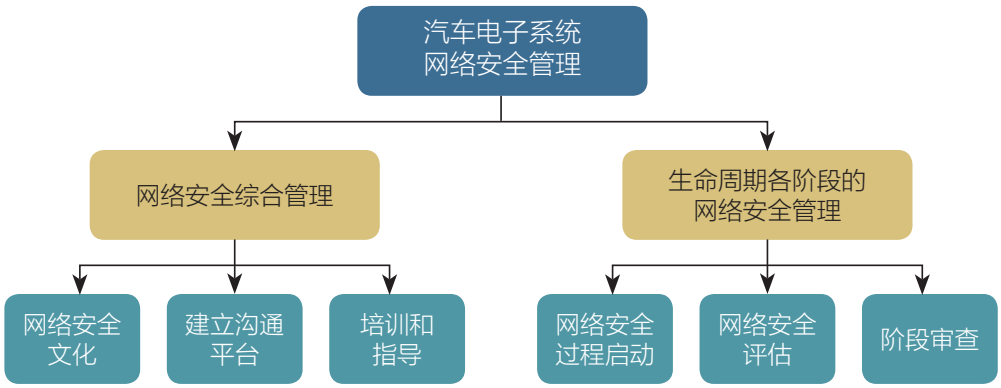


图3–4 汽车电子系统网络安全管理结构

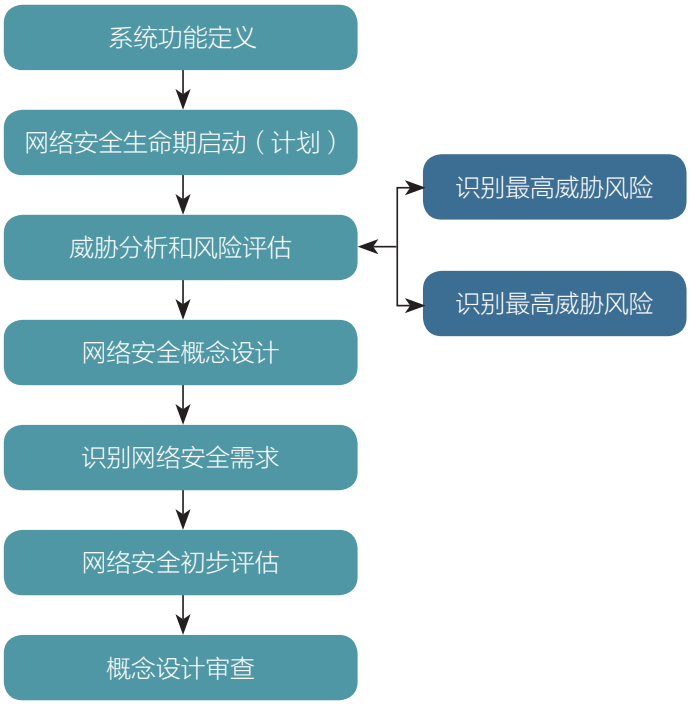


图3–5 概念设计阶段活动流程

产品开发阶段包括：系统层面产品开发阶段、硬件层面产品开发阶段和软件层面产品开发阶段。图3-6展示了产品开发阶段的基本过程，以及系统层面、硬件层面和软件层面产品开发之间的关系。为了简洁，图中没有画出任何迭代过程，但其实其中有许多阶段，都需要反复迭代，才能实现目标。

系统层面产品开发阶段主要包括系统层面产品开发启动、技术化网络安全需求规格、系统设计、系统功能集成和网络安全测试、网络安全验证、网络安全评估以及产品发布等环节的工作，如图3-7所示。

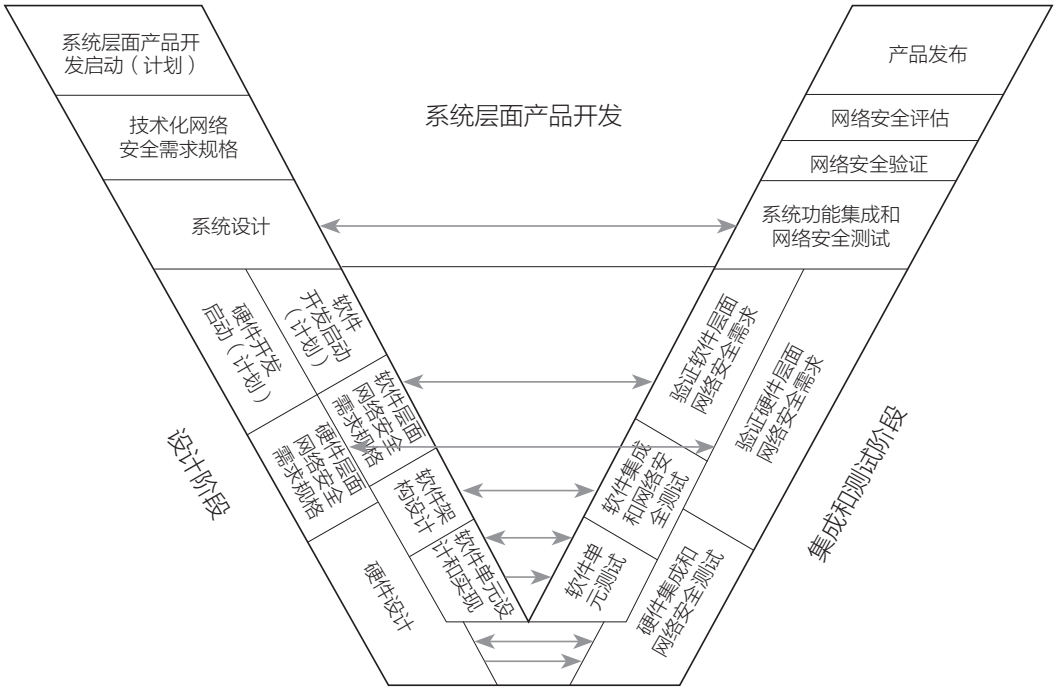


图3–6 系统层面、硬件层面与软件层面产品开发的关系

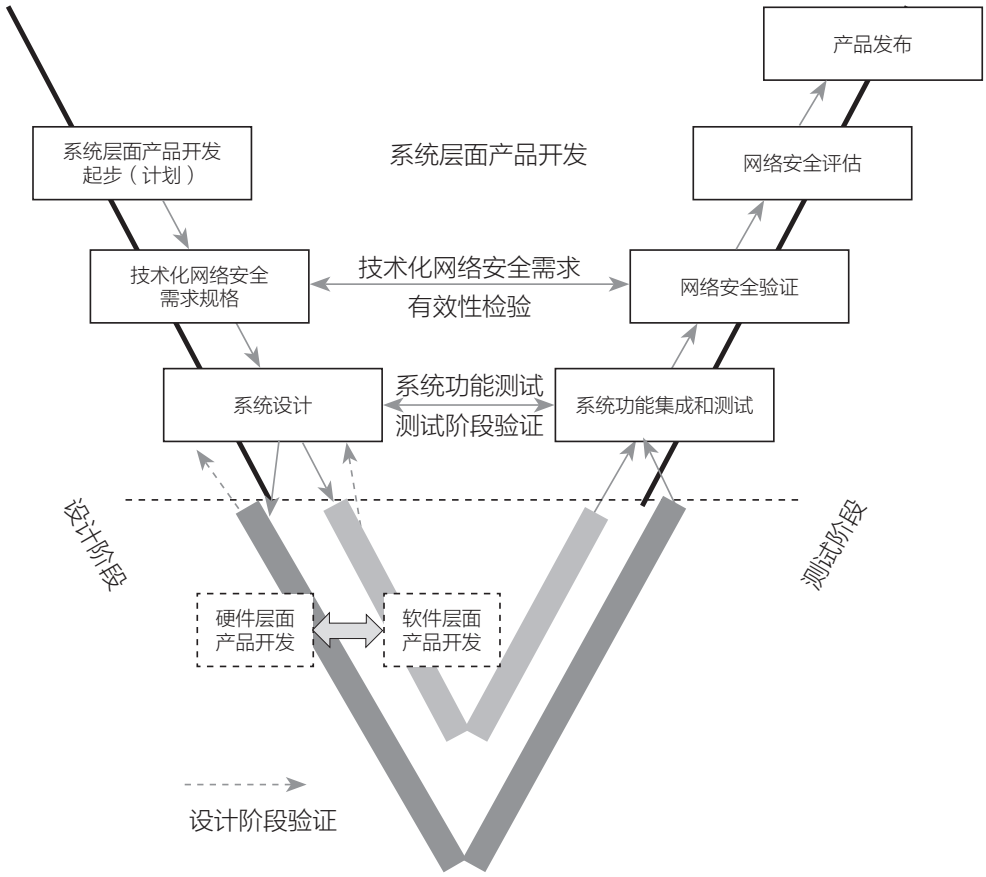


图3–7 系统层面产品开发过程V型图

硬件层面产品开发阶段主要包括硬件开发的启动、硬件层面网络安全需求规格、硬件设计、硬件集成和网络安全测试、硬件网络安全需求验证、细化网络安全评估等环节，如图3-8所示。

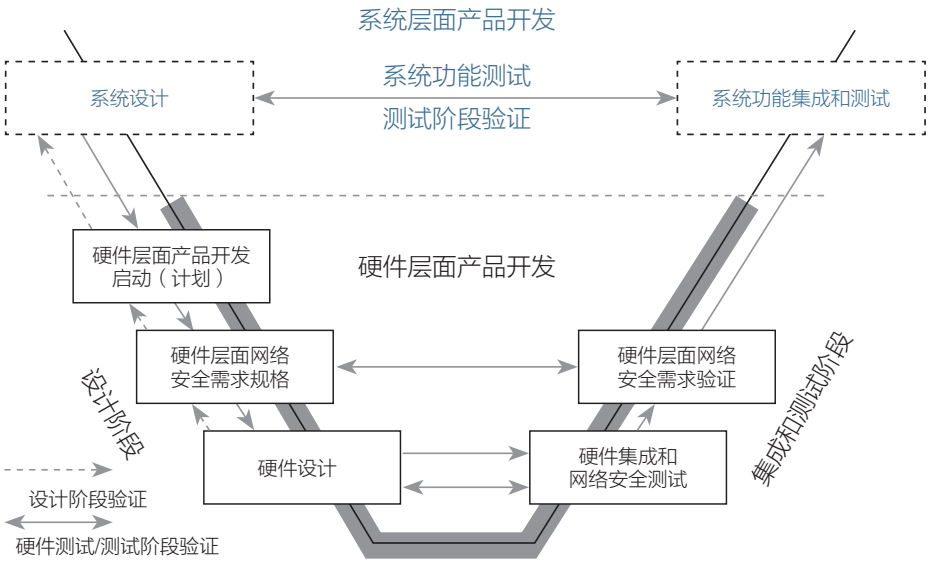


图3–8 硬件层面产品开发过程活动的V型图

软件层面产品开发阶段主要包括软件开发启动、软件网络安全需求规格、软件架构设计、软件单元设计与实现、软件单元测试、软件集成和网络安全测试、软件网络安全需求验证、细化网络安全评估等环节，如图3-9所示。

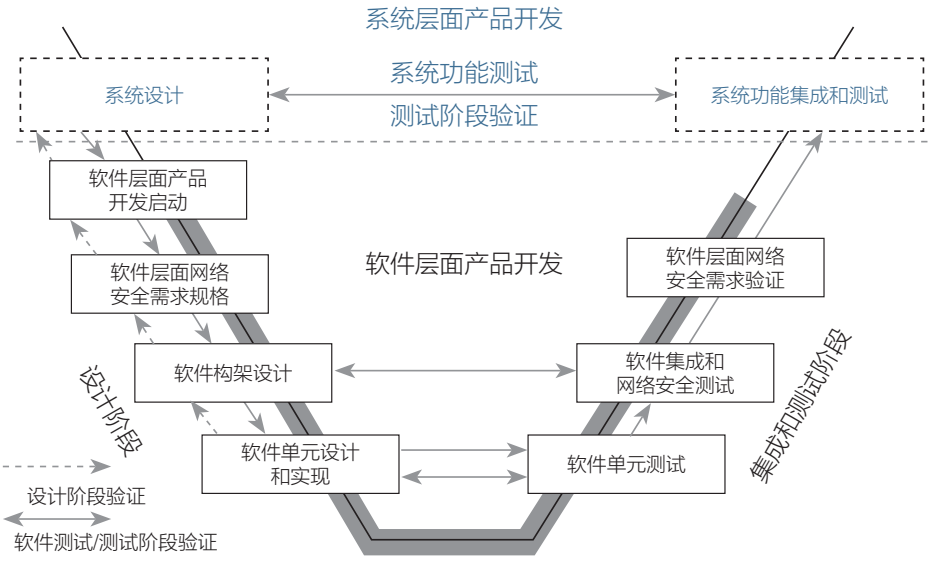


图3–9 软件层面产品开发过程活动的V型图

产品生产、运行与服务阶段主要包括现场监控和事件响应活动。

汽车电子系统网络安全支持过程主要包括配置管理、需求管理、变更管理、文档管理、供应链管理等方面的活动。

组织可以根据自身实际情况，对上述的网络安全过程框架及生命周期阶段活动进行配置和裁剪，并考虑与组织现有的管理体系（比如质量管理体系）的机构设置、过程活动进行结合，以便落实本标准所要求的网络安全生命周期活动，以较小的代价实现高效的管理。

3.3 汽车电子网络安全参考架构研究

汽车电子系统涉及到的功能由内至外可以分为不同的层次，各个层次对于安全的定义和需求也不尽相同，因此需要定义合理规范的系统架构，将不同的功能区域进行合理的隔离，分割为不同的安全区域。不同区域之间的信息流转加以严格的控制，从而满足在车联网环境中汽车电子系统的一系列网络安全要求。因此，建立如下图所示的汽车电子网络安全参考架构，以便构建分层次的汽车电子网络安全纵深防御体系。

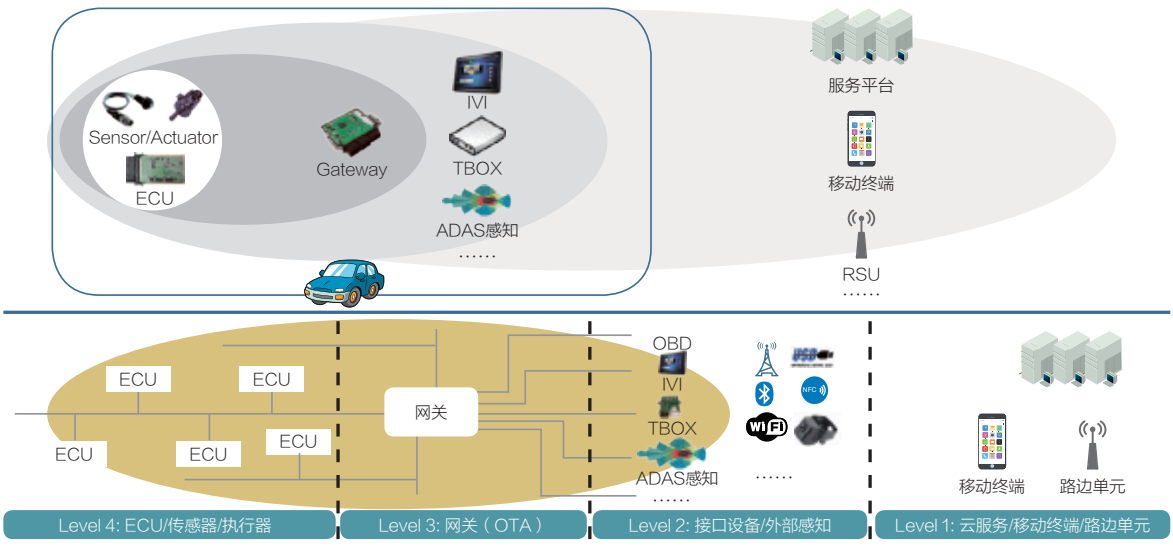


图3–10 汽车电子网络安全参考架构

该参考架构从网络分段的角度，将网络安全的防御分为4个层次：

- Level 1：涵盖车辆外部的所有元素，包括云端服务平台、移动终端、路边单元；
- Level 2：连接车辆与其外部环境的各种车载接入设备（包括IVI、T-BOX、OBD等），以及有关的外部感知部件。这些接口设备实现车辆与外界环境（包括后台服务器、移动终端设备、路边单元等）的通信、互联，连接方式可以是有线或无线的，甚至可能具备基础安全模式，如USB、蓝牙、WIFI、GPS、3G/4G等；
- Level 3：车载网关，实现车辆内部各个总线网络的连接，以及与接入设备的连接；
- Level 4：包含车辆内部控制网络中所有的ECU、传感器和执行器。ECU与传感器之间、ECU与执行器之间通过相应的内部通信总线连接，而车内通信总线也可以分为多个不同的网段（或域）。

应该说，汽车电子的网络安全风险与功能安全密切相关，在参考架构的4个层次中，Level 4中ECU具有相对最高的风险水平。但是基于以下方面因素，当前往往是在车载接入设备（比如车机、T-BOX）上部署最为丰富、完整的安全防护措施：（1）基于纵深防御的思想，在最为接近外部环境的车载接入设备层部署丰富的防护措施，有利于尽早地降低安全威胁；（2）资源可行性：相对软硬件资源较为匮乏的ECU/传感器/执行器等车控领域的设备，车载接入设备具有更为丰富的软硬件资源、性能优越；（3）供应商体系及自主可控性：目前ECU的供应商还主要来自国外，自主可控程度较低，短时间内部署国产自主的安全防护技术的可行性较低。

因此在车辆端，设计一系列的安全机制，包括密码模块、启动安全、通信安全、应用安全、访问点安全、系统安全、数据安全、CAN总线访问控制、安全监控等，为车载接入设备（IVI/T-BOX）、网关、ECU等提供网络安全防护，并结合风险分析结果、根据车辆端设备子系统中3个防御

层次的风险水平差异，考虑各部件在硬件、软件资源及实时性能上的不同需求，上述安全机制在接入设备、车载网关、ECU/传感器/执行器上的差异性部署需求。

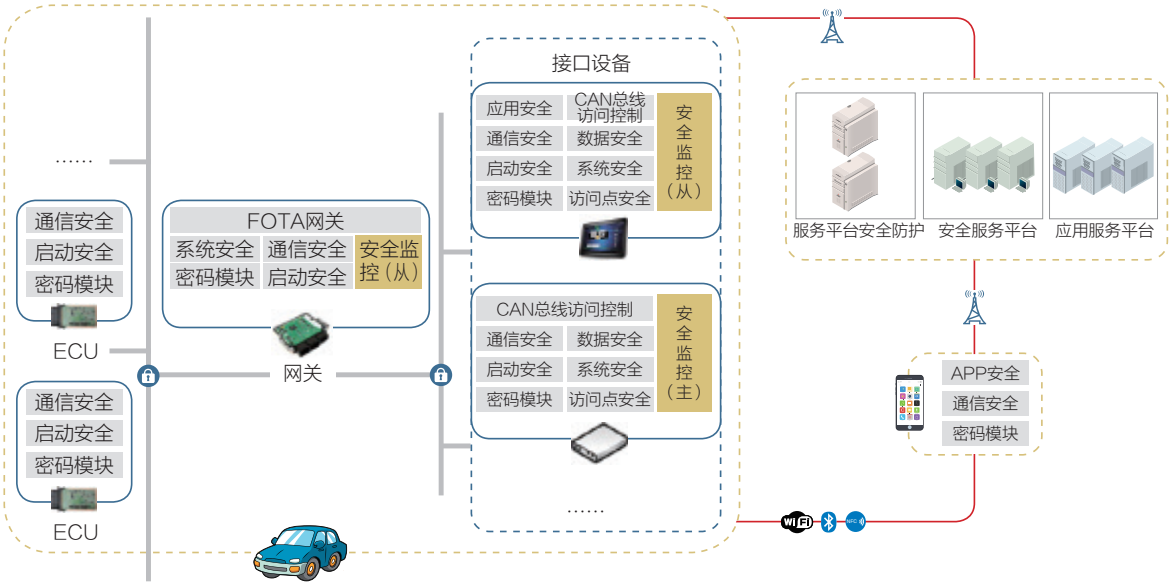


图3–11 基于参考架构的网络安全机制

第四章　汽车电子网络安全标准化工作

汽车电子网络安全不仅涉及某个部件、设备、系统或者产品的安全，而且与所处工作环境、应用场景、服务平台等密切相关，面临的安全风险和挑战更加多样，其标准化需求也同样更加复杂。我们在研究《国家车联网产业标准体系建设指南》系列文件当前内容的基础上，结合汽车电子网络安全标准化需求，提出汽车电子网络安全标准体系框架和工作建议。

4.1 汽车电子网络安全标准体系

（一）网络安全标准化需求

根据我国汽车电子领域发展实际需求，结合3.1节归纳的安全风险当前现状及发展趋势，汽车电子网络安全的影响范围涵盖了基础元器件、软硬件设备、系统、通信总线、协议与接口、外部连接终端及平台等各个方面，目前主要存在如下标准化需求。

1. 汽车电子网络安全领域相关术语定义、通用方法和指南需要进一步规范。鉴于汽车电子领域的特殊性，传统信息安全领域中能够直接使用的基础共性标准相对较少，缺乏针对性很强的安全需求分析方法、参考架构、概念模型等内容，故需就解决对此类问题加紧制定支撑性的基础共性类标准。

2. 汽车电子关键产品、设备、网络、数据的安全技术要求标准急需制定。在过去相对独立运作模式下，传统汽车与外界进行交互的需求很少，企业内部标准已经可以在自身完整服务框架体系内解决绝大部分的安全问题。但当现代汽车面临越来越多的车与车、车与路交互这样的V2X场景，并且考虑到未来需要融入智慧交通这一大环境体系中去时，协调一致的安

全技术要求显得尤为重要且必不可少，标准化需求十分迫切。

3. 当前汽车电子相关各类服务需要相应安全管理标准支撑。随着汽车网联化的深入，以安全漏洞修复、车载软件升级为代表的汽车网络服务频率越来越高，黑客可借助此类服务通过利用签名漏洞或伪造签名等手段植入相应后门，从而达到长期控制汽车的目的；为防范此类安全风险，除了加固相应安全功能外，还应对服务管理提出相应安全要求，包括在服务平台层面，并且安全事件不可避免的发生后应急响应管理同样需要标准化指引。

4. 针对产品、系统、整车的安全测评类标准缺乏，传统风险评估标准方法并不完全适用。汽车需要网络安全这一理念已经逐渐被市场接受并认同，但汽车电子产业链上各级厂商、测评机构普遍反映没有对应的安全标准给出统一测试项目、方法、指标进行指导，也就难以比较同类别产品之间网络安全水平的优劣，从市场需求方面考虑急需此类标准的制定和发布。

（二）体系框架图

图4-1 汽车电子网络安全标准体系框架

（三）标准体系内容

基于上述标准化需求分析，结合信息安全标准体系通用框架，现将汽车电子网络安全标准体系框架定义为“基础通用”、“技术要求”、“服务管理”、“测评规范”四个部分，同时根据各具体标准类在内容、技术等级上的共性和区别，对四部分做进一步细分，形成内容基本完整、结构基本合理的13个子类（如图4-1所示，框内数字为体系编号）。

1.基础通用（100）

基础通用类标准主要包括术语和定义、安全模型框架等两类标准。术语和定义标准用于统一汽车电子网络安全相关的基本概念，为各相关方协调兼容奠定基础，同时也为其它各部分标准制定提供支撑；安全模型框架标准用于对各种汽车电子应用场景下的安全需求提供通用分析模型及方法。

2.技术要求（200）

技术要求类标准主要包括安全指南、设备安全、网络防护安全、数据安全、密码应用等五类标准。安全指南标准用于指导一般汽车电子相关企业开展安全实践活动，实现最基本的网络安全保障；设备安全标准主要包括基础电子产品、终端、操作系统、软件以及智能汽车、新能源汽车关键电子部件等安全标准；网络防护安全标准主要用于为车内总线网络、传感网络以及外联网络（蓝牙、Wi-Fi、RFID、LTE-V2X等）提供网络安全防护；数据安全标准主要用于为汽车电子相关各类数据（包括状态数据和用户数据）的采集、存储、传输、监测等提供安全保障；密码应用标准主要用于规范当前在汽车电子产品中应用越来越多的密码技术，提供适用于汽车环境的应用指导。目前已经立项制定的《信息安全技术 汽车电子系统网络安全指南》即属于安全指南类标准，同时可优先重点考虑推进车载操作系统及应用软件安全、车载ECU安全、车用网关设备安全、T-BOX安全、数据安全保护、充电设备安全等标准研究。

3.服务管理（300）

服务管理类标准主要包括漏洞修补与软件升级、应急响应与管理、服务运营平台安全等三类标准。漏洞修补与软件升级标准主要针对目前汽车电子普遍采用的OTA服务模式中潜在的安全威胁提供防护方法和控制措施；应急响应与管理类标准主要为针对各类突发汽车电子相关安全事件的应急预案的制定和实施，以及相应维护管理要求提供支持；服务运营平台安全标准主要针对汽车电子相关服务运营平台的安全问题，提出相应的安全运维要求。

4.测评规范（400）

测评规范类标准主要包括风险评估、产品测评、系统测评等三类标准。风险评估类标准主要根据汽车电子系统与传统IT系统之间的区别来重新定义相应的风险评估流程、方法等内容；产品测评类、系统测评类标准主要针对产品级、系统级两个层面的网络安全要求给出相应测试评价方法，以满足各层级厂商、测评机构和监管组织机构的需求。优先重点考虑推进车用网关设备安全测评、T-BOX安全测评等标准。

4.2 下一步工作考虑

在信息技术飞速发展的时代，标准化工作是组织现代化生产，提升产品质量与安全保障的重要手段，为实现针对企业与产业发展的科学管理奠定基础。汽车电子网络安全标准化工作围绕标准体系建设、标准研制、宣贯培训、检测认证等一系列活动，为汽车电子网络安全技术应用、产业化推广和运维服务提供重要支撑。**汽车电子系统作为集电控技术、信息技术、网络技术和汽车技术于一体的复杂系统，是实现联网汽车网络安全的重要基础**。因此，汽车制造商、零部件供应商等应聚焦汽车电子系统，围绕网络安全标准化工作，多层次制定汽车网络安全管理制度与规范，多角度实施汽车网络安全防范与保障措施，多节点融合汽车网络安全生命周期

活动，有效应对各类网络安全事件，防范针对联网汽车的网络安全攻击，保障汽车产业各环节安全稳定运行。

后续我们将在国标委等有关部门指导下，加强与相关标委会、行业组织的沟通、协调，强化已建立的联络员互派机制，促进车联网产业相关领域标准化工作的有效开展，特别是在汽车电子网络安全标准化方面，具体有关建议如下：

（1）紧跟产业发展步伐，不断完善汽车电子系统网络安全标准化顶层设计，重点实现汽车电子网络安全标准体系的迭代优化。网络安全标准体系建设是具有内在联系的各类标准组成的科学有机整体，是促进标准组成趋向科学合理化的重要手段。汽车电子网络安全标准体系建设与完善过程，应明确汽车电子在“端-管-云”的车联网架构中的重要占位与作用，实现与车联网产业标准体系的对接嵌套。同时，汽车电子与信息技术的发展可能产生新型应用与服务模式，通过分析其网络安全威胁变化，优化调整标准体系结构与标准目录，实现标准体系完善过程与汽车电子技术、网络安全技术等发展过程的有效衔接，发挥标准体系在构建安全的车联网网络空间过程中基础性、规范性、引领性作用。跟踪联网汽车网络安全产业发展模式与安全防护新技术，做好标准体系建设完善向标准制修订、宣贯培训、实施评估的全过程模式转变，推动联网汽车各层级网络安全防护与治理方面工作的开展。

（2）挖掘汽车领域网络安全特殊需求，实现汽车电子网络安全重点标准的先行研制。建议整车制造、汽车电子、通信运营、服务集成、安全供应商等领域企业深度参与标准研制与验证过程，围绕汽车电子这一核心，开展包括**网络安全指南、安全技术要求、安全管理要求、安全测评方法等标准的前期研究，为汽车电子系统网络安全相关标准的制定提供参考。**理清汽车网络安全风险点与网络安全特殊需求，建立基础通用、智能网联汽车、信息通信和电子产品与服务等不同细分应用领域标准化技术委

员会之间的沟通机制，推进标准立项和制定工作的科学、高效、有序进行；发挥主机厂安全主体责任，将主机厂已经落地的安全标准或好的做法吸纳进入行业或国家标准草案，推动网络安全指南与安全测评等急需标准的研究制定，为汽车网络安全产业发展提供全局性的标准化支撑。

（3）促进网络安全与汽车全生命周期的深度融合，推动汽车电子系统网络安全指南等标准验证与实施。汽车智能化、网联化发展使得电子信息产品各阶段贯穿于整车生命周期，汽车网络安全在根本上取决于汽车电子系统的网络安全防护能力。依据汽车电子概念设计、产品研发、测试验证、生产运行、运维服务、废弃处理等生命周期阶段划分，推动网络安全活动与汽车电子系统全生命周期深度融合，逐步形成覆盖软件与硬件、系统与应用、终端与服务等层面的全生命周期安全模型，整体提升汽车网络安全防护能力。同时，建议各领域企业建立评估试点，从安全管理、安全支撑、安全生命周期、供应链管理等方面组织开展汽车网络安全评估和风险防护活动。启动汽车电子系统网络安全指南等重点标准的验证实施工作，针对现有管理状态与防护技术，分析制约达标的关键因素，提出标准制修订建议，提升汽车电子网络安全标准应用适用性与实施有效性。

（4）搭建汽车电子网络安全测试平台，推动汽车电子行业供应链安全管理和可信机制的建立。从用户角度，整车制造商应保障汽车整体安全性，标准化工作应支撑促进整车制造商解决汽车制造产业链的安全可信问题。每个联网汽车都可看作一个多元素复杂的集成系统，系统的可信赖性取决于对所有主体厂商的信任，各厂商通过将信任要求制定为系统规范的一部分向上保证支撑或向下渗透分解，从而促使信任机制的建立。通过覆盖汽车电子网络安全技术要求、测评指标、测评方法等内容，搭建检测环境，推动建设中立可信的汽车电子网络安全测试平台。建议各主体厂商加强关键防护技术的标准化应用与实践，重点针对汽车电子网络产品和服务在设计开发、安装测试、使用维护和转让废弃等过程进行安全测试与验证

能力建设，降低汽车潜在攻击的影响。通过建设开放的汽车信息安全检测实验室，为小众化的安全公司、民间白帽子等提供测试资源，促进汽车行业与互联网、通信、金融等行业的融合。

缩略语

ADAS	先进驾驶辅助系统	Advanced Driver Assistant System
AES	高级加密标准	Advanced Encryption Standard
API	应用编程接口	Application Programming Interface
BLE	低功耗蓝牙	Bluetooth Low Energy
CA	证书认证	Certificate Authentication
CAICV	中国智能网联汽车产业创新联盟	China Industry Innovation Alliance for the Intelligent and Connected Vehicles
CAN	控制域网络	Control Area Network
CanIf	CAN接口	CAN Interface
CanTp	CAN传输协议	CAN Transport Protocol
CCSA	中国通信标准化协会	China Communications Standards Association
CEN	欧洲标准化组织	Comité Européen de Normalisation
DAC	数字模拟转换器	Digital to analog converter
DNS	域名系统	Domain Name System
DSRC	专用短程通信	Dedicated Short Range Communication
ECC	椭圆曲线密码	Elliptical Curve Cryptographic
ECU	电子控制单元	Electronic Control Unit
ETSI	欧洲通信标准化协会	European Telecommunications Standards Institute
Flash	闪存	Flash EEPROM
Flex Ray	高速实时总线协议	FlexRay Consortium
FrIf	FlexRay接口	FlexRay Interface
FrTp	FlexRay传输协议	FlexRay Transport Protocol
GPS	全球定位系统	Global Position System
HSM	硬件安全模块	Hardware Security Module
IDS	入侵检测系统	Identification Section
IHU	车载中控屏	Infotainment Head Unit
ISO	国际标准化组织	International Organization for Standardization

ITS	智能交通系统	Intelligent Transport System
ITU-T	国际电信联盟电信标准分局	International Telecommunication Union-Telephone
IVI	车载专用中央处理器	In-Vehicle Infotainment
KM	密钥管理系统	Key Management
LDAP	轻量目录访问协议	Lightweight Directory Access Protocol
LIN	局域互联网络	Local Interconnect Network
MAC	媒体访问控制	Media Access Control
MCU	微控制单元	Micro-Control Unit
NFC	近场通信	Near Field Communication
NHTSA	美国交通部道路交通安全管理局	National Highway Traffic Safety Administration
NVM	非易失性存储器	Non-Volatile Memory
OBD	车载诊断系统	On-Board Diagnostic
OBU	车载单元	On-Board Unit
OCSP	在线证书状态协议	Online Certificate Status Protocol
OEM	原始设备制造商	Original Equipment Manufacturer
OS	操作系统	Operating System
OTA	空中下载技术	Over-The-Air
PAN	个人局域网	Personal Area Network
PDU	协议数据单元	Protocol data unit
PKI	公钥基础设施	Public Key Infrastructure
PRNG	伪随机数生成器	pseudo Random Number Generator
RA	证书注册系统	Registration Authority
RAM	随机访问存储器	Random Access Memory
RISC	精简指令集计算机	Reduced Instruction Set Computer
ROM	只读存储器	Read-Only Memory
RTOS	实时操作系统	Real Time Operating System
SA	安全服务处理	Security Association
SAC	全国信息技术安全标准化技术委员会	Standardization Administration of the People's Republic of China

SAE	国际自动化工程师学会	Society of Automotive Engineers
SDK	软件开发工具包	Software Development Kit
SHE	安全硬件扩展	Secure Hardware Extension
SPI	串行外设接口	Serial Peripheral Interface
SSL	安全套接层协议	Secure Sockets Layer
STRIDE	微软提出的结构化，定性的安全方法，以发行软件系统存在的威胁位	Spoofing/Tampering/Repudiation/Information Disclosure/Denial of Service/Elevation of Privilege
SVS	签名验证服务器	Sign & Verify Serve
T-BOX	智能网联汽车的通信网关	Telematics BOX
TCU	终端控制器	Terminal Control Unit
TEE	可信执行环境	Trusted execution environment
TIAA	车载信息服务产业应用联盟	Telematics Industry Application Alliance
TP	传输协议	Transport Protocol
TRNG	真随机数生成器	True Random Number Generator
TSM	可信服务管理器	Tivoli Storage Manager
TSP	汽车远程服务提供商	Telematics Service Provider
TUI	可信用户界面	Text User Interface
UART	通用异步收发器	Universal Asynchronous Receiver and Transmitter
UI	用户界面	User Interface
UICC	通用集成电路卡	Universal Integrated Circuit Card
UMTS	通用移动通信网络	Universal Mobile Telecommunications System
UMTS	通用移动通信系统	Universal Mobile Telecommunication System
UN TFCS	联合国工作组	United Nations

参考文献

[1] 中华人民共和国网络安全法，2016

[2] 工业和信息化部. 国家车联网产业标准体系建设指南（总体要求）（征求意见稿），2017年9月

[3] 工业和信息化部. 国家车联网产业标准体系建设指南（智能网联汽车），2017年12月

[4] 工业和信息化部. 国家车联网产业标准体系建设指南（信息通信）（征求意见稿），2017年9月

[5] 工业和信息化部. 国家车联网产业标准体系建设指南（电子产品和服务）（征求意见稿），2017年9月

[6] 中国信息通信研究院. 车联网网络安全白皮书，2017年9月

[7] HIS. Secure Hardware Extension Functional Specification. 2009

[8] OVERSEE Project. https://www.oversee-project.com/

[9] SAE J3061. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. 2016

[10] SAE J3101. Requirements for hardware protected security for ground vehicle applications.

[11] EVITA Project. http://www.isi.fraunhofer.de/isi-de/t/projekte/fri-evita.php

[12] AUTOSAR. AUTOSAR Foundation Release Overview. 2016

[13] AUTOSAR. AUTOSAR Classic Platform Release Overview. 2016

[14] PRESERVE Project. https://www.preserve-project.eu/

[15] ETSI. ETSI TS 102 731 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Security; Security Services and Architecture.

[16] ETSI. ETSI TS 102 940 V1.2.1 (2016-11) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.

[17] ETSI. ETSI TS 102 941 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

[18] ETSI. ETSI TS 102 942 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Access Control.

[19] ETSI. ETSI TS 102 943 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Confidentiality services

[20] NHTSA. Cybersecurity Best Practices for Modern Vehicles. 2016

[21] WP.29 ITS/AD. Guidelines on measures ensuring cyber security and data protection of connected vehicles and vehicles with automated driving technologies. 2016

[22] ISO. 27001 – Information security management system.

[23] NIST. 800-30 - Guide for conducting risk assessments.

附录A

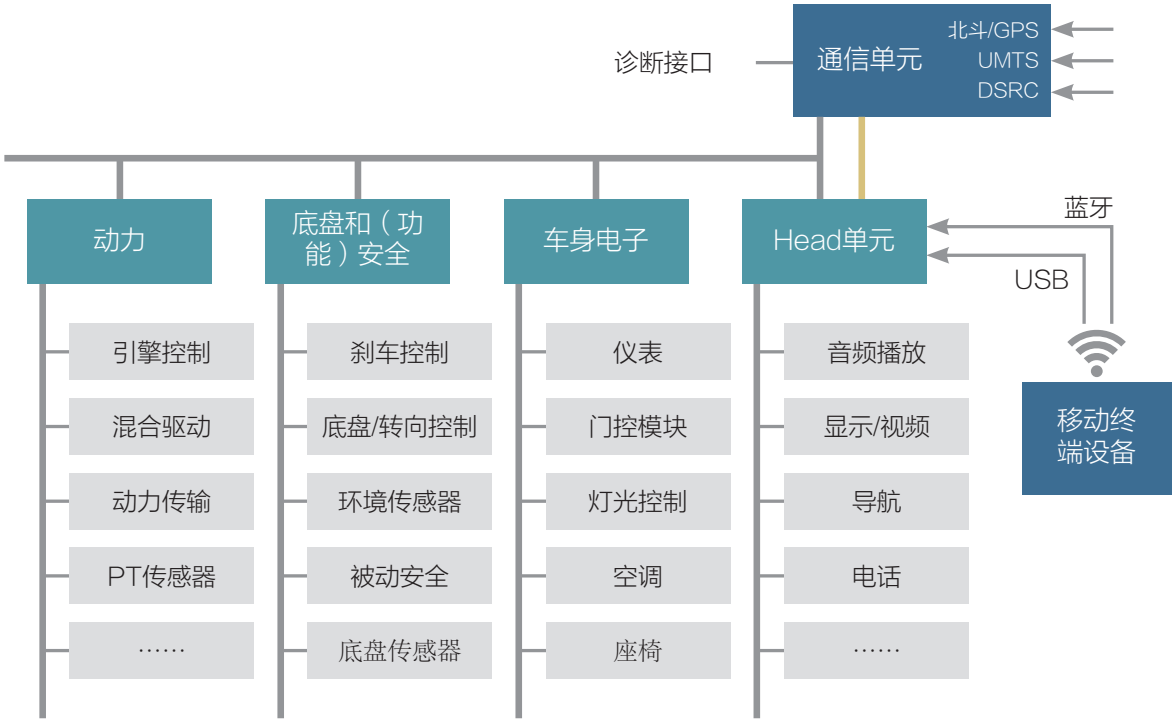
汽车电子网络安全行业应用实践

本部分主要列举了国外部分行业应用安全实践内容，供相关方学习参考。

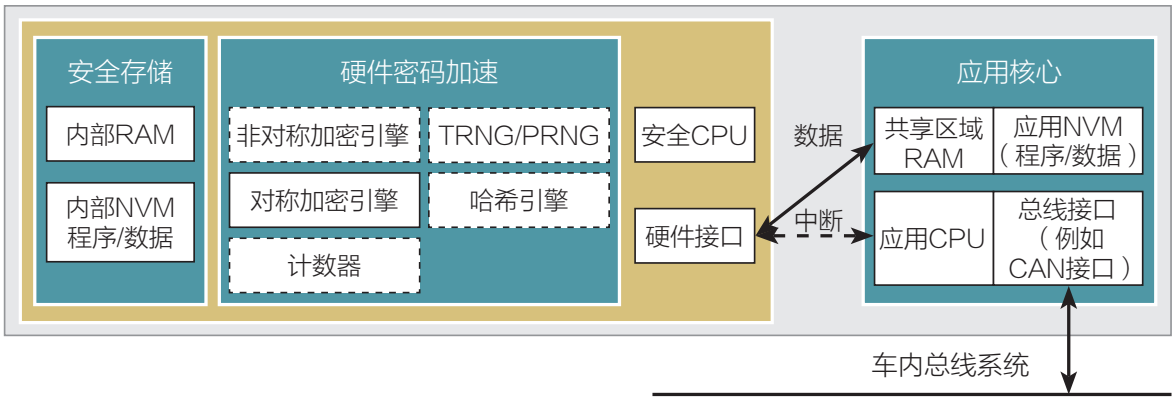
附录A1 EVITA：安全车辆入侵保护应用

EVITA（E-safety vehicle intrusion protected applications）是欧盟第七框架计划（Seventh Framework Programme）资助的项目（2008-2011），旨在为车载网络的体系架构进行设计、验证、形成原型，以防止安全相关的组件被篡改，并保护敏感数据以免受到攻击。项目的主要参与机构包括：BMW Group Research and Technology GmbH、Continental Teves AG & Co. oHG、escrypt GmbH、EURECOM、Fraunhofer Institute for Secure Information Technology、Fraunhofer Institute for Systems and Innovation Research、Fujitsu Services AB、Infineon Technologies AG、· Institut Télécom、Katholieke Universiteit Leuven、MIRA Ltd.、 Robert Bosch GmbH、TRIALOG等。

EVITA关于车载网络的参考架构如图附A1-1所示，主要包括三方面的资产：车载电子组件，如ECU、传感器、执行器等；组件之间和ECU内部的连接；ECU中的软件。EVITA以基于硬件的安全机制为目标，主要对作为信任根的硬件安全模块（Hardware Security Module）进行了研究，所提出的面向汽车硬件安全模块的通用结构如图附A1-2所示。图中，ECU的应用CPU拥有一个密码协处理器HSM。HSM负责执行所有密码应用，包括基于对称密钥的加解密、完整性检查、基于非对称密钥的加解密、数字签名的创建与验证，以及用于安全应用的随机数生成功能。



图附A1–1 EVITA关于车载网络的参考架构

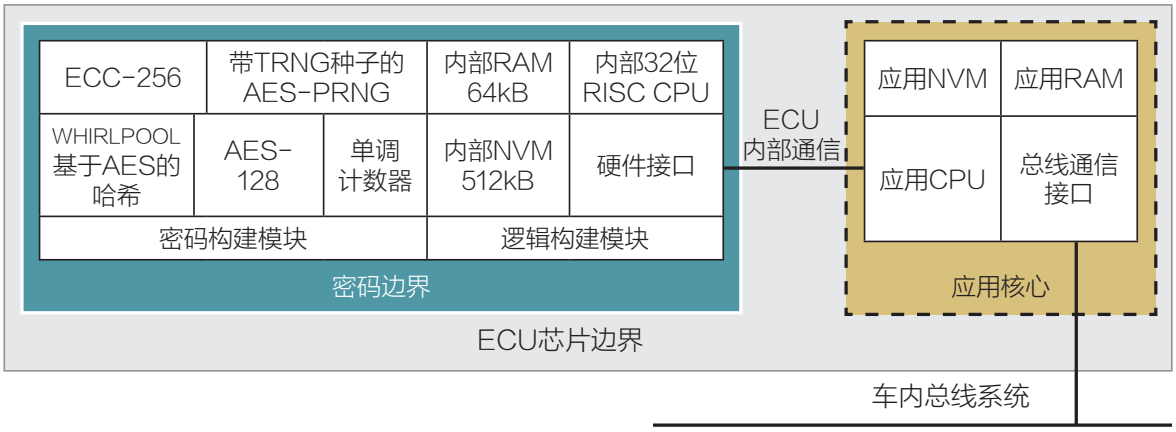


图附A1–2 EVITA关于HSM的基本结构

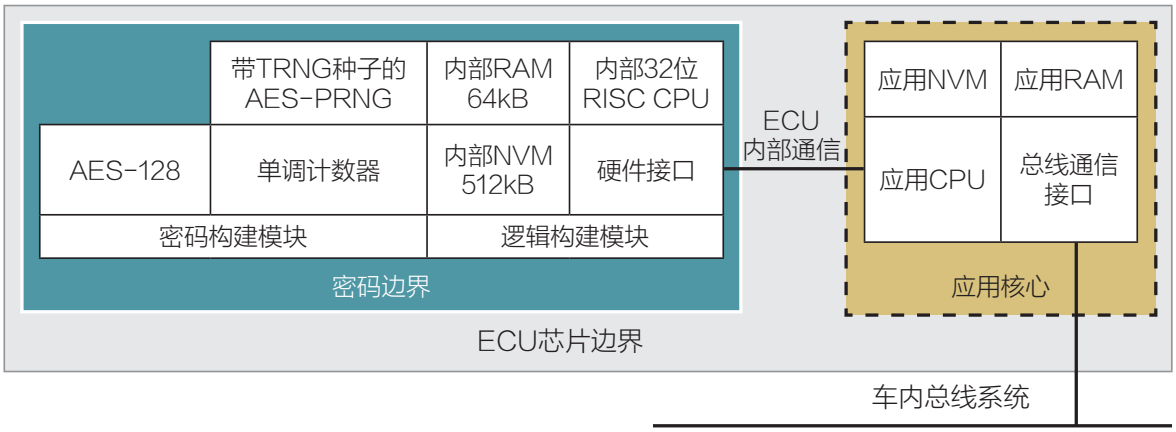
EVITA把硬件安全模块划分为三个等级：EVITA full HSM、EVITA medium HSM、EVITA light HSM（或是EVITA small HSM）。其中，EVITA full HSM主要用于V2X的通信单元，以及中央网关；EVITA medium HSM用于ECU之间通信场景的ECU；EVITA light HSM则用于传感器、执行器。

EVITA full HSM、medium HSM和light HSM的结构分别如图附A1-3~5

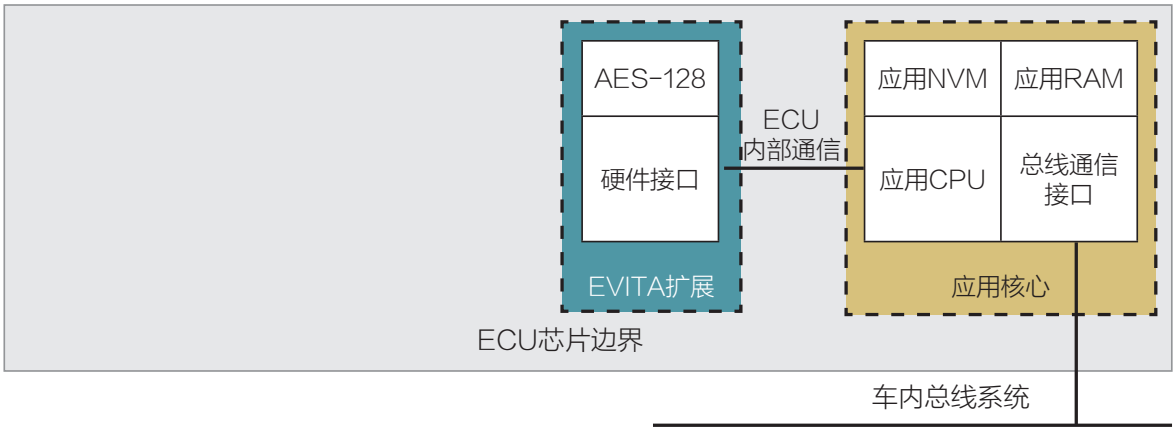
所示。另外，EVITA HSM包括两部分内容：实现所有密码硬件操作的密码模块；连接EVITA 硬件和通常ECU应用模块的内容。



图附A1–3 EVITA full HSM的结构



图附A1–4 EVITA medium HSM的结构

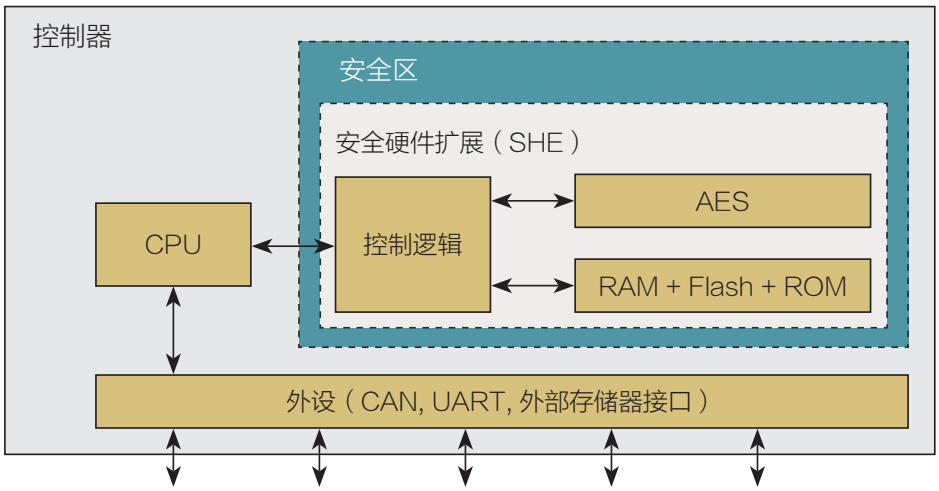


图附A1–5 EVITA light HSM的结构

与full HSM相比，medium HSM没有包括ECC-256和WHIRLPOOL 密码模块（NIST提出的基于AES 的hash函数），并且，medium HSM所包含的CPU性能要低一些。因此，medium HSM没有基于硬件加速的非对称密码和哈希算法。一方面，可以通过软件的方式来执行一些时间性能要求不高的非对称密码操作；另一方面，基于效率和成本方面的考虑，ECU之间通信的保护采用对称密码算法具有合理性。

light HSM只包含基于AES-128的对称加解密模块，以满足传感器和执行器在成本和效率方面的严格需求（消息大小、时间、协议限制、处理器能力等）。基于light HSM，使得传感器和执行器能够保证通信数据的真实性、完整性和机密性。另外，同full和medium HSM相比，light HSM没有提供独立的处理和存储单元，应用处理器和应用软件可以完整访问所有的密码数据。为此，可以考虑对light HSM进行安全增强，提供内部的非易失性存储器和RAM，以及基于AES的伪随机数生成器。这样，light HSM可以更加安全地生成、处理和存储密钥。

除EVITA外，还有SHE、TPM（Trusted Platform Module）和智能卡（smartcard）等方面的硬件安全策略。SHE（Secure Hardware Extension）是由HIS（由Audi、BMW、Porsche、Volkswagen形成的组织）制定的标



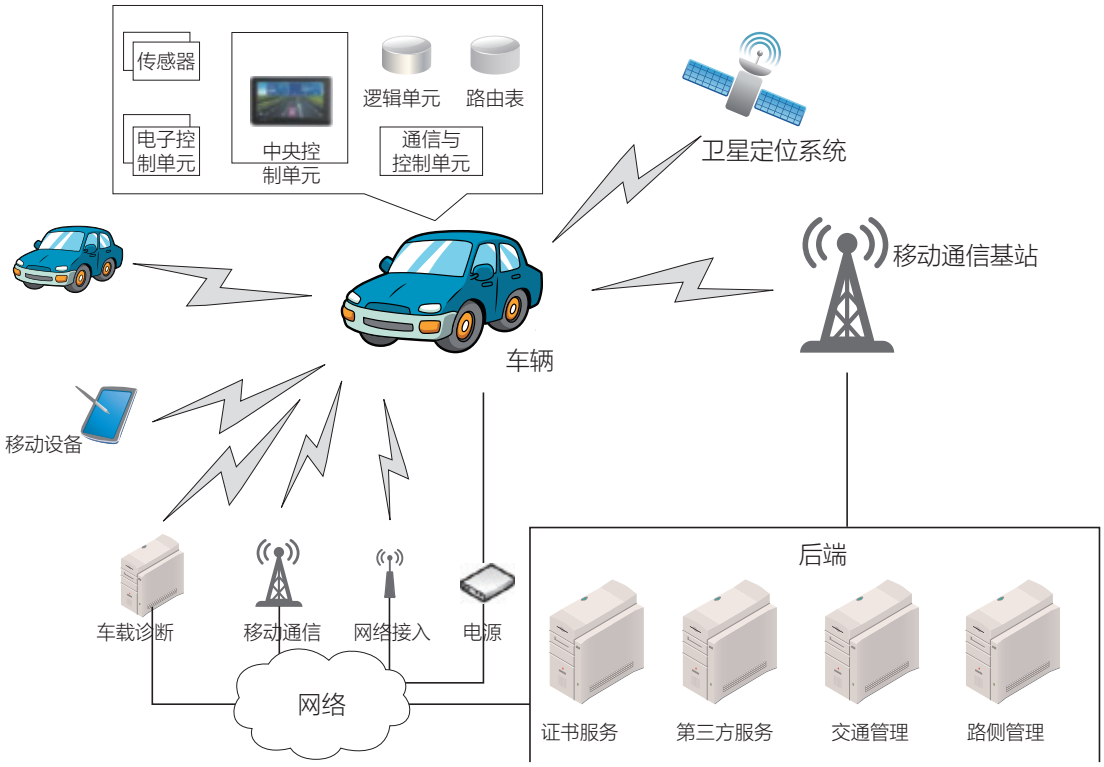
图附A1–6 SHE的基本结构

准，以通过硬件提供基于AES-128的密码服务：加解密；消息认证码；引导加载程序的认证；唯一的设备ID等，并可以应用不可直接访问的方式存储密钥。SHE的基本结构如图附A1-6所示。

附录A2 PRESERVE：V2X安全通信系统

PRESERVE（PREparing SEcuRe VEhicle-to-X Communication Systems）是欧盟第七框架计划资助的项目（2011-2015），目标是设计、实现和测试一个安全、可扩展的V2X安全子系统。项目包含如下参与单位：University of Twente (coordinator)、荷兰；Escrypt GmbH (SME)、德国；Fraunhofer SIT、德国；Kungliga Tekniska Hoegskolan (KTH)、瑞典；Renault、法国；Trialog (SME)、法国。

PRESERVE为V2X通信提供接近于实际应用的安全和隐私保护措施，为V2X系统提供安全和隐私子系统。PRESERVE以SeVeCom、EVITA、PRECIOSA等项目的成果为基础，并与ETSI（European Telecommunications Standards Institute）、IEEE（Institute of Electrical and Electronics Engineers）、C2C-CC）（Car-to-Car Communication Consortium）等方面的标准兼容。

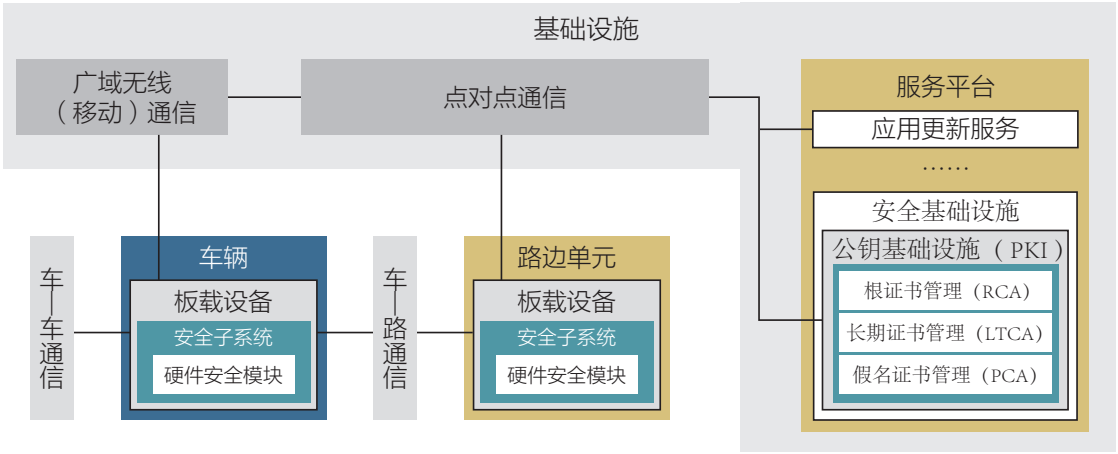


图附A2–1 PRESERVE的ITS系统

PRESERVE以下图所示的智能交通系统（Intelligent Transportation System，ITS）为背景。其中，Routing Table（Network layer routing table）存放相邻节点的位置信息，包括节点最近更新的时间戳；LDM（Local Dynamic Map）用来收集和管理所有收到的消息，相关信息与交通安全性和交通效率有关；CCU（Communication & Control Unit）是不同通信链路的中央路由器，比如ITS G5A/B/C 等。

PRESERVE的车辆安全架构主要包括ITS通信的三个组成部分：车辆（Vehicle Station）、路侧设施（Roadside Station）和后台服务（Central Station），如图附A2-2所示。其中，通信的参与方和通信通道来源于美国交通部和ETSI关于ITS的体系架构。另外，车辆包括运行ITS应用的车载单元（On-board Unit，OBU）、通信设施（如无线电、通信栈等）和与车载网络的连接。安全子系统为车载通信和外部的V2X通信提供保护，并通过硬件安全模块（HSM）存储密码证书、加速密码算法。路侧设施与车辆具有相同的架构，为车辆通信和固定点之间的通信提供网关功能。后台服务主要关注安全应用服务（为车辆和路侧设施提供软件）和安全体系架构（提供安全的证书服务，如PKI体系）。

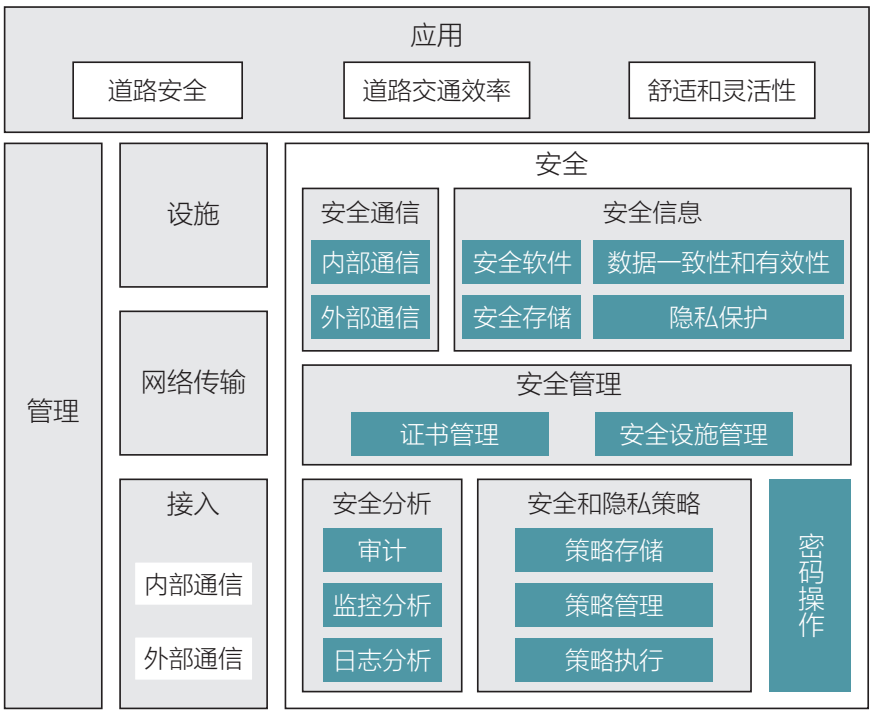
PRESERVE为车辆和路侧设施提供的抽象安全架构（PRESERVE VSA）如图附A2-3所示。PRESERVE VSA的多数内容来源于SeVeCom、



图附A2–2 PRESERVE的ITS体系架构

EVITA、PRECIOSA等项目，为V2X和内部通信提供安全保障。PRESERVE VSA把安全功能分为六个方面：安全通信（Secure Communication）、安全信息（Secure Information）、安全管理（Secure Management）、安全分析（Secure Analysis）、安全和隐私策略（Security & Privacy Policies）、密码算法（Cryptographic Operations）。

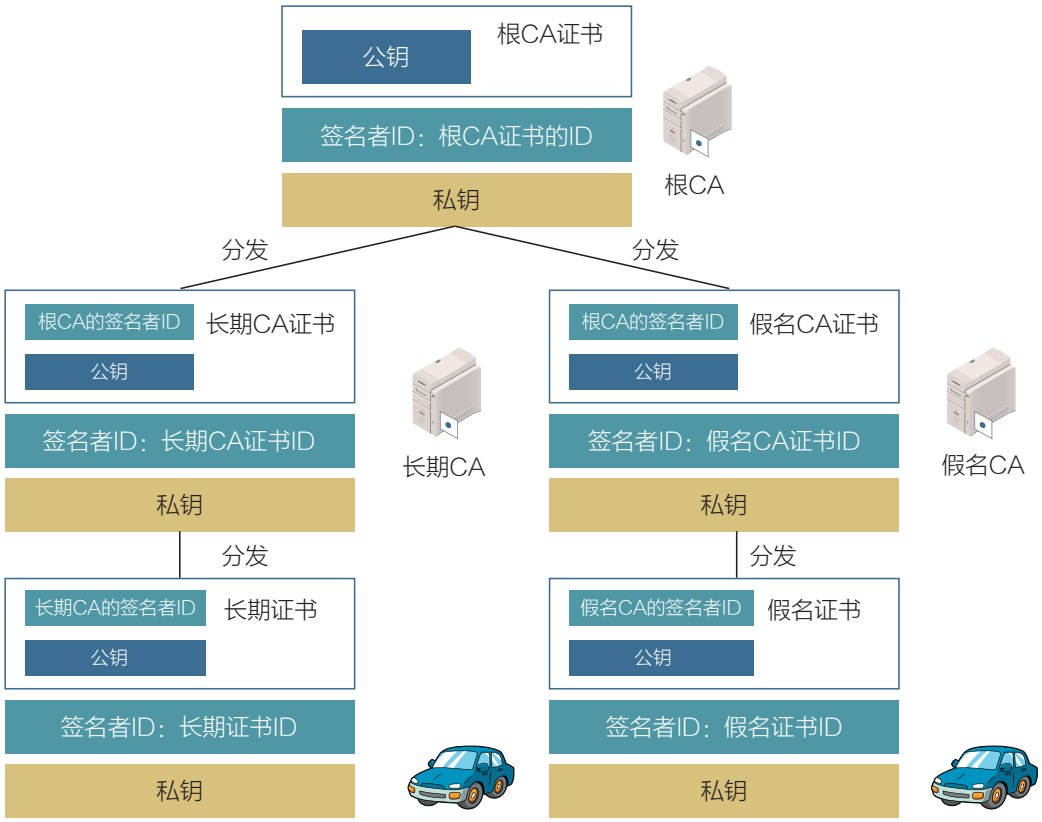
安全通信关注内部和外部的安全通信问题。对于内部通信，如传感器数据、命令和信号等，需要进行安全传输以确保数据不会被篡改；对于外部通信，接收方至少需要验证发送方的真实性和授权特性，以及所传输数据的完整性。安全信息对车辆和路侧设施存储、交换的数据进行保护，包括安全存储、安全软件、隐私保护、数据一致性、数据合理性。安全管理负责对安全通信所需要的证书进行组织管理。安全分析对安全相关的信息进行监控、审计和日志。安全和隐私策略负责管理、存储和执行安全和隐私方面的策略，定义系统资源的访问控制规则、管理匿名和其他隐私保护策略。密码算法提供基本的安全功能，如加解密、签名的生成与验证等。



图附A2–3 PRESERVE的车辆/路侧设施抽象安全体系架构

PRESERVE的具体安全架构以SeVeCom、EVITA、PRECIOSA等项目的成果为基础进行构建，其内容包括车辆或是路侧设施的系统安全，为车辆或是路侧设施的内部通信提供保护；为车辆和路侧设施提供驾驶人员或是拥有人员的隐私保护机制；以及为V2X通信提供消息保护。

在PRESERVE中，消息发送和消息接收方采用基于PKI的数字证书来保障通信的可信性，如图附A2-4所示，主要包含三个实体：根CA（Root Certificate Authority，RCA）、长期CA（Long-Term Certificate Authority，LTCA）、匿名CA（Pseudonym Certificate Authority， PCA）。RCA是PKI的信任锚（trust anchor），RCA的证书由RCA自身签名，对证书通过hash函数生成摘要，作为证书ID：cert-ID；LTCA负责管理ITS系统的长期证书；PCA负责管理ITS系统的匿名证书。PCA用于V2X通信，以保证V2X通信过程的匿名特性，达到保护车辆隐私的目的。



图附A2–4 V2X PKI的证书体系

附录A3 现代汽车网络安全最佳实践

2016年10月，美国高速公路交通安全管理局（NHTSA）发布了一份《现代汽车网络安全最佳实践》（Cybersecurity Best Practices for Modern Vehicles）（以下简称“最佳实践”），是继9月份发布的《自动驾驶汽车政策》之后，对“智能网联汽车”发布的又一重要指导性文件。“最佳实践”全文分为九大部分，包括目的、使用范围、背景、定义、通用性网络安全指导、汽车工业网络安全指引、网络安全教育、后装设备、车辆维护可用性。

为减轻车辆网络安全威胁给用户带来的功能安全风险及个人敏感信息泄露危险，NTHSA代表美国交通部积极参与车辆网络安全研究，积极推动加强车辆网络安全保护，努力提升车辆网络空间安全能力。NTHSA前期采取的措施还包括2015年督促克莱斯勒大规模召回存在网络安全隐患的吉普自由光汽车、2016年向美国国会提交一份关于客运机动车辆电子系统防止非法入侵的安全措施提案、2016年召集由OEM、政府机构、行业协会等广泛参与的公共车辆网络安全圆桌会议等，前期NHTSA还建立了汽车信息共享与分析中心。

“最佳实践”开篇阐明了发文的原因，即由于美国现行的汽车安全标准中没有包括“网络安全”的内容，而汽车作为网络安全的“物理载体”，其网络安全的脆弱性与人身安全和公共安全息息相关。“最佳实践”适用者为制造、设计汽车系统或软件的个人和组织，包括汽车设备设计方、供应商、制造商和改装企业等。

“通用性网络安全指导”一章提出了“分层方法”和“IT安全控制”两个内容。NHTSA认为，针对车辆网络安全的分层方法能够降低网络入侵的成功率并减轻非授权访问带来的不良后果。分层方法须建立在汽车工业遵循美国国家标准与技术研究所制定的“网络安全框架”提出的“识

别、保护、检测、响应和恢复”五项主要功能要求基础上，其具体内容包括：

（1）建立基于风险的车辆安全关键控制系统和个人可识别信息的优先识别和保护策略；

（2）提供及时发现和快速响应机制应对潜在的车辆网络安全事件；

（3）设计安全恢复方法和措施应对车辆网络安全事故的发生；

（4）将车辆网络安全事件信息采集工作制度化，通过行业内有效的信息分享，加速吸取行业内车辆网络安全事件教训。

在“IT安全控制”中，NHTSA认为汽车工业应学习借鉴已在金融、能源、通信等行业中广泛采用的CIS CSC（Critical Security Controls for Effective Cyber Defense，针对有效网络防御的关键安全控制）方法，尤其是需要特别关注CIS CSC提到的20个高优先级网络安全防护点。此外，“IT安全控制”还建议汽车工业采用CIS CSC推荐的下列网络安全控制方法：

（1）执行网络安全差距评估流程；

（2）制定实施路线图；

（3）有效和系统地执行网络安全计划；

（4）将网络安全控制集成到车辆系统并在业务操作过程中实行；

（5）在重复周期内执行流程监控和报告制度。

“汽车工业网络安全指引”为“最佳实践”中最为重要的环节，提出汽车开发流程里需要有明确的网络安全考量，例如考虑采用SAEJ3061推荐的《信息物理汽车系统网络安全指南》。在产品的网络安全防护方面，NHTSA建议汽车企业在开发或集成车辆的安全关键系统时，需要优先考虑车辆网络安全并从组织管理上给予保障，具体建议包括：

（1）在组织内，安排专门的队伍和资源，研究、分析、测试、验证产品网络安全方面的防护措施及其脆弱性；

（2）建立快速（与公司各关联方）沟通渠道，应对产品网络安全事务；

（3）在汽车安全设计流程中，需要允许汽车网络安全考量作为独立意见影响产品设计。

依据美国“行政命令 13691”（EO 13691），要求国土安全部（DHS）促进网络安全信息共享，大力鼓励信息共享和分析组织 (ISAOs) 的发展。2015年，在NHTSA推动下，汽车行业的信息共享和分析组织Auto ISAC成立。与此同时，NHTSA还支持额外的信息共享机制，如漏洞报告和披露程序。这些措施已在其他行业有效，并将有利于汽车工业。NHTSA认为，汽车行业成员应考虑创建自己的漏洞报告/披露政策，或采用其他行业或技术标准中使用的政策，这些政策将最终指导任何外部的网络安全研究人员如何向汽车企业披露安全漏洞。

“脆弱性/漏洞利用/安全事件的响应流程”则要求车厂等汽车企业应对车辆网络安全的脆弱性/漏洞利用/安全事件等问题，需要有文档化的流程，并且流程中必须包括影响评估、控制、恢复、补救措施以及相关测试等内容。在“Self-auditing(自审计)”中，NHTSA要求文档化以下内容以便审计和追责，包括：风险评估，渗透测试结果，组织决策。

“基础性车辆网络安全保护措施”来源于NHTSA的相关研究及汽车行业经验分享，被NHTSA认为是汽车企业需要重点实施的车辆网络安全防护措施，其具体包含了11项内容：

（1）ECU开发者调试接口访问限制：软件开发者有很多途径访问ECU，例如通过一个开放的调试端口或者串行控制台。但是，这样的访问应该被限制，特别是当开发者没有对ECU持续访问的可预见的操作原因时，访问应该被拒绝。而如果持续的开发者访问是必要的，那么任何开发者级调试接口应该得到适当的保护，即仅限制于访问授权的特权用户。此外，物理上隐藏用于开发调试访问的连接器、针脚等不应被视为接口被安全保护的充分形式。

（2）密钥/密码安全保护：任何能提供车辆系统平台访问能力的密钥

或密码应该被安全保护以防泄露。同时，从单个车辆系统平台获得的任何密钥不应能够用于访问其他车辆。

（3）诊断访问限制：诊断操作需要尽可能施加较多的限制措施，例如限制某个诊断操作的影响范围或时间。另一方面，诊断操作应被设计为当其被滥用时能够最小化潜在的安全风险。

（4）固件恶意访问防护：ECU固件程序是常见的攻击目标。在固件程序开发过程中，需要实施安全代码开发等措施。同时，为防止固件程序被非授权分析，可以考虑对固件程序进行加密。此外，固件程序的升级过程中，也必须保证升级程序的机密性。

（5）固件恶意修改防护：限制修改固件的能力将使恶意固件程序被安装在车辆上更具挑战性。例如，使用数字签名技术可以防止汽车ECU启动被恶意修改/未经授权的固件程序。此外，采用数字签名技术的固件更新系统可以防止安装非授权方提供的软件更新。

（6）网络端口、协议和服务使用限制：汽车ECU上网络服务器的使用应仅限于其必要的功能，服务端口应加以保护以防止未经授权的使用。

（7）在汽车电子架构设计中使用分段和隔离技术：特权分离与边界控制能够提升系统安全性。逻辑和物理隔离技术应用于将处理器、车辆网络和外部连接分开，以限制和控制外部威胁到车辆内部的路径。而强大的边界控制技术，如严格的基于白名单的段间消息过滤机制，应被用于保障接口访问安全。

（8）车辆内部通讯控制：安全关键消息直接或间接影响着汽车安全关键控制系统的运行。因此，在公共数据总线上传递安全信号应该尽可能避免。如果安全关键信息必须在通讯总线上传输，则该信息应该在与连接外部网络的ECU隔离的通讯总线上传递。对于只能在非隔离的通讯总线上传输的安全关键消息，则需要实施消息验证策略，以防止消息诱骗。

（9）网络攻击事件日志：一个不能更改的事件日志能够充分揭示网

络安全攻击或成功入侵行为，因此，应该让具备资质的相关人员维护和定期审查网络攻击事件日志，以发现网络攻击态势。

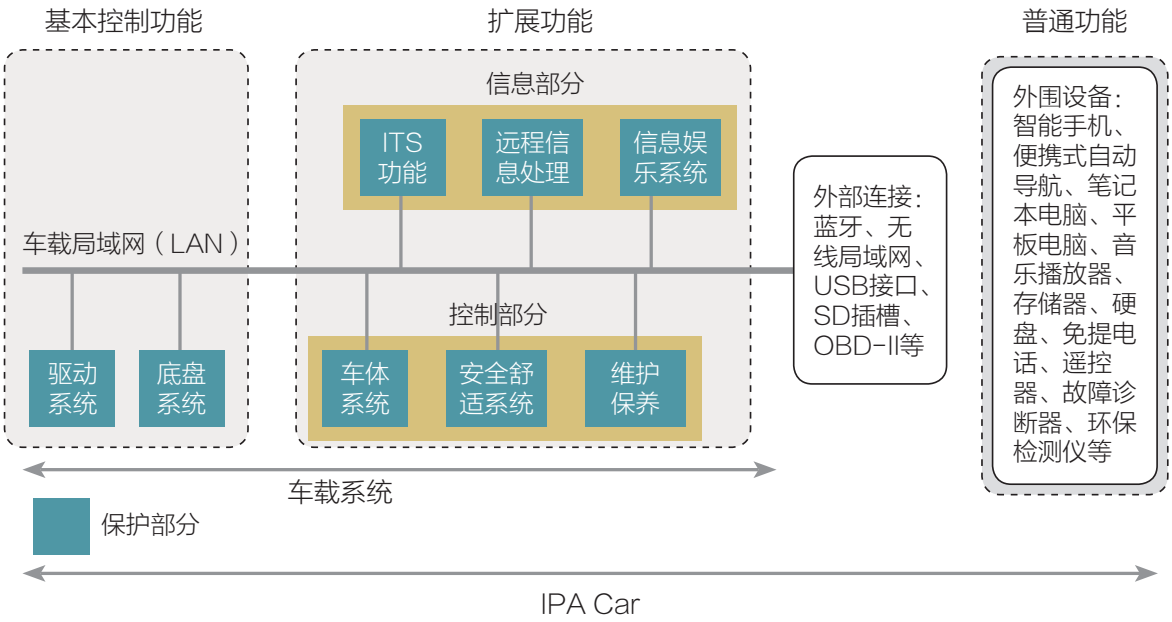
（10）后台服务器访问控制：加密措施应用于任何基于IP的外部服务器和车辆之间的业务通信过程中。与这些措施一致，此类网络连接不应接受无效证书。

（11）无线接口访问控制：在某些情况下，可能需要对车辆与蜂窝无线网络的连接施加细粒度控制。应该规划和设计可以使网络路由规则变化迅速传播和应用到单个的、一个子集的或所有的车辆的相应功能。

“最佳实践”最后还阐述了网络安全培训教育的基本原则方法，并指出消费者后装设备对于车辆信息物理系统可能的安全风险，最后强调了汽车工业还应考虑授权的第三方对车辆部件和系统的可维护性。

附录A4 日本汽车信息安全模型

日本在2013年就通过日本信息处理推进机构（IPA）发布了汽车信息安全指南《Vehicle information security guide》。IPA通过分析与汽车网络安全相关的攻击方法，提出直接攻击、从外围产品入侵、从外部网络攻击共三种汽车网络攻击途径。指南中定义了汽车信息安全模型（IPA Car），IPA Car模型对可能攻击汽车系统的途径、不同汽车功能模块的信息安全对策等做出了系统的整理。



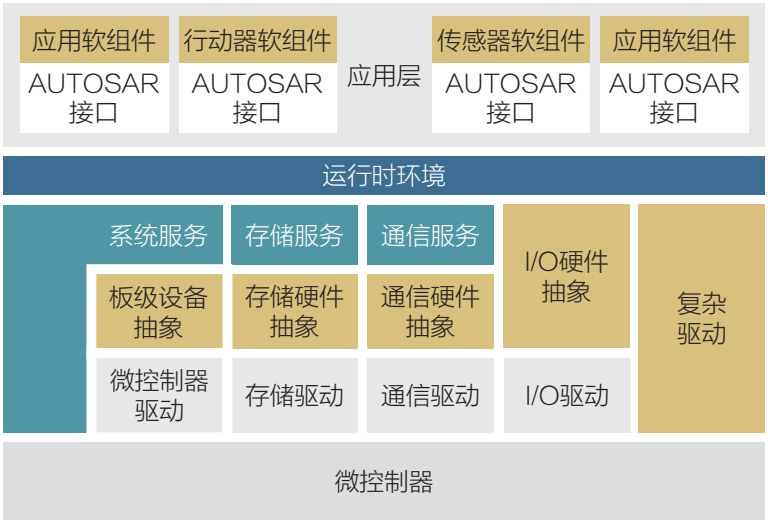
图附A4-1 汽车信息安全模型（IPA Car）

附录A5 AUTOSAR

AUTOSAR（AUTomotive Open System ARchitecture）由宝马集团（BMW）、博世公司（Bosch）、大陆集团（Continental）、戴姆勒-克莱斯勒公司（DaimlerChrysler）、西门子威迪欧（Siemens VDO）汽车电子公司以及大众公司（Volkswagen）于2003年7月联合建立，旨在为汽车电气/电子构架开发一套开放的行业标准。AUTOSAR是汽车制造商、供应商和其他来自电子、半导体和软件方面公司的联盟，以模块化、可扩展、可转换、可重用为目标，致力于为汽车电子控制单元定义层次化的基础软件架构。目前，AUTOSAR已经被国内外厂商广泛应用，成为ECU在基础软件方面的架构标准。

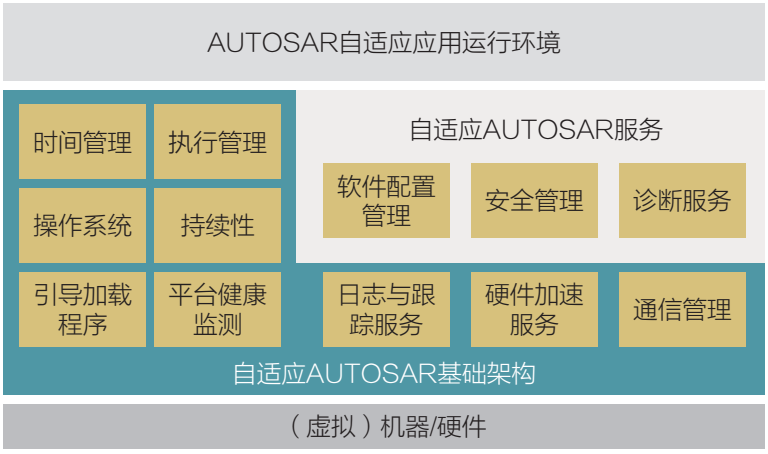
在发布4.2.2版本后，AUTOSAR的标准体系分为四个部分：基础标准（Foundation）、经典平台（classic platform）、自适应平台（adaptive platform）和符合性测试（Acceptance Tests）。其中，基础平台主要考虑AUTOSAR平台之间的互操作性，包括在AUTOSAR平台之间可以共享的公共需求和技术规格；经典平台用于满足具有硬实时和功能安全需求的嵌入式系统；自适应平台用于需要进行高性能计算需求的ECU，如高度自主驾驶的系统。

经典平台包括三个主要层次：应用（Application）、运行时环境（Runtime Environment）和基础软件（Basic Software），如附A5-1所示。其中，应用软件基本上与硬件无关；RTE表示面向应用的所有接口；基础软件分为三个主要层次（服务、ECU抽象和微控制器抽象）和一个复杂驱动（Complex Drivers）。在服务方面，又分为系统、存储和通信三个方面的内容。



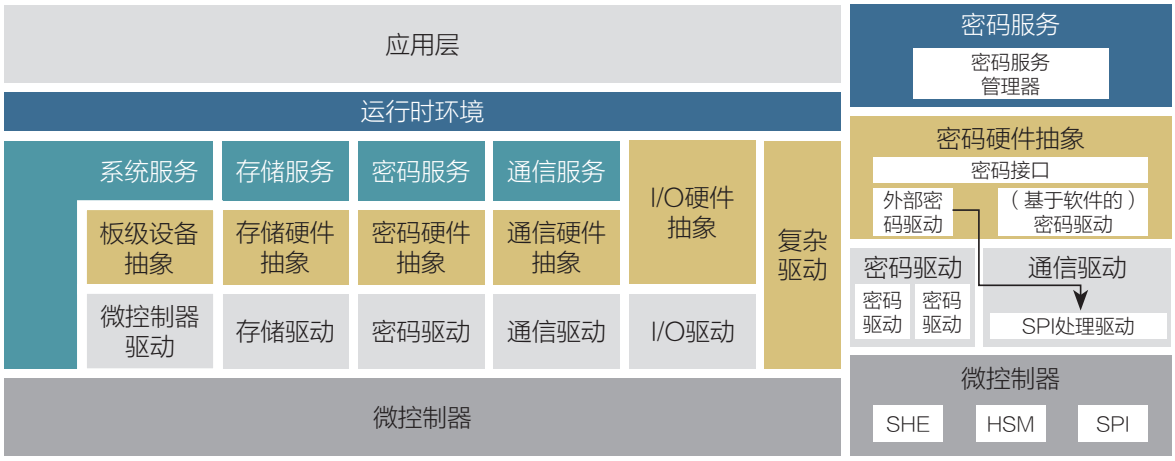
图附A5–1 AUTOSAR的经典平台

AUTOSAR自适应平台为自适应应用实现AUTOSAR运行时环境，提供两类接口：服务（services）和APIs，如图附A5-2所示。与经典平台相比，自适应平台在运行时实现客户端（clients）和服务端（services）的连接。



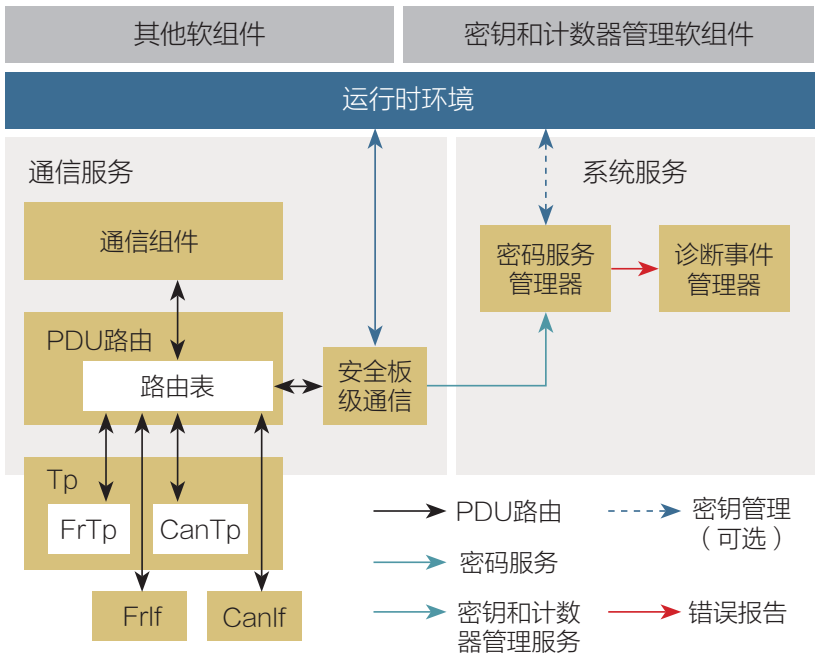
图附A5–2 AUTOSAR的自适应平台

在AUTOSAR经典平台中，以硬件安全模块为基础，提供了密码服务方面的层次架构，如图附A5-3所示。增加了密码方面的服务后，AUTOSAR经典平台的服务分为四个方面：系统、存储、密码和通信。同其他服务一样，密码服务分为三个层次：密码服务管理、密码硬件抽象和密码驱动程序。



图附A5–3 AUTOSAR经典平台的密码服务体系

此外，AUTOSAR经典平台还提供了安全通信方面的功能（SecOC，Secure Onboard Communication），如图附A5-4所示。SecOC在协议数据单元层面（PDUs）为关键数据提供可行、具有资源有效特性的真实性机制。SecOC与AUTOSAR的通信系统协同，PDU Router负责对接收的消息进行路由，对发送的安全相关协议数据单元提供给SecOC模块。SecOC随后增加或是处理安全相关信息后，把协议数据单元返回给PDU Router，由



图附A5–4 AUTOSAR经典平台的安全通信架构

PDU Router进行进一步的路由处理。此外，SecOC将使用密码服务体系提供的密码服务。

应该说，AUTOSAR软件平台为国内自主汽车嵌入式软件平台的研制提供了重要的参考，也在客观上促进了自主汽车软件的标准化和平台化的发展。

附录B

汽车电子网络安全技术应用案例

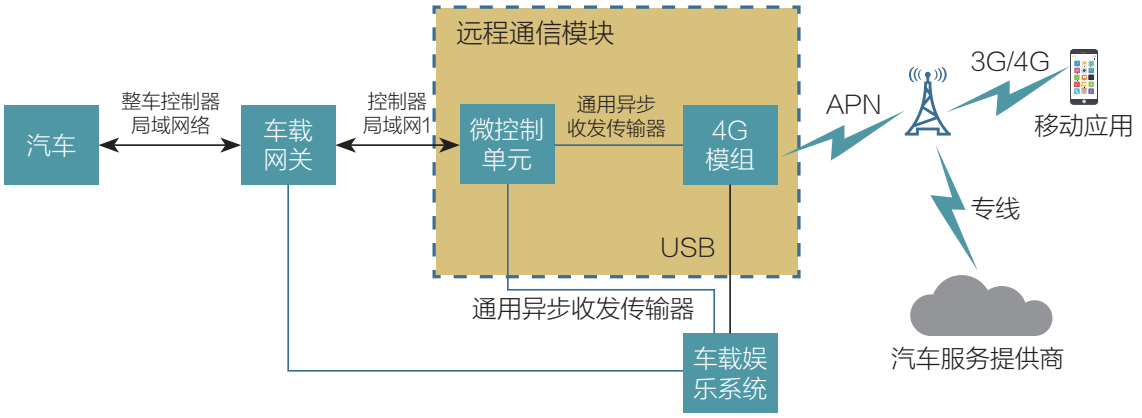
本部分是由部分厂商提供的网络安全技术在汽车电子中的应用案例，供相关方学习参考。

附录B1 T-BOX安全技术应用

概念：T-BOX全称Telematics BOX，主要用于和TSP平台/手机APP通信，是智能网联汽车的通信网关。T-BOX一方面可与CAN总线通信，实现指令和信息的传递，另一方面内置调制解调器，可通过数据网络、语音、短信等与车联网云平台交互，是车内外信息交互的纽带。

模块组成和功能：T-BOX主要由MCU和4G模块组成，MCU主要负责整车CAN网络数据接收与处理、信息上传、电源管理、数据存储、故障诊断以及远程升级等功能；4G模块主要负责网络连接与数据传递，为用户提供WIFI热点连接、为DA提供上网通道，同时为TCU与服务器之间的信息传递提供通道。

逻辑图：



安全威胁：T-BOX主要面临几方面的安全威胁：

一是协议破解，控制汽车的消息指令是在 T-BOX 内部生成的，并且是使用 T-BOX 的蜂窝网络调制解调器的扩展模块进行加密的，相当于在传输层面是加密，所以无法得到消息会话的内容，解决的方法就是需要通过分析固件内部的代码，找到加密方法和密钥，才能够知道消息会话的内容。所以需要对 T-BOX 进行拆解。然后把 FLASH 芯片吹下来，逆向固件。发现发送的控制指令，获取加密算法和密钥，解密通讯协议；

二是信息泄露，还有的一些T-BOX出厂的时候是留有调试接口的，这样就不需要吹 FLASH攻击者通过 T-BOX 预留调试接口就可以读取内部数据了；

三是中间人攻击，攻击者通过伪基站、DNS 劫持等手段劫持 T-BOX 会话，进一步伪造协议而实施对汽车制动装置的控制。

安全技术应用：

T-BOX硬件安全的目的是确保车机硬件中的系统程序、终端参数、用户数据及敏感数据等不被篡改或非法获取。

系统安全层面对T-BOX系统的启动、升级、恢复及访问进行保护和限制。结合T-BOX总线接口的设计方案对总线的指令通道进行正向保护并通过旁路监控的方式保护总线接口的调用安全。同时建立系统分区、文件系统及服务的监控机制及最小功能开发，保障T-BOX操作系统安全运行。

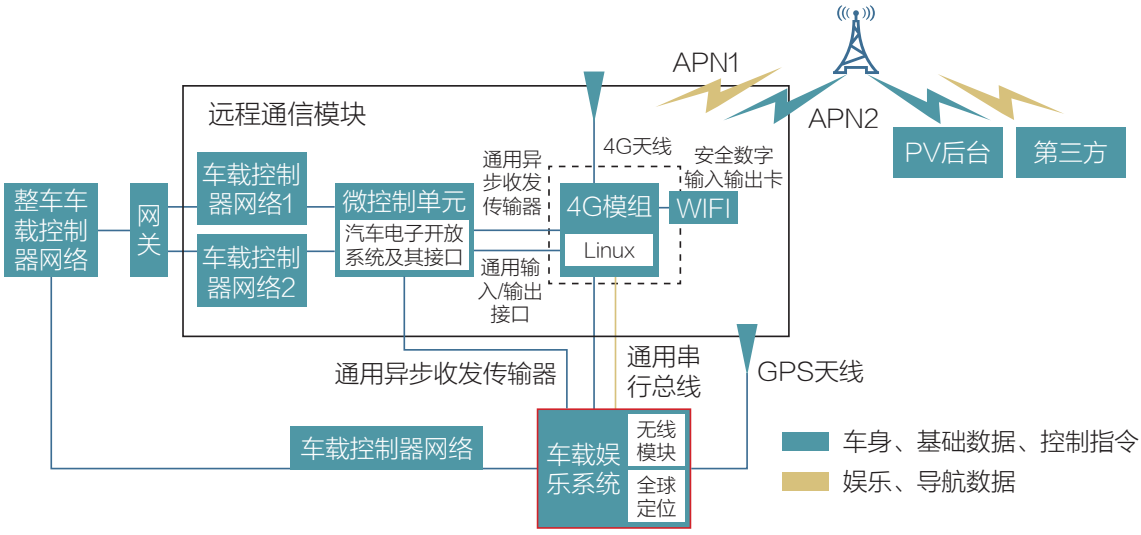
T-BOX应用安全层面的安全目标一方面要保证车机自身应用的安全，不被劫持、篡改。另一方面应建立起三方应用的准入机制，对车机应用生态系统进行保护。同时通过应用监控措施实时对系统中的应用程序的活动行为、网络流量、权限等进行监控，保障车机应用生态系统安全。

附录B2 车载信息娱乐系统安全技术应用

概念：车载信息娱乐系统是采用车载芯片，是采用车载专用中央处理器，基于车身总线系统和互联网服务，形成的车载综合信息娱乐系统。

模块组成和功能：车载信息娱乐系统能够实现包括三维导航、实时路况、IPTV、辅助驾驶、故障检测、车辆信息、车身控制、移动办公、无线通讯、基于在线的娱乐功能及TSP服务等一系列应用，极大的提升了车辆电子化、网络化和智能化水平。

逻辑图：



威胁分析：车载信息娱乐系统基于嵌入式操作系统或移动操作系统架构，提供的攻击面比其他任何车辆部件都广，对车载信息娱乐系统的攻击也可分为软件攻击和硬件攻击。软件攻击跟传统网络安全威胁相同：一是系统本身可能存在内核漏洞，例如 WinCE、Unix、Linux、Android、iOS 等均出现过内核漏洞，其迁移操作系统也存在系统漏洞风险；二是系统存在被攻击者安装恶意应用的风险,可能影响车载信息娱乐系统功能的可用性；三是第三方应用可能存在安全漏洞，存在信息泄露、数据存储、应用鉴权等风险。

此外，车载信息娱乐系统的底层可信引导、系统层证书签名、PKI 证书框架等也是经常存在风险的点。车载信息娱乐系统需要加强防护，避免传统信息安全攻击。硬件安全方面，通过拆解DA硬件，分析车载信息娱乐系统的硬件结构、调试引脚、WIFI 系统、串口通信、代码逆向、车载信息娱乐系统指纹特征等研究点，对其他的车联网设施进行攻击。

对这些嵌入式系统风险可采取一些安全措施避免掉，比如选择嵌入式系统和浏览器时避免选择存在漏洞的版本，能够在一定程度上降低被攻击风险。

安全技术应用：车载信息娱乐系统系统硬件安全是确保车机硬件中的系统程序、终端参数、用户数据不被篡改或非法获取。

车载信息娱乐系统系统安全方面是对操作系统的启动、升级、恢复及访问进行保护，通过DAC、MAC权限机制和沙箱机制保护文件系统安全，建立对设备的安全要求保障系统接口的使用安全。结合车机总线接口的设计方案对总线的指令通道进行正向保护并通过旁路监控的方式保护总线接口的调用安全。同时建立系统分区、文件系统及服务的监控机制以及最小功能开发，保障车机操作系统安全运行。

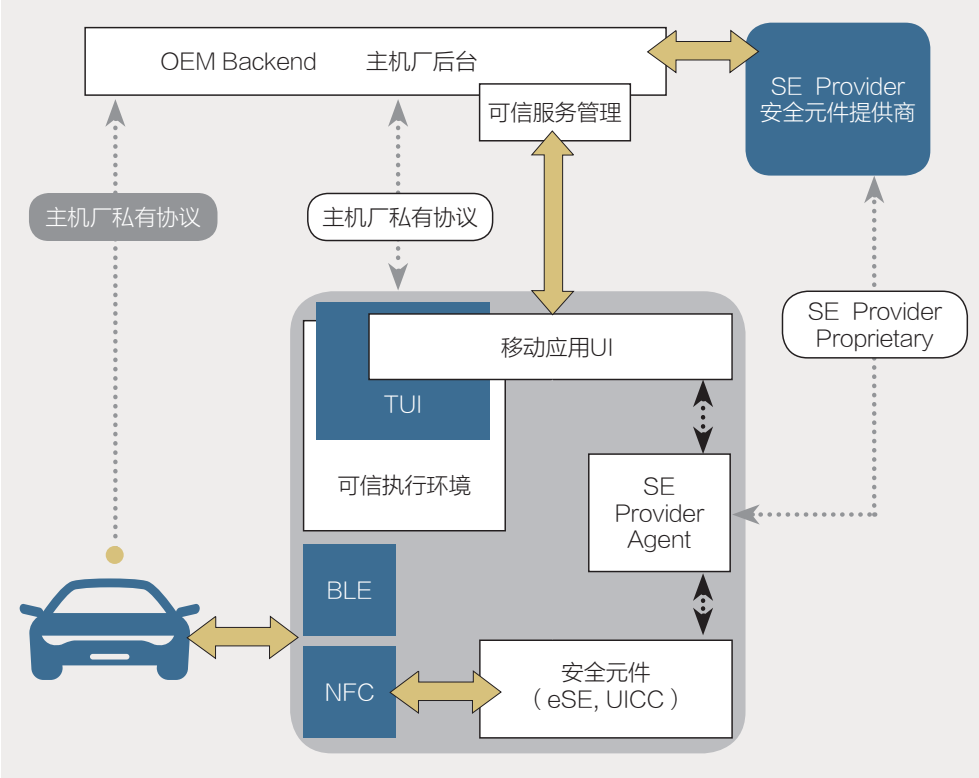
车载信息娱乐系统应用安全一方面要保证车机自身应用的安全，不被劫持、篡改。另一方面应建立起三方应用的准入机制，对车机应用生态系统进行保护。同时通过应用监控措施实时对系统中的应用程序的活动行为、网络流量、权限等进行监控，保障车机应用生态系统安全。

附录B3 数字钥匙系统安全技术应用

概念：随着移动互联网和车联网技术的加速普及，数字钥匙（经常也被称为蓝牙钥匙或者虚拟钥匙）将成为下一代汽车的标准配置。数字钥匙主要是利用进场通信技术，使得用户可以通过智能手机或可穿戴智能设备（例如智能手表）来进行车门的开锁，闭锁以及车辆的启动等操作。数字钥匙除了能够给用户带来很大的便利性，其本身数字化的本质也使得数字钥匙成为很多新的车联网应用和服务的基础设施，例如汽车共享，分时租赁，租车业务，快递到后备箱等。

模块组成和功能：一个完整的数字钥匙系统包括车内蓝牙模块，安全芯片（SE），后台服务，和相对应的手机端App。实现数字钥匙的功能并不复杂，具有挑战的是如何在整个生命周期内保障数字钥匙服务的安全性和可用性。这需要从架构设计，测试验证以及安全运营三个阶段去保障。

TSM（可信服务管理器）：通过允许访问智能设备中的（嵌入式）



安全元件，使服务提供商（OEM）能够远程分发和管理他们的非接触式应用程序。

移动UI：OEM/TSM和智能设备之间的接口。这也被称为OEM应用程序。

安全组件SE：安全存储在智能设备上。它可以采用嵌入式安全元件或UICC安全元件的形式。

SE Provider: SE的所有者，它提供对TSM的SE访问。

SE提供商代理：SE提供商的SE访问接口。SE提供商可以通过专有接口/功能访问它。

TUI：可信用户界面。它通常是TEE的一部分。

TEE：可信执行环境。在主机应用程序处理器上安全的应用程序。

其他相关的数字钥匙服务的标准：

蓝牙低功耗 BLE 无线技术标准，用于短距离交换来自固定和移动设备的数据并构建个人局域网（PAN）。

GP 在安全芯片技术上实现多个嵌入式应用的安全且交互操作的部署和管理。

NFC 在电子设备之间实现简单而安全的双向互动，使消费者能够进行非接触式交易，访问数字内容并通过一次触摸链接电子设备。

安全需求：持有数字钥匙的消费者设备必须实施保护数字钥匙的机制，并防止未经授权使用数字钥匙。需要密钥保护以防止未经授权复制，修改和删除现有密钥；未经授权的创建和提供新的；和拒绝服务（如干扰OEM应用程序或车辆与智能设备之间的连接）。数字密钥的未授权使用包括未经授权的用户使用，或者在允许的适用范围之外的授权用户使用。安全机制需要处理以下威胁：

软件攻击者获得root访问权限并在设备上安装恶意应用程序并重置设备。

物理攻击者读取并修改存储在设备上的任何数据。

通信攻击者控制设备和车辆之间的所有通信或中继通信。

数字密钥相关消息在持有数字密钥的设备与车辆（密钥使用），另一设备（对等密钥共享）和远程后端（密钥供应）之间交换。安全体系结构必须使这些消息的接收者能够验证消息的可信性。与持有数字密钥的设备进行任何消息交换必须满足以下目标：

可信度 设备应该只接受可信设备的消息，即攻击者不应该能够创建虚假消息。

完整性 设备应该检测到攻击者已经删除了整个消息或部分消息。

时效性 攻击者不能重播旧消息。

绑定 数字密钥应当安全地绑定当前用户，即攻击者不得伪装成以前的用户。

独立性 消息交换不应披露关于同一个或另一个数字密钥不需要的属性的消息。

对于拥有和管理数字密钥的设备，我们假设一个基于硬件的可信执行环境，它可以支持任意制造商签名代码的安全执行，也可以限制为预定义的功能。另外，我们假设设备具有操作系统（os）安全框架，其中可以限制对安全服务的访问。OS安全框架提供运行时隔离和隔离存储。我们假设操作系统安全框架本身的完整性受到保护。

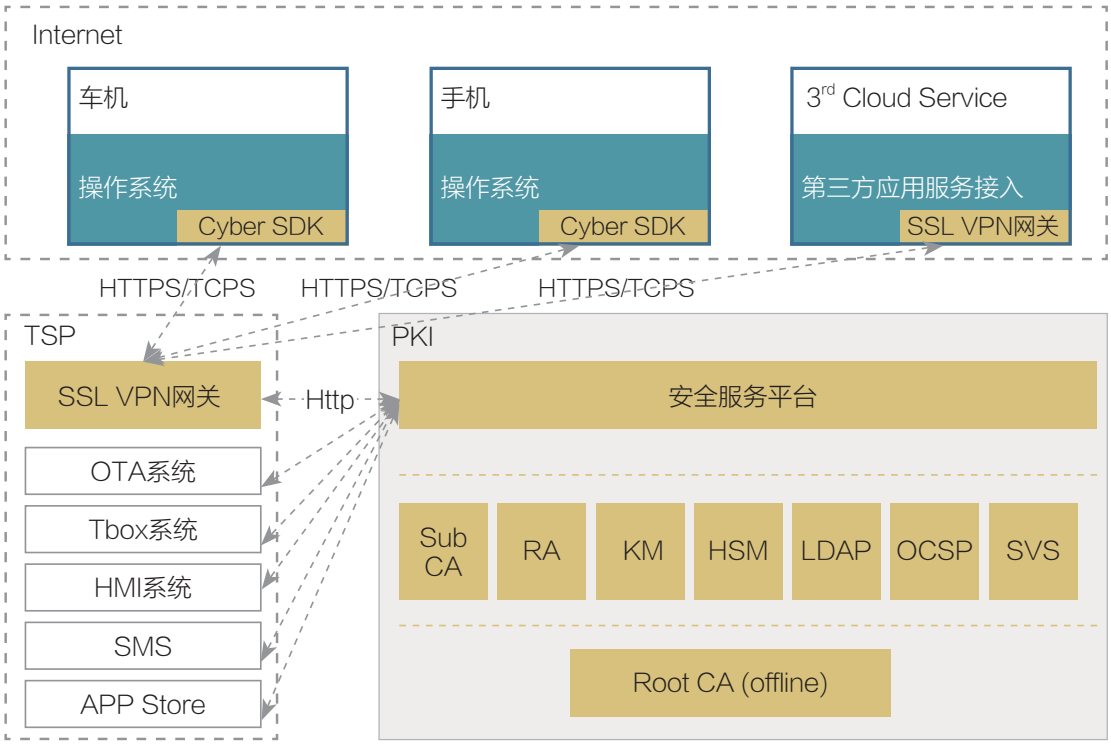
结论：汽车数字钥匙毫无疑问将会成为新一代汽车的标准配置。很多汽车制造商在构建数字钥匙解决方案的时候并没有充分的考虑到数字钥匙其实是一项非常重要的服务。而如何保障这项服务的安全性需要汽车制造商后者出行服务商在最初的设计阶段就通过结构业务场景下的不同用例，分析具体的安全需求，从而选用合适的技术和标准来构建安全的数字钥匙系统。还有很重要的一点是，数字钥匙服务的生命周期较长（5~10年），是否具备完整的更新能力也将决定数字钥匙服务在整个生命周期内的安全性。

附录B4 车云网络通信安全PKI技术应用

概念：公钥基础设施（Public Key Infrastructure，简称PKI）是目前网络安全建设的基础与核心。PKI主要通过对密钥及数字证书的管理，为车载终端与车企TSP平台建立安全可信的运行环境，有效的保障了车载终端到后台服务间通信连接、数据交互的安全可信。

模块组成和功能：PKI采用一套软硬件系统和安全策略的集合，利用公钥技术和X.509证书为车企建立一整套安全信任机制，其后台服务系统包括：CA数字证书认证系统、RA证书注册系统、KM密钥管理系统、安全管理服务平台、HSM密码机、SVS签名验签服务器、SSL安全认证网关、LDAP目录服务器以及OCSP证书状态在线查询系统。车载终端TBOX、IHU及手机等设备可以通过集成Cyber SDK方式与后台建立安全连接，实现包括：证书生命周期管理、密钥协商及运算、数字签名与验签、证书状态查询等功能。

逻辑图：



威胁分析：车联网服务平台在公网环境下与车载终端设备进行通信，负责车辆控制以及敏感信息传输等业务操作，如果没有较强的身份识别，访问控制技术保障信息安全，使攻击者可以轻易的通过伪造凭证方式访问车联网服务平台，通过网络攻击从而轻易获取高价值数据信息（如：车主身份、车辆标识、车辆行驶轨迹等），实现终端数据伪造、车远程控制，给车企造成巨大的财产损失、威胁车主人身安全甚至牵涉国家安全。

安全技术应用：PKI身份认证体系，解决了数据在不可信的网络环境中传输的机密性、完整性、不可重复性以及传输节点的身份识别问题，其在车联网中典型的应用场景包括：终端设备认证、APP应用签名与验签、FOTA、虚拟钥匙等业务。此外，密码技术是PKI体系的核心保障，我国绝大部分行业核心领域长期以来都是沿用国际通用的密码算法体系（主要包括：DES、3DES、AES、RSA、SHA256等等），为了保障国家对商用密码安全、实现自主可控的目标，国家商用密码管理办公室制定了一系列密码标准，包括SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等，该系列算法已经在国家密码管理局大力推广下，在政府、金融、电信等行业实施落地。在汽车电子网络安全的研究中，车企以及汽车电子相关领域的企事业单位应尽可能以国家信息安全为导向，关注国家对密码应用的原则以及政策措施。

附录B5 车载系统FOTA安全技术应用

概念：FOTA（Firmware Over-The-Air）是指通过云端升级技术，为具有连网功能的设备提供固件升级服务。车载电子设备，如T-BOX，车载信息娱乐系统，或其它一些有升级需求的ECU，在联网后通常采用FOTA方式进行固件系统升级。

模块组成和功能：传统的FOTA方案包括软件提供商、OTA服务平台及车载终端升级程序，由于缺少安全机制容易被攻击者利用。因此安全FOTA方案在原有架构上增加安全服务平台、终端OTA安全组件，具体说明如下。

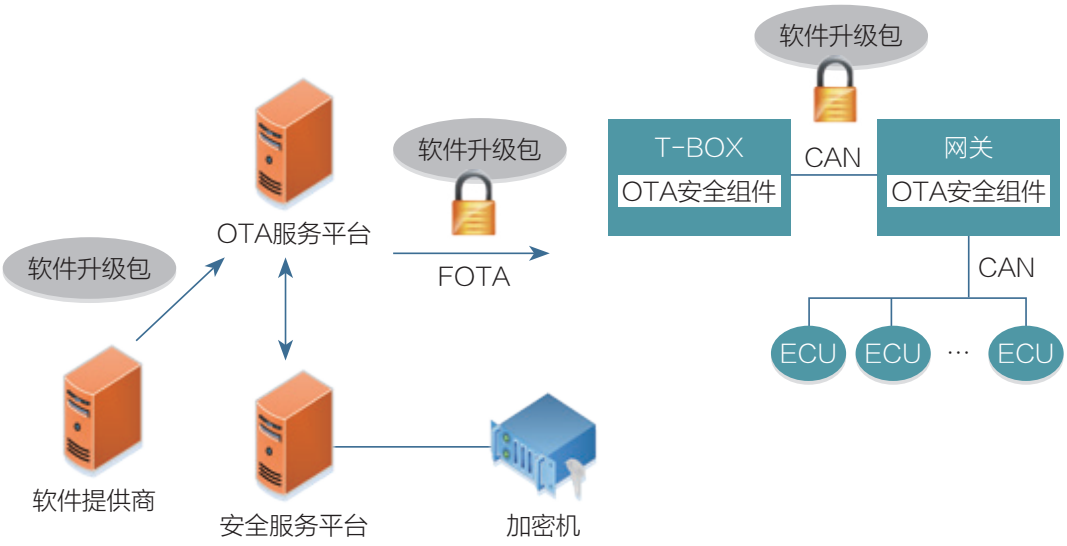
软件提供商：原始固件升级软件包发布者。

安全服务平台：为OTA服务平台提供安全服务，包括密钥证书管理服务，数据加密服务，数字签名服务等。

OTA服务平台：为车载终端提供OTA服务。

终端OTA安全组件：对升级包进行合法性验证，适配安全升级流程。

逻辑图：



威胁分析：在FOTA流程中，主要存在传输风险和升级包篡改风险。终端下载升级包的传输流程中，攻击者可利用网络攻击手段，如中间人攻击，将篡改伪造的升级包发送给车载终端，如果终端在升级流程中同时缺少验证机制，那么被篡改的升级包即可顺利完成升级流程，达到篡改系统，植入后门等恶意程序的目的。攻击者还可能对升级包进行解包分析，获取一些可利用的信息，如漏洞补丁等，升级包中关键信息的暴露会增加被攻击的风险。

安全技术应用：安全FOTA通常从升级包发布、升级包传输、终端升级三个阶段进行防御。

为抵御攻击者对升级包的逆向分析攻击、篡改攻击，OTA服务端可增加部署安全服务器，提供安全基础设施，如密钥生成与管理、数字加密、数字签名等。基于安全服务器实现升级包加固功能，最终由OTA服务器发布加固后的升级包。安全服务器的基础功能可使用软件方案实现，也可配合部署硬件加密机实现。

在OTA服务端与车机端构建安全传输通道，实现双向身份认证，及传输加密等功能，保证升级包传输过程的安全。

终端系统在升级流程前增加升级包校验机制，对升级包进行解密和合法性验证，验证通过方可进入系统升级流程。由于车载系统的多样性，操作系统和硬件性能差异较大，FOTA安全方案在终端上的实施需要考虑具体系统条件，在安全等级与目标系统支持能力之间找到平衡点。

全国信息安全标准化技术委员会
信息安全评估标准工作组

通信地址：北京市东城区安定门东大街1号
联 系 人：龚洁中 李琳
联系电话：010-64102740
邮　　箱：gongjz@cesi.cn