全面解读
汽车网络安全

通过应对关键车辆安全挑战解锁机遇

Empowering Tomorrow's Automotive Software
www.etas.cn

ETAS

摘要

在车辆的整个生命周期中，具有静态配置的车辆时代已经过去。如今，数字化和互联性为增强用户体验、创新和移动出行解决方案提供了新的机遇，这得益于互联网功能、空中下载（OTA）更新以及车辆与基础设施通信等功能。尽管这些进步带来了一些挑战，但它们也为开发强大的网络安全框架开辟了道路，这些不仅增强了车辆的可靠性，还保护道路用户和保护隐私。事实上，网络安全是确保未来移动出行生态系统在商业模式中取得成功的独特机遇。

从开发和制造流程到互联移动网络内的交互，网络安全现在已成为车辆生命周期不可或缺的一部分。随着远程更新、智能手机集成以及在充电站无缝注册等新功能成为常态，重点转向确保这些创新的安全性。开发人员必须走在潜在风险的前面，持续加强车辆生态系统，同时确保用户充分享受尖端技术的优势。安全标准的不断演进为创新和优化车辆开发提供了更多机会。

本白皮书是应对汽车网络安全动态世界的战略指南。它指出了车辆制造商面临的主要挑战和机遇，并提供了涵盖整个车辆生命周期和生态系统的全面视角——从深度嵌入的软件（ECU）到车载计算机。无论您是传统制造商、供应商还是软件驱动的初创企业，网络安全都可以为您提供战略优势。通过重新思考经典的开发流程，可以发掘出具有深远影响的优化潜力。本文还探讨了如何通过应用四大核心安全原则来增强DevSecOps 和V模型等开发方法，为汽车软件开发的未来提供了一条安全、创新的路线图。

目录

1. 导言

数字化使车辆的使用更加便捷，无论是通过空中下载（OTA）软件更新、高级驾驶辅助系统（ADAS），还是支持互联网的娱乐系统。它为制造商和供应商创造了独立于机械进步之外的创新机会，并提供了销售以外的服务，使车辆在整个生命周期内都能产生收入。虽然每一项重大技术突破都会带来新的机遇，但从纯机械车辆向“轮上计算机”的转变是一次真正的革命。这一转变也伴随着新的挑战，尤其是在网络安全方面：巨大的增长和创新机遇也意味着保护敏感个人数据以及确保整个车型免受潜在网络攻击的责任。通过主动应对这些风险，制造商可以构建更强大、更具弹性的系统，为在日益数字化的汽车领域中取得长期成功和信任奠定基础。

如何维护（数字化）安全的车辆是目前移动出行领域的主要议题之一。根据最近的一项市场调查[1]，网络安全风险甚至被视为汽车公司增长的主要外部障碍。行业内的这种高度意识总体上是积极的：新的风险已被识别，并且正在开发应对和管理这些风险的方法。

这不仅涉及原始设备制造商（OEM）。现代车辆是众多软件和硬件组件的相互作用，包括车载和车外组件，这些组件从开发到运营都在为安全做出贡献，而这些组件由全球供应商和以软件为中心的公司的网络提供。供应链中的所有参与者都有责任了解威胁环境、最小化风险、遵守所有必要的法规，并为整体车辆安全贡献自己的力量。

加强网络安全的发展并非完全出于内在需求。它还源于一系列法律法规和标准的制定，这些法规和标准旨在为整体网络安全概念提供指导，并首先确保道路使用者的安全。在我们深入探讨具体威胁领域之前，有必要仔细研究当前汽车网络安全的监管环境。

2. 汽车网络安全的监管格局

大多数车辆制造商和供应商在多个国家或地区销售其产品。因此，他们还必须了解并遵守其软件、零部件或车辆出口市场的所有法规。这些法规不断演变，新的要求与日益增长的网络安全威胁同步增加。除了法律法规外，行业标准和最佳实践也起着决定性作用。遵守这些标准被强烈推荐，在某些情况下甚至可能是强制性的。因此，对于移动出行领域的制造企业来说，全球化是一个复杂的挑战；需要在一片不断演变的规则丛林中航行，如图1所示。

对于希望在联合国欧洲经济委员会（UNECE）56个成员国销售产品的车辆制造商来说，2021年发布的具有法律约束力的UN R 155是最重要的法规，目前涵盖乘用车、公交车、卡车和拖车。它要求强制实施网络安全管理系统（CSMS），并参考ISO/SAE 21434《道路车辆——网络安全工程》标准作为指导。该法规可能很快会扩展到包括摩托车和踏板车，这也将给这些行业带来压力，要求其改进网络安全流程。中国、美国和印度则有自己的法律法规。因此，全球销售的车型可能必须同时满足多个标准，或者推出不同版本。

虽然新强制性法规的引入确保了道路使用者的高度安全，但它也可能对行业内的OEM和供应商产生深远的经济影响。一些已经开发的车型可能需要重新设计，以符合新的具有约束力的法规框架。这可能导致整个系列停产或仅在特定国家销售，例如保时捷718 Boxter[2]或大众Up[3]。这些例子表明，最佳的网络安全方法需要在整个组织中具备灵活性和前瞻性，而不仅仅是严格遵守当前的法规现状。因此，了解关键的网络安全威胁对于在不断变化的环境中保持竞争力至关重要。然而，企业不必独自应对这一复杂的局面：经验丰富的国际合作伙伴可以提供所需的支持和工具，使其不必每次都从头开始。

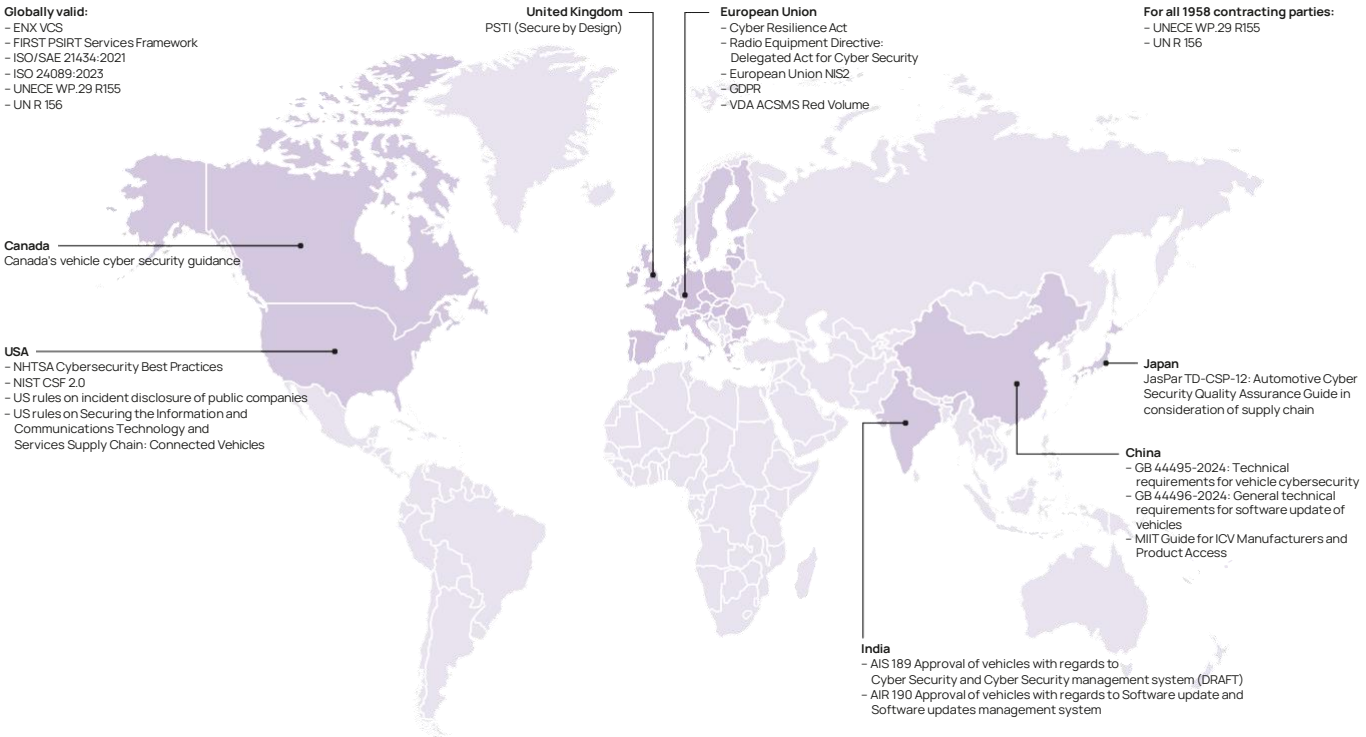

图1: 联网设备的网络安全法规

3. 关键网络安全威胁 - 概述

作为一家解决方案提供商和汽车安全行业的领导者， ETAS 在全球拥有大量客户和案例，始终在汽车行业的脉搏上保持着领先地位。基于这些经验， ETAS 确定了三个关键威胁领域：组件 / 架构级别的漏洞和风险，复杂供应链和售后服务所带来的风险和网络安全挑战，以及不断增长的生态系统带来的挑战。制造商和供应商必须意识到这些威胁，并在流程的早期解决这些威胁，因为它们对于为最终产品的整体网络安全铺平道路至关重要。

3.1 组件 / 架构层面的软件漏洞

让我们从电子控制单元（ ECU） 开始，他们负责执行基本但至关重要的安全功能。凭借其无与伦比的实时操作能力，这些装置中多达 150 个在一辆车上监控和控制发动机性能，排放，变速箱和制动系统等。 他们对输入信号立即做出反应，确保驾驶员在任何情况下都能安全。因此，尽管汽车行业正转向软件定义车辆 (SDV)，这些关键组件（ECU）仍将是未来 （E/E） 架构的重要组成部分。

由于 ECU直接参与了车辆中与安全相关的流程，外部攻击者可以利用不断演变的技术手段对其进行篡改，从而带来了新的风险：从通过外部 CAN 总线访问劫持整个汽车功能，到利用安全性较低的身份验证机制（“依赖保密性而非安全性”)进行攻击。

在这些情况下，操纵者可以通过互联网连接入侵系统更新的数字途径，甚至不必靠近车辆即可实施攻击。

由于车辆 ECU 处于确保驾驶员安全，舒适性和车辆性能的前沿，涵盖软件开发各个阶段的整体安全概念，以从根本上消除潜在威胁，并确保车辆在整个生命周期内始终采用最先进的身份验证流程。但不幸的是， ECU 软件开发通常依赖传统开发体系，这些系统很难应对网络威胁的快速演变，这使它们容易受到攻击。此外，由于车企普遍专注于快速迭代，突出功能创新，往往忽略了对基础ECU软件的持续优化和安全加固。

如图 2 所示，将车辆计算机捆绑在一起的新趋势是另一个安全挑战，它要求使用各种强大的安全框架，包括专用虚拟机，硬件安全模块，可信执行环境，防火墙系统和入侵检测机制。为了充分利用车辆计算机方法的优势，这项工作是必要的，即在消费电子行业中大幅简化应用程序编码的开发流程模拟。

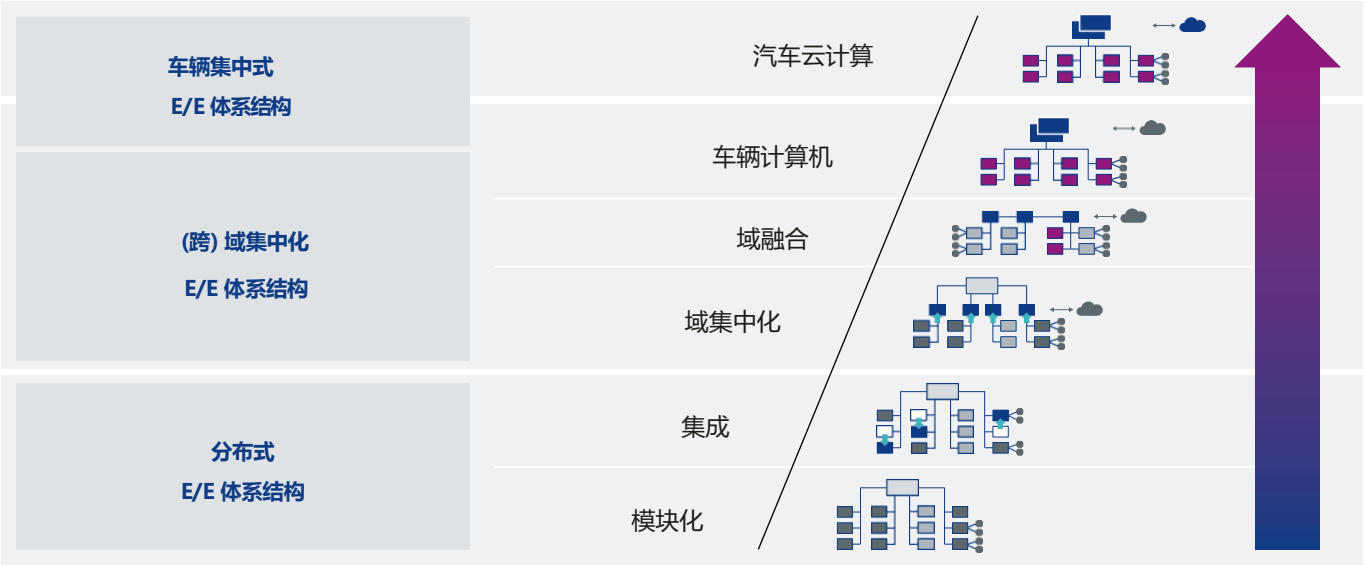

图 2: 车辆 E/E 架构从分布式到集中式的持续演变。

32 复杂的供应链带来的风险与网络安全挑战

汽车供应链是极其复杂的生态系统，涉及众多利益相关者、承包商和分包商、软件提供商以及共享开发平台。从供应链的早期阶段开始，组件和系统的可访问性和可更新性已成为必备条件。这为恶意软件或数据盗窃提供了更多的入口，因为网络犯罪分子会专门尝试利用这些可能保护较弱的系统进行攻击。选择合适的合作伙伴并确保他们符合所有标准并遵守合同义务，已成为减少第三方漏洞的重要步骤，从而实现全面的端到端网络安全。

一旦投入运营，现代车辆的连接选项使原始设备制造商OEM能够对车辆软件进行修改，这对于多种用例至关重要——从快速响应新发现的漏洞到提供附加功能或售后服务。无论此类更新是通过空中下载（OTA）、电缆还是OBD接口进行：它始终涉及制造商的责任。UN R 156规定，必须为每个可更新组件建立功能正常的软件更新管理系统（SUMS）。该功能由外部组织审核，证书必须在类型批准时提交，并每三年重新审核一次。此外，制造商现在负责评估单个更新是否影响已授予的类型批准。因此，使特定组件具备可更新性也成为制造商的经济考量。然而，从原则上讲，复杂组件的连接选项的优势超过了额外的努力，例如通过避免在出现错误时进行成本高昂的召回。

OTA连接显然是最用户友好的方法。它节省了维修店访问和手动更新的时间，对于大型车队来说是一个巨大的时间节省器。在各种类型的OTA更新中，例如软件空中下载（SOTA）、固件空中下载（FOTA）和空中服务配置（OTASP）。此外，在车辆测试阶段已经使用了各种其他无线连接选项与授权来源。从安全角度来看，它们都具有多个系统渗透级别，并针对电子/电气架构的各种组件。然而，它们都有一个共同点：它们作为未经授权软件进入系统的潜在入口。

制造商的一个普遍趋势是通过向车辆用户提供各种付费服务，将OTA接口用作数字收入渠道。这需要更多的努力来维护安全，因为可能还会交换支付和使用信息。然而，OTA可访问性的主要风险因素是通过移动网络、Wi-Fi或其他无线技术与外部主机或提供商进行双向连接，包括将功能或数据存储容量转移到云端（车辆云计算）并建立（永久）连接。通过突破车载/车外边界，为渗透恶意软件或提取数据打开了大量新的可能入口。检索驾驶行为、磨损和故障信息对于组件制造商来说非常重要，因为回流的数据能够实现持续改进。另一方面，更频繁的数据传输也带来了更多的风险。黑客致力于揭示任何弱点，并从众多现实场景中学习。

THREAT #3

3.3 日益增长的互联生态系统中的挑战

到目前为止，我们一直关注的是车辆制造商及其供应商在安全管理中扮演核心角色的场景。然而，一旦现代车辆投入运营，它将面临各种潜在的风险情况——从未经授权的维修店访问到用户发起的更新（例如来自第三方来源），再到连接到充电点、交通管理站等。这些车辆到一切（V2X）的连接可能性（甚至义务）将继续增加：车辆到车辆（V2V）、车辆到基础设施（V2I）、车辆到行人（V2P）以及车辆到网络（V2N）不仅将成为（半）自动驾驶汽车的推动者，还将把商业物流和公共交通提升到一个新的水平。

此外，来自移动通信和计算领域的软件公司越来越多地参与其中，引入了新的动态。这些提供商为个人用户和车队提供了宝贵的云和数据存储选项，以及数据分析服务。然而，它们也引发了关于数据主权和潜在滥用的重要问题，特别是因为这些服务可能在全球范围内根据不同的安全法规运营。随着汽车生态系统的不断发展，平衡这些创新的优势与安全数据处理的需求将至关重要。

这种完全互联的移动出行未来的愿景清楚地表明，启用新功能与网络安全相关问题的增加密切相关。这意味着需要在生命周期、生态系统和供应链这三个维度上持续努力，确保其安全性，如图3所示。因此，现在是时候以全局视角来彻底改革当前的开发流程了。

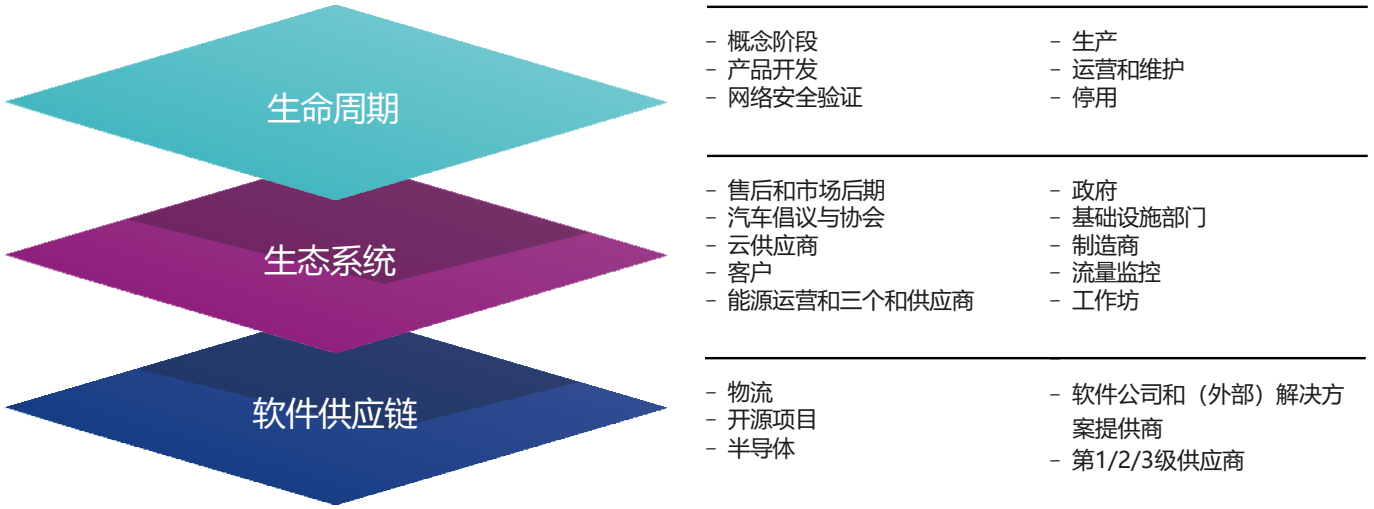

图 3: 生命周期，生态系统和供应链的三个维度涵盖影响现代车辆的所有影响因素。

4. DevSecOps 与 V 型：不同方法，相同的网络安全关注点

现代车辆正处于一个两难的境地：一方面，许多关键功能仍然依赖嵌入式软件，来确保行车安全；另一方面，为了满足对创新软件定义车辆（SDV）应用的需求，车辆架构正在向基于区域控制器的架构转变。

安全域和非安全域在车辆中不能完全分离，因为许多功能依赖于它们之间的交互。然而，目前在开发车辆软件时，主要采用两种不同的方法：V模型（图5）和DevOps周期（图4）。这两种方法都必须根据不断变化的威胁环境以及法律安全和安全要求进行调整。

对于深度嵌入的功能，考虑到硬件和软件之间仍然（部分）存在的紧密联系，增强安全性的V模型是首选的开发流程。该流程涉及明确的抽象层次分离；在开发的明确终点有一个最终产品，硬编码以处理特定的关键功能。

对于非安全功能，DevOps周期被设计为一个持续的软件开发过程，它延伸至 SOP（Start of Production，量产开始）并包括运营阶段。对于ETAS来说，它已经演变为DevSecOps（开发、安全、运营）周期，以完全满足确保端到端安全的新要求。这种新方法不需要对步骤进行重大更改，只需基于第5章中描述的四项安全原则，从工具箱中进行能力升级。

一般来说，V模型需要进行相同的调整，以成为"V-Sec模型"。基于在流程的每个环节都积极考虑安全性的前提，安全原则的引入必须从需求规范阶段开始，同时为该模型开放所需的迭代循环，并转向更敏捷的开发流程。这与V模型的基本理念并不矛盾，因为它绝不是线性的。抽象层次只需与验证和确认活动中的对应部分保持一致，而顺序是可以协商的。基本原则是：必须在每个步骤中实现安全性。对于资源有限的电子控制单元（ECU）来说，这并不是一项容易的任务，因为它们需要轻量级、高效的安全协议，以确保在不影响性能的情况下实现强大的保护。

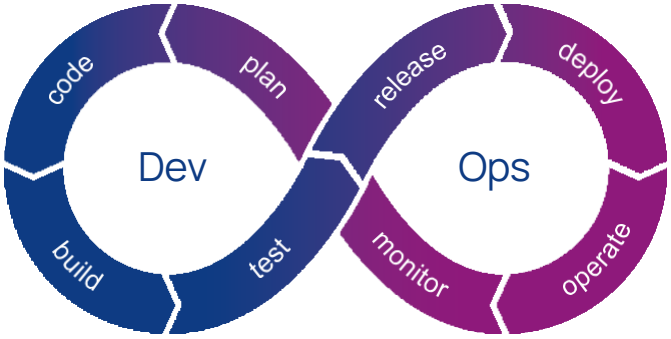

图 4: 车辆软件开发的 DevOps 循环

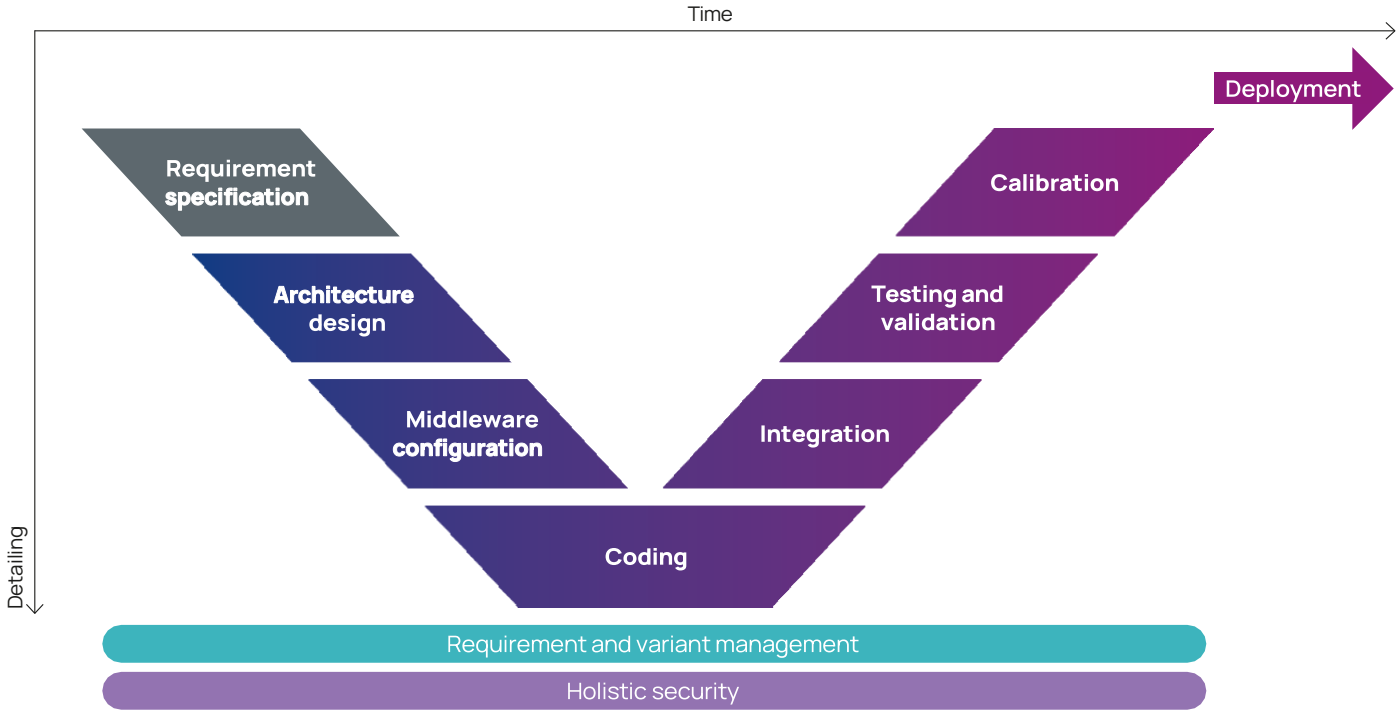

图 5: V 模型将软件开发分为两个主要部分，本版本是基于 ECU 软件开发流程。

对网络安全的关注最终使这两种方法更加紧密地结合在一起，如图6所示。考虑到电气/电子（E/E）架构正朝着车辆计算机和系统级芯片（SoC）设置的方向发展，这种趋势模糊了关键功能和通用功能之间的界限，因此这种结合是必要的。例如，当制动系统作为一项复杂功能的一部分，用于根据物体识别自动触发操作时，它永远不会像标准V模型所要求的那样完全定型。因此，所应用的V-Sec模型需要一个“-Ops”附录（或者在DevSecOps中加入一个大写的V），以便能够持续优化这一关键功能。通过实施四项安全原则，开发流程可以适应网络安全的要求，同时朝着整体网络安全管理的方向迈进。

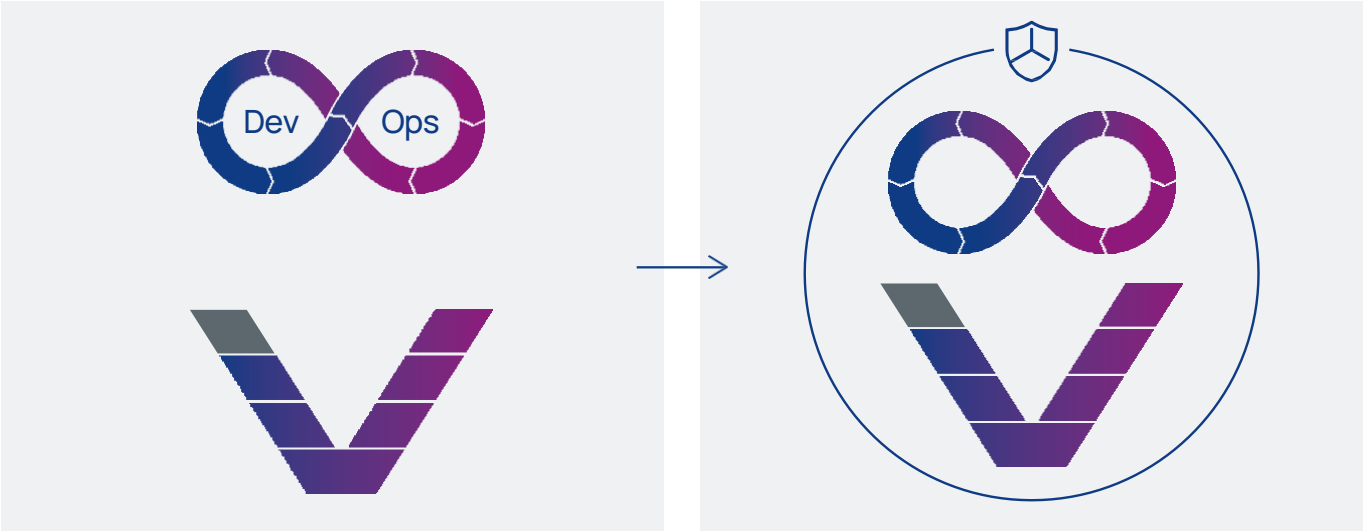

图 6: 在 V 模型和 DevOps 循环这两种方法中，网络安全的全面集成贯穿整个流程，使两者的界限变得模糊。

5. 四大安全原则

认识到变革的必要性是一回事，实际实施则是另一回事。在这里，战略必须逐步分解为可以转化为具体流程的要素。以下是四个可以作为指导的原则：安全设计（Security by Design）、深度防御（Defense in Depth）、风险管理与监控（Risk Management and Monitoring）以及组织安全（Organizational Security）。这些原则应在高成熟度水平上应用和利用，以在生命周期、生态系统和软件供应链三个维度上实现端到端的网络安全。这些原则涵盖了组织内产品安全的各个方面：流程、技术、信息，当然还包括人员和文化。

5.1 原则一：设计安全

从开发过程的一开始，安全就被纳入考虑，并在每个步骤中得到体现，包括遵守（法律）安全法规和实施适当的安全架构。无论是在DevSecOps还是V模型中，这种在整个开发过程中持续考虑所有安全方面的做法，可以避免在项目后期或销售后因返工而产生的高成本。根据安全设计原则开发的软件在其整个生命周期中都具有鲁棒性和弹性。根据当今的威胁形势扩展这一原则，还可以永久优化在任何时间点修复漏洞所需的时间。

5.2 原则二：深度防御

拥有多道防线意味着单一道防线的失效不会直接危及整体安全，这是深度防御原则的核心：通过建立多重保护机制，避免任何单点故障被黑客攻破。在传统的电气/电子（E/E）架构中，曾经理想的方式是采用层次化的方法（从深度嵌入的组件一直到顶层，例如车辆网络），同时利用了硬件层面仍然强大的功能分离和隔离优势。如今，随着更加集中化的车辆架构和车辆云计算登上舞台，必须通过额外的“虚拟”层级来应对复杂性，最终朝着零信任安全模型的方向发展。

5.3 原则三：风险管理与监控

随着潜在风险数量的增加，有针对性和全面的管理是不可避免的。例如，威胁分析和风险评估（TARA）的执行是ISO/SAE 21434 标准中的一个主要组成部分。它为制造商和供应商提供了一个蓝图，用于发现潜在威胁并制定适当的保护措施。 在威胁分析阶段，系统地识别车辆面临的所有网络安全威胁，包括评估潜在的网络攻击场景，以制定适当的应对措施。随后，在风险评估阶段对这些风险进行优先级排序，并分析它们对开发过程的影响。总体目标是通过一致应用安全设计和深度防御原则，将威胁水平降至最低。开放的生态系统和不断变化的威胁形势也需要重新思考，因为大多数传统开发系统缺乏相应的工具和流程，无法持续识别风险、分析问题并弥补安全漏洞。

5.4 原则四：组织安全管理

为了实现全面的网络弹性，组织内部必须进行根本性的变革。这首先包括所有相关人员思维方式的转变。复杂且不断变化的威胁形势需要合作、灵活性、沟通以及高度主动的网络安全意识，而不仅仅是“清单式思维”。同时，法律要求详细规定了流程的设置方式。例如，联合国欧洲经济委员会（UNECE）法规要求建立一个全面的网络安全管理系统（CSMS），涵盖运营、风险管理/合规性以及内部审计。遵循所谓的“三道防线框架”，安全不再是单个部门的孤立话题，而是贯穿所有流程并覆盖产品的整个生命周期。这需要时间并进行调整，特别是在全面整合组织内所有利益相关者及软件供应链的情况下。

6. 通过移动出行专家的指导与解决方案应对复杂性

无论是了解威胁形势、掌握所有法规和标准，还是熟悉四项原则，都需要专家将这些理论知识付诸实践。正如我们所概述的，提供最先进的网络安全需要对汽车制造商和供应商的开发、制造和售后流程进行根本性和全面的调整。最终，这些概念必须通过软件和硬件解决方案、开发工具以及具体的操作指南转化为日常实践。

例如，根据原则1（安全设计）和原则2（深度防御）采用多层安全架构，意味着在现有的遗留系统中设置最先进的加密、身份验证、入侵检测和安全启动机制。如果从零开始，这需要一个独立的网络安全部门。因此，许多公司依赖外部支持来应对日益增长的复杂性，同时节省时间和资源。这一趋势在汽车网络安全市场预测中也很明显：预计2024年至2031年间，其复合年增长率（CAGR）为18.93%，市场规模将从2023年的78.3亿美元增长到2031年的313.4亿美元，如图7所示。

然而，实施外部网络安全解决方案也面临自身的挑战，例如供应商锁定、不兼容性或集成困难。因此，选择合适的合作伙伴以开发一个全面且面向未来的网络安全概念至关重要，这一概念需要涵盖个体情况和遗留系统。在法规合规性方面，具体且结构化的指导方针至关重要。由于法律对每家公司都是一样的，因此无需反复开发自己的解决方案。ETAS开发了ESCRYPT产品安全组织框架（PROOF），作为一种经过验证的方法，通过遵循八个步骤来建立网络安全管理系统（CSMS），根据原则4（组织安全管理），并根据每个客户的成熟度水平进行个性化定制。

像ETAS这样的合作伙伴还能够提供软件和硬件层面的解决方案，并高度关注流程优化：其产品组合包括用户友好的工具和管理平台，这些工具和平台最大限度地减少了手动操作，具有高度的自动化，并且能够动态和持续地进一步发展。该产品组合（见图8）分为设计、启用和管理安全三大类，以便客户可以根据自身需求选择所需的网络安全解决方案支持。

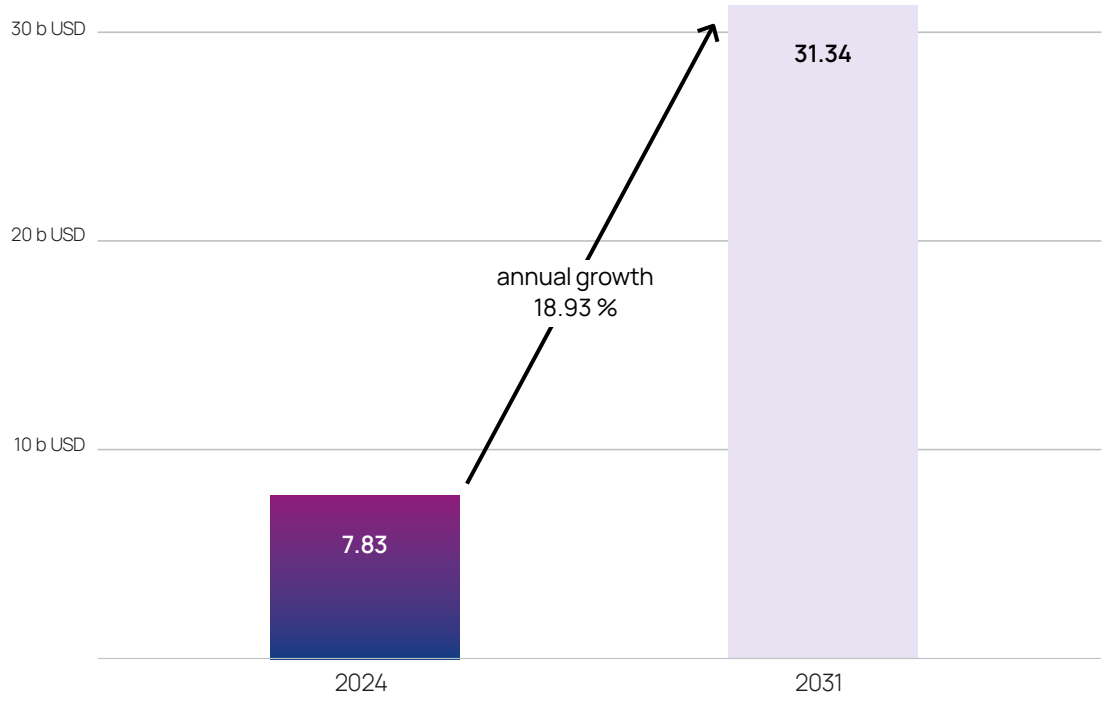

图 7: 汽车网络安全市场预测2024年至2031年

设计安全

我们提供了一个产品安全组织框架，以实现 ISO 21434 合规性和安全工具，用于风险管理和渗透 / 模糊测试。

ESCRYPT 网络安全管理系统 (带证明)
优化网络安全效率的成熟方法

ESCRYPT CycurFUZZ
用于汽车系统的智能模糊测试工具

ESCRYPT CycurRISK
用于威胁分析和风险评估的软件

启用安全性

我们还提供嵌入式软件产品，例如硬件安全模块（HSM）和加密库，适用于微控制器和车辆计算机（如系统级芯片，SoC），以防止加密密钥的滥用。此外，我们还提供入侵检测与防护解决方案，包括汽车防火墙，以保护数据和通信免受篡改。

ESCRYPT CycurHSM
为您提供强大的安全软件ECU

ESCRYPT CycurSoC
确保软件定义车辆的安全和信任

ESCRYPT CycurGATE
高性能汽车
以太网 /IP 防火墙和路由器

管理安全性

在ETAS，我们为全球车队提供集成的入侵检测和防护解决方案。我们通过车载入侵检测系统，通过车辆安全运营中心（Vehicle Security Operations Centers）对整个联网车队进行安全监控，以及通过空中下载（OTA）更新实现持续风险管理，帮助您有效管理安全。

ESCRYPT CycurIDS
嵌入式入侵检测系统，适用于CAN和以太网网络

ESCRYPT 漏洞 管理解决方案
通过基于风险的漏洞管理增强产品安全性

ESCRYPT 车辆安全运营中心
针对车队需求量身定制的托管安全服务，包括整合车队和车辆后端系统的事件源，提供全面的安全监控和响应

ESCRYPT 入侵检测和预防解决方案
对车队进行永久监控，识别新兴安全威胁。建立专门的事件响应机制，并在整个生命周期内保持稳定的安全水平。

图 8: ETAS 车辆网络安全产品组合，集中于设计、启用和管理安全

7. 结论

网络安全是汽车行业的首要问题，并在日益互联的未来中将发挥越来越重要的作用。然而，将流程调整为全面的网络安全战略不应被视为一种繁重的义务。相反，这首先是汽车制造商和供应商将开发和生产提升到新水平、并通过新的售后服务积极提升市场竞争力的绝佳机会。**ETAS 2024年网络成熟度报告[5]**明确指出：成熟度越高，企业在这一竞争市场中的地位就越强。无论企业处于这一旅程的哪个阶段，好消息是：针对每个成熟度水平、网络威胁和法规要求，像ETAS这样的合作伙伴已经铺平了道路——或者说在丛林中开辟了一条小径。他们的支持范围从公司流程的全面蓝图到针对ECU或车辆计算机的具体软件解决方案；可以作为一次性购买或持续的托管服务，使制造商和供应商无需建立和维护自己的资源。通过合作，网络安全的挑战可以转化为机遇，道路使用者的安全也可以长期保持在最高水平。

关于ETAS

ETAS GmbH成立于1994年，是罗伯特·博世有限公司（Robert Bosch GmbH）的全资子公司，在欧洲、北美、南美和亚洲等主要汽车市场均设有本地分支机构。ETAS为软件定义汽车的实现提供全面的解决方案，涵盖软件开发解决方案、车辆操作系统、车辆云服务、数据采集与处理解决方案、集成客户解决方案以及网络安全等领域。

作为网络安全领域的行业先驱，我们通过经过验证的车载和离车软件产品组合以及专业安全服务，帮助客户管理与网络安全相关的复杂性，降低网络风险，并最大化其商业潜力。

ETAS的汽车安全解决方案正在保护全球数百万车辆系统，并为软件定义汽车的网络安全树立标准。

参考

1) Rockwell Automation, 9th annual State of Smart Manufacturing Report: Automotive Edition, accessed 2024/11/10, https://www.rockwellautomation.com/content/dam/rockwell-automation/documents/pdf/campaigns/state-of-smart-2024-automotive/2024-state-of-smart-manufacturing-for-automotive.pdf

2) Forbes, accessed 2024/11/11, https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/

3) Automotive IT, accessed 2024/11/11, https://www.automotiveit.eu/technology/volkswagen-streicht-modelle-wegen-cybersecurity-vorgaben-99-311.html

4) Faist Group, accessed 2024/11/11, https://www.faistgroup.com/news/growth-challenges-automotive-cybersecurity/

5) ETAS Cyber Maturity Report, accessed 2024/11/11, https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-automotive-cyber-maturity-report-2024-en-20240719.pdf

联系信息

Christian Schleiffer
Get in touch on LinkedIn
Contact me
www.etas.com/wesecurethefuture

Last updated: 12/2024