引用格式： 张兴辉，刘建建，黄志晨，等. 基于ISO/SAE 21434标准的智能网联电动自行车网络安全研究[J]. 标准化学报，2026(8)：16-25.
ZHANG Xinghui, LIU Jianjian, HUANG Zhichen, et al. Research on Cybersecurity of Intelligent Connected Electric Bicycles Based on ISO/SAE 21434 Standard[J]. Journal of Standardization, 2026(8): 16-25.

基于 ISO/SAE 21434 标准的智能网联电动自行车网络安全研究

张兴辉　刘建建　黄志晨　王 豪　郑 兢　陈 良*
（厦门市产品质量监督检验院）

摘　要：【目的】针对智能网联电动自行车（ICEB）面临的网络安全新挑战，依据ISO/SAE 21434等标准，开展网络安全研究，为该类产品的网络安全开发与全生命周期防护提供支撑。【方法】首次将威胁分析与风险评估（TARA）方法论系统应用于ICEB领域。在识别软硬件等5类核心资产及安全属性基础上，采用STRIDE法挖掘典型威胁场景，并多维度开展影响评级；运用攻击树解析攻击路径，结合CVSS量化攻击可行性，构建风险矩阵并划定风险等级；依据分级处置原则提出对应技术防护方案。【结果】形成完整的ICEB网络安全分析框架；识别出远程劫持、数据泄露、信道不可用等典型威胁，评定出风险等级；提出多因素认证等针对性防护措施。【结论】本研究兼顾产业成本敏感的特性，可为产品网络安全开发、全生命周期安全防护及产业链协同安全建设提供理论与实践支撑。

关键词： TARA；智能网联电动自行车；网络安全；威胁分析；风险评估
DOI编码： 10.3969/j.issn.2097-857X.2026.08.002

Research on Cybersecurity of Intelligent Connected Electric Bicycles Based on ISO/SAE 21434 Standard

ZHANG Xinghui　LIU Jianjian　HUANG Zhichen　WANG Hao　ZHENG Jing　CHEN Liang*
(Xiamen Institute of Product Quality Supervision and Inspection)

Abstract: [Objective] To address emerging cybersecurity challenges for intelligent connected electric bicycles (ICEBs), this study conducts cybersecurity research based on standards such as ISO/SAE 21434 to support cybersecurity development and full lifecycle protection for such products. [Methods] This study pioneers the systematic application of the Threat Analysis and Risk Assessment (TARA) methodology within the ICEB domain. Following the identification of five core asset categories (including software and hardware) and their security attributes, the STRIDE method was employed to uncover typical threat scenarios, with impact ratings conducted across multiple dimensions. Attack trees were utilized to analyse attack paths, combined with CVSS to quantify attack feasibility, thereby constructing a risk matrix and defining risk levels. Corresponding technical protection measures were proposed based on graded response principles. [Results] A comprehensive cybersecurity analysis framework for ICEB was established. Typical threats such as remote hijacking, data

基金项目： 本文受2024年度国家市场监督管理总局科技计划项目“基于AI模型的智能可穿戴设备信息安全检测技术研究”（项目编号：2024MK148）；2025年福建省工业和信息化厅软件业技术创新重点攻关及产业化项目“基于DeepSeek的智能交通车载信息交互系统”（闽工信函软件〔2025〕587号）资助。

作者简介： 张兴辉，硕士，高级工程师，研究方向为物联网、车联网、自动驾驶、车路协同和信息安全等。
陈良，通信作者，博士，高级工程师，研究方向为汽车及电动自行车的检验方法及标准、机电类仪器设备开发等。

leakage, and channel unavailability were identified and risk levels were assessed. Targeted protective measures, including multi-factor authentication, were proposed. [Conclusion] This study, accounting for the industry's cost-sensitive nature, provides theoretical and practical support for product cybersecurity development, full lifecycle security protection, and collaborative security construction across the industrial chain.

Keywords: TARA; intelligent connected electric bicycles; cybersecurity; threat analysis; risk assessment

0 引言

当前全球网络安全事件频发，多种风险叠加[1]。以智能健康产品为例，近源攻击风险、数据安全风险及网络传输风险较为突出[2]。智能网联电动自行车（ICEB）是指搭载电子控制单元，其电池管理系统模块、控制部件、显示部件、传感器等具有总线交互功能，可实现车、路、人等之间的信息交互和多种智能辅助骑行模式的电动自行车[3]。作为新型个人智能出行工具，其深度融合了物联网、云计算、4G/5G移动远程通信、NFC/蓝牙近场通信、北斗定位等先进技术，并通过车载传感器、控制器和执行器实现车辆状态监测、远程控制、位置服务等功能。近十年来，电动自行车智能化、网联化程度不断提升[4]。新国标GB 17761—2024《电动自行车安全技术规范》首次将北斗定位、通信传输与动态安全监测纳入标准要求[5]。然而，这种技术融合也带来了新的、复杂的信息安全挑战。2025年，UN ECE R155-2025/5[6]法规第3号修正案将L类两轮或三轮机动车辆纳入法规适用范围。可预见，ICEB网络信息安全开发与防护已经提上日程。

目前，ICEB网络信息安全相关标准缺失，亟须加快构建覆盖全生命周期的网络安全标准体系，明确安全基线与技术要求，推动标准与产业实践深度融合，为网络安全开发、测试认证及监管提供统一依据。威胁分析与风险评估（Threat Analysis and Risk Assessment，TARA）作为ISO/SAE 21434标准的核心方法论[7]，为道路车辆提供了一套过程导向的、系统化的网络安全分析框架。该框架贯穿产品全生命周期，从概念阶段开始识别潜在威胁并评估风险，为制定网络安全目标和需求提供依据。与传统IT系统安全分析不同，ICEB的TARA分析需要特别关注功能安全与信息安全融合、资源受限环境下（成本低）的安全机制及海量设备的规模化安全管理等独特挑战。

因此，本研究针对GB 17761—2024《电动自行车安全技术规范》等新国标要求的ICEB，参考ISO/SAE 21434《道路车辆 网络安全工程》、UN ECE R155、GB 44495—2024《汽车整车信息 安全技术要求》[8]等法规和标准，首次将TARA方法论系统应用于ICEB领域。研究旨在识别ICEB全系统安全风险，提出针对性防护策略，为ICEB的网络安全开发和全生命周期防护提供理论依据和实践指导。

1 TARA分析方法论

UN ECE R155和GB 44495—2024是国内外智能网联汽车领域具有代表性的网络安全法规和标准。UN ECE R155以过程为导向，要求参考ISO/SAE 21434标准开展TARA活动，实施网络安全开发和全生命周期防护。GB 44495—2024以结果为导向，明确技术要求和测试方法。ISO 21434的TARA分析流程可以概括如图1所示[7]。

结合项目管理知识体系指南[9]，整理其活动的过程、输入、输出及工具与技术，如表1所示。

2 智能网联电动自行车TARA分析

2.1 智能网联电动自行车系统架构

ICEB采用分层设计技术架构，是由终端设备层、网络传输层、中心平台层和用户应用层四大部分构成的复杂生态系统[4]。值得注意的是，GB

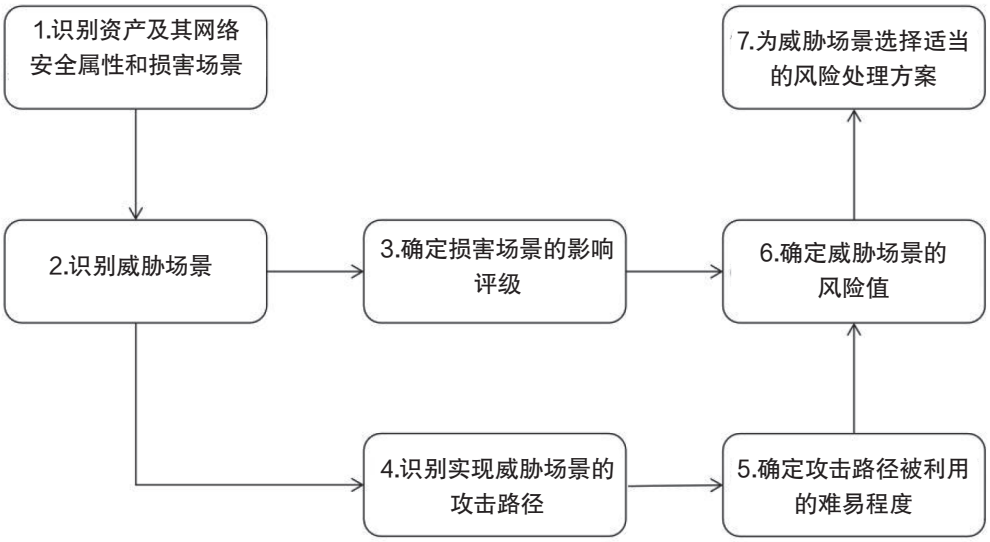

图1 TARA分析流程图

表1 TARA活动过程

活动	过程	输入	输出	工具与技术
识别资产及其网络安全属性和损害场景	（a）应识别损害场景，损害场景可包括：项目功能与不利后果之间的关系、对道路使用者及/或相关资产伤害的描述； （b）应识别其遭到破坏会导致损害场景的具有网络安全属性的资产	（a）项目定义； （b）网络安全规范	（a）损害场景； （b）具有网络安全属性的资产	（a）专家判断； （b）文件分析； （c）产品分析
识别威胁场景	应识别威胁场景，且威胁场景应包括：目标资产、资产被破坏的网络安全属性以及网络安全属性被破坏的原因	（a）项目定义； （b）网络安全规范； （c）损害场景； （d）具有网络安全属性的资产	威胁场景	（a）小组讨论； （b）EVITA、TVRA、PASTA、STRIDE等框架的威胁建模方法
确定损害场景的影响评级	（a）应分别针对安全、财务、运营和隐私（S、F、O、P）影响类别中道路使用者的潜在不利后果评估损害场景。 （b）对于每个影响类别，损害场景的影响评级应确定为以下之一： 严重、重大、中等、轻微	（a）损害场景； （b）项目定义； （c）具有网络安全属性的资产	与相关影响类别对应的影响评级	（a）专家判断； （b）数据分析
识别实现威胁场景的攻击路径	应对威胁场景进行分析，以识别攻击路径。攻击路径应与通过该攻击路径造成的威胁场景相关联	（a）项目定义或网络安全规范； （b）威胁场景； （c）网络安全事件中的弱点； （d）产品开发过程中发现的弱点； （e）架构设计； （f）先前识别出的攻击路径； （g）漏洞分析	攻击路径	（a）专家判断； （b）自上而下的方法，例如攻击树、攻击图； （c）自下而上的方法，从已识别的漏洞构建攻击路径

续表1

活动	过程	输入	输出	工具与技术
确定攻击路径被利用的难易程度	对于每条攻击路径，应按高、中、低、极低确定攻击可行性评级	（a）攻击路径； （b）架构设计； （c）漏洞分析	攻击可行性评级	（a）基于攻击潜力的方法； （b）基于通用漏洞评分系统（CVSS）的方法； （c）基于攻击向量的方法
确定威胁场景的风险	对于每个威胁场景，应根据相关损害场景的影响以及相关攻击路径的攻击可行性来确定风险值。风险值应为1到5之间，1代表最小风险	（a）威胁场景； （b）相关影响类别对应的影响评级； （c）攻击可行性评级	风险值	（a）风险矩阵； （b）风险公式
为威胁场景选择适当的风险处理方案	对于每个威胁场景，考虑其风险值，应确定以下一种或多种风险处理选项：规避风险、降低风险、分担风险、接受风险	（a）项目定义； （b）威胁场景； （c）风险值； （d）网络安全规范； （e）项目或组件的，或之前类似项目或组件的风险处理决策； （f）与相关影响类别对应的影响评级； （g）攻击路径； （h）攻击可行性评级	风险处理决策	（a）专家判断； （b）SWOT分析； （c）成本效益分析； （d）备选方案分析

17761—2024首次将北斗定位功能和通信与动态安全监测纳入标准要求。其中，动态监测要求电动自行车应具备向企业等建设的信息管理平台发送动态安全监测信息的功能[5]。这意味着，ICEB车端电子电气架构将以控制器为核心，集成电池及电池管理系统（BMS）、充电器、智能仪表等关键组件，通过数据总线（CAN或其他串行总线协议）进行内部通信。其配备多种传感器（如北斗位置、车速、温度、电流、电压等）和执行器（如电机、制动系统、蜂鸣器等），并通过4G/5G远程通信模块和NFC/蓝牙近场通信模块实现对外数据交互，甚至实现OTA远程升级。这些资产将成为网络安全的重要攻击面，需特别关注其安全防护。

2.2 关键资产分类与损害场景识别

按照专家小组（6位成员：博士学位1人、硕士学位5人；信息安全高级工程师3人、电动自行车质量检测工程师3人；专业涵盖检测、电子、信息、通信、车辆等领域；按照少数服从多数的决策意见，如票数相同，按照信息安全高级工程师的意见再遵循少数服从多数决策）讨论意见，结合ICEB具体应用场景，划分以下核心资产类别：

1）硬件资产。控制器（ECU）、智能仪表；传感器系统，如北斗位置、车速、电流、电压、温度等检测；执行器组件，如蓄电池、电机、制动器、电子锁、蜂鸣器等；内部通信总线；外部通信接口，如4G/5G远程通信模块、NFC/蓝牙近场通信模块等。

2）软件资产。传感器、主控制器、智能仪表、执行器等硬件设备中的嵌入式软件，负责数据采集、处理、显示与控制，比如BMS软件用于管理电池充放电；手机端应用程序，用户可以实时查看车辆状态、远程控制车辆。

3）通信资产。内部通信总线，实现控制器、智能仪表和充电器之间数据传递；4G/5G远程通信网络，可将动态安全监测信息实时上报至企业信息管理平台，也可下载OTA远程升级指令；NFC和蓝牙通信网络，用于近距离控制和数据传输；UDP、MQTT等通信协议，用于数据传输；企业信息管理平台，用于接收、存储和处理车辆数据。

4）数据资产。车辆运行数据，包括电池电压、电流、温度，行驶速度、里程、轨迹等；用户隐私数据，如身份信息、位置轨迹、骑行习惯等；车辆控制指令如电机调速信号、制动命令等；安全认证凭据，如数字证书、密钥等；故障数据，如故障类型、位置、时间以及故障发生前后车辆状态数据。

5）功能资产。驱动控制功能，如电机调速、扭矩输出；电池管理功能，如充放电控制、均衡管理；以及车辆锁定功能、固件更新功能（OTA升级或离线升级）、远程监控、故障诊断与预测、智能调度与出行服务等。

资产网络安全属性识别一般以资产的3个基本安全属性进行衡量，即机密性（Confidentiality）、完整性（Integrity）、可用性（Availability），简称CIA。机密性是指网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息的特性；完整性是指网络信息或系统未经授权不能进行更改的特性；可用性是指合法许可用户能够及时获取网络信息或服务的特性。目前，国家信息风险评估标准对资产的CIA赋值划分为五级（5—很高、4—高、3—中等、2—低、1—很低）。参考GB 44495—2024中外部连接安全、通信安全、软件升级安全和数据安全四大类划分方式[8]，选取以下部分典型资产识别网络安全属性，如表2所示。

表2 资产安全属性识别示例

资产类别	资产名称	C	I	A
硬件资产	主控制器	3	5	5
通信资产	4G/5G远程通信	5	4	2
数据资产	用户隐私数据	5	2	2
功能资产	OTA功能	2	5	2

损害场景识别过程示例如下。

1）主控制器

机密性（3分），损害场景是主控制器存储的控制逻辑、算法参数等泄露导致竞品模仿，但不影响骑行，机密性要求中等。

完整性（5分），损害场景是主控制器程序或配置被篡改可能会直接导致车辆失控（如BMS参数篡改，可能导致热失控引发火灾），危及用户安全，完整性破坏影响很高。

可用性（5分），损害场景是主控制器失效会导致车辆完全无法运行（如无法响应传感器信号、无法控制执行器），直接丧失基本功能，可用性要求很高。

2）4G/5G远程通信

机密性（5分），损害场景是4G/5G远程通信传输数据包括用户隐私（位置）、控制指令（远程启动）泄露，造成个人信息泄露，或车辆处于不安全状态，机密性要求很高。

完整性（4分），损害场景是4G/5G网络数据被篡改（如修改OTA包、伪造定位信息）导致功能异常，影响骑行，完整性要求高。

可用性（2分），损害场景是4G/5G网络中断影响远程交互，但不阻碍本地骑行，可用性要求低。

3）用户隐私数据

机密性（5分），损害场景是用户隐私数据泄露导致用户隐私侵犯、被追踪或网络暴力攻击，机密性要求很高。

完整性（2分），损害场景是隐私数据被篡改，但不直接危及行驶安全，完整性要求低。

可用性（2分），损害场景是隐私数据丢失，影响数据分析和用户查看，但不影响本地骑行，可用性要求低。

4）OTA功能

机密性（2分），损害场景是OTA升级过程泄密，不涉及用户敏感信息，机密性要求低。

完整性（5分），损害场景是OTA升级被篡改推送恶意固件导致安全风险，完整性要求很高。

可用性（2分），损害场景是OTA升级功能失效

影响远程维护，不影响本地行驶，可用性要求低。

2.3 典型威胁场景与影响评级

2.3.1 典型威胁场景

典型威胁场景分析方法包括头脑风暴法、由误用实例引出法和基于STRIDE分类法等[7]，其中前两类方法依靠分析人员经验，而STRIDE分类法具有系统化、结构化的优势。ICEB面临多维度网络安全威胁，以表2的资产为例，按照STRIDE（Spoofing假冒、Tampering篡改、Repudiation抵赖、Information Disclosure信息泄露、Denial of Service拒绝服务、Elevation of Privilege权限提升）的威胁建模方法，列举部分典型威胁场景，如表3所示。

表3 部分典型威胁场景示例

威胁场景	资产	STRIDE	损害场景
信道不可用	主控制器	拒绝服务	远程解锁功能失效
远程劫持	4G/5G远程通信	假冒	车辆失控
数据泄露	用户隐私数据	信息泄露	隐私侵犯
固件篡改	OTA功能	篡改	功能失效、隐私侵犯

典型威胁场景描述如下：

信道不可用场景。对控制器外部通信信道发送大量高频恶意消息（拒绝服务攻击），导致通信信道可用性受损，数据不能传输，车辆远程解锁功能失效。

远程劫持场景。伪装成合法用户，通过云端API接口入侵车辆控制系统，发送恶意控制指令，如紧急制动指令，可能导致车辆失控事故。

数据泄露场景。企业信息管理平台或用户手机端程序被未授权实体获取，用户隐私数据泄露。

固件篡改场景。篡改OTA升级包，破坏升级包完整性或植入恶意固件让非授权实体获取信息，可能导致车辆OTA功能失效或者隐私受到侵犯。

当然，一个威胁场景可能导致多个损害场景，一个损害场景可能对应多个威胁场景，上述威胁场景仅为示例。

2.3.2 影响评级

影响评级是从Safety（安全）、Financial（财务）、Operational（操作）、Privacy（隐私）4个维度评估损害场景的影响等级。每个维度分为4个等级：Severe（严重）、Major（重大）、Moderate（中等）、Negligible（可忽略）[7]。按照影响评级标准，重点关注损害场景对用户的影响，根据小组讨论意见，对表3示例的功能失效、车辆失控、隐私侵犯等损害场景分析如下。

1）远程解锁功能失效

安全影响。通信不可用导致远程解锁失效，但物理锁仍可用，不会直接引发安全事故，无伤害，后果可忽略不计。

财务影响。财务损失没有影响，后果可忽略不计。

操作影响。远程解锁失效，部分功能不可用，后果中等。

隐私影响。拒绝服务攻击不涉及数据窃取，无隐私泄露风险，后果可忽略不计。

2）车辆失控

安全影响。恶意指令（如紧急制动）可致行驶车辆失控，引发碰撞，甚至危及生命，后果严重。

财务影响。车辆失控可能导致重大财务损失，后果严重。

操作影响。用户丧失车辆控制权，核心功能受损，后果严重。

隐私影响。攻击者可能获取账户ID及骑行轨迹（敏感但难关联具体身份），不涉及身份证号等核心隐私，后果中等。

3）隐私侵犯

安全影响。不直接引发安全事故，无即时人身伤害风险，后果可忽略不计。

财务影响。不直接造成用户经济损失，无即时财务损失，后果可忽略不计。

操作影响。未导致车辆功能受损或造成不可察觉的损害，后果可忽略不计。

隐私影响。泄露用户姓名、身份证号、精确骑行轨迹等高度敏感、易关联信息，可能会对道路使用者造成重大甚至不可逆转的影响，后果严重。

4）功能失效

安全影响。恶意固件可禁用制动系统或篡改BMS参数，导致制动功能或热管理功能失效，直接引发骑行安全事故或火灾安全事故，后果严重。

财务影响。功能失效可导致重大财务损失，后果严重。

操作影响。可能导致核心功能失效，后果严重。

隐私影响。恶意固件可植入后门，可获取高度敏感精确骑行轨迹，侵犯隐私，但不直接关联用户信息，可能会对用户造成重大甚至不可逆转的影响，后果中等。

影响评级示例如表4所示。

表4 影响评级示例

损害场景	安全	财务	操作	隐私
远程解锁功能失效	可忽略	可忽略	中等	可忽略
车辆失控	严重	严重	严重	中等
隐私侵犯	可忽略	可忽略	可忽略	严重
功能失效	严重	严重	严重	中等

2.4 攻击路径分析与攻击可行性评估

2.4.1 攻击路径分析

攻击路径分析包括自顶向下的方法（也称演绎法）、自底向上的方法（也称归纳法）以及两者结合的方法等[10]。自底向上的归纳法非常依赖人员理论经验，目前通常使用自顶向下演绎法，如攻击树。讨论小组使用攻击树方法对表3所示的信道不可用、远程劫持等典型威胁场景进行攻击路径分析。

1）信道不可用

路径1：蓝牙信道拒绝服务。比如，攻击者生成高频连接请求，通过蓝牙接口持续发送至ECU，ECU的蓝牙接口过载，无法处理合法解锁指令（如用户终端发送的解锁请求），导致近场解锁失败。

路径2：NFC信道拒绝服务。比如，攻击者模拟高频NFC读写操作，发送大量无效认证消息至ECU，ECU的NFC信道瘫痪，用户无法通过NFC近场解锁车辆。

路径3：4G/5G信道拒绝服务。比如，攻击者向ECU或与之相关的后端服务器发送大量的虚假数据包，占用网络带宽和处理资源，使ECU无法接收远程指令或后端服务器无法处理正常的通信请求，导致远程解锁失败。

2）远程劫持

路径1：身份伪造攻击。比如，攻击者利用窃取的账号密码登录控制端，伪装成车主发送恶意控制指令。

路径2：API接口滥用。比如，攻击者伪造并高频调用“加速–制动”循环API，使车辆失控。

路径3：中间人篡改指令。比如，攻击者截获骑行者“解锁”指令，并将其篡改为“上锁并开启防盗警报”，导致远程解锁失败。

3）数据泄露

路径1：云端数据库越权访问。比如，攻击者利用ICEB企业信息管理平台的API接口漏洞（如未授权访问或SQL注入），直接访问或批量导出后台数据库，非法获取包含用户姓名、手机号、身份证号、家庭住址及完整历史骑行轨迹在内的敏感信息。

路径2：移动端APP本地数据窃取。比如，攻击者通过利用手机系统漏洞提权，或诱使用户安装恶意软件，直接读取该APP的私有存储区域，窃取用户的登录令牌及近期骑行GPS轨迹等缓存数据。

路径3：车端存储数据物理提取。比如，攻击者通过物理拆解车辆，直接读取存储介质，或通过暴露的诊断接口（如UART、JTAG）连接设备导出近期行驶日志、最后一次成功连接的服务端地址等信息数据，从而获取可用于关联和追踪用户的隐私信息。

4）固件篡改

路径1：OTA升级包劫持与替换。比如，攻击者通过中间人攻击劫持车辆与官方服务器之间的固件无线升级通信链路，将传输中的合法固件升级包替换为自行制作的、包含后门或恶意逻辑的篡改包。

路径2：供应链或维护渠道植入。比如，攻

击者在ICEB生产环节的固件烧录阶段，或后期在非官方维修点进行维护时，通过物理接触或内部网络，将带有恶意代码的固件程序刷写至控制器中。

路径3：利用车端漏洞进行本地提权与刷写。比如，攻击者利用操作系统或某个应用组件的已知漏洞，获取对控制器的底层访问权限，进而绕过官方的固件签名验证机制，强行刷入篡改后的固件。

2.4.2 攻击可行性评估

攻击可行性评估旨在分析攻击路径被成功利用的技术难度，通常包括基于攻击向量的方法、基于通用漏洞评分系统（CVSS）的方法和基于攻击潜力的方法等[7]。基于攻击向量的方法简单，需要输入的信息量少，适用于开发早期缺乏足够详细信息时进行比较粗糙的评估。基于CVSS的方法被ISO 21434采纳，其标准化程度高，从攻击向量、复杂度、权限要求等维度打分，输出标准化、可横向对比的漏洞风险值。基于攻击潜力的方法，综合耗时、专业知识、所需设备、项目知识和机会窗口评估，更加依靠分析人员经验。

以CVSS基础指标评价为例，可利用性指标包括：攻击向量AV（网络N：0.85/相邻A：0.62/本地L：0.55/物理P：0.2）、攻击复杂性AC（低L:0.77/高H：0.44）、权限需求PR（无N：0.85/低L：0.62/高H：0.27）、用户交互UI（无N：0.85/需要R：0.62）4个维度。整体可利用性值可通过公式（1）计算：

$$E=8.22\times C\times V\times P\times U \quad (1)$$

式中：E为可利用性值；V为与攻击向量相关的数值，范围为0.2至0.85；C为与攻击复杂度相关的数值，范围为0.44至0.77；P为与所需权限相关的数值，范围为0.27至0.85；U为与用户交互相关的数值，范围为0.62至0.85。

通过量化评估，最终将可行性评级划分为四级：高（2.96~3.89）、中（2.00~2.95）、低（1.06~1.99）、很低（0.12~1.05）。

针对表3识别的典型威胁场景攻击路径，评估攻击可行性结果，如表5所示。

2.5 风险评估与处置建议

2.5.1 风险等级评估矩阵

风险值评定由损害场景等级和威胁场景的可行性进行评估，风险矩阵模型如表6所示[7]。

表5 攻击可行性评估示例

威胁场景	攻击路径	CVSS基础指标	可行性评分	可行性评级
信道不可用	蓝牙信道拒绝服务	AV:A/AC:L/PR:N/UI:N	2.83	中
	NFC信道拒绝服务	AV:P/AC:L/PR:N/UI:N	0.91	很低
	4G/5G信道拒绝服务	AV:N/AC:L/PR:N/UI:N	3.89	高
远程劫持	身份伪造攻击	AV:N/AC:L/PR:L/UI:R	2.07	中
	API接口滥用	AV:N/AC:L/PR:N/UI:N	3.89	高
	中间人篡改指令	AV:A/AC:H/PR:N/UI:R	1.18	低
数据泄露	云端数据库越权访问	AV:N/AC:L/PR:N/UI:N	3.89	高
	移动端APP本地数据窃取	AV:L/AC:L/PR:L/UI:R	1.34	低
	车端存储数据物理提取	AV:P/AC:H/PR:H/UI:N	0.17	很低
固件篡改	OTA升级包劫持与替换	AV:A/AC:L/PR:N/UI:N	2.83	中
	供应链或维护渠道植入	AV:P/AC:L/PR:H/UI:N	0.29	很低
	利用车端漏洞本地提权与刷写	AV:L/AC:H/PR:L/UI:N	1.04	很低

表6 风险矩阵模型

影响等级	攻击可行性			
	极低	低	中	高
严重	2	3	4	5
重大	1	2	3	4
中等	1	2	2	3
可忽略	1	1	1	1

针对表4的影响评级和表5的攻击可行性评估结果，采用风险矩阵确定各威胁场景的风险值，如表7所示。

表7 威胁场景风险确定示例

威胁场景	对应损害场景	最高影响等级	最高可行性评级	风险值	风险等级
信道不可用	远程解锁功能失效	中等	高	3	中
远程劫持	车辆失控	严重	高	5	极高
数据泄露	隐私侵犯	严重	高	5	极高
固件篡改	功能失效、隐私侵犯	严重	中	4	高

风险分析表明，远程劫持和数据泄露为极高风险（风险值5），因二者均具有严重影响且攻击可行性高；固件篡改为高风险（风险值4），虽影响严重，但当前可行性中等；信道不可用为中风险（风险值3），主要影响操作可用性。

2.5.2 风险处置策略与技术措施

风险处置决策包括消除/避免风险、降低风险、转移/分担风险和接受/保留风险，针对不同风险等级，遵循分级处置原则[7]。比如：

1）极高风险处置（远程劫持、数据泄露）

处置策略以消除风险为主。可采取技术措施：①强化身份与访问管理，实施多因素认证（MFA），如指纹、人脸识别等生物识别。②实现端到端数据加密，如传输层采用TLS协议，敏感数据（如用户身份、位置轨迹）使用加密存储。③实施数据脱敏与生命周期管理，如对非必要敏感信息（如完整身份证号）进行脱敏处理，制定数据保留策略，自动过期删除等。

2）高风险处置（固件篡改）

处置策略以降低风险为主。可采取技术措施：①固件签名与完整性验证，包括OTA升级包必须经厂商私钥签名，车端固件启动时需验证签名，支持安全回滚机制。②可信执行环境，关键代码（如BMS控制逻辑）在安全环境中运行。③网络传输安全，包括OTA下载通道使用HTTPS等加密协议，防止中间人劫持等。

3）中风险处置（信道不可用）

处置策略以分担和保留为主，辅以基础防护并进行安全监控和漏洞管理。可采取技术措施：①通信协议优化与冗余，包括对蓝牙/NFC近场通信引入抗DoS设计（如连接频率限制、请求超时控制），并保留物理钥匙等备用解锁方式。②流量监控与异常检测，如在网络边界部署IPS/IDS，监测异常流量模式。③服务冗余与快速恢复，如云端服务采用负载均衡和自动伸缩，确保单点故障不影响整体服务。

3 结 论

本研究成功将TARA方法论应用于智能网联电动自行车这一新兴领域，构建了一套覆盖“资产识别—威胁分析—风险评估—处置决策”的完整网络安全分析框架。研究结果表明，远程劫持（导致车辆失控）与用户隐私数据泄露为极高风险等级，固件篡改为高风险等级，这些是ICEB网络安全防护中需优先应对的核心威胁。通信信道拒绝服务、电池管理系统（BMS）攻击等风险同样不容忽视。

本研究的主要价值体现在以下3个方面：

1）研究紧密贴合GB 17761—2024、GB 44495—2024等国内最新标准要求，并参考ISO/SAE 21434等国际标准，为ICEB企业应对将来可能的信息安全难题提供了前瞻性的网络安全工程实践指南。

2）示例的风险处置策略应充分考虑ICEB成本

敏感、资源受限的特性，应实现安全性与成本的平衡，并促进功能安全与信息安全的融合。

3）示例的整车企业（OEM）与零部件供应商（Tier1）在网络安全活动中的责任界面，例如供应链或维护渠道植入威胁场景，OEM可基于TARA结果定义顶层的网络安全目标（Cybersecurity Goals），而Tier1则可据此推导出部件级的技术安全需求（TSR），为产业链上下游的协同安全开发提供了清晰的工作框架。

最后，未来研究方向或将聚焦于开展车路云协同安全，研究ICEB与充电设施、交通信号系统等车路云协同应用中的新型安全挑战。

参考文献

[1] 王淼，朱思婧. 网络安全形势与我国标准化竞争策略研究[J]. 标准科学，2024（8）：46–49.

[2] 卓圣钧，黄林轶，赖怡聪，等. 基于Windows系统的智能健康产品信息安全检测技术研究[J]. 标准科学，2025（10）：107–113.

[3] QB/T 5870—2023 电动自行车电子控制单元(ECU)通用技术规范[S].

[4] 张兴辉，刘建建，高田芳，等. 电动自行车智能化网联化历史、现状与发展趋势[J]. 中国自行车，2024（1）：112–117.

[5] GB 17761—2024 电动自行车安全技术规范[S].

[6] UNECE R155–2025/5 United Nations Economic Commission for Europe (UNECE). Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system[S].

[7] ISO/SAE 21434–2021 Road vehicles – Cybersecurity engineering[S].

[8] GB 44495—2024 汽车整车信息安全技术要求[S].

[9] 美国项目管理协会. 项目管理知识体系指南（PMBOK®指南）：第6版[M]. 北京：电子工业出版社，2018：4.

[10] 许瑞琛. 智能汽车信息安全和软件升级测评技术[M]. 北京：化学工业出版社，2025.