专题：智能网联汽车

智能网联汽车一体化安全问题与内生安全

贾宏颖[1]，李玉峰[1,2]
（1. 紫金山实验室，江苏 南京 211111；
2. 上海大学，上海 200444）

摘　要：车路云一体化发展趋势下，信息物理融合促进汽车安全的内涵和外延发生全新变革，功能安全、网络安全、数据安全深度融合，产生了难以分割的一体化安全（security & safety，SS）新域挑战。在综合分析智能网联汽车一体化安全问题和现有安全技术局限性的基础上，以内生安全存在性定理为指导，提出了一种基于动态异构冗余（dynamics heterogeneous redundancy，DHR）的内生安全构造技术，以一体化的构造效应解决三重安全交叠问题，实现不依赖先验知识的已知/未知威胁防御。大量内生安全白盒插桩注入测试结果表明，内生安全DHR架构具备100%差模抑制能力。为推动实现内生安全上车的总体目标，还探索了一条以“事前可阻断－事中可防御－事后可溯源”为核心的智能网联汽车内生安全上车近景规划方案。

关键词：智能网联汽车；动态异构冗余；一体化安全；内生安全
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024258

Security & safety issues and endogenous security for intelligent connected vehicles

JIA Hongying[1], LI Yufeng[1,2]
1. Purple Mountain Laboratories, Nanjing 211111, China
2. Shanghai University, Shanghai 200444, China

Abstract: With the rapid development of vehicle-road-cloud integrated system (VRCIS), physical space and cyber space were deeply intertwined, resulting in a brand-new transformation of automobile safety. New challenges arise in the integrated security domain, where safety, security and information security were deeply overlapped. Based on a comprehensive analysis the integrated security problem of intelligent connected vehicle (ICV) and limitations of existing security defense methods, guided by the endogenous security existence theorem, a dynamics heterogeneous redundancy (DHR) based endogenous security construction technology was proposed to solve the triple security overlap problem with integrated construction effects, achieving known and unknown threat defense without relying on prior knowledge. The results of a large number of endogenous safety white-box pile injection tests show that the endog-

收稿日期：2024−11−25；修回日期：2024−12−10
通信作者：李玉峰，liyufeng_shu@shu.edu.cn
基金项目：国家重点研发计划项目（No.2023YFB2504800）
Foundation Item: The National Key Research and Development Program of China (No.2023YFB2504800)

enous safety DHR architecture had 100% differential mode suppression capability. In order to promote the overall goal of achieving endogenous safe boarding, a close range planning scheme for intelligent connected vehicles with the core of “pre blocking, mid defense, and post traceability” had also been explored.

Key words: intelligent connected vehicle, dynamic heterogeneous redundant, security & safety, endogenous security

0 引言

国家高度重视智能网联汽车产业发展，率先提出并实践智能网联汽车“车路云一体化”的中国方案，致力于构建集聪明的车、智慧的路、实时的云、可靠的网于一体的复杂信息物理系统（cyber physical system, CPS）[1]，推动汽车从传统移动空间驶入智能网联空间。车路云一体化系统示意图[2]如图1所示。

图1中，在智能网联空间内，车的安全、路的安全和网的安全高度耦合，网络安全成为智能网联汽车健康发展的重大挑战。大规模、多主体的互联互通致使车路云一体化系统暴露的攻击面随之增大，网络安全风险急剧提高。软件定义汽车新趋势下，车内软件代码数量激增，漏洞、后门呈几何级增长，且未知漏洞、未知后门难以彻查。攻击者可以绕过重重设防的安全机制，发起致瘫、致乱、窃情等攻击行为，危害行车安全乃至国家安全。2019年以来车联网安全典型事件见表1。Upstream公司发布的《2023年全球汽车网络安全报告》显示，过去5年中全球汽车行业因网络攻击造成的损失超5 000亿美元[3]。

车路云一体化趋势下，信息物理融合促使汽车安全的内涵和外延发生新变革，功能安全（safety）、网络安全（security）、数据安全（information security）深度交叠，产生了难以分割的一体化安全（security & safety，SS）新域挑战。域内功能安全、网络安全、数据安全三者此消彼长，传统分而治之的安全方案难以为继。例如，为了增强自动驾驶汽车内部网络的安全性，可能需要对内部网络相关通信进行认证和加密，但是认证和加密技术的实施，却可能损害功能安全相关系统处理信息的实时性；而从保障功能安全角度实施或增加的许多技术措施，会增大网络

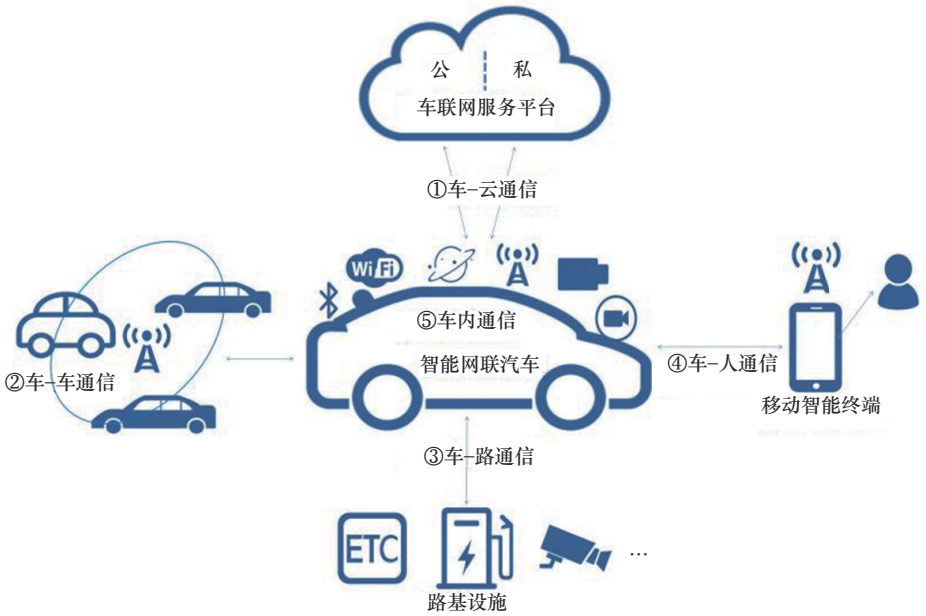


图1 车路云一体化系统示意图[2]

表 1　2019 年以来车联网安全典型事件

序号	事件
1	2019 年，中国工业和信息化部在车联网网络安全专项调研、检测中发现，85% 的汽车网联关键部件存在着安全漏洞
2	2021 年 6 月，加拿大程序员 Shankar Gomare 在开发“Voice for Tesla”程序时，发现特斯拉蓝牙钥匙存在技术漏洞，攻击者利用该漏洞可解锁任意特斯拉汽车
3	2022 年 2 月，奇安信星舆实验室 Kevin2600 发现本田汽车钥匙存在设计缺陷（CVE-2021-46145）
4	2022 年 5 月，特斯拉的“无钥匙进入系统”曝出重大安全漏洞，攻击者可以通过对 BLE 低功耗蓝牙通信的中继攻击，在 10 s 内解锁一辆特斯拉 Model 3 或 Model Y
5	2022 年 9 月，黑客操纵了俄罗斯本土网约车服务平台 Yandex Taxi，伪造车辆调度信息并向平台下发虚假订单，使大量网约汽车在莫斯科市中心集聚，造成了长达 2 h 的交通堵塞
6	2023 年 4 月，安全研究员发现汽车盗窃犯通过拆卸大灯旁的保险杠接入控制器区域网络（controller area network，CAN）总线，发送特定的 CAN 报文欺骗车辆认为钥匙是有效的，以此盗窃丰田 RAV4 2021 款汽车
7	2023 年 9 月，汽车零部件供应商 ALPINE 遭受勒索软件 BLACKBYTE 攻击，1 029.22 MB 数据被公开，其中包含护照、收据、文档等
8	2024 年 2 月，总部位于德国的现代汽车欧洲分部遭受 Black Basta 勒索软件攻击，攻击者声称窃取了 3 TB 企业数据

攻击面，加大网络安全的防御压力。现阶段，虽然美欧国家提出了众多系统安全工程的弹性设计方法，但仍缺乏“串珠成链”的一体化安全架构统领，难以付诸工程实践。

针对智能网联汽车功能安全、网络安全、数据安全一体化保障难题与韧性抗毁的高安全需求，本文探索出了一条以内生安全赋能智能网联汽车韧性工程的技术路径。（1）基于内生安全存在性定理，论证了任何不确定性扰动均可以概率形式表达为动态异构冗余（dynamics heterogeneous redundancy，DHR）域内的差模/共模安全事件；（2）本文提出了一种基于动态异构冗余的内生安全构造技术，以一体化的构造效应解决三重安全交叠问题，可有效应对已知/未知威胁；（3）应用内生安全白盒测试方法，量化评估目标系统韧性安全能力，并开展实车验证。在此基础上，规划内生安全上车近景目标及方案，力争为车企塑造新的竞争优势，助力车路云一体化应用试点建设，保障智能网联汽车产业安全高质量发展。

1　智能网联汽车一体化安全问题

智能网联技术的发展推动汽车向高级别自动驾驶和车路云一体化方向迈进，信息空间与物理空间加速融合，智能网联汽车面临的安全风险从“信息域”向“信息域+物理域”扩展。网联化“信息虚体”的智能感知与规划决策能力，深度融入传统车、路组成的“物理实体”之中，形成以虚知实、以虚控实、虚实结合的新型 CPS 系统。对一个庞大的 CPS 而言，信息虚体的功能故障、性能局限、网络攻击、数据错误等，不仅能够在信息空间造成各种安全问题，还可能将安全风险大规模地投射于物理空间。

作为空前复杂的 CPS，车路云一体化的智能网联汽车的功能安全、网络安全、数据安全三者深度交织、相互叠加，演进为难以分割的 SS 新域安全问题，如图 2 所示。一方面，单纯的功能安全问题和网络安全问题仍然存在，例如，随机性的物理失效、不确定性的软件失效、人为的网络攻击等；另一方面，多重安全间存在着难以解耦的复杂因果链[4]，例如，功能安全中的软硬件故障可能会破坏网络安全防御屏障，而网络安全中基于高危漏洞/后门的攻击，也往往会使智能网联汽车功能安全设计失效，SS 因果链复杂交织[4]如图 3 所示。

针对各类不确定性扰动交织演化带来的 SS 新域安全问题，传统分而治之的防御策略左支右绌。如何设计目标系统的一体化安全机制，保障系统或设备在同时面对随机性故障和人为性攻击时，仍然

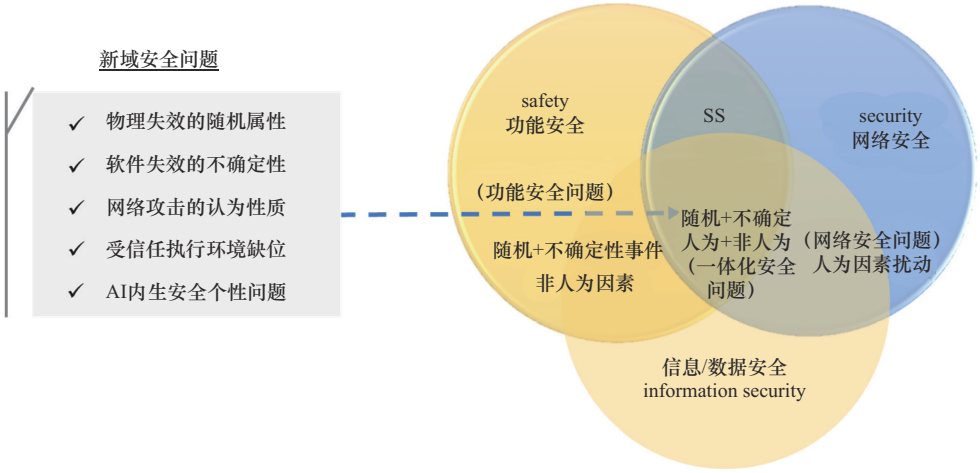


图2　多重安全深度交织引发新域安全问题

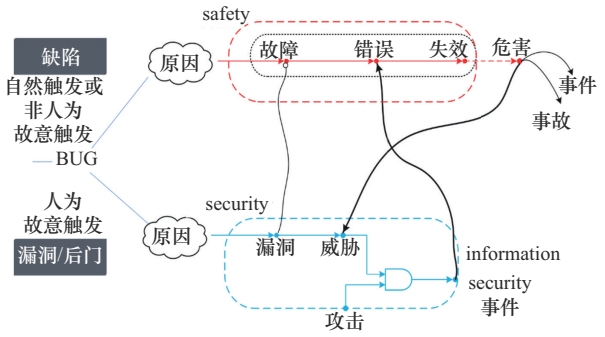


图3　SS因果链复杂交织[4]

能够正确执行预期功能，且能保证敏感信息或数据的私密性、完整性、可信性，是智能网联汽车“车路云一体化”发展亟待突破的难点问题。

2　国内外技术发展现状及挑战

2.1　功能安全与网络安全双V模型发展路线

现阶段，相关研究普遍将智能网联汽车的功能安全问题和网络安全问题分开考虑，沿双V模型各自发展，如图4所示。在功能安全问题上，主要以国际标准《道路车辆功能安全》（ISO 26262）、国家标准《道路车辆 功能安全》（GB/T 34590）为基本遵循，结合多样化的监测方案、失效可运行或失效降级的安全模式、仿真与实车相结合的功能安全测试、全流程的产品过程管理等[5]，提高智能网联汽车系统的可靠性，降低随机性失效或系统性失效带来的风险。在网络安全问题上，基于国际标准《道路车辆-信息安全工程》（ISO/SAE 21434），将传统互联网行业中经典安全技术在智能联网汽车上优化适配、组合复用。例如，世界著名汽车零部件供应商博世给出的汽车网络安全防护方案[6]如图5所示，其主要技术思路便是将互联网中的入侵检测、隔离、加密、认证等技术引入智能网联汽车的安全保障。

然而，上述传统的安全防护技术主要以对威胁的精确感知为基本前提，遵循“威胁感知，认知决策，问题移除”的防御模式，难以有效抵御利用软硬件未知漏洞、后门等发起的不确定性攻击，难以可靠应对高级可持续的网络威胁入侵。例如，以震网（Stuxnet）、火焰（Flame）、毒曲（Duqu）、BlackEnergy、Industroyer、Triton等为代表的针对CPS的恶意攻击层出不穷。CPS一旦遭到恶意攻击，则可引发控制系统、通信系统、信息管理系统、信息化基础设施的隐私性、完整性和可用性受到破坏，进而造成底层智能网联汽车物理设备破坏/故障、连锁式事故，威胁汽车生产安全、人身安全等。以熔断、幽灵、恩智浦（NXP）、Bleedingbit等为代表的芯片级漏洞，和以永恒之蓝（WannaCry）、内核安全漏洞（TCP SACK PANIC）等为代表的操作系统级漏洞，给大量采用有缺陷软

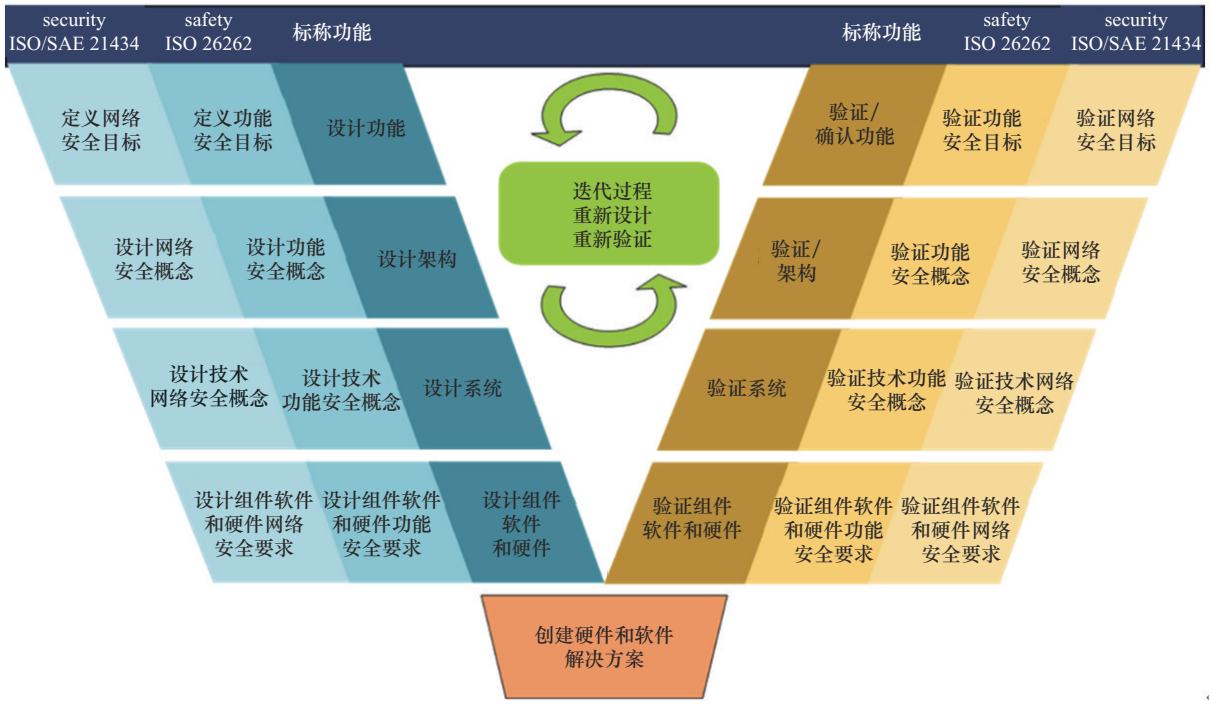


图4　智能网联汽车功能安全与网络安全双V模型发展路线

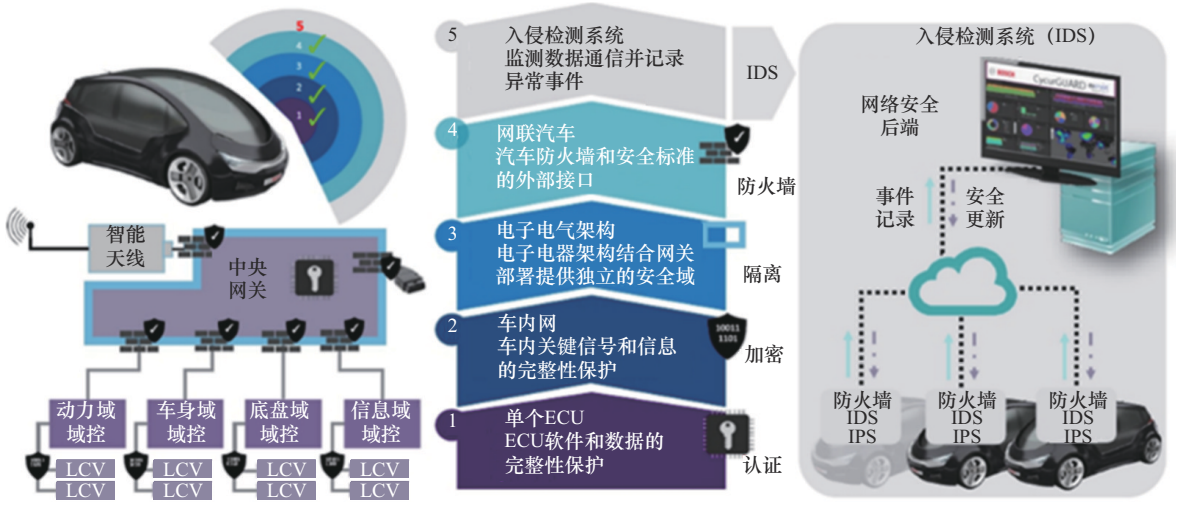


图5　博世汽车网络安全防护方案[6]

注：LCV为轻型商用车（light commercial vehicle），ECU为电子控制单元（electronic control unit），IPS为入侵防御系统（intrusion prevention system）。

硬件制造的汽车控制系统带来了严重的安全隐患。

综上，现有网络安全方案难以抵御基于未知漏洞、后门发起的不确定性攻击，而现有功能安全设计在高危漏洞攻击得手后可能失效。智能网联汽车功能安全与网络安全分而治之的双V模型存在安全效益的不可加性，无法满足智能网联汽车的高安全需求。

2.2　美欧网络弹性工程发展路线

传统安全设计侧重从预防、抵御两方面制订防护目标及措施，难以提升智能网联汽车应对未知风险、未知威胁的快速恢复、主动适应的能力。2023年，美国国家公路交通安全管理局（National Highway Traffic Safety Administration，NHTSA）在其网络安全主页上增加了设计入内的网络弹性（design-in

cyber resiliency）方法[7]，强调不仅要具有预防、抵御威胁的能力，还应具备系统功能快速恢复和主动适应的能力，即弹性能力。

实际上，早在2010年，美国研究机构MITRE就率先提出了网络弹性的概念[8]，2018年被美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）采纳。NIST将网络弹性定义为“包含网络资源的实体所具备的对各种不利条件、压力、攻击或损害的预防、抵御、恢复和适应能力”。自此，网络弹性受到美欧各国重视。2020年以来，欧盟紧锣密鼓出台《网络弹性法案》[9]，预计于2025年生效。2023年，美国发布《国家网络安全战略》，强调建立一种弹性数字生态系统[10]。2024年，美国总统办公厅和总统科技顾问委员会发布《信息物理系统网络弹性战略》。

NIST在2022年年底正式发布《开发网络弹性系统——系统安全工程方法》（NIST SP 800-160V2R1）[11]，包含系统安全弹性设计的4个目的、8个目标；列举了14类技术、49种方法供系统工程师采用；提出了5条战略性设计准则，用于描述组织的风险管理策略，并进一步细化为14条结构化设计原则，如图6所示。

在当前的技术背景下，美欧等国虽已提出了众多系统安全工程的弹性设计方法，如动态重构、动态威胁感知、深度防御、特性验证、起源追踪等，但这些方法仍缺乏一个统一的安全架构来指导整合，使得各项突破性技术难以在工程实践中得到有效实施。目前，国内一些企业和单位正在积极跟踪这一方向，探索通过实施融合安全策略，综合运用内生安全、动态防御、安全监控等技术，使CPS系统具有预测、感知、承受、恢复和适应不利条件和攻击的能力。

3 构造决定的一体化安全：内生安全

3.1 内生安全存在性定理

从攻击方视角来看，攻击链的有效性和可靠性都十分依赖目标系统的静态性、确定性和相似性，其中任一环节的变化都可能使网络攻

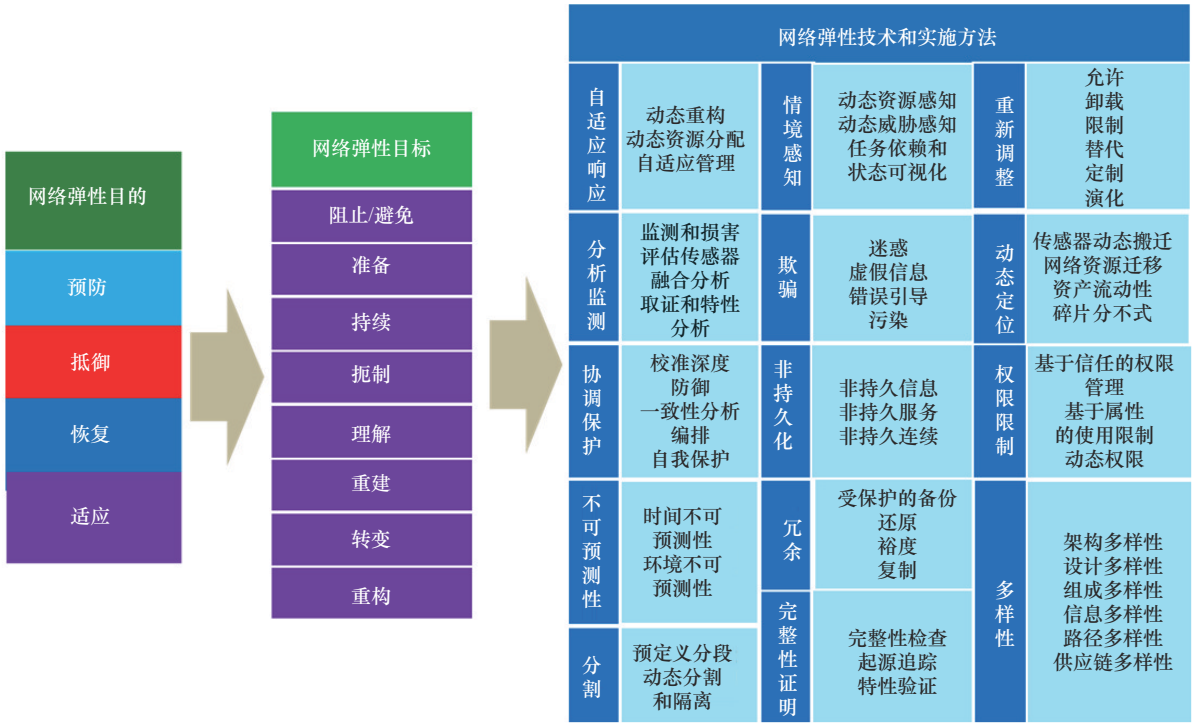


图6 NIST《开发网络弹性系统——系统安全工程方法》的目的、目标和技术框架

击无法实现。例如，在系统探测、漏洞挖掘等阶段导入随机性、动态性可以有效对抗隐蔽渗透；在系统控制、系统损毁等阶段导入异构冗余择多判决机制可以应对潜伏攻击。对于网络安全防御机制而言，存在3个核心要素：动态性/随机性（dynamics，D）、多样性/异构性（heterogeneous，H）、冗余性（redundancy，R）。这3个核心要素对于增加系统不确定性和防范未知安全威胁及未知风险至关重要。

基于不可能三角理论和文氏图的运用，构建DHR三元解构模型[12]，如图7所示。针对D、H、R三要素在未知威胁防御中的技术作用展开定性分析，以明确各要素组合形态的安全属性、适用前提，以及内在缺陷。基于DHR三元解构模型的安全技术分析见表2，分析表明，如果系统防御机制的D、H、R三要素始终处于不完全相交状态，那么该系统一定不具备抵御基于内部未知安全问题的内外协同攻击的能力。

由此，可以推导出内生安全存在性定理：如果一种构造或算法同时具备动态性、多样性和冗余性三要素的完全相交表达，则即使在缺乏先验知识条件下，也能够基于构造的内源性效应管控构造内基于任何未知漏洞、后门、病毒、木马等的差模攻击，抑制随机性或不确定性因素引发的差模性质扰动。

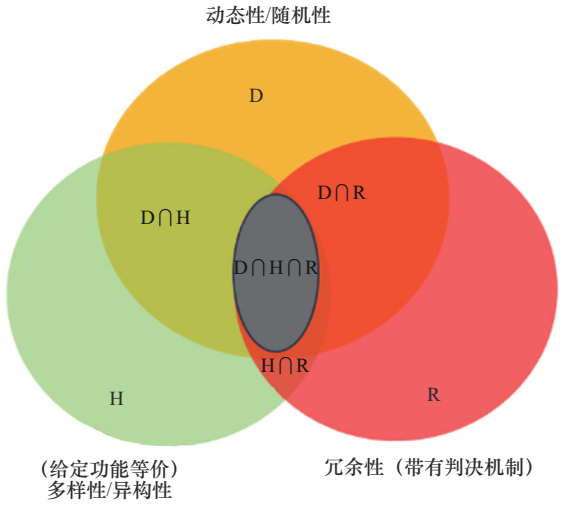


图7　DHR三元解构模型[12]

3.2　内生安全构造技术

以内生安全存在性定理为指导，提出基于动态异构冗余（DHR）架构的内生安全构造，如图8所示。在非相似余度构造基础上，导入状态或输出反馈控制机理，能够使DHR构造内的各环节、

表2　基于DHR三元解构模型的安全技术分析

	典型技术	局限性及缺陷
D域	—	只有单一作用对象的动态性，无工程应用意义和效果
R域	同构冗余	存在大量共模漏洞，易发共因故障
H域	—	固定作用对象的多样性，无工程应用意义和效果
D∩H域	移动目标防御	通过动态调换功能等价的多样化目标对象，可以提高攻方漏洞利用的不确定性，但无法抵御基于未知漏洞/后门的内外协同攻击
R∩H域	非相似余度构造	利用并行的异构冗余执行体结合择多判决机制，在满足$f\leqslant(n-1)/2$条件下可识别并屏蔽差模行为，但受限于系统架构的静态性和确定性，无法抵御持续性渗透攻击
D∩R域	动态同构冗余	利用并行的同构冗余执行体结合择多判决机制，在满足$f\leqslant(n-1)/2$条件下可识别并屏蔽差模行为。通过动态调度机制使系统具备不确定性，可应对持续性渗透攻击，但无法抵御基于共模漏洞/后门的网络攻击或共因故障
D∩H∩R域	加密/认证	遵循“一次一密”原则的加密/认证技术具备内生安全特性，其最大隐患在于宿主软硬件是否处于可信执行环境
	区块链技术	区块链的分布式节点允许动态加入或退出，节点间具备异构能力，采用基于冗余的共识机制，本质上属于D∩H∩R域的子集，但在实践上难以保障各节点的软硬件宿主系统同样具有内生安全特性
	零信任技术	零信任是一种基于先验知识库的持续性安全防护创新理念，从技术集和体系化排布的角度看属于D∩H∩R域子集，但工程实践过程中部署策略的确定往往伴随D、H、R特性的破坏，不再具备应对未知威胁和未知风险的能力

注：n是冗余度数，f是允许同时存在的差模问题冗余体数量。

各要素或各变量间构成前后相连、首尾相顾、因果相关的反馈，任何一个环节或要素的变化，都会引起其他环节或要素的变化，从而形成反馈回路和控制运动。因此，反馈控制在机理上能够通过迭代收敛的动态性（D）来实时调节多样性（H）和冗余度（R），从而满足DHR完全相交要求，以一体化的构造效应解决系统架构内未知威胁或网络攻击等功能安全、网络安全乃至信息安全三重安全交织问题，在“隘口设防、要地防御”中形成高可信、高可靠、高可用“三位一体”的系统级安全能力。

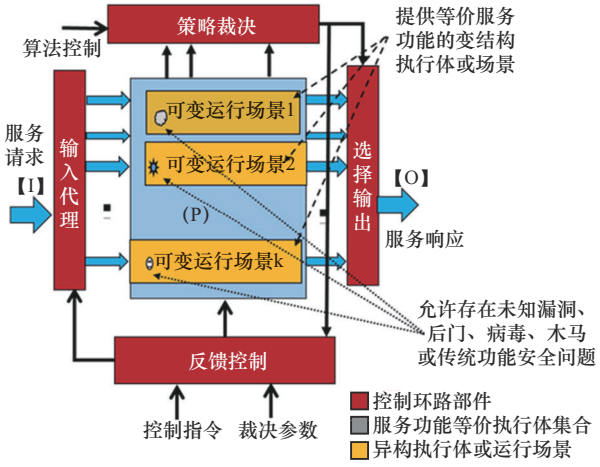


图8　DHR架构的内生安全抽象模型

借鉴香农信息论中“完美保密”模型的“一次一密”特性，内生安全DHR架构在感知到差模扰动后，在拟态裁决指导下，通过反馈控制模块以迭代收敛后向验证机制清洗掉异常运行场景，并阻断攻击链，实现可信运行环境的“一次一重构”。每次重构后，目标构造内的结构缺陷或环境漏洞都会被重新加密，使攻击者无法长期占据单向透明优势。从密码学的视角来看，DHR架构本质上是一种基于结构编码构造加密方式，以获得“完美安全”的创新方法[12]。

3.3　内生安全功能白盒测试

为检验评估目标系统的内生安全功能及性能，提出了一种白盒插桩注入测试方法。该方法针对目标构造内的敏感功能代码段，以人工植入钩子或加载测试模块的方式，向被测对象系统内植入一定数量、具备差模性质且不为设备制造者和使用者所知悉的“漏洞后门、病毒木马”测试用例。测试方可在DHR架构输入端构造与测试例相应的激励序列，并观察输出端的响应信息，依此可测量出现安全事件的概率。

以DHR架构三余度测试模型为例，阐述内生安全白盒测试的步骤流程。图9中，A、B、C分别代表被测系统的3个异构执行体环境，三者间具有相同的服务功能交集P。

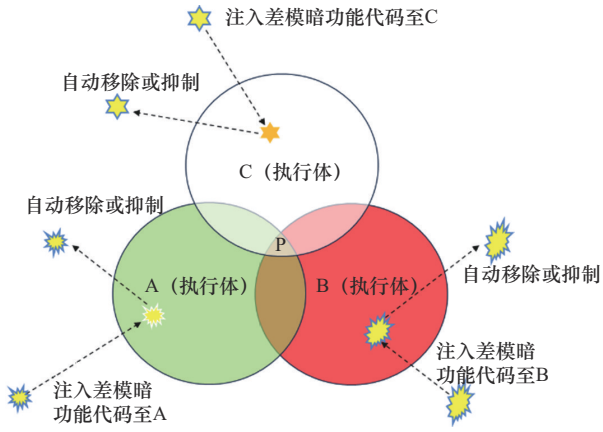


图9　DHR架构三余度差模测试例注入

步骤1　分别在执行体环境A、B、C内注入差模测试例，所有测试例均属于被测目标的未知项。

步骤2　从输入端注入测试例激活序列，观察输出端是否出现攻击响应序列。

预期效果如下。被测对象应该无法从输出端获得受测试序列和植入差模测试例共同作用的响应序列。所有落在3个异构执行体（A，B，C）区域内的差模攻击均可被DHR架构内的策略裁决模块感知并屏蔽，通过反馈控制模块以迭代收敛后向验证机制清洗掉异常执行体，并阻断攻击链，实现可信运行环境的动态重构。

大量测试积累，全面验证了内生安全DHR架构具备100%差模抑制能力。从理论和实践上，

都证明了内生安全DHR构造可有效应对任何差模性质的广义功能安全扰动，包括基于未知漏洞、后门、病毒、木马等的差模攻击，以及基于随机性或不确定性因素引发的差模性质扰动等。

4　智能网联汽车内生安全方案与实践

车路云一体化架构下，智能网联汽车面临的安全风险从“信息域”向“信息域+物理域”扩展，迫使安全技术随之转型，呈现以下发展趋势：其一，从“功能安全”“网络安全”遵循的双V模型各自发展，向“功能安全+网络安全+数据安全”一体化保障转型；其二，从“用户侧外挂”向“制造侧内生”转型，强调在系统功能设计之初，就将安全同步设计入内。这与NHTSA 2023年倡导的“设计入内的网络弹性”理念不谋而合。如前所述，美欧网络弹性工程围绕“预防、抵御、恢复、适应”的目的，已在技术上形成《开发网络弹性系统——系统安全工程方法》。然而，受限于美欧等国在数字生态系统底层驱动领域的优势壁垒和对尖端技术的信息封锁，我国车企无法靠跟踪美欧网络弹性路线实现自身安全。

4.1　内生安全赋能智能网联汽车韧性工程

紫金山实验室在邬江兴院士的带领下，长期聚焦智能网联汽车一体化安全问题，探索出了一条以内生安全赋能智能网联汽车网络弹性工程的技术路径，如图10所示。以内生安全DHR架构作为“钢筋骨架”的架构统领，以其固有的融合特性，将美欧网络弹性工程技术要素与传统网络安全技术以“混凝土砂浆”形态自然融入其中[13]，依靠结构产生“同素异形体”效应获得指数量级的系统安全增益，这是目前靠堆砌或层层部署各种附加安全技术很难达成的目标。2023年12月第三方权威测试报告评估表明：以100%屏蔽任何差模性质安全事件为目标，对现有信息基础设施进行内生安全升级，改造代价只耗费系统总投资的6%～16%。

在理论研究层面，针对制约全球汽车产业发展的一体化安全保障难题，提出了智能网联汽车功能安全和网络安全联合分析模型，将网络攻击及故障失效转化为广义差模/共模干扰问题，如图11所示；基于内生安全DHR架构，设计了冗余度、异构度、闭环响应时间可调的智能网联汽车内生安全总体技术架构，支持内生安全DHR改造增量式部署和演进式发展；通过稳定状态分布，量化分析不同影响参数下系统功能的可用性，为功能安全、网络安全一体化保障提供了一种可量化设计、可验证度量的新方法[14]，获得行业专家的高度评价。

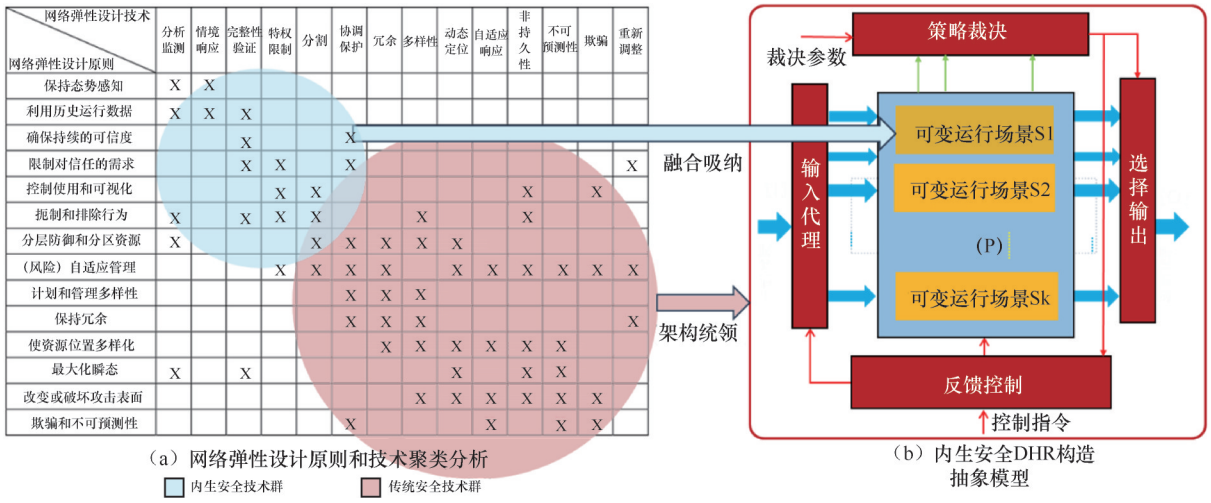


图10　DHR赋能网络弹性工程框架的设计原则和技术方法

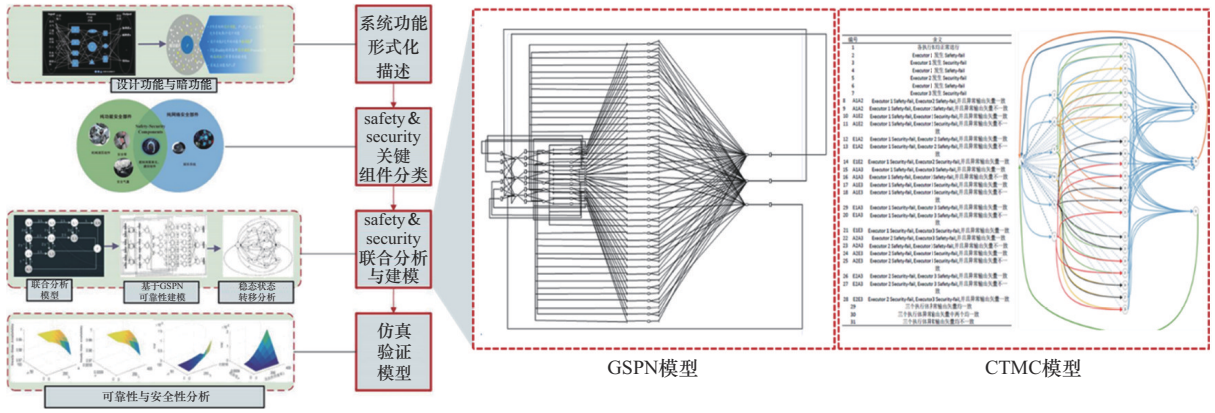


图11　智能网联汽车功能安全和网络安全联合分析模型

注：GSPN模型，是基于广义随机Petri网络（generalized stochastic petri network，GSPN）的SS联合异常分析模型；CTMC模型，是基于连续时间马尔可夫链（continuous time Markov chain，CTMC）的SS联合状态分析模型。

在技术实践层面，以“隘口设防，要地部署”思想为指导，面向智能网联汽车智驾域、网联域等内部脆弱节点，研制了国际首套车端系列化内生安全原型系统，包括：高级驾驶辅助系统（advanced driver assistance system，ADAS）原型系统、内生安全车载网联终端（telematics BOX，T-BOX）原型系统、自动驾驶记录与还原原型系统等，分别如图12、图13、图14所示。系统均已通过权威第三方测试，验证上述内生安全原型系统具备多重安全一体化保障能力，支持抵御感知核心部件功能故障与未知网络安全威胁，支持典型应用场景下黑盒/白盒攻击测试和验证。2023年，联合宇通客车、沃行科技在两种量产车型上完成了内生安全ADAS原型系统和内生安全T-BOX原型系统的实车验证，在郑州、南京两座省会城市开展了为期1年的自动驾驶内生安全应用示范。2024年年初，自动驾驶记录与还原原型系统通过业内某知名品牌的技术定点和商务定点。

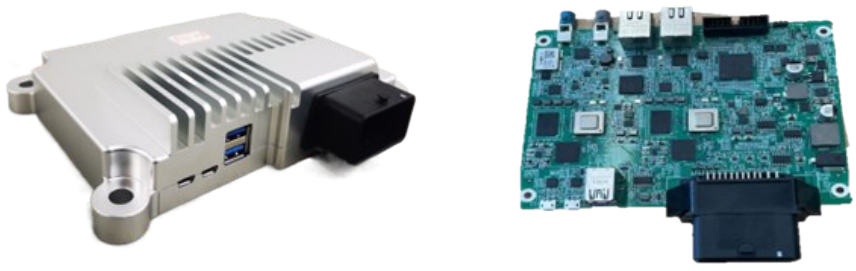


图12　内生安全ADAS原型系统

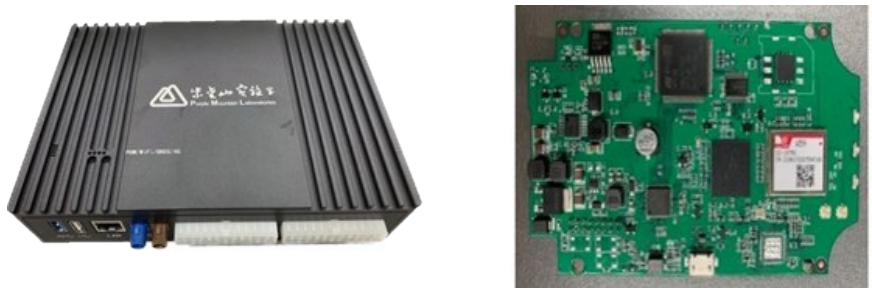


图13　内生安全T-BOX原型系统

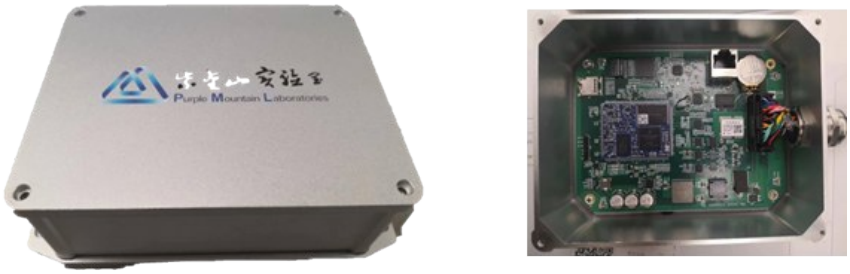


图 14　自动驾驶记录与还原原型系统

4.2　内生安全方案实车验证

为检验智能网联汽车内生安全方案的防御效果，设计了如图 15 所示的实车验证环境。在该环境中，搭建了 2 条相互独立的攻击链路：（1）商用设备链路，备有 10 台商用 T-BOX 设备、10 台商用 ADAS 设备作为攻击靶标；（2）内生安全设备链路，以研制的内生安全 T-BOX 原型系统、内生安全 ADAS 原型系统为攻击靶标。攻击方可以 T-BOX 为入口，挖掘网关和 ADAS 的信息，并经由网关攻入 ADAS，形成完整攻击链路，伪造、篡改指令达到远程控车目的，具体步骤如下。

步骤 1　对 T-BOX 设备进行安全研究，通过端口扫描、密码爆破等方式，获得 T-BOX 设备用户权限。

步骤 2　采集信息，获得 T-BOX 原型系统和 ADAS 原型系统的固件包等信息。

步骤 3　通过对 T-BOX 固件的分析、试探等方式，找到车辆控制开门的指令，最终通过 T-BOX 下发控车指令以控制车门和车灯。

步骤 4　分析网关和 ADAS 固件，分别获取登录网关和 ADAS 的用户名和密码。先登录网关，再通过网关访问 ADAS，根据找到的车辆控制指令，最终通过 ADAS 控制车轮的加减速和转向。

借助紫金山实验室举办的“强网”拟态防御国际精英挑战赛，邀请国内外精英战队对靶标设备进行持续性高强度攻击，在实车验证环境下开展智能网联汽车内生安全方案的效果众测，如图 16 所示。连续 72 h 内，60 支国际精英战队发起网络攻击超 50 万次，最终有 3 支战队通过商用设备链路实现了车门控制、加减速等远程控车操作。测试中，攻击手段以协议类攻击、提权类攻击、Web 应用和漏洞类攻击为主，如图 17 所示。

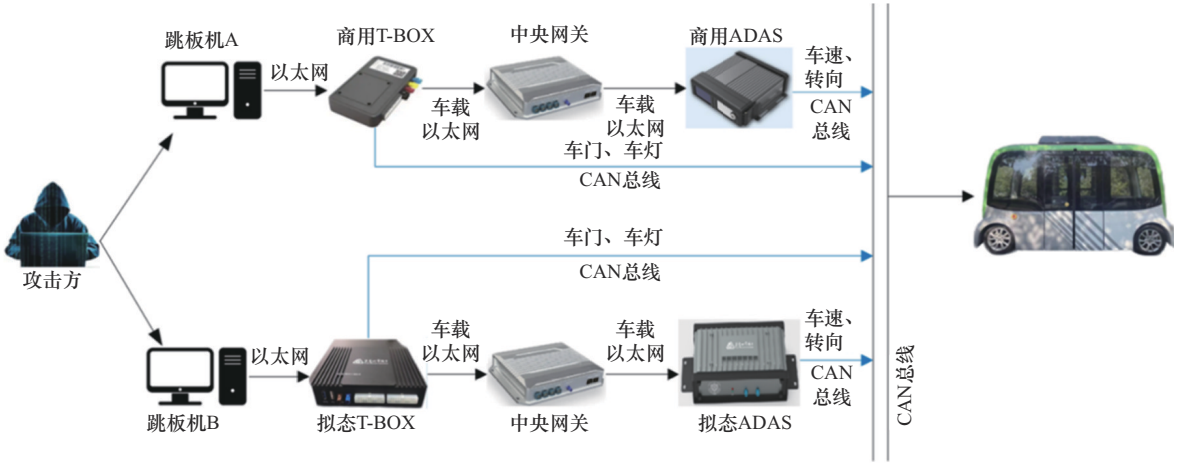


图 15　实车验证环境拓扑示意图

图16　基于DHR的智能化网联化原型系统众测情况

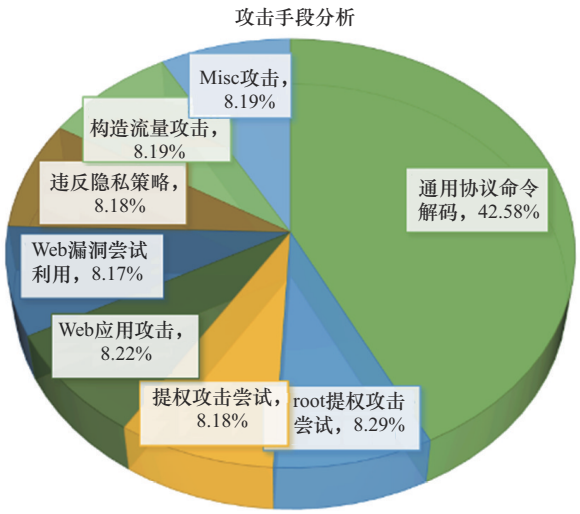


图17　攻击手段统计与分析

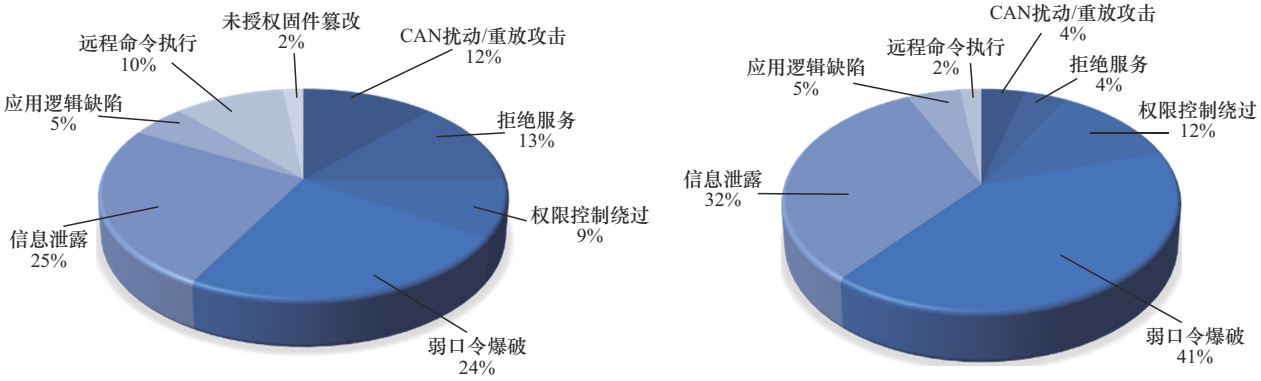
两条攻击链路的实车众测结果见表3。在内生安全设备攻击链路上，内生安全T-BOX原型系统和内生安全ADAS原型系统成功抵御住所有黑盒攻击，仅少数白盒注入攻击造成扰动，被裁决模块及时感知并通过执行体调度斩断攻击链路，并未实现对车辆的实际控制；商用设备攻击链路上，20余台主流商用ADAS和T-BOX设备在高强度的持续性攻击下相继被攻破，无一幸免，大量潜在漏洞被发现，图18反映了主流商用ADAS和T-BOX设备漏洞情况。该测试结果充分验证了基于DHR的内生安全技术方案在未知威胁防御方面的有效性，以及应用于车联网设备安全加固中的优异性能。未来，内生安全理论和技术有望突破美欧“高墙小院”的封锁，为智能网联汽车韧性工程实现提供一条切实可行的创新路径。

4.3　内生安全上车近景规划

为推动实现内生安全上车的总体目标，在整车设计验证阶段，同步开展轻量化内生安全构件设计，打造“事前可阻断－事中可防御－事后可溯源”的智能网联汽车内生安全纵深防线，方案

表3　两条攻击链路的实车众测结果

	黑盒攻击/次	黑盒扰动/次	白盒攻击/次	白盒扰动/次	能否控车
商用T-BOX设备	1 205 066	50	—	—	是
商用ADAS设备	1 124 133	389	—	—	是
内生安全T-BOX原型系统	115 519	0	284 471	4	否
内生安全ADAS原型系统	115 947	0	287 395	10	否



（a）商用ADAS设备漏洞分析　　（b）商用T-BOX设备漏洞分析

图 18　商用 ADAS 和 T-BOX 设备漏洞

设计如图 19 所示。构建系统内在的动态、异构、冗余特性，使系统在不依赖漏洞或攻击特征的情况下，有效应对漏洞导致的网络攻击。即使系统存在未修复的漏洞，也能安全稳定地运行，不会产生网络安全事件。

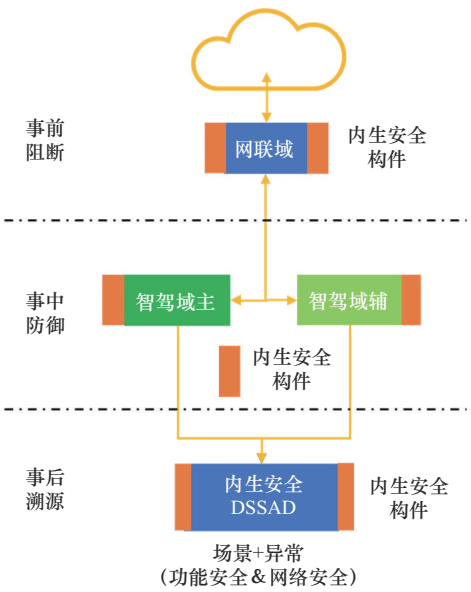


图 19　内生安全上车近景规划方案设计

针对事前阻断需求，研制内生安全构件，以安全模组形式集成部署到网联域，在入口处提供对异常攻击行为的阻断能力，支持防御缓存区溢出攻击、远程执行漏洞攻击等注入攻击，实现阻断攻击者利用漏洞入侵车端系统的安全目标。

针对事中防御需求，研制内生安全构件，以安全模组方式集成部署到智驾域主、辅域控上，通过动态重构、拟态伪装、系统调用监控等，实现对关键域内从操作系统到应用程序的未知威胁主动防御。其中，动态重构模块，以攻击者无法追踪的方式对应用程序和操作系统进行环境重构，通过闭源异构、危险函数加固、库环境异构等多样化方法阻断内存型漏洞攻击信息链；拟态伪装模块，通过布设系统及应用程序伪装陷阱诱使攻击来源暴露；系统调用监控模块，对主、辅域控内系统异常调用情况进行监控并实施用户态程序运行保护。总体上达到“成本可控、安全可防”的效果，解决车端资源受限引发的实用性难题。

针对事后溯源需求，提供自动驾驶数据记录系统（data storage system for automated driving，DSSAD）产品。提取并记录车辆横纵向速度、加速度、转向角等功能安全相关信息，以及入侵监测结果日志等网络安全相关信息；集成分析并识别功能安全致因场景和网络安全致因场景，分别基于功能共振链和攻击自动化生成实现安全事件溯源与风险评估。基于系统过程理论与贝叶斯理论，设置一体化安全事件溯源与联合风险评估，确保在遭受功能故障或恶意网络攻击时，系统

能准确记录/溯源相关信息，并实现功能故障与网络威胁的联合分析与风险评估，为自动驾驶车辆的事故责任划分提供强大技术支持与保障。

综上所述，内生安全上车近景规划聚焦于“事前可阻断-事中可防御-事后可溯源”安全核心需求，形成了三点技术优势：可有效应对基于已知/未知漏洞、后门的攻击；可融合经典防御技术形成指数级安全增益；冗余机制可保障系统功能的高可靠性。该规划不仅为汽车企业贯彻国家标准《汽车整车信息安全技术要求》（GB 44495-2024）提供了技术支撑，也为满足美欧等国汽车安全的网络弹性工程要求提供了实践方案。

5 结束语

针对智能网联汽车功能安全、网络安全、数据安全一体化保障难题与韧性抗毁的高安全需求，本文探索出了一条以内生安全赋能智能网联汽车韧性工程的技术路径，即基于动态异构冗余的内生安全构造技术，以一体化的构造效应解决功能安全、网络安全、数据安全交叠问题，可有效应对系统架构内的已知/未知威胁或网络攻击。经大量白盒插桩注入测试积累，全面验证了内生安全DHR架构具备100%差模抑制能力。最后，规划了内生安全上车近景目标及方案，力争为车企塑造新的竞争优势，助力车路云一体化应用试点建设，支撑智能网联汽车产业安全高质量发展。

参考文献：

[1] 中国智能网联汽车产业创新联盟. 车路云一体化融合控制系统白皮书[R]. 2020.
China Intelligent Connected Vehicle Industry Innovation Alliance. White Paper on vehicle road cloud integrated fusion control system[R] .2020.

[2] 中国信息通信研究院. 车联网网络安全白皮书（2017年）[R]. 2017.
China Academy of Information and Communications Technology. White paper on Internet of vehicles network security (2017)[R]. 2017.

[3] Upstream. 2023年全球汽车行业网络安全报告[R].2023.
Upstream. 2023 Global automotive cybersecurity report[R]. 2023.

[4] 邬江兴. 智能网联汽车内生安全问题与对策[J]. 重庆邮电大学学报(自然科学版), 2023, 35(3): 383-390.
WU J X. Endogenous security problems and countermeasures of intelligent connected vehicle[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2023, 35(3): 383-390.

[5] 中国软件评测中心, 工业和信息化部装备工业发展中心, 国家智能网联汽车创新中心, 等. 车载智能计算基础平台参考架构 2.0[R]. 2023.
China Software Evaluation Center, Equipment Industry Development Center of the Ministry of Industry and Information Technology, National Intelligent Connected Vehicle Innovation Center, et al. Reference architecture 2.0 for vehicle mounted intelligent computing basic platform[R]. 2023.

[6] Bosch Mobility. Trends of future E/E-Architectures[EB]. 2024.

[7] NHTSA. Vehicle cybersecurity[EB]. 2023.

[8] MITRE. Building secure, resilient architectures for cyber mission assurance[R]. 2010.

[9] European Parliament and Council. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [EB]. 2024.

[10] Executive, Office of the President President’s Council of Advisors on Science and Technology. Strategy for cyber-physical resilience: fortifying our critical infrastructure for a digital world[R]. 2024.

[11] Ron Ross, Victoria Pillitteri, Richard Graubart, et al. Developing cyber resilient systems: a systems security engineering approach special publication (NIST SP) [R]. 2019.

[12] 邬江兴. 网络空间拟态防御原理-下册: 广义鲁棒控制与内生

安全[M]. 2版. 北京: 科学出版社, 2018.

WU J X. Principles of virtual defense in cyberspace - volume 2: generalized robust control and endogenous security[M]. Version 2. Beijing: Science Press, 2018.

[13] 邬江兴. 内生安全赋能网络弹性工程[M]. 北京: 科学出版社, 2023.

WU J X. Endogenous security empowering network resilience engineering[M]. Beijing: Science Press, 2023.

[14] LI Y F, LIU Q, ZHUANG W H, et al. Dynamic heterogeneous redundancy-based joint safety and security for connected automated vehicles: preliminary simulation and field test results[J]. IEEE Vehicular Technology Magazine, 2023, 18(2): 89-97.

[作者简介]

贾宏颖（1995– ），女，博士，紫金山实验室助理研究员，主要研究方向为车联网信息安全、多传感器感知算法安全等。

李玉峰（1975– ），男，博士，上海大学教授，博士生导师，紫金山实验室车联网安全学术带头人，国家“新能源汽车”重点专项专家，上海市智能网联汽车网络安全产业协同创新中心主任，上海市智能网联汽车网络安全重点实验室执行主任，中国汽车工程学会信息安全专委会副主任，主要从事车联网安全研究工作。