汽车电子控制单元（ECU）信息安全防护技术标准化需求研究报告

汽标委智能网联汽车分标委

汽车信息安全标准工作组

2020 年 6 月

目　录

前　言

信息安全是智能网联汽车的核心技术之一，并涉及国家战略安全。近年，美、欧、日等发达国家均大力推进汽车信息安全技术的研发，抢占这一战略技术制高点。在智能网联汽车技术蓬勃发展的当下，汽车行业的从业者对于产品信息安全的防护意识不断增强，然而受制于技术积累和实际开发经验，汽车 ECU（Electronic Control Unit）的信息安全防护技术水平尚有提升空间。

围绕汽车 ECU 的标准制定工作仍有待完善加强。目前，国际和国内正在如火如荼地制定汽车信息安全相关的法律、法规、标准等，旨在通过一系列强制或推荐性文件提升整个行业的信息安全防护水平。就国内而言，围绕汽车 ECU 的相关标准制定也已经开展。当前汽标委在制定的若干标准，例如，《汽车网关信息安全技术要求》、《车载信息交互系统信息安全技术要求》等，但这些标准仅针对某些车载关键 ECU 来制定。考虑到汽车上搭载的众多 ECU，尚有大部分 ECU 的信息安全技术要求未被覆盖。

当前的汽车 ECU 上已经在部署一些信息安全技术措施了，然而存在百家争鸣、尚未有统一的技术要求。对于汽车 ECU 的开发商而言，也需要一份技术参考来指导产品的设计开发工作。此外，汽车 ECU 因计算能力和应用场景等因素的限制，无法部署复杂的信息安全防护措施，相关防护技术的参考方案需要围绕汽车的特殊场景来定义，以提高落地实施的可行性。

本研究报告拟对汽车 ECU 的信息安全防护技术进行综述，并提出 ECU 信息安全防护技术的标准化建议，为后续制定技术标准和推动行业技术进步提供支撑和借鉴。全文框架如下：第一章节，对汽车 ECU 信息安全技术研究背景和标准研究必要性进行了阐述；第二章节，从软件、硬件、数据、车内通讯接口、车外通讯接口共 5 个维度介绍了当前汽车行业中部署的典型信息安全关键技术；第三章节，阐述了汽车 ECU 信息安全标准化的必要性；第四章节，分析了 ECU 信息安全标准化需求，阐述标准范围和标准撰写思路；第五章节，针对后续的标准化工作提出了建议，包括区分和其它标准的关系，后续待处理的问题和工作计划。附录 A 介绍了常见汽车 ECU 的信息安全分析方法；附录 B 介绍了工作组的工作历程。

在此衷心感谢参加研究报告编写的各单位、组织及个人。

组织指导：汽标委智能网联汽车分标委

牵头单位：联合汽车电子有限公司，北京百度网讯科技有限公司

参与单位：中国汽车技术研究中心有限公司，大陆汽车投资（上海）有限公司，博世汽车部件（苏州）有限公司，北京中电华大电子设计有限责任公司，东软集团股份有限公司，北京汽车研究总院有限公司，东风汽车有限公司东风日产乘用车公司，重庆长安汽车股份有限公司，上海瓶钵信息科技有限公司，英飞凌科技（中国）有限公司，北京奇虎科技有限公司，中国信息通信研究院，国民技术股份有限公司，襄阳达安汽车检测中心有限公司，一汽-大众汽车有限公司，安徽江淮汽车集团股份有限公司

参与人员：罗勇，李显杰，孙航，彭伟，李宝田，刘洋洋，邵学彬，方熙宇，王奕，马博，俞若晨，郑亮，赵敬超，苑中魁，张雷，李峰，张丽花，武扬，贠东鑫，罗薇，程唐平，陈汉顺，饶萌，张屹，詹鹏翼，孙娅苹，杨贤伟，高海龙，秦宏伟，王林林

1 汽车 ECU 信息安全技术研究背景

1.1 智能网联汽车发展背景

近年来，新一轮科技革命和产业变革的加速融合，中国智能网联汽车产业发展迅速，已经成为产业发展的重要趋势。尤其随着《智能汽车创新发展战略》《汽车产业中长期发展规划》等文件的发布，更是将智能网联汽车提升至国家战略高度。2018 年 12 月，工业和信息化部印发了《车联网(智能网联汽车)产业发展行动计划》，发展行动计划目标在 2020 年，实现车联网(智能网联汽车)产业跨行业融合的突破，具备高级别自动驾驶功能的智能网联汽车实现特定场景规模应用，车联网综合应用体系基本构建，用户渗透率大幅提高。

智能网联汽车的发展，是由汽车承载的应用功能发展来作为驱动力的，而且离不开智能网联汽车电子电器架构的发展。如图 1 所示，在未来汽车 ECU 将会承载越来越多的功能，而且不同的电子电器架构下呈现的信息安全状态也有所不同，例如，整车越来越多的互联化需求会催生车辆上的网联 ECU，同时车载电脑形态的 ECU 和车云计算 ECU 的复杂度提升，以及逐渐趋同于 IT 行业的计算机，也可能会带来新的信息安全威胁和攻击手段。

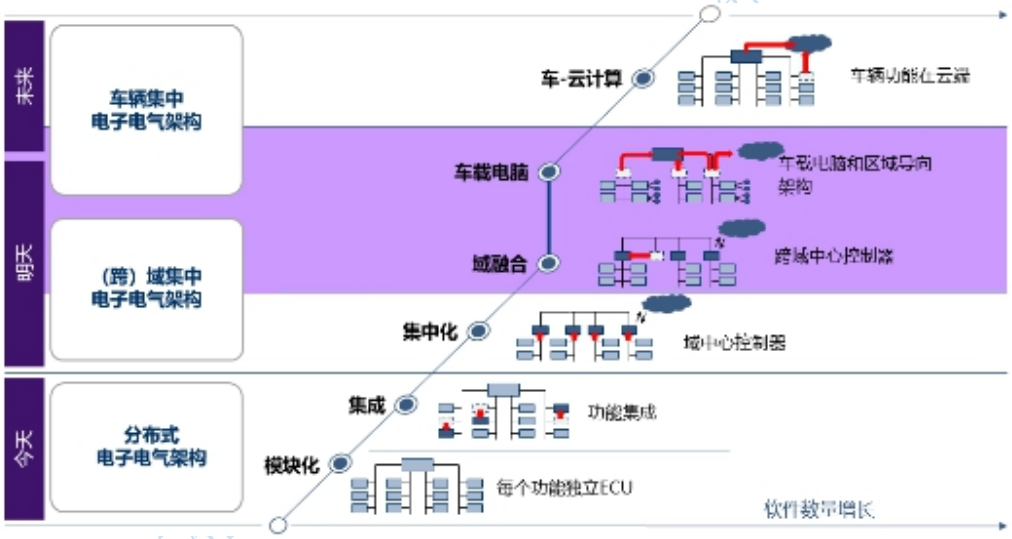

图 1 汽车电子电器架构发展趋势（图片来源 Bosch）

1.2 智能网联汽车面临的信息安全风险

智能网联汽车主要功能的实现离不开汽车 ECU，且攻击者针对智能网联汽车的攻击通常也是针对于汽车 ECU 展开的，因此智能网联汽车面临的信息安全风险也是汽车 ECU 面临的风险。

随着汽车的智能化、网联化发展，越来越多的 ECU 电子控制单元部署在汽车上，例如，车载信息娱乐系统 IVI、汽车联网模块 TBOX、高级驾驶辅助系统 ADAS、电子防抱死刹车系统 ABS、无钥匙进入和启动系统 PEPS 等。然而，由于 ECU 计算资源和能力的局限，导致难以设计有效的安全方案，而且传统的安全机制难以直接部署到 ECU 上。另外，随着车上 ECU 功能越来越多，实现的代码量增加，潜在的代码漏洞问题越来越突出。

如下图 2 所示，智能网联汽车系统常包括云端、车端、用户端和路端，系统中存在诸多潜在可被利用的信息安全漏洞，任何一处的短板都可能导致整个系统的崩塌。

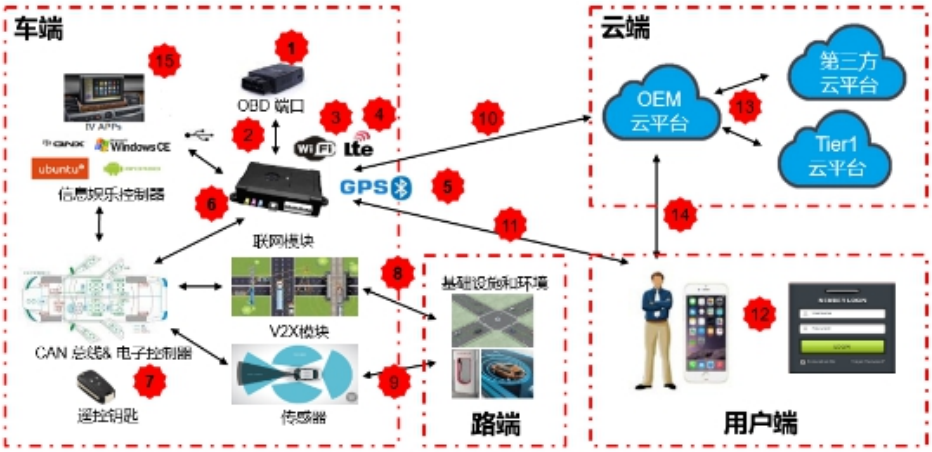

图 2 智能网联汽车系统可能存在的安全威胁

车端 ECU 面临的常见信息安全风险包括：A. 汽车车内网络目前大多采用 CAN/CAN-FD 协议进行通讯，而 CAN/CAN-FD 的字节长度有限、仲裁机制、无源地址域和无认证域等问题也有很大潜在的信息安全隐患；B. ECU 硬件可能存在可读丝印和暴露的调试口，容易遭受防逆向分析等的机制。C. ECU 的固件刷写机制未进行信息安全保护，可能导致 ECU 固件或其配置数据被篡改； D. ECU 中的敏感数据（如调校数据、虚拟钥匙数据、地图数据、配置数据等）的存储、访问过程中，若未采取加密存储和访问控制等防护措施，则可能导致数据被篡改或泄露。被篡改的数据可能导致系统功能偏离预期，甚至带来其他信息安全方面的隐患。

1.3 汽车 ECU 信息安全工作挑战

智能网联汽车的信息安全话题目前在行业中引起了巨大的关注，越来越多的玩家在加入这个领域，例如，制定法规和标准的组织机构，提供信息安全技术解决方案的公司，提供安全咨询服务的公司，提供安全测试服务的公司等。尽管如此，在汽车 ECU 信息安全领域，仍存在如下问题点有待进一步加强。

1.3.1 标准法规有待持续完善

当前，国内外正在如火如荼地制定汽车信息安全的标准法规，例如，国际的汽车信息安全标准-SAE J3061, ISO 21434, UN WP.29 汽车信息安全法规；国内的汽车信息安全标准-国家智能网联汽车信息安全标准体系，工信部智能网联汽车准入管理办法等。

然而，目前行业仍缺乏非常完善的标准法规体系，以给智能网联汽车 ECU 的开发提供明确的技术指导参考。

1.3.2 产品信息安全技术措施实施程度有待提高

尽管汽车信息安全已成为一个研究热点，然而汽车 ECU 的产品开发周期较长，较难在短时间内进行技术升级切换，使得当前产品信息安全技术措施的实施程度有待提高。此外，产品信息安全技术措施的实施会增加一部分产品的成本，例如，增加故障排查调试难度，增加产品报废率等，相应增加成本被市场认可接受的程度还有待提升。

1.3.3 产品信息安全意识需要持续提升

在汽车 ECU 的开发过程中，尽管很多公司已经普遍意识到了汽车产品信息安全的重要性，很多 ECU 的开发并未有一套系统化的产品信息安全开发，然而在实际产品研发管理环节的行为意识仍需持续提升，同时需要在产品信息安全领域持续关注和投入。

1.3.4 产品信息安全开发能力有待持续加强

围绕汽车 ECU 的产品信息安全开发能力，需要涵盖从系统开发、软硬件开发、生产、测试和运维等多方面的能力，然而目前很多公司没有办法打通并落地实施每个环节中的要求。

首先，需要建立和加强信息安全的开发流程体系，其次，加强开发能力的建设，包括技术规范要求建设、开发流程体系建设、工具链建设等，此外，产品研发活动中的信息安全要求需要规范化。

1.3.5 产品信息安全运维机制需要持续完善

和以往汽车 ECU 的开发过程不同，产品信息安全对于运维机制的要求更高。汽车 ECU 的产品信息安全状态并非一成不变，需要动态地关注汽车 ECU 的信息安全漏洞并及时修补，这部分的能力隶属于安全运维范畴。对于汽车制造商而言，需要建立并持续维护这部分体系能力。

1.3.6 产品信息安全相关的协作机制需要加强

产品信息安全工作的开展离不开协作。例如，对于密码材料等高度敏感数据的管理，包括密码材料的生成、传递、存储、使用、更新、注销等环节，要实现完善的管理机制需要跨部门(研发，测试，生产和 IT 等部门)，跨公司（整车厂 OEM，零部件供应商 Tier 1 和后台运营公司等）之间的多方协作，确保在整个环节中做到敏感数据的妥善管理。除此之外，在整个产品信息安全的生命周期内的诸多环节，都需要建立和强化工作协作机制。

1.4 相关法律法规标准背景

1.4.1 国际情况

国际上在汽车信息安全标准制定方面有一定基础。

A. 美国

SAE 发布了“ Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles ”-J3016 和“ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”-J3061 两项重要的汽车行业国际标准。ISO 和 SAE 正在合作制定 ISO/SAE AWI 21434 “Road Vehicles -- Cybersecurity engineering ”。

NHTSA（美国国家公路交通安全管理局）发布了《现代汽车信息安全最佳实践指南》。

B. 欧洲

欧洲网络信息安全局制定了《智能汽车信息安全与快速恢复的正确实践与建议》。英国也制定了《联网与自动驾驶汽车信息安全主要原则》。欧盟出台《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）

C. 日本

日本汽车业标准化组织 JASPAR（Japan Automotive Software Platform and Architecture）在牵头制定汽车信息安全相关的标准规范，以提升日本汽车制造商的整体技术水平，涉及车内网络安全通讯、车载防火墙、软件升级、VLAN 等方面

1.4.2 国内情况

我国在 2016 年 11 月 7 日发布《中华人民共和国网络安全法》，在保障信息安全，维护网络空间主权和国家安全、社会公共利益，促进经济社会信息化健康发展方面提供法律依据。

近年来，我国国务院以及工信部、发改委、质检总局、国家标准委等相关部委相继发布了《中国制造 2025》、《装备制造业标准化和指令提升规划》、《汽车产业中长期发展规划》、《智能汽车创新发展战略》等文件纷纷强调要开展汽车信息安全能力和标准体系的建设。工业和信息化部、国家标准化管理委员会共同组织制定了《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（电子品与服务）》、《国家车联网产业标准体系建设指南（智能网联汽车）》、《国家车联网产业标准体系建设指南（信息通信）》，为汽车标准体系提供了指导和方向。

汽标委智能网联分标委下陆续开展了多项汽车信息安全标准的制定工作，包括：《汽车信息安全通用技术要求》、《汽车网关信息安全技术要求》、《车载信息交互系统信息安全技术要求》、《汽车诊断接口信息安全技术要求》等等。

标准名称			类型	状态
NTCAS 全国汽标委	第一批次	《汽车网关信息安全技术要求及试验方法》	推荐	报批
		《汽车信息安全通用技术要求》	推荐	报批
		《车载信息交互系统信息安全技术要求及试验方法》	推荐	报批
		《电动汽车远程服务与管理系统信息安全技术要求及试验方法》	推荐	报批
		《电动汽车充电系统信息安全技术要求》	推荐	立项
	第二批次	《汽车诊断接口信息安全技术要求》	推荐	提交立项
		《汽车软件升级通用技术要求》	推荐	立项
		《汽车信息安全应急响应管理指南》	推荐	提交立项
		《汽车信息安全风险评估规范》	推荐	提交立项
	第三批次	《汽车整车信息安全技术要求与测试方法》	推荐	预研
		《道路车辆 信息安全工程》	推荐	提交立项
		车载计算平台标准化需求研究	研究项目	预研
		汽车电子控制单元（ECU）信息安全防护技术要求研究	研究项目	预研

全国信息安全标准化技术委员会(TC260)归口的 GB/T 38628-2020《信息安全技术-汽车电子系统网络安全指南》于 2020 年 4 月 28 日正式发布，并将于 2020 年 11 月 1 日起正式实施。

然而，当前仍缺乏相应的标准对汽车各类 ECU 信息安全进行整体的方法梳理和实践指导。

1.5 小结

在整个智能网联汽车发展的背景下，汽车 ECU 可能面临诸多的信息安全风险，一旦被攻击者非法破解将导致严重后果，部署产品信息安全防护措施十分必要。

汽车行业也在逐步建立信息安全方面的技术能力，目前遇到了一些工作上的挑战，在目前法律法规标准尚不成熟的情况下，加强和加速相关信息安全能力建设的工作显得尤为重要。

此外，汽车 ECU 的信息安全状态并非一成不变，需要持续被关注。随着攻击技术的提升，已部署信息安全防护措施的 ECU 可能存在新的信息安全风险，相应的防护技术也需要进一步提升。

2 汽车 ECU 信息安全关键技术

为了应对信息安全风险，目前汽车 ECU 已经部署了若干信息安全防护措施。如图 3 所示，参考《汽车信息安全通用技术要求》中的信息安全技术框架，针对于车载 ECU 产品，从软件、硬件、数据、车内通讯和车外通讯的维度进行信息安全关键技术的分析。

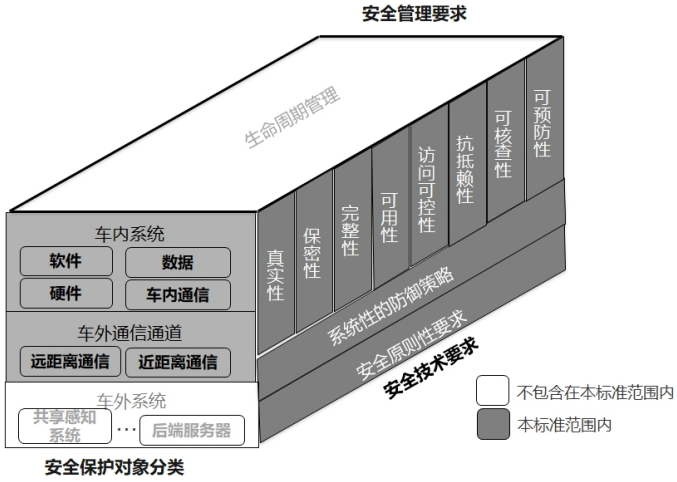

图 3 智能网联汽车 ECU 的信息安全技术框架

汽车 ECU 上已经在部署一定的信息安全防护技术措施了。然而，由于不同 ECU 的应用场景和功能定义不尽相同，不同厂商的设计开发思路不尽相同，导致当前 ECU 的信息安全技术开发路线较难有统一的共识。而且，汽车 ECU 因计算能力和系统资源的限制，较难部署复杂的信息安全防护措施。在具体的开发过程中还需要考虑多种技术限制，按需选择适合的技术方案并落地实施。

此外，大多汽车 ECU 厂商在部署信息安全防护技术措施时仍缺乏明确的参考指导。

3 汽车 ECU 信息安全标准化的必要性

3.1 提升行业在汽车 ECU 信息安全技术开发方面的整体能力

当前汽车行业在 ECU 信息安全技术开发水平上存在参差不齐的情况，各家厂商有自己的技术路线规划，尚未进行统一。通过相关 ECU 标准化工作，可以将行业的整体开发能力统一提升到某个技术水平，有助于行业的进步。

3.2 为汽车 ECU 产品开发工作提供技术参考

对于网关、车载信息交互系统、车载充电系统等车载 ECU 而言，当前已经有明确的技术标准在制定过程中了。除此之外，车上还有很多其它功能和形态的 ECU，目前在技术要求方面仍处于空白状态，很多厂商在定义技术要求或执行开发工作时，常常不知所措。

通过汽车 ECU 产品的技术标准化工作，可以为汽车 ECU 产品开发提供技术指导，便于明确定义 ECU 的技术要求。

3.3 方便行业开展技术交流和合作

汽车 ECU 的标准化工作可以促进行业内的技术交流和合作，体现在：A. 统一名词和术语，方便沟通交流；B. 统一方法论，采用同样的方法思路和技术语言，更有利于开展技术探讨；C. 统一技术建议或要求，便于引用来指导实际的产品开发工作，以及促进技术方案的推广。

3.4 为未来的技术监管工作提供指导

除了几个车载关键 ECU 之外，制定汽车 ECU 信息安全防护技术标准，可覆盖更多的 ECU 产品，以弥补车载 ECU 信息安全技术要求的灰色地带，可以为未来的技术监管工作提供指导。

4 汽车 ECU 信息安全标准化需求分析

4.1 标准范围界定

依据车载 ECU 的名词定义，可发现：本标准涉及的对象范围广，标准需要考虑的内容体系庞大；不同 ECU 的功能和应用场景多样，标准较难实现统一化定义和描述；车载 ECU 的开发厂商众多，且有不同的技术特点，不好提强制性要求，以防约束企业的开发灵活性。

本标准囊括所有车载 ECU，作为一个宏观指导准则，不涉及具体的技术细节要求，但跟现有标准的技术要求保持不冲突。实际开发过程，可以具体技术要求的相关标准为开发依据。

如图 4 所示按照汽标委智能网联汽车分标委的标准框架建议，共分了 3 个层级：第一层级为基础标准层级，起到整个汽车信息安全标准体系的基础支撑作用，例如《汽车信息安全通用技术要求》包含的术语和定义、流程定义、分级定义等；第二层级为共性标准层级，将定义和规范汽车信息安全的各项标准中具有共性要求的内容，如操作系统、ECU、安全启动等；第三层级为系统与应用层级，针对具体的系统、部件和业务应用管理等确定需要满足的信息安全要求，如网关、充电系统、远程服务系统的安全要求等。

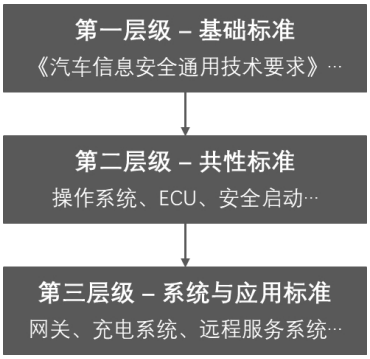

图 4　标准层级划分

按照此分级定义，本报告研究的 ECU 产品信息安全技术标准定位于第二层级，作为汽车信息安全的各项标准中具有共性要求的内容进行整理。

4.2 标准内容撰写思路

4.2.1 业界的信息安全防护技术分析方法

参考 SAE J3061 和 ISO 21434 中提到的方法，针对于特定应用场景，可以利用 HEAVENS、STRIDE 和攻击树模型等方法开展安全分析（参考附录 B），并得出 ECU 的信息安全技术需求，思路如下：

Step1：识别系统关键资产
Step2：围绕系统关键资产，分析并识别威胁场景
Step3：分析威胁场景的攻击路径
Step4：从威胁等级和影响等级两个维度，结合 HEAVENS 分析方法进行安全等级评估
Step5：根据评估得出的安全等级，制定相应的信息安全技术要求

此分析方法在功能应用场景相对固定的情况下更适用，能更有针对性地分析出该场景下的信息安全技术要求。然而如图 5 所示，针对于宏观“ECU”的定义，因涉及的 ECU 范围广（囊括了车内上百种 ECU）、功能场景多样（不同 ECU 的功能各不相同，同一 ECU 在不同场景下功能不同）、不好提强制要求（因考虑到实施成本和开发灵活性等方面），上述分析方法存在较大的应用难度。

图 5　ECU 信息安全防护技术要求标准化特点

4.2.2 标准撰写思路描述

按照“筛子分类”的思路开展标准内容的撰写工作。此方案旨在定义不同车内 ECU 的基础防护措施，便于大家理解和开展技术交流，灵活地部署性价比更高的安全防护措施。对于每个分类中的 ECU，实际开发过程可参考 ISO 21434 中的方法论识别具体资产、并识别详细的风险和进行安全评级，以定义出更详细的，针对性更强的安全措施。

如图 6 所示，所定义的“筛子分类”思路，包括两个步骤：

4.2.2.1 步骤 1：对车载 ECU 进行分类

在开发之初对车载 ECU 产品进行大致分类，不涉及 ECU 的详细 TARA 分析。后续仍可进行详细 TARA 分析，得出具体场景的安全威胁分析结果，再针对性设计技术方案。

4.2.2.2 步骤 2：根据不同分类来定义安全防护措施

根据 ECU 的大致分类，推荐基础安全措施，不涉及详细的信息安全技术需求定义，避免限制 ECU 厂

商的开发灵活性。

为了使得安全防护措施的指导性和实施性更强，定义安全防护措施时可采用如下两种思路：

A. 定义通用化的安全防护措施，作为基线功能的推荐。举例说明：对于网关产品建议部署信号完整性和机密性校验措施，例如，防火墙等。

B. 结合 ECU 的功能定义和应用场景来定义安全防护措施，区分出 ECU 的基本功能和增量功能，来分别定义基线功能集和增量功能集。举例说明：对于网关产品，基础功能是完成车内的数据路由转发功能，部署防火墙功能是基线功能；而在某些场景下，增量功能可能是网关要支持远程程序升级的功能，则针对于增量功能需要部署刷新完整性和机密性校验措施，例如，刷新包的数字签名和刷新包加密存储措施。

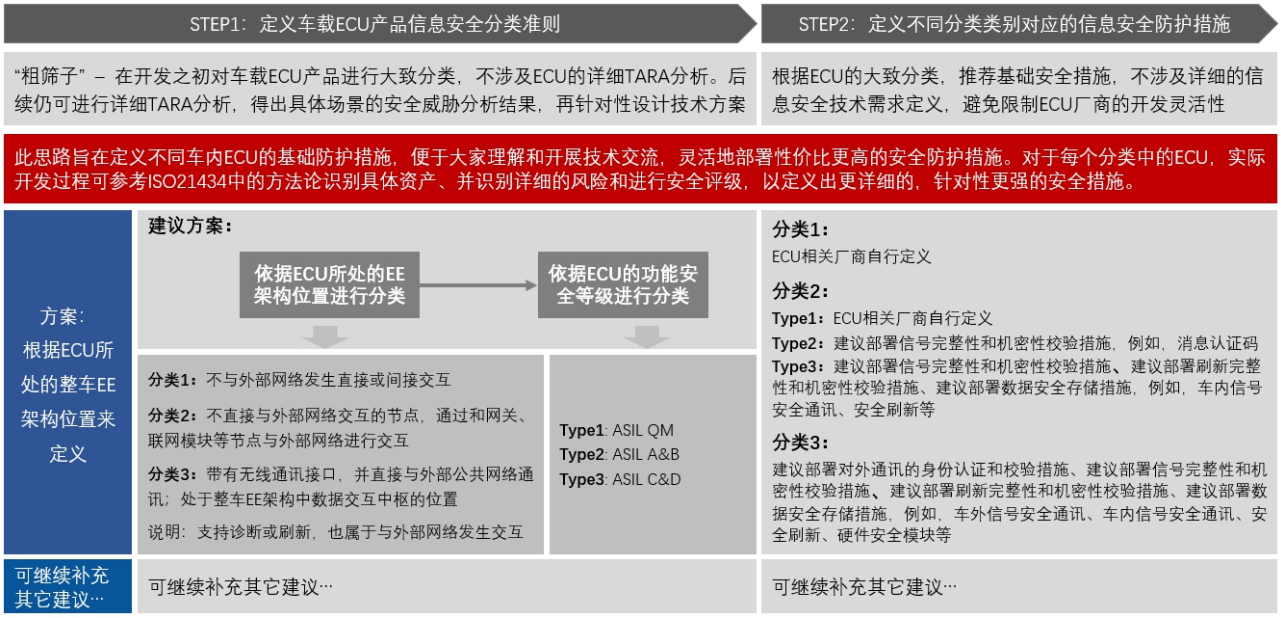

图 6 “筛子”分类思路详细阐述

4.2.3 具体执行步骤

此步骤中，按 ECU 所处的 EE 架构位置和 ECU 功能安全等级进行分类，详细分类规则如图 7 所示。

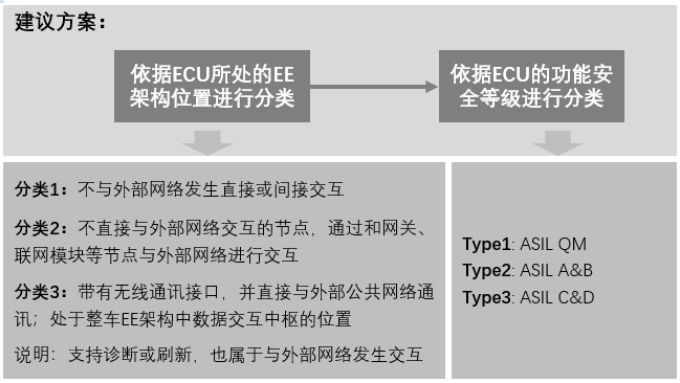

图 7 “筛子”分类思路 – 分类步骤

结合步骤一中的分类 1-3 和 Type1-3，来定义相应的安全防护措施，具体操作步骤如图 8 所示

分类1：

ECU相关厂商自行定义

分类2：

Type1：ECU相关厂商自行定义

Type2：建议部署信号完整性和机密性校验措施，例如，消息认证码

Type3：建议部署信号完整性和机密性校验措施、建议部署刷新完整性和机密性校验措施、建议部署数据安全存储措施，例如，车内信号安全通讯、安全刷新等

分类3：

建议部署对外通讯的身份认证和校验措施、建议部署信号完整性和机密性校验措施、建议部署刷新完整性和机密性校验措施、建议部署数据安全存储措施，例如，车外信号安全通讯、车内信号安全通讯、安全刷新、硬件安全模块等

图 8 “筛子”分类思路 – 技术要求定义

4.2.4 应用案例

基于当前常见的汽车 ECU，来试用上述的分类方法进行评估。如图 9 所示，用于评估的 ECU 包括：CGW (Central Gateway，中央网关), IVI (In Vehicle Infotainment，车载信息娱乐模块), EMS (Engine Management System，发动机管理系统), PEPS (Passive Entry Passive Start，无钥匙进入启动系统), ESCL (Electronic Steering Column Lock，电子转向柱锁)。

相应产品所定义的安全防护措施，可作为 ECU 模块开发商的参考，为了不限制开发技术方案的灵活性和自由度，本标准所定义的安全防护措施为推荐性。实际开发过程中，ECU 开发厂商可根据企业的技术特点，依据本标准定义的安全防护措施指导原则，来灵活选择相应的技术措施。

图 9 “筛子”分类思路 – 应用案例

5 后续工作建议

5.1 处理和其余标准的关系

一方面，当前已经能识别到若干标准会与本标准内容产生一些交集，潜在可能会产生一些技术要求上的冲突，例如，《网关信息安全技术要求》、《车载信息交互系统信息安全技术要求》等。基于此，本标准将尽量兼容当前标准的内容，做到抽象化描述，不涉及具体技术细节。实际应用中，本标准仍可作为厂商开发过程的参考，具体的技术实施要求可以用相应技术要求标准作为开发和测试的依据。

另一方面，未来也会有其它形态的汽车 ECU 产品和相关技术标准要求，例如，可预见的区域控制器、车载计算平台等。针对于此，标准撰写的过程中，会基于当前可预见的未来趋势，将相关要求体现在本标准的内容中。未来，根据技术应用的实际情况酌情调整本标准的内容，以适应新的技术要求。

5.2 待讨论的问题

基于研究项目组前期的讨论内容，在后续正式开展标准的起草编写工作之后，将对如下问题开展针对性的研讨和讨论。

1) 车载传感器是否应纳入 ECU 的范畴？例如，ADAS 系统的摄像头、毫米波雷达、激光雷达等
2) 分类方法的进一步细化，远程接口(Cellular) & 近程接口(BLE, USB, OBD)，or 其它?
3) 分类方法中考虑数据隐私的维度
4) 梳理存在潜在关联的现有标准，并考虑内容上的区分度
5) 讨论未来的 ECU 发展趋势，在标准内容上进行兼容考虑

附录 A 信息安全分析方法介绍

依据经验知识和实践教训提出汽车 ECU 信息安全问题缓解方案是关键方法之一，但目前，也存在科学的方法对汽车 ECU 信息安全进行分析。《ISO/SAE 21434 道路车辆：信息安全工程》提出利用风险评估的方法对汽车（包括汽车 ECU）信息安全需求进行导出。本部分介绍三种汽车 ECU 信息安全分析的方法并罗列汽车 ECU 面临的信息安全威胁。

B.1. STIRDE 威胁分析模型

STRIDE 威胁分析模型是微软安全工程和通信部门开发的威胁建模的系统方法，是安全开发生命周期（SDL）中一部分，对系统面临的威胁进行分类从而辅助系统设计人员改进系统的安全性设计。STRIDE 是包含六个含义的字母缩略词，代表 6 种威胁，其中“S”指代 Spoofing 即假冒，“T”指代 Tampering 即篡改、“R”指代 Repudiation 即否认、“I”指代 Information disclosure 即信息泄漏、“D”指代 Denial of service 即拒绝服务、“E”指代 Elevation of privilege 即提升权限。其具体解释如表 1 所示：

表 1 STRIDE 威胁分析模型说明

序号	威胁	说明
1	假冒（Spoofing）	通过伪造的身份来访问系统，非法存取和使用其他被授权用户的验证信息，比如用户名和密码信息。
2	篡改（Tampering）	恶意地修改正常数据，或在未经授权的情况下改变永久数据如数据库中存储的数据，或修改不同 ECU 之间传输的数据，使数据的完整性受到威胁。
3	否认（Repudiation）	用户拒绝承认参与了某事务处理操作，即无法追踪用户的行为。
4	信息泄漏（Information disclosure）	隐私数据被泄漏给无知情权的个人，即没有读取权限的人读取到了数据，或不法分子读取到了正在传输中的数据。
5	拒绝服务（Denial of service）	拒绝服务也即 DoS 攻击，指的是攻击者使用一些方法使合法的用户无法使用本来能够使用的服务，比如一定时间内让 Web 服务器暂时不能被使用，导致系统的可用性受到威胁。
6	提升权限（Elevation of privilege）	攻击者利用一些漏洞攻破系统防线，从而成为系统中被信任的一员，进而提升自己的权限，导致本没有使用权限的人可以获得存取权限，要知道，足够的存取权限甚至可以摧毁整个系统。

如表 2 所示，STRIDE 威胁分析模型是基于系统的安全属性进行分析的，涉及机密性、完整性、可用性、身份验证、授权、不可否认性等 6 个属性。

表 2 安全属性说明

序号	安全属性	属性解释
1	机密性	系统的数据和资源只能被具有权限的人员访问
2	完整性	系统的数据和资源只能被适当的人员以适当的方式更改
3	可用性	系统在需要时一切就绪，能正常执行操作
4	身份验证	需要给用户建立身份，当然接受匿名用户也是可以的
5	授权	给用户赋予权限，从而明确地允许或拒绝用户访问资源
6	不可否认性	用户无法在执行了某操作后否认执行了这一操作

STRIDE 所表示威胁与系统的安全属性形成一一对应的关系，上述的 6 种安全属性基本涵盖了系统安全的所有属性，其对应关系如表 3 所示：

表 3　安全威胁和安全属性对应关系

序号	威胁	安全性属性
1	假冒	身份验证
2	篡改	完整性
3	否认	不可否认性
4	信息泄露	机密性
5	拒绝服务	可用性
6	提升权限	授权

利用 STRIDE 威胁模型进行 ECU 信息安全威胁时，有两个方向：1. 将系统分解为相关的组件，并分析每个组件是否易受到威胁攻击，从而找到减轻威胁所带来的影响的方法；2. 将组件组合在一起形成系统时，分析其受到的威胁，此时，利用数据流关系图 DFD 的方法，逐个分析每个数据流关系图的元素容易受到的威胁攻击。

数据流关系图使用一组标准符号，其中包括了四个元素，分别是数据流、数据存储、进程以及交互方。考虑到目的是为了进行威胁建模，所以添加了信任边界这一新的元素。正确的数据流关系图是确保威胁模型正确的关键，所以在对系统进行威胁建模前，首先需要绘制出正确的数据流关系图，确保其显示系统的所有项。而每个 DFD 元素分别具有一组自己易受攻击的威胁，这为威胁分析过程提供了很好的参考价值。就数据流和数据存储来说，容易受到篡改、信息泄漏、拒绝服务这三类攻击的威胁；就进程这一元素来说，容易受到 STRIDE 六类攻击的威胁；对于交互方来说，容易受到假冒、否认这两类攻击的威胁；对于信任边界这一元素，也具有影响自身的独特威胁。除此之外还需关注的是，有的威胁一旦被利用，同时可能引发其他的威胁。

以上 STRIDE 模型可应用于汽车 ECU 信息安全威胁分析。

B.2.　ATTACK TREE 攻击树模型

攻击树模型将攻击目标逐级细分成单个攻击手段和相应的攻击路径，用于分析系统所面临的安全威胁。提供了一种思维方式，帮助开发者站在攻击者的角度来思考系统可能存在的漏洞，此方法很大程度上依赖于具备的黑客经验。

如图 10 所示，攻击树模型主要结构包括攻击目标、攻击子目标、“与/或”门、攻击手段和攻击路径组成。通过将攻击目标逐层拆解分析得出最终的攻击路径，用于分析系统所面临的安全威胁。

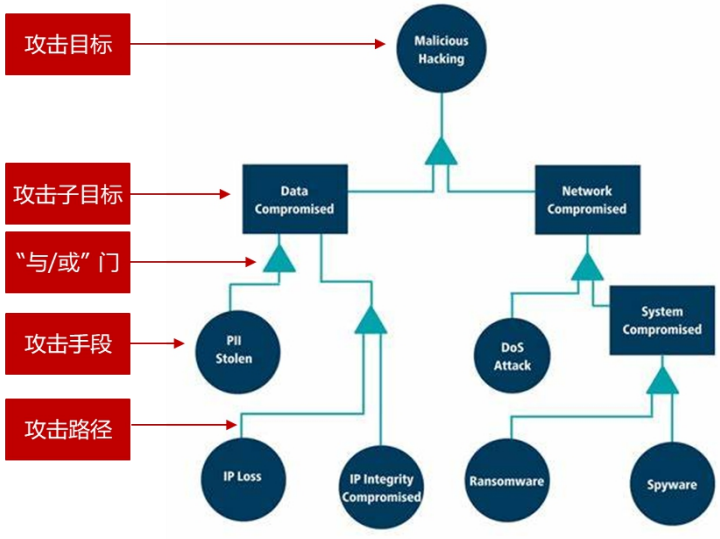

图 10　攻击树模型示意图

B.3.　HEAVENS 模型

HEAVENS 模型是较完整的风险评估的方法，在 SAE J3061 中有相应内容的介绍。其在汽车信息安全领域（包括汽车 ECU）具有很强的应用实际。如图 11 所示，下面对 HEAVENS 模型进行介绍。

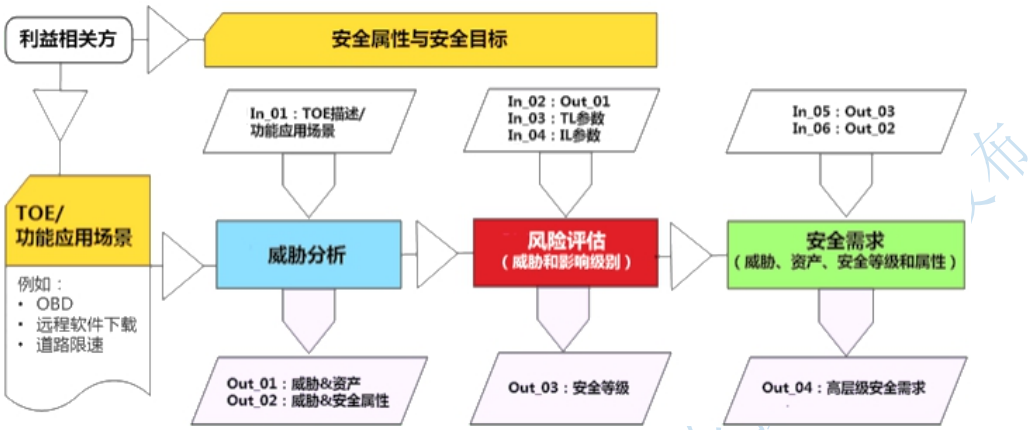

图 11　HEAVENS 模型示意图

对框架的流程介绍：1）相关利益方明确自己的安全属性和安全目标，同时提供相应评估对象或功能的典型应用场景，作为整个流程的输入；2）进行威胁分析，通过评估对象或功能典型应用场景，将威胁与评估对象、安全属性进行映射，形成对应关系；3）对威胁与评估对象进行等级划分，具体是通过综合考虑威胁和影响级别两个维度实现安全等级划分；4）将威胁、评估对象、安全属性和安全等级这四个维度进行整合形成安全需求；5）开发人员拿到这些需求，根据安全等级最终确定开发优先级。下面对每个阶段的评估内容进行详细描述（汽车相关参数进行了修改）：

1）威胁分析

威胁分析是指识别与评估资产相关威胁以及威胁与安全属性的映射。在该阶段中可使用了微软的 STRIDE 方法对威胁进行分析，详细内容见 2.1.

2）风险评估

确定每个威胁和资产对应的安全等级（Security Level）。安全等级用于衡量安全相关资产满足特定安全级别所需的安全机制强度。安全级别的是通过确定威胁等级（Threat Level），即对应于风险的“可能性”，和影响等级（Impact Level），即风险的“影响”程度，这两个维度共同确定的。

a.　威胁等级

威胁等级指发动攻击时而成功引发该漏洞的难易程度，分为窗口、知识技能、设备、评估对象的知识等四类因子。

窗口指发动攻击时利用该漏洞时，所采用的攻击途径，分为远程、近距离、本地、物理接触等四等：

1）远程：攻击者可以通过互联网利用该漏洞对汽车发动攻击，比如 4G、3G 等；

2）近距离：攻击者可以通过共享的物理或逻辑利用该漏洞对汽车发动攻击，比如蓝牙、Wi-Fi、IEEE 802.11、本地 IP 子网等；

3）本地：攻击者通过读/写操作或运行应用程序/工具来利用该漏洞，即本地需要进行参与，该漏洞才能被利用，比如攻击者需要本地登录、需要用户去下载、接受恶意的内容；

4）物理接触：攻击者必须物理接触汽车才能发动攻击，例如通过 OBD II 对汽车总线进行攻击。

知识技能指发动攻击时，使用基本原理、方法、知识群体受众面等综合考量，即发动攻击时的难易程度，分为业余者、熟练操作者、汽车安全专家、多领域安全专家等四等：

1）业余者：攻击者利用现有的攻击执行简单的指令来发动攻击，但不会对攻击方法和攻击工具进行改进；
2）熟练操作者：攻击者有一定的安全领域或汽车领域的相关知识，并能进行相关的业务，知道简单和流行的攻击流程，可对所利用的攻击工具进行改善；
3）汽车安全专家：熟悉汽车 ECU 等关键零部件底层的算法、协议、硬件、架构或安全领域最新定义的攻击技术和工具、牢固的密码学知识、经典的攻击方法；
4）多领域专家：攻击者以漏洞利用发动攻击，不同的攻击步骤上，需要不同专业领域的知识。

设备指发掘和利用漏洞和发动攻击所使用的设备的高级程度，分为公开的硬件设备和软件、公开的专用硬件设备和软件、定制或专有的硬件设备和软件、多种定制或专有的硬件和软件等四等：
1）公开的硬件设备和软件：发动攻击时所使用的设备是已经公开可得到的，传统的安全领域的比较常见的，比如协议分析仪、下载器、通用 IT 设备-笔记本等等；
2）公开的专用硬件设备和软件：攻击者不容易得到的设备，但可以通过购买或者开发攻击脚本，比如车载通信设备，Vehicle Spy，CANoe，USRP 等；
3）定制或专有的硬件设备和软件：该设备是特殊生产的或是特别复杂的软件，该设备或软件是受控的，或者是非常昂贵的，比如某种国家机构专用的脱壳工具；
4）多种定制或专有的硬件和软件：攻击者在发动攻击时，不同的攻击步骤上，需要不同专业定制的设备或软件。

评估对象的知识指获得攻击知识的途径，分为公共、受限、敏感和重要等四个等级，如

表 4 所示：
1）公共：通过公开途径获取，比如网络等；
2）受限：仅能在某权限部门获取知识，比如技术开发部门；
3）敏感：仅能在某权限部门中某几个团队共享，并仅限于指定团队成员；
4）重要：仅限于少数指定团队且具有严格控制。

表 4　威胁等级评分说明

参数名称	等级	评分
窗口	远程	3
	近距离	2
	本地	1
	物理接触	0
知识技能	业余者	0
	熟练操作者	1
	汽车安全专家	2
	多领域安全专家	3

设备	公开的硬件设备和软件	0
	公开的专用硬件设备和软件	1
	定制或专有的硬件设备和软件	2
	多种定制或专有的硬件和软件	3
评估对象的知识	公共	0
	受限	1
	敏感	2
	重要	3

威胁等级最终数值由下表确定，如表 5 所示：

表 5　威胁等级评分数值

TL 参数值总和	威胁等级（TL）	TL 数值
大于 9	无	0
7～9	低	1
4～6	中	2
2～3	高	3
0～1	严重	4

b.　影响等级

影响等级指对汽车发动攻击后表示产生危害的相关等级，分为人身安全、财产、操作、隐私及法规等四类因子。

人身安全指发动攻击后，在汽车中人受到安全伤害的严重程度，分为无、轻度伤害、严重伤害、生命威胁等四等：

1）无：不产生人身伤害；

2）轻度伤害：驾驶员及乘车人受到轻微伤害，但能够自由行动；

3）严重受伤：驾驶员及乘车人不能自由行动；

4）生命威胁：驾驶员及乘车人生命危机，或受伤人数较多。

财产指得发动攻击后，对于汽车厂商、零部件厂商以及个人直接和间接的损失的财产总和考量，分为无、低、中、高等四等：

1）无：可不产生财产损失；

2）低：单车的财产损失；

3）中：多车的财产损失；

4）高：整车厂或零部件厂受到巨大财产损失甚至国家的汽车行业遭到巨大的财产损失。

操作指发动攻击后，在汽车功能方面，引起意想不到的损失，分为无、低、中、高等四等：

1）无：可不产生操作影响；

2）低：只对娱乐系统操作影响；

3）中：对车身系统操作影响；

4）高：对动力控制系统操作影响。

隐私指的是发动攻击后，因侵犯个人隐私数据引起的损失，分为无、低、中、高等四等，如表 6 所示：

1）无：可不产生隐私数据及法规的损失；

2）低：侵犯个人账户、密钥、通讯录等隐私数据，引起轻微的法律法规的破坏；

3）中：侵犯多人账户、密码、通讯录等隐私数据；

4）高：整个车型、整个整车厂甚至全部车厂相关用户隐私数据，引起严重的法律法规的破坏。

表 6　影响等级评分说明

参数名称	等级	评分
人身安全（PS）	无	0
	轻度伤害	10
	严重伤害	100
	生命威胁	1000
财产（PP）	无	0
	低	10
	中	100
	高	1000
操作（OA）	无	0
	低	10
	中	100
	高	1000
隐私及法规（PA）	无	0
	低	1
	中	10
	高	100

影响等级最终数值由表 7 确定：

表 7　威胁等级评分数值

影响等级参数值总和	影响等级（IL）	IL 数值
0	没影响	0
1～19	低	1
20～99	中	2
100～999	高	3
大于和等于 1000	严重	4

c.　安全等级

安全等级的评估综合威胁等级和影响等级两个方面进行，如表 8 所示。

表 8　安全等级评分说明

安全等级（SL）		影响等级（IL）				
威胁等级（TL）		0	1	2	3	4
	0	QM	QM	QM	QM	低
	1	QM	低危	低危	低危	中等
	2	QM	低危	中等	中等	高危
	3	QM	低危	中等	高危	高危
	4	低	中等	高危	高危	严重

3）安全需求

对资产、威胁、安全属性和安全级别进行评估的列表。研发人员根据列表中的安全级别，确定开发优先级。有可能存在一个资产会存在多个威胁，因此这个资产也会有多个安全等级，在进行开发的时候，通常的做法是关注安全等级最高的。

HEAVENS 是较完整的风险评估方法，可应用于汽车信息安全风险评估的需求导出。但相关参数需要改进。

附录 B 工作组工作历程

汽标委智能网联汽车分标委汽车信息安全标准工作组根据单位申请情况成立了标准研究项目组，确定百度和联合汽车电子有限公司为牵头单位，并在此基础上明确了任务和分工，积极开展标准的研究、调研、讨论、报告起草等工作。

主要的工作历程如图 12 所示，主要分成两个阶段：

- **阶段 1：ECU 分级思路调研和讨论**

此阶段围绕整个标准研究项目的核心开展，即回答如何来编写后续的标准内容。考虑到汽车 ECU 囊括的对象范围巨大，所涉及的 ECU 多种多样，很难用统一的一套标准来定义技术要求。因此，项目组一致认可的是对 ECU 进行一个区分，再针对不同的类别进行安全防护措施的定义。经过若干次的讨论，确定了本报告第四章节的内容撰写思路。

- **阶段 2：标准研究报告编写和讨论**

在确定了 ECU 分级思路之后，项目组开始了标准研究报告的编写和讨论。首先，工作组讨论确定了报告的框架，即报告要呈现哪方面的内容；其次，根据框架进行了工作分工，大家各自完成相应内容的编写，并反馈给牵头单位进行汇总整理。最后，形成了研究报告草稿。

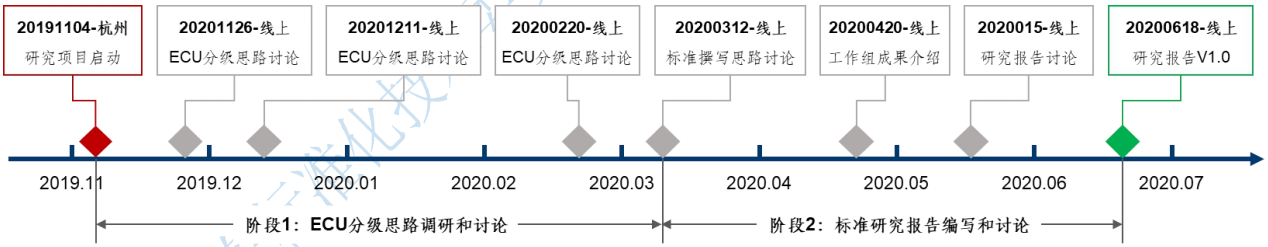

图 12　标准研究项目组主要工作历程

未完待续

完整版请扫描二维码下载