VSRQ：车辆智能网联系统安全风险定量评估方法

Tian Zhang、Wenshan Guan、Hao Miao、Xiujie Huang、成员，*IEEE*，Zhiquan Liu、成员，*IEEE*，Chaonan Wang、成员，*IEEE*，Quanlong Guan*、成员，*IEEE*，Liangda Fang、成员，*IEEE*，Zhifei Duan

arXiv:2305.01898v1 [cs.AI] 3 May 2023

摘要—**现代车辆智能网联系统领域持续扩展，随着时代的发展，车辆的功能变得越来越复杂。这也导致车辆漏洞数量不断增加，并引发了诸多安全问题。因此，识别高风险车辆智能网联系统尤为重要，因为这能够帮助安保人员了解哪些系统最容易受到攻击，从而对其开展更全面的检查和测试。本文通过将 I-FAHP 与 FCA 聚类相结合，开发了一种新的车辆风险评估模型：VSRQ 模型。我们提取了与车辆安全相关的重要指标，采用模糊聚类分析（FCA）结合模糊层次分析法（FAHP），挖掘车辆智能网联系统中的脆弱组件，并对脆弱组件进行优先级测试，以降低风险并确保车辆安全。我们在 OpenPilot 上对该模型进行了评估，并通过实验验证了 VSRQ 模型在识别车辆智能网联系统安全性方面的**有效性。**该实验完全符合 ISO 26262 和 ISO/SAE 21434 标准，且与其他模型相比，我们的模型具有更高的准确率。这些结果为预测车辆智能网联系统的安全风险提供了一个有前景的新研究方向，并为 VSRQ 提供了典型的应用任务。实验结果表明，准确率为 94.36%，召回率为 73.43%，比所有其他已知指标至少高出 14.63%。**

指标术语—**车辆安全，ISO 26262，ISO/SAE21434，FCA，模糊层次分析法，智能网联系统，脆弱组件**

*通讯作者

Tian Zhang 和 Wenshan Guan 就职于中国广州暨南大学信息科学与技术学院网络空间安全系，邮编 511486（电子邮箱：tianzhang@stu2022.jnu.edu.cn；gg-wsh@stu2022.jnu.edu.cn）。

Hao Miao 就职于中国广州暨南大学信息科学与技术学院计算机科学系，邮编 510632（电子邮箱：miaohao77@stu2020.jnu.edu.cn）。

Xiujie Huang 就职于中国广州暨南大学信息科学与技术学院、暨南大学广东省智慧教育研究院，邮编 510632（电子邮箱：t xiujie@jnu.edu.cn）。

Zhiquan Liu 就职于中国广州暨南大学网络空间安全学院，邮编 510632。（电子邮箱：zqliu@vip.qq.com）

Chaonan Wang 任职于中国广州 510632 暨南大学信息科学技术学院，同时任职于中国广东省基因数据处理与分析工程技术研究中心（电子邮箱：c wang@jnu.edu.cn）。

Quanlong Guan 就职于中国广州 510632 暨南大学信息科学与技术学院计算机科学系（电子邮箱：gql@jnu.edu.cn）。

Liangda Fang 任职于中国广州 510632 的暨南大学信息科学与技术学院计算机科学系，同时任职于广州 510330 的琶洲实验室，以及中国桂林 541004 的桂林电子科技大学广西可信软件重点实验室（电子邮箱：fangld@jnu.edu.cn）。

Zhifei Duan 任职于广州小鹏汽车科技有限公司，地址为中国广州天河区长兴街岑村松岗路8号（电子邮箱：duanzf@xiaopeng.com）。

I. 引言

VEHICLE 安全是研究并实践通过设计、建造、装备和法规来最大限度减少机动车辆交通事故发生及其后果的一门学科。1886年车辆刚发明时，还没有安全部件。人们购买车辆时，主要关注车辆的物理特性。随着车辆的发展，车辆于1959年开始配备安全带，1970年开始普遍配备儿童座椅，1980年开始普遍安装安全气囊。车辆安全电子化应用的标志，是德国博世在20世纪50年代发明的ABS（防抱死制动系统）的出现。进入21世纪以来，随着车辆技术的发展以及人们对车辆安全性能要求的不断提高，车辆安全变得尤为重要。因此，有必要预测和评估车辆风险。

迄今为止，已有许多用于预测和评估车辆风险的模型，例如 EVITA[1], ”汽车功能安全 = 安全 + 安保”[2], HEAVENS 1。0[3], AVSDA[4],RLE[5], P2BA[6], TROVE[7],等。尽管这些模型能够准确量化车辆的安全性，但其量化结果都是一个固定值。事实上，由于材料和温度等各种复杂因素的影响，安全量化结果以区间表示会更加准确。然而，要建立良好的车辆风险评估量化模型，仍面临一些挑战：首先，目前尚无模型能够在车辆投放前预测和评估其风险；由于车辆部件彼此独立，车辆投放前的风险预测比投放后更不确定。此外，由于车辆投放前的数据不公开，这些数据由各汽车企业私有。

为了解决上述挑战，过去三年中，前人提出了一些模型，并进行了若干风险预测。以自动驾驶汽车的传感器、操作系统、控制系统和车联网连接的攻击面为例， [8] 和 [9]考察了自动驾驶的安保。 [10] 基于自动化威胁面评估，将其作为汽车网络安全工程中用于难度分析的自动识别方法。 [11]使用贝叶斯防御图评估了自动驾驶汽车相关的风险。 [12]提出了一种基于边缘计算概念、高效且保护隐私的 VANET 数据下载方案。

[13] 提出的机制首先利用采用权益证明（PoS）共识的区块链，实现性能记录的可验证聚合和不可篡改传播。本文提出了一种名为 VSRQ 的模型。该模型标准为 ISO 26262[14] 和 ISO/SAE 21434[15]，并将风险等级划分为若干层级。当 VSR 大于或等于 0.758 时，车辆智能网联系统面临严重风险，车辆处于危险状态，系统需要立即整改。当 VSR 大于或等于 0.506 且小于 0.758 时，车辆智能网联系统处于轻度至严重风险状态，车辆处于临界状态。此时，应根据第一阶段识别出的脆弱组件开展详细研究。如果第一阶段影响因素中的电子控制单元（ECU）耦合风险处于较高水平，则需要整改整车的 ECU 系统，直至风险达到正常或最低水平。当 VSR 大于或等于 0 且小于 0.506 时，车辆智能网联系统的风险处于正常或最低水平，车辆处于稳态。此时无需更新车辆智能网联系统[14] ，因为其已达到质量管理水平。最后，我们还提出了一种基于 VSRQ 模型的车辆软件风险评估系统，利用 FCA 算法调整车辆指标的权重，设置动态参数，并使用纯追踪（PP）和 FAHP 算法建立车辆智能网联系统风险定量评估系统。该系统便于软件工程师预测车辆中的脆弱组件；其目的是在车辆投放前及时检查潜在风险，从而避免潜在危险。与其他模型相比，VSRQ 具有以下优势：首先，VSRQ 能够在合理范围内预测车辆风险，解决以往模型对车辆安全风险参数的预测过于绝对的问题。其次，我们的模型还会分析脆弱组件，自动且有效地识别车辆中可能存在的脆弱组件，计算车载软件的安保等级，并系统地发现车载集成系统的安保问题。

本文其余章节安排如下：第二节简要回顾了与车辆安全相关的一些已有研究。第三节给出了车辆智能网联系统安全的指标定义和问题陈述。第四节详细介绍了所提出的 VSRQ 模型。第五节评估了该模型的有效性和效率。最后，第六节总结全文并给出结论。

II. 相关工作

集成这一概念源于车辆控制单元复杂度的增加，其定义最初来自 IT行业标准。车辆智能网联系统的安全评估是一项相对困难的任务，与传统软件系统有着相当大的区别。它没有中央处理

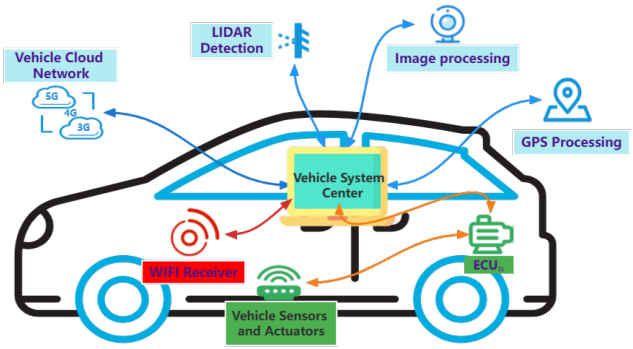


图 1：通用车辆智能网联系统模型

系统，而是利用车辆上的电子控制单元交互来实现车辆功能，车辆的通信方式和技术也与其他系统大不相同 [16]。

A. 国际标准的发展

现有车辆安全标准依据国际标准进行评估，其中包括 2011[14]发布的 ISO 26262《道路车辆—功能安全》标准。随后，2016年发布了《信息物理车辆系统网络安全指南》SAE J3601[17]，该指南详细定义了结构化的网络安全流程框架，这意味着汽车信息安全首次被提升到与功能安全同等甚至更重要的地位。最后，2021年8月，ISO 和 SAE 发布了汽车信息安全领域的首个国际标准 ISO/SAE 21434《道路车辆—网络安全工程》 [15]，该标准规定了汽车开发项目的详细风险评估流程，并提出了车辆信息安全风险评估方法 TARA。TARA 分析包括资产识别、威胁场景识别、攻击路径分析、攻击可行性评级、风险等级评估和风险处置措施等步骤，但该标准未规定具体的实施方法。

B. 现有模型框架开发

EVITA威胁与风险模型 [1] 于2009年首次发布，被认为是汽车行业有效的风险评估模型之一，也是汽车电气/电子系统开创性的风险评级方法。该模型侧重于识别针对特定目标的所有可能攻击，并考虑风险评级的四个参数：安保、财务、运营和隐私，但未充分研究这四个参数各自所占的比重。随后，Burton等人于2012年扩展了ISO 26262标准，并提出一种全面的“汽车功能安全 = 安全 + 安保” [2]方法。他们分析了通过系统开放接口蓄意操纵电气控制系统这一第三类危害，为车辆提供了更好的防护和安全保障。随后，Wolf和

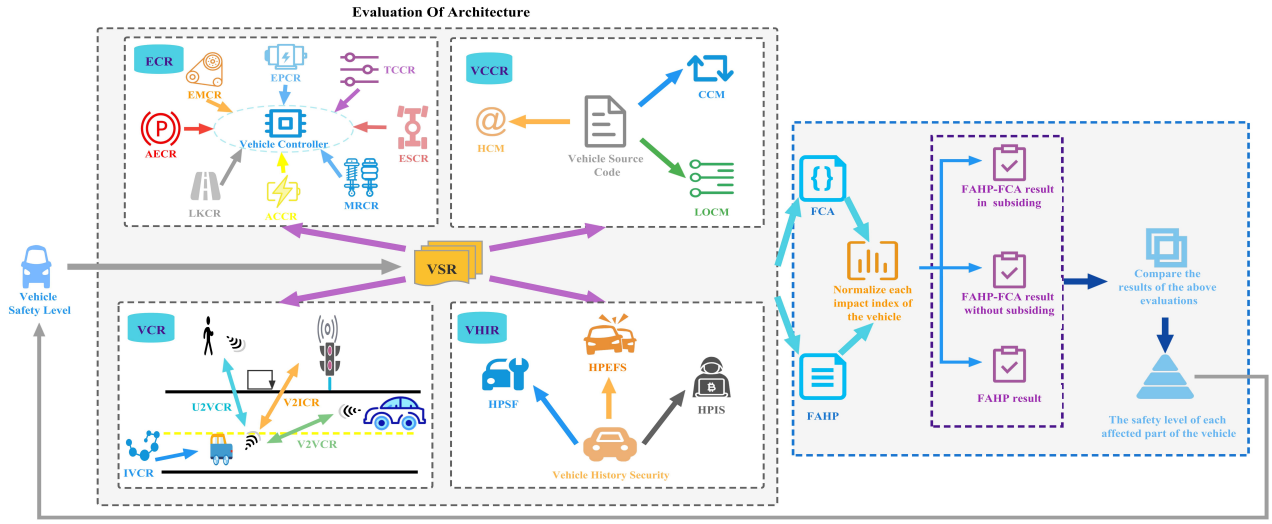


图2：车辆风险分析结构图

Scheibel等人 [18]将现有技术整合到汽车系统的风险评级框架中，并使用 perasset 根据安全问卷定义攻击树。在实施风险评估框架 HEAVENS1.0[3] 后，Islam等人提出，该框架完全符合功能安全标准 ISO 26262，并基于 ISO 26262 中的 ASIL 概念引入了“安全等级”。最后，Moukahal等人于2022年提出了 AVSDA安全衰减评估框架 [4] ，该框架可对汽车软件系统进行量化评估，不受开发阶段限制，还可评估车辆在运营阶段的安全性。

III. 初步分析

本节首先定义车辆系统的漏洞评估结构，然后定义各种因素对车辆损害严重程度的影响。根据图1所示的通用车辆智能网联系统模型，我们设计了本文提出的车辆风险分析结构图，如图2所示。

A. 脆弱组件评估结构

我们采用二阶多指标体系，对车辆概念阶段的智能网联系统风险进行量化。图2展示了我们评估车辆软件系统的流程。该流程由两部分组成：第一部分是对车辆系统中的脆弱部分进行定量评估；第二部分是评估车辆系统的风险等级，并确定车辆系统遭受攻击的可能性。

首先，为了分析车辆智能网联系统脆弱组件的影响因素，应考虑所有与车辆软件系统相关的信息流，如图 3 所示。图 3 描述了图 1 中的信息流，其中 Vehicle Communication Center（车辆通信中心）代表车联网。提供的信息如下：(1)GPS处理（车辆位置）；(2)图像处理（车辆监控与跟踪）；(3)激光雷达检测（周围环境监测）；(4)(5)车辆启动或停止命令；(6)(7)车辆启动或关闭状态数据；(8)(9)制动控制命令（例如车辆制动位置）；(10)(11)车辆推进控制命令（例如推进目标距离）；(12)(13)车辆推进状态数据（例如实际前进位置）；(14)(15)车辆转向控制指令（例如目标转向角）；(16)(17)车辆转向状态数据（例如实际转向角）；(18)(19)控制车辆平稳行驶的命令（例如车辆转向弹簧变形）；(20)(21)调整车辆悬架高度（例如减少车身位置变化）；(22)车辆实际状态数据（例如车辆周围环境、车辆系统危险）；(23)车辆网络中心数据（例如传输车辆信息）。需要注意的是，根据 [19], [20]，我们根据车辆的四个通信域，将车辆系统的通信风险（VCR）分为四类：车内通信风险（IVCR）、用户到车到车通信风险（U2VCR）、车到车通信风险（V2VCR）以及车到基础设施通信风险（V2ICR）。

随后，根据图3所示的信息流模型，我们将车辆系统脆弱组件结构的评估划分为以下三个层级。第一层为目标层级（车辆系统的脆弱组件）。第二层为指标层，包括车辆组件的耦合风险（ECU耦合）、通信风险、复杂性风险以及安全问题历史记录。第三层由第二层的子指标层组成，如图2所示。下文将详细定义各层的指标。

*1) ECU*耦合风险 *(ECR)*：ECU（电子控制单元）与普通计算机类似，由微控制器（MCU）、存储器（ROM、RAM）、输入/输出接口（I/O）、模数转换器（A/D）以及整形和驱动等大规模集成电路组成。

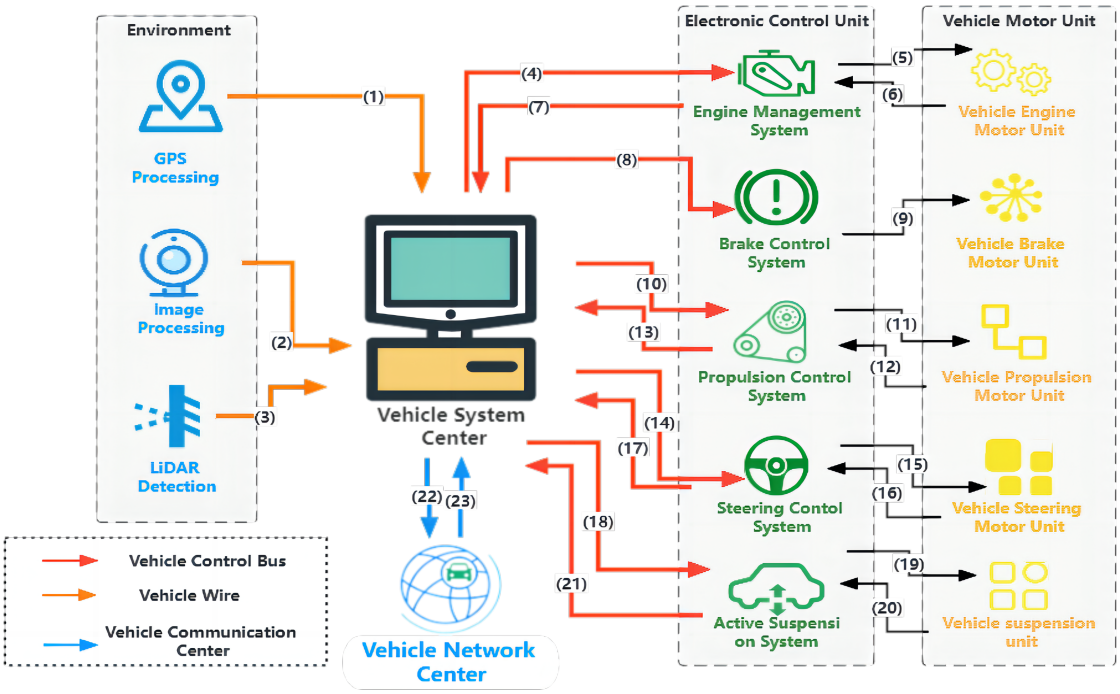


图 3：车辆智能网联系统中信息流示例图

理论上，功能越复杂，ECU的耦合程度越高；而ECU耦合会使恶意消息得以传播，并且随着ECU耦合程度的增加，车辆的安全性能也会下降。假设恶意消息在一辆配备复杂组件的车辆的ECU中传播，并且可以从该ECU传播至另一个ECU；若车辆中有更多实体通过控制系统相连，这种行为将对车辆造成极大损害。因此，在识别车辆软件系统中的脆弱组件时，应考虑ECU的耦合程度。

在该电子控制单元的耦合分析中，我们不考虑网络通过总线拓扑互联的情况，而将在二阶指标中分析总线拓扑的通信风险，具体介绍如下：

定义 *1*（发动机管理系统耦合风险（*EMCR*））：发动机管理系统（EMS）通过控制进气、燃油喷射和点火来实现发动机功率、经济性、排放及其他性能之间的平衡，并集成了整车的扭矩分析功能。

定义 *2*（变速器控制单元耦合风险（*TCCR*））：通过电磁阀控制油压，实现离合器的自动接合或分离，在适当时间完成换挡，提升车辆的动力性和平顺性。

定义 *3*（电动助力转向耦合风险（*EPCR*））：电机辅助驾驶员转向，降低驾驶难度。

定义 *4*（车身稳定性控制耦合风险（*ESCR*））：它集成了 TCS、ABS、电子稳定控制系统（ESC）等功能，并通过控制车轮端的制动力，实现车辆的稳定行驶。

定义 *5*（主动悬架系统耦合风险（*MRCR*））：控制电磁阀以调节悬架系统的高度或阻尼，从而提升车辆的行驶稳定性和舒适性。

定义 *6*（自适应电池寿命耦合风险（*ACCR*））：车辆根据前车的运动情况，在保持安全车距的同时，通过控制驱动力或制动力，尽可能按照驾驶员期望的速度行驶，从而解放驾驶员的手脚。

定义 *7*（车道保持辅助耦合风险（*LKCR*））：在识别车道线的基础上，控制方向盘转角，使车辆保持在车道中央。

定义 *8*（自动紧急制动耦合风险（*AECR*））：在紧急情况下，控制制动力使车辆停止，以避免发生碰撞事故。

在 ECU耦合风险类别中，各子系统的耦合方程定义如下：

$$E = \sum_{i=1,j=1}^{N} \delta_{ij}/2 \tag{1}$$

其中，N 表示车辆系统中的子部件总数。当两个子系统 s_i 和s_j之间存在连接时，表示二者之间存在调用关系，此时 δ_{ij} 的值为 1，否则该值为 0。

以 EMSC 为例，其中 N 表示发动机管理系统中的子部件总数

车辆中的耦合（EMSC）系统。当两个子系统 EMSC$_i$ 和 EMSC$_j$之间存在连接时， δ_{ij} 的值为 1，否则为 0。

2) 车辆通信风险（*VCR*）：车辆信息与通信系统为驾驶员提供有关道路状况的最新关键信息。我们根据车辆的四个通信域，将车辆系统的通信风险分为四个类别。

定义 *9*（车内通信风险（*IVCR*））：车内通信是指网联汽车中唯一的非外部通信，它满足不同电子控制单元（ECU）之间的所有通信需求。车内通信使用 LIN（局部互连网络）、CAN（控制器局域网）、FlexRay 和 MOST（面向媒体的系统传输）等网络 [19]。因此，我们将车内通信风险定义为

$$V_1 = \sum_{i=1}^{N} \varrho_1 n_{LIN_i} + \varrho_2 n_{CANL_i} + \varrho_3 n_{CANH_i} + \varrho_4 n_{FL_i} + \varrho_5 n_{MOST_i} \quad (2)$$

ϱ 表示每种通信攻击对车辆的严重程度，n_{LIN} 表示车辆中使用LIN网络进行通信的模块数量，n_{CANH} 表示车辆中使用高速CAN网络进行通信的模块数量，n_{CANL} 表示车辆中使用低速CAN网络进行通信的模块数量，n_{FL} 表示车辆中使用FlexRay网络进行通信的模块数量，n_{MOST} 表示车辆中使用MOST网络进行通信的模块数量，i 表示车辆中的每个模块，N 表示车辆系统的模块总数。

定义 *10*（用户到车辆通信风险（*U2VCR*））：用户到车辆（U2V）主要是指为驾驶员提供车载服务。在正常情况下，车辆到用户的通信主要指蓝牙和专用短程通信（DSRC）[19]，这也可以被视为车内通信的一种特殊情况。我们将用户到车辆通信的风险定义为

$$V_2 = \sum_{i=1}^{N} n_{DSRC_i} \quad (3)$$

其中，n_{DSRC} 表示车辆中通过DSRC网络进行通信的模块数量。

定义 *11*（车辆间通信风险（*V2VCR*）：）两辆车辆之间的通信通常是为了共享交通信息。这种通信可以通过一种称为车载自组网（VANETs）的自组网进行 [21]。然而，这也会带来相应的风险，例如窃听车辆消息、转发错误，甚至损坏电子控制单元（ECU） [22]。因此，我们将车辆到车辆通信风险定义为

$$V_3 = \sum_{i=1}^{N} n_{VANETs_i} \quad (4)$$

其中，n_{VANETs} 表示使用车载自组织网络进行车对车通信的模块数量。

定义 *12*（车辆与基础设施通信风险（*V2ICR*））：车辆到基础设施主要是指车辆与道路交通之间的信息共享，以提高车辆行驶安全和改善车辆行驶路线。主要采用以下三种通信技术：车载自组织网络、Wi-Fi 和蜂窝通信，因此我们将车辆与基础设施通信风险定义为

$$V_4 = \sum_{i=1}^{N} \alpha_1 n_{VANETs_i} + \alpha_2 n_{WF_i} + \alpha_3 n_{Cel_i} \quad (5)$$

其中， α 表示每次通信损害对车辆造成的伤害程度，n_{VANETs} 表示车辆与基础设施之间使用车载自组织网络进行通信的模块数量，n_{WF} 表示车辆中使用 Wi-Fi 进行通信的模块数量，n_{Cel} 表示车辆中使用蜂窝网络进行通信的模块数量。

3）车辆代码复杂度风险（*VCCR*）：现代汽车系统的代码行数（LOC）已超过 1 亿行，并且近年来将迅速增加到 3 亿行[23]。然而，代码行数越多，复杂度越高，风险也越大[24], [25]。攻击者可以利用这些车辆软件漏洞危害车辆系统，因此我们使用车辆代码复杂度风险作为一项指标[24], [25]。我们提及的指标定义如下：

定义 *13*（源代码行指标风险（*LOCM*））：n_{LOC} 表示车辆每个模块中可执行语句的源代码行数。因此，源代码行的复杂度定义为

$$C_1 = \sum_{i=1}^{s} n_{LOC_i}, \quad (6)$$

其中，s表示车辆中的代码模块。 车辆。

定义 *14*（运算符和操作数复杂度指标风险（*HCM*））：HCM 根据车辆软件系统中运算符和操作数的数量进行计算。运算符表示车辆代码中需要执行的运算符号，而操作数表示车辆系统代码中需要进行运算的基本逻辑单元。因此，HCM 定义为

$$C_2 = \sum_{i=1}^{s} (N_1 + N_2) log_2(n_1 + n_2)/3000 \quad (7)$$

其中，n_1 表示运算符的类别数，n_2 表示操作数的类别数，N_1表示运算符出现的次数，N_2表示操作数出现的次数。

定义 *15*（代码度量风险的圈复杂度（*CCM*））：CCM 主要关注车辆软件模块中循环结构图复杂度的风险测量，并为车辆软件代码中的不同控制结构分配不同的权重。因此，CCM 定义为

$$C_3 = \sum_{i=1}^{s} E - H + 2 \quad (8)$$

其中，E 是控制流图中的边数，H 是控制流图中的节点数。

4) 车辆历史安全问题风险（*VHIR*）：在评估无人驾驶车辆的脆弱组件时，我们还会考虑车辆此前的软件错误和安全攻击所导致的风险。我们将车辆历史安全子指标分为以下三类，包括车辆功能安全历史问题、车辆预期功能安全历史问题以及车辆信息安全历史问题。

定义*16*（车辆安保功能历史问题（*HPSF*））：车辆安保功能问题主要指车辆电子电气系统发生故障，包括巡航控制系统故障、车身控制模块故障。这些功能性安保问题造成的后果往往最为严重，甚至需要更换零部件才能解决。我们将其定义为

$$H_1 = \sum_{d=1}^{Y} \eta_d + \lambda \tau_d \tag{9}$$

其中，η_d 表示上次召回的此类车辆数量，τ_d 表示上次因电气和电子系统故障而维修的此类车辆数量，λ 表示遗忘因子，用于计算车辆购买后更换所需时间的车辆部件。时间越长，λ 的值越小。

定义*17*（车辆预期功能安全历史问题（*HPEFS*）：）车辆预期功能安全是指对车辆所经历物理环境的识别。由于标定不明确，车辆可能产生错误认知或错误执行，从而导致车辆中存在潜在安全危害，包括系统功能限制和环境干扰等。因此，我们将其定义为

$$H_2 = \sum_{i=1}^{N} n_{spl_i} \tag{10}$$

其中，n^{spl} 表示因系统性能限制而导致的车辆事故数量。

定义*18*（车辆信息安全历史问题（*HPIS*）：）车辆信息安全问题是指车辆系统遭受黑客攻击，从而导致车辆系统出现一系列安全问题。黑客攻击包括分布式拒绝服务、模糊攻击和欺骗攻击。信息安全防护应纳入车辆设计和开发阶段，因此我们根据车辆的核心部件对车辆信息安全进行分类，并将其设定为

$$H_3 = \sum_{i=1}^{N} \varepsilon_1 n_{Ve_i} + \varepsilon_2 n_{Te_i} + \varepsilon_3 n_{Ne_i} + \varepsilon_4 n_{Cl_i} \tag{11}$$

其中，n_{Ve} 表示对车辆终端的攻击次数，n_{Te} 表示对车辆终端的攻击次数，n_{Ne} 表示车辆网络侧遭受的攻击次数，n_{Cl} 表示.....的次数。对车辆云端的攻击，以及 ε 表示攻击对车辆各核心部件造成的损害严重程度。

B. 车辆损害严重程度（*D*）

为了定量评估车辆智能网联系统，我们使用四个指标综合考虑车辆损害的严重程度：D_1（安全性，即部件损害对车辆的总体影响）、D_2（隐私，即车辆数据攻击对车辆造成的影响）、D_3（财务，即受损部件给车辆造成的财务损失）、D_4（运营损失，即受损部件给车辆造成的运营损失）。我们根据 SAE J3061 [17],RACE[26] 和 VeRA[27]中车辆损害严重程度的定义，列出了表 I。本文采用上述严重程度向量的最大值来表示车辆损害严重程度等级。例如，假设上述严重程度向量 [6, 3, 5, 4]（即$D_1 = 6$、$D_2 = 3$、$D_3 = 5$、$D_4 = 4$），则可知车辆损害的严重程度等级为$D = 6$。

然而，我们无法准确预测每个影响因素造成的绝对损害程度。因此，我们根据主要车辆数据网站披露的安全数据和财务数据（来源请参见 n3.datasn.io、www.crysys.hu 及一些先前的论文 [16], [27], [26]），构建了一个矩阵，用于反映各影响车辆指标损害程度的相对重要性，如表 II、III、IV、V、VI 所示，并采用以下核心算法模型，通过各影响因素动态调整车辆损害的严重程度，从而使我们的车辆智能网联系统评估模型更加准确。

IV. 评估模型的建立

本文采用多指标体系评估车辆软件集成系统的风险，主要包括评估结构、风险模型的建立和校准评估。第三节已对评估结构作出说明；第四节建立风险模型时，将结合上述车辆软件安全四个二阶指标中选取的 15 个子指标与车辆风险数据图谱。此外，校准评估基于 I-FAHP方法，用于校准评估因素的主观权重。下文将详细介绍我们建立的车辆风险评估模型。

A. 架构评估

在车辆的ECU耦合方面，相关风险指标包括主要系统中的ECU耦合（如EMCR、TCCR、EPCR、ESCR）。对于车辆通信风险，包括IVCR、U2VCR、V2VCR、V2ICR。代码复杂度风险表示车辆智能网联系统中代码的LOCM、HCM、CCM。最后，车辆的安全历史风险用HPSF、HPEFS、HPIS表示。因此，车辆智能网联系统风险可以使用公式（12）进行概念性描述。

$$VSR = ECR \otimes VCR \otimes VCCR \otimes VHIR \tag{12}$$

表 I：车辆损害严重程度 [26], [27], [17]

严重程度 D	安全 D_1	隐私 D_2	财务 D_3	运营 D_4
0	无人受伤	未发生未经授权的数据访问	0 ≤ 损失<100	对性能没有影响
1 – 3	轻伤	访问匿名数据	100≤损失<1000	驾驶员未察觉到影响
4 – 6	重伤，伴随生存	车辆或驾驶员识别	1000≤损失<10000	驾驶员意识到性能退化
7 – 9	危及生命，可能导致死亡	驾驶员或车辆跟踪	损失≥10000	对性能的显著影响

表 II：VSR 一阶因子损伤严重程度矩阵

VSR	ECR	VCR	VCCR	VHIR
ECR	1.000	1.143	2.000	2.667
VCR	0.875	1.000	1.750	2.333
VCCR	0.500	0.571	1.000	1.333
VHIR	0.375	0.429	0.750	1.000

表 III：ECR 指标损伤程度严重性矩阵

ECR	EMCR	TCCR	EPCR	ESCR	MRCR	ACCR	LKCR	AECR
EMCR	1.000	1.167	0.778	0.875	1.400	1.750	1.400	0.778
TCCR	0.857	1.000	0.667	0.750	1.200	1.500	1.200	0.667
EPCR	1.286	1.500	1.000	1.125	1.800	2.250	1.800	1.000
ESCR	1.143	1.333	0.889	1.000	1.600	2.000	1.600	0.889
MRCR	0.714	0.833	0.556	0.625	1.000	1.250	1.000	0.556
ACCR	0.571	0.667	0.444	0.500	0.800	1.000	0.800	0.444
LKCR	0.714	0.833	0.556	0.625	1.000	1.250	1.000	0.556
AECR	1.286	1.500	1.000	1.125	1.800	2.250	1.800	1.000

其中，符号 ⊗ 仅用于表示车辆软件系统风险公式的叠加分析。我们认为，不同影响因素对车辆智能网联系统风险的影响程度不同，因此，将不同评价因素及其相应权重结合起来，用于车辆智能网联系统的风险评估，并使用公式（13）重新定义VSR。

$$\begin{aligned} VSR = \omega_E(\sum_{i=1}^{n} e_i E_i)_{ECR} \otimes \omega_V(\sum_{j=1}^{n} v_j V_j)_{VCR} \\ \otimes \omega_C(\sum_{k=1}^{n} c_k C_k)_{VCCR} \otimes \omega_H(\sum_{l=1}^{n} h_l H_l)_{VHIR} \end{aligned} \tag{13}$$

其中，ω_E、ω_V、ω_C 和 ω_H 分别为车辆ECU耦合风险指标、车辆通信风险指标、车辆代码复杂度风险指标以及车辆历史信息安全事件风险权重问题指标。

表 IV：VCR 指标损伤程度严重性矩阵

VCR	IVCR	U2VCR	V2VCR	V2ICR
IVCR	1.000	1.600	2.667	1.143
U2VCR	0.625	1.000	1.667	0.714
V2VCR	0.375	0.600	1.000	0.429
V2ICR	0.875	1.400	2.333	1.000

表 V：VCCR 指标损伤程度严重性矩阵

VCCR	LOCM	HCM	CCM
LOCM	1.000	0.333	0.200
HCM	3.000	1.000	0.600
CCM	5.000	1.667	1.000

表 VI：VHIR 指标损伤程度严重性矩阵

VHIR	HPSF	HPESF	HPIS
HPSF	1.000	2.667	1.600
HPESF	0.375	1.000	0.600
HPIS	0.625	1.667	1.000

根据上述评估结构，我们对每个影响子指标进行了分析和处理。为了获得准确的评估结果，在叠加各影响指标之前，我们先对上述车辆影响因素进行归一化处理，归一化后的车辆软件安全影响指标取值范围为 $[0, 1]$。归一化方法如公式（14）所示。

$$\beta_{ij} = \frac{\alpha_{max} - \alpha_{ij}}{\alpha_{max} - \alpha_{min}} \tag{14}$$

其中，β_{ij} 是车辆影响因素的标准化值；α_{max} 和 α_{min} 分别对应车辆系统各影响子因素的最大值和最小值。α_{ij} 表示车辆中二阶影响因素的原始值。

为评估车辆软件的安保风险，我们将区间模糊层次分析法（I-FAHP）引入上述评估框架。I-FAHP方法在层次分析法的基础上使用区间模糊数，在判断矩阵中表示各车辆二阶影响因素的重要性。下一小节将详细介绍所使用的I-FAHP方法。

B. I-FAHP方法介绍

区间模糊层次分析法的权重计算基于上述车辆智能网联系统安全风险评估结构。各评价因素的判断矩阵（φ）可由公式（15）表示：

$$\varphi = [\varphi^-, \varphi^+] = (\varphi_{ij})_{m\times m} = (\varphi_{ij}^-, \varphi_{ij}^+)_{m\times m}$$

$$= \begin{cases} [1,1] & [\varphi_{12}^-, \varphi_{12}^+] \cdots [\varphi_{1i}^-, \varphi_{1i}^+] \cdots [\varphi_{1m}^-, \varphi_{1m}^+] \\ [\frac{1}{\varphi_{12}^-}, \frac{1}{\varphi_{12}^+}] & [1,1] \quad \cdots [\varphi_{2i}^-, \varphi_{2i}^+] \cdots [\varphi_{2m}^-, \varphi_{2m}^+] \\ \cdots & \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ [\frac{1}{\varphi_{1i}^-}, \frac{1}{\varphi_{1i}^+}] & [\frac{1}{\varphi_{2i}^-}, \frac{1}{\varphi_{2i}^+}] \quad \cdots \quad [1,1] \quad \cdots [\varphi_{im}^-, \varphi_{im}^+] \\ \cdots & \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ [\frac{1}{\varphi_{1m}^-}, \frac{1}{\varphi_{1m}^+}][\frac{1}{\varphi_{2m}^-}, \frac{1}{\varphi_{2m}^+}] \cdots [\frac{1}{\varphi_{im}^-}, \frac{1}{\varphi_{im}^+}] \cdots & [1,1] \end{cases} \tag{15}$$

区间判断矩阵（φ）分为两部分：下限判断矩阵（φ^-）和上限判断矩阵（φ^+）。φ_{ij}^- 和 φ_{ij}^+ 是判断矩阵 φ中的元素，表示因素 φ_i 相对于因素φ_j的重要性。当 φ_i比φ_j重要得多时，将 φ_{ij}设定为

9，并将φ_{ji}设定为1/9，其中$1/9 \le \varphi_{ij}^{-} \le \varphi_{ij}^{+} \le 9$。区间判断矩阵的权重向量可根据公式（16）计算。

$$\begin{cases} \vec{\gamma} = [\gamma_1, \gamma_2] = [\mu\gamma^{-}, \nu\gamma^{+}] \\ \mu = \sqrt{\sum_{j=1}^{m} \frac{1}{\sum_{i=1}^{m} \varphi_{ij}^{+}}} \\ \nu = \sqrt{\sum_{j=1}^{m} \frac{1}{\sum_{i=1}^{m} \varphi_{ij}^{-}}} \end{cases} \tag{16}$$

γ^{-} 和 γ^{+} 分别为下界矩阵和上界矩阵的权重。 γ_1 和 γ_2 为区间判断矩阵的权重；当区间模糊层次分析法的权重反复覆盖原始层次分析法的权重时，区间判断矩阵 $\vec{\gamma}$ 被认为是合理的，其中 γ 是通过AHP方法校准的权重。如公式（17）所示。

$$\gamma_1 \le \gamma \le \gamma_2 \tag{17}$$

C. 描述 *FCA* 方法

FCA方法主要用于修正通过I-FAHP方法获得的权重，并分析车辆数据样本与上述车辆评价标准之间的相对关系。假设有x 辆车辆，具有评价样本数据和y 个影响指标，则形成的特征向量为:

$$N = (n_{ij})_{x\times y} = \begin{bmatrix} n_{11} & n_{12} & \cdots & n_{1y} \\ n_{21} & n_{22} & \cdots & n_{2y} \\ \vdots & \vdots & \ddots & \vdots \\ n_{x1} & n_{x2} & \cdots & n_{xy} \end{bmatrix} \tag{18}$$

矩阵元素中的n^{ij} 是车辆影响因素j 对车辆数据样本i 的特征值。为消除车辆数据规模不同所带来的影响，我们根据公式（14）对矩阵N 中的每个元素进行归一化。

假设车辆中有y 个二阶影响因素，对x 个评价样本数据进行a 类聚类，因此形成的模糊聚类矩阵P 可由公式（19）表示:

$$P = (p_{ei})_{a\times x} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1x} \\ p_{21} & p_{22} & \cdots & p_{2x} \\ \vdots & \vdots & \ddots & \vdots \\ p_{a1} & p_{a2} & \cdots & p_{ax} \end{bmatrix} \tag{19}$$

其中，p_{ei} 表示车辆数据样本i 与类别a之间的相对关联度，$0 \le p_{ei} \le 1$, $\sum_{e=1}^{a} p_{ei} = 1$。$x$ 表示车辆样本数据的数量，e 表示类别的数量。其中，类y 指标的特征值表示为聚类中心，因此模糊类中心矩阵 S 可由公式 (20) 表示:

$$S = (s_{ja})_{y\times e} = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1e} \\ s_{21} & s_{22} & \cdots & s_{2e} \\ \vdots & \vdots & \ddots & \vdots \\ s_{e1} & s_{e2} & \cdots & s_{ye} \end{bmatrix} \tag{20}$$

其中，s_{ja} 表示车辆指标j 与类别a之间的相对关联度， $0 \le s_{ja} \le 1$。

根据上述矩阵P和S，车辆评价样本的特征值类别计算公式如下，即公式（21）：

$$R_i = \sum_{e=1}^{a} p_{ei} \cdot e \tag{21}$$

其中，R_i 表示车辆数据样本i的特征值类别。根据R_i的值，可以确定车辆数据评价样本的风险类别。

D. 综合评价模型

我们再次强调，本文的主要贡献在于使用FCA和FAHP方法，在车辆上路前对车辆智能网联系统进行风险评估。在车辆软件风险评估领域，目前尚无更好的评估方法。通过上述FCA，我们可以得到相应的敏感度系数 ρ，其中 ρ主要用于修正I-FAHP方法得到的权重，修正后的权重 φ 如公式（22）所示:

$$\varphi = \rho\varphi_s + (1-\rho)\varphi_o \tag{22}$$

其中， $0 \le \rho \le 1$, φ_s 表示主观权重，可通过I-FAHP方法进行校准； φ_o 表示客观权重，用于反映车辆评价数据样本的特征。

然后，我们使用投影寻踪（PP）方法校准φ_{oj}的值。假设n_{ij}是车辆评价数据样本N 指标i的系数j，最佳校准向量为 $\vec{}l$，则可根据PP得到如下方程（23）:

$$\phi_j = \sum_{j=1}^{y} \vec{l}_j z_{ij}, \quad i \in [1, x], j \in [1, y] \tag{23}$$

其中，x表示评价样本数据的数量，y表示影响指标的数量。方向向量 $\vec{}l_j$表示车辆数据样本的特征， $\vec{}l_j = (l_1, l_2, l_3 \cdots, l_y)$，而$z_{ij}$表示车辆影响因素$i$的归一化因子$j$。为获得优化后的 $\vec{}l_j$，建立目标函数$f(l)$，如下方程（24）所示:

$$\begin{cases} A_\phi = (\frac{\sum_{i=1}^{x}(\phi_i - \bar{\phi})}{x-1}) \\ b_{ia} = \|\phi_i - \phi_a\| \\ B_\phi = \sum_{i=1}^{x} \sum_{a=1}^{x} (b - b_{ia}) \cdot f(b - b_{ia}) \\ maxR(l) = A(l) \cdot B(l) \end{cases} \tag{24}$$

在上述公式中， $\bar{\phi}$ 表示 ϕ_i的平均值，A_ϕ 表示车辆数据评估样本的标准差，B_ϕ 表示局部密度函数，$f(b-b_{ia})$是单位阶跃函数，如公式（25）所示:

$$f(b - b_{ia}) = \begin{cases} 1, & b - b_{ia} \ge 0 \\ 0, & b - b_{ia} < 0 \end{cases} \tag{25}$$

V. 实验结果

本节将以 OpenPilot 为例开展实验研究。 [28] OpenPilot 是一种较为成熟的L_2 辅助驾驶型开源自动驾驶系统， [28],基于端到端模型实现自适应巡航、车道保持辅助和驾驶员状态监测等辅助驾驶功能。此外, OpenPilot 只需搭配装有 OpenPilot 软件的手机和高通骁龙821 芯片，即可实现 L2+ 自动驾驶。最后但同样重要的是，在基于消费者使用情况评估的 2020年 评估报告中, OpenPilot 的综合得分高达 78，排名第一。因此，我们综合考虑后选用 OpenPilot 进行实验。我们将在 OpenPilot 上介绍所提评估方法的测试步骤[28],，包括第 5.1 节中 I-FAHP 各车辆影响因素权重的校准、第 5.2 节中车辆评估指标的分析，以及最后第 5.3 节中 OpenPilot 车辆指标评估结果的说明。实验在一台运行 Windows 10 企业版的计算机上进行，该计算机配备 64 位 Core(TM) i5-9400、主频为 2.90 GHz 的英特尔酷睿处理器以及 16 GB 主存。

A. 评估模型权重校准

车辆软件集成系统风险评估模型的权重校准主要分为两部分。第一部分采用 I-FAHP方法校准权重，第二部分采用 FCA方法修正通过 I-FAHP 得到的权重。本文中，各评价因素的数据来源如下。(1) E_i 分别表示：E_1 表示 EMCR，E_2 表示 TCCR，E_3表示 EPCR，E_4 表示 ESCR，E_5 表示 MRCR，E_6 表示 ACCR，E_7 表示 LKCR，E_8 表示 AECR；E_1 至 E_5 的数据来源为《主要车辆智能网联系统平台》，E_6 至 E_8 的数据来源为《主动驾驶辅助系统: 测试结果与设计建议》。(2) V_i 分别表示：V_1 表示 IVCR，V_2 表示 U2VCR，V_3 表示 V2VCR，V_4表示 V2ICR；V_i 的数据来源为《主要车辆通信架构》。(3) C_i 分别表示：C_1 表示 LOCM，C_2 表示 HCM，C_3 表示 CCM；C_i 的数据来源为《主要车辆系统核心源代码》。(4) H_i 分别表示：H_1 表示 HPSF，其数据来源为《主要车辆维护记录》；H_2 表示 HPESF，其数据来源为《主要车辆交通安全事故》；H_3 表示 HPIS，其数据来源为《主要车辆系统攻击数据》。

1) 通过*I-FAHP*获得权重：根据上文图2所示的评价结构，我们采用I-FAHP方法对车辆评价影响指标的权重进行校准。为了获得区间模糊权重，首先应对原始AHP权重进行校准，即采用对车辆影响因素进行两两比较的形式来表示车辆影响因素的相对重要性。表II、III、IV、V、VI列出了我们的主要车辆影响指标数据，然后基于一致性判断矩阵即可得到相应的区间判断矩阵。表VII列出了通过I-FAHP方法校准后的车辆影响指标权重，其中AHP权重位于I-FAHP权重范围内，这证实了我们的I-FAHP判断矩阵的适用性。

2) FCA校准区间权重：根据I-FAHP方法校准得到的车辆影响因素主观权重，使用FCA方法计算的敏感度系数 ρ 对主观权重进行修正。然后，根据获得的车辆敏感度系数和车辆影响指数的目标权重，利用上述公式（22）即可得到车辆各影响因素的修正权重，修正权重列于表VII倒数第二列。ECR的权重为$E_i = (E_1,E_2,E_3,E_4,E_5,E_6, E_7, E_8) =$([0.087192,0.176398],[0.051338,0.13285],[0.137686,0.202734],[0.119758,0.166852],[0.07350,0.106024],[0.054522,0.079150],[0.080648,0.096534],[0.137688,0.263554])；VCR的权重为$V_j = (V_1, V_2, V_3, V_4) =$([0.301822,0.38003],[0.19191,0.246806],[0.121712,0.137128],[0.267714,0.352784])；VCCR的权重为$C_k = (C_1,C_2,C_3)=$ ([0.115458, 0.119876],[0.310876,0.36878],[0.505986,0.575546])；VHIR的权重为$H_l = (H_1,H_2,H_3) =$ ([0.452454,0.52145],[0.175528,0.201284],[0.289674,0.358012])。

B. 车辆影响因素分析

随后，我们根据 ISO26262[14] 和 ISO/SAE 21434[15]，中的风险评估表，对上述定义的车辆影响指标进行归一化，并定义了一个全新的车辆软件集成系统风险评估矩阵。由于需要将 HARA 和 TARA 中的等级数量从 4 级增加到 5 级，我们选择直接构建一个全新的矩阵，而不是先对 HARA 和 TARA 中的表格进行归一化，再增加等级数量并重新调整。各影响指标新提出的评级映射表见表 VIII、IX、X、XI。随后，根据上述表格，采用重叠区间下限法，并结合表 VII 中列出的相应权重，可得到表 XII 中一级影响指标的评级映射。其中，ECR_{nor}、VCR_{nor}、$VCCR_{nor}$ 和 $VHIR_{nor}$ 分别表示 ECR、VCR、VCCR 和 VHIR 的归一化参数之和。最后，根据上述车辆影响指标的评级映射表和表 XII，并结合目标函数方程（13），构建车辆智能网联系统风险评估矩阵的评级映射（如表 XIII 所示）。

然后，在风险矩阵的基础上，我们创新性地定义了车辆智能网联系统的三种状态：稳态、临界状态和危险状态，并进一步提出了相应的安全措施。

表 XIII 对车辆智能网联系统的风险等级进行了划分。可以看出，当 VSR 大于或等于 0.758 时，车辆智能网联系统处于严重风险状态。此时，车辆处于危险状态，应对集成系统进行修复；当 VSR 大于或等于 0.506

表 VII：根据 I-FAHP 和 FAHP-FCA 校准的车辆智能网联系统影响指标权重

指标层			子指标层				
指标	AHP	I-FAHP	因素	AHP	I-FAHP	FCA-AHP	FCA-I-FAHP
ECR	0.3636	[0.2949,0.3702]	EMCR	0.1321	[0.0861,0.1810]	0.130432	[0.087192,0.176398]
			TCCR	0.1132	[0.0785,0.1333]	0.113956	[0.081338,0.132850]
			EPCR	0.1698	[0.1351,0.2043]	0.170304	[0.137686,0.202734]
			ESCR	0.1510	[0.1180,0.1681]	0.150778	[0.119758,0.166852]
			MRCR	0.0943	[0.0702,0.1048]	0.096154	[0.073500,0.106024]
			ACCR	0.0755	[0.0495,0.0757]	0.078962	[0.054522,0.079150]
			LKCR	0.0943	[0.0824,0.0993]	0.091834	[0.080648,0.096534]
			AECR	0.1698	[0.1380,0.2719]	0.167580	[0.137688,0.263554]
VCR	0.3182	[0.2778,0.4013]	IVCR	0.3478	[0.2935,0.3767]	0.352864	[0.301822,0.380030]
			U2VCR	0.2174	[0.1938,0.2522]	0.214094	[0.191910,0.246806]
			V2VCR	0.1305	[0.1241,0.1405]	0.127728	[0.121712,0.137128]
			V2ICR	0.3043	[0.2643,0.3548]	0.305314	[0.267714,0.352784]
VCCR	0.1818	[0.1527,0.1911]	LOCM	0.1111	[0.1089,0.1136]	0.117526	[0.115458,0.119876]
			HCM	0.3333	[0.3097,0.3713]	0.333060	[0.310876,0.368780]
			CCM	0.5556	[0.5094,0.5834]	0.549414	[0.505986,0.575546]
VHIR	0.1364	[0.1211,0.1435]	HPSF	0.5000	[0.4524,0.5258]	0.497198	<escape>[0.452454,0.521450]</escape>
			HPESF	0.1875	[0.1786,0.2060]	0.183894	[0.175528,0.201284]
			HPIS	0.3125	[0.2814,0.3541]	0.318908	[0.289674,0.358012]

表 VIII：ECR 影响因素评价标准

ECR	正常	轻微	较严重	严重	极其严重
E_1	0-0.30	0.30-0.45	0.45-0.60	0.60-0.80	0.80-1.00
E_2	0-0.35	0.35-0.55	0.55-0.70	0.70-0.85	0.85-1.00
E_3	0-0.20	0.20-0.35	0.35-0.55	0.55-0.70	0.70-1.00
E_4	0-0.25	0.25-0.40	0.40-0.55	0.55–0.75	0.75-1.00
E_5	0-0.40	0.40-0.55	0.55-0.80	0.80-0.90	0.90-1.00
E_6	0-0.45	0.45-0.65	0.65-0.85	0.85-0.92	0.92-1.00
E_7	0-0.40	0.40-0.55	0.55-0.80	0.80-0.90	0.90-1.00
E_8	0-0.20	0.20-0.35	0.35-0.50	0.50-0.70	0.70-1.00

表 IX：VCR影响因素评价标准

VCR	正常	轻微	较严重	严重	极其严重
V_1	0-0.30	0.30-0.40	0.40-0.60	0.60-0.80	0.80-1.00
V_2	0-0.35	0.35-0.55	0.55-0.75	0.75-0.90	0.90-1.00
V_3	0-0.45	0.45-0.60	0.60-0.75	0.75-0.85	0.85-1.00
V_4	0-0.35	0.35-0.45	0.45-0.70	0.70-0.90	0.90-1.00

或小于 0.758 时，车辆智能网联系统处于轻微严重风险状态，此时车辆处于危急状态。此时，应根据第一阶段的脆弱组件进行具体分析，例如，如果第一阶段影响因素中的 ECU 耦合风险处于严重等级，则应对车辆 ECU 系统进行整改，直至 ECU 耦合风险达到正常或轻微等级，且 VSR 小于 0.506，此时车辆智能网联系统处于正常或轻微风险等级；当 VSR 大于或等于 0 且小于 0.506 时，车辆智能网联系统处于正常或轻微风险状态。此时，车辆处于稳态，表明车辆智能网联系统已达到质量管理水平 [2], , 无需对车辆智能网联系统进行整改。

表 X：VCCR 影响因素评价标准

VCCR	正常	轻微	较严重	严重	极其严重
C_1	0-0.40	0.40-0.60	0.60-0.80	0.80-0.90	0.90-1.00
C_2	0-0.20	0.20-0.45	0.45-0.70	0.70-0.85	0.85-1.00
C_3	0-0.15	0.15-0.40	0.40-0.65	0.65-0.80	0.80-1.00

表 XI：VHIR 影响因素评价标准

VHIR	正常	轻微	较严重	严重	极其严重
H_1	0-0.20	0.20-0.50	0.50-0.70	0.70-0.90	0.90-1.00
H_2	0-0.40	0.40-0.55	0.55-0.75	0.75-0.85	0.85-1.00
H_3	0-0.30	0.30-0.45	0.45–0.70	0.70-0.80	0.80-1.00

C. 评估结果分析

OpenPilot平台上的车辆智能网联系统安全性随后受到本节第3节中所提出指标的影响。

*1) OpenPilot*平台实验：通过查看自动驾驶系统接收的 CAN 消息类型，我们能够根据公式 (1) 确定车辆的 ECU耦合风险信息。由于车辆的自动驾驶功能仅使用两种通信方式——用于接收附近车辆位置信息的车辆到车辆通信，以及用于连接传感器、雷达和电子控制单元的车内通信，因此我们只能使用公式 (2) (3) (4) (5) 估算车辆智能网联系统的通信风险。随后，使用公式 (6)、(7) 和 (8) 确定车辆智能网联系统的源代码行数（LOCM）、运算符和操作数（HCM）以及圈复杂度（CCM），进而确定车辆的代码复杂度风险。公式 (9)、(10) 和 (11) 用于计算车辆的功能安全历史风险、预期功能安全风险以及信息

表 XII：车辆一阶影响因素的评价标准

Rask 评级	正常	轻微	较严重	严重	极其严重
ECR_{nor}	0-0.2258343	0.2258343-0.3484771	0.3484771-0.4962365	0.4962365-0.6103646	0.6103646-1.0
VCR_{nor}	0-0.3061854	0.3061854-0.4197778	0.4197778-0.6037095	0.6037095-0.7585744	0.7585744-1.0
$VCCR_{nor}$	0-0.1842563	0.1842563-0.4115634	0.4115634-0.6388705	0.6388705-0.7729456	0.7729456-1.0
$VHIR_{nor}$	0-0.2476042	0.2476042-0.4531207	0.4531207-0.6511356	0.6511356-0.7881466	0.7881466-1.0

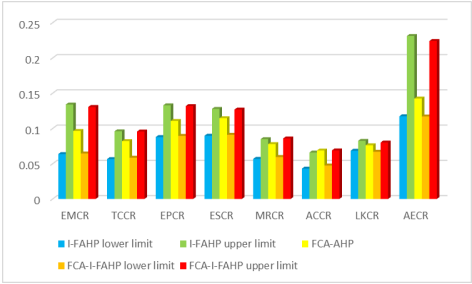


图4：OpenPilot 的 ECR 风险评估值对比

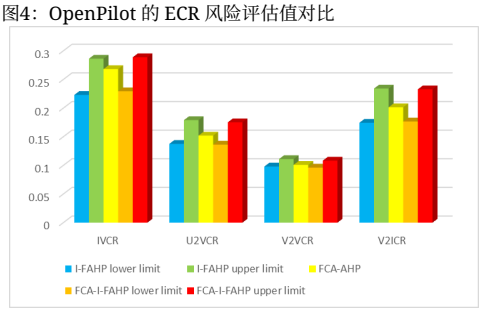


图5：OpenPilot 的 VCR 风险评估值对比

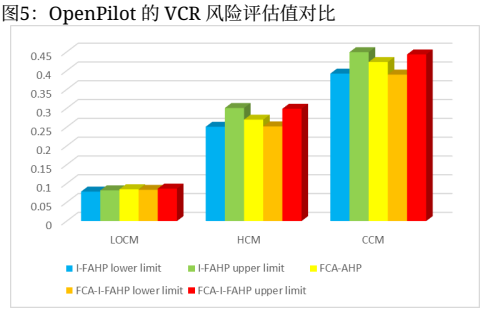


图6：OpenPilot 的 VCCR 风险评估值对比

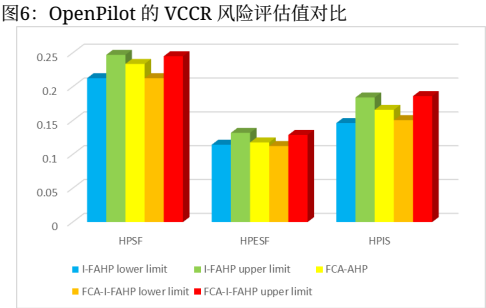


图7：OpenPilot 的 VHIR 风险评估值比较

安保。然后使用这些信息来确定车辆安全的历史风险。

然后，通过上述公式计算得到的车辆影响指数数据，为了更便捷、准确地评估车辆智能网联系统的风险，我们使用公式（14）对上述数据进行归一化，从而得到表 XIV。

然后，基于各种车辆智能联网系统的风险指标数据，-

根据上文表 XIV 所列 OpenPilot 平台上智能网联系统的各项指标，结合本文给出的目标函数公式（13），我们可以计算出 OpenPilot 系统的风险评估值为 [0.514567,0.911115]，，该值恰好属于所定义的安全风险评估区间中的严重风险等级。这也与公开的 OpenPilot 系统 ASIL 等级 D=S3 + E4 + C3 相符，其中 D 级是 ISO 26262 标准中风险等级的最高级别，这与本文的评估结果一致，也证明了我们的评估结果是可靠的。

其中，图4、5、6和7展示了使用 I-FAHP 和 FCA-I-FAHP 得到的修正权重，以及车辆智能网联系统的电子控制单元耦合风险、通信风险、代码复杂度风险、车辆历史安全事件风险和车辆综合风险。根据上述内容，我们还可以从各图中看出，FCA-I-FAHP方法和 I-FAHP方法对车辆智能网联系统进行风险评估所得的结果具有可比性。然而，通过比较采用层次分析法和 FCA-I-FAHP 方法的模型结果可以发现，FCA-I-FAHP方法能够更精确、全面地确定车辆智能网联系统当前的风险等级。可以对 I-FAHP 和 FCA-I-FAHP 方法的结果进行比较，这种比较还可以表明，I-FAHP 和 FCA方法可用于确定风险等级较高的车辆智能网联系统的风险等级。

如图4、5、6所示，采用上述 FCA-I-FAHP 方法进行评估后，车辆的 ECU耦合风险、通信风险和代码复杂度风险均处于严重程度等级；而图7中的结果表明，车辆历史安全事件的风险等级为轻微风险。实验结果对比证实，车辆的 ECU耦合风险、通信风险和代码复杂度风险会加剧 OpenPilot 车辆智能网联系统的风险。

*2）OpenPilot*平台的改进：通过上述模型方法的计算，我们可以判定 OpenPilot 系统处于风险状态，因此需要对 OpenPilot 系统进行改进，直至其达到稳态。

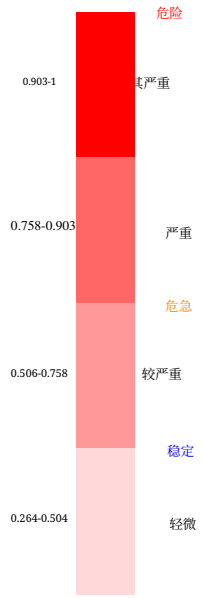
因此，为了评估我们通过改进模型方法提高系统安全性的效果，我们比较了 OpenPilot 系统过去各文件中发现的安全漏洞数量。截至2022年12月，OpenPilot平台共有1684个文件，其中175个为错误文件。在审查已报告的缺陷后，我们将其中64个文件与上述已修复问题对应的系统文件关联起来。

表 XIII：车辆智能网联系统风险评估矩阵

ECR	VHIR \ VCCR	VCR 0-0.306					VCR 0.306-0.42					VCR 0.42-0.604		
		0-0.184	0.184-0.412	0.412-0.639	0.639-0.773	0.773-1	0-0.184	0.184-0.412	0.412-0.639	0.639-0.773	0.773-1	0-0.184	0.184-0.412	0.412-0.639
0-0.226	0 – 0.248	[0,0.277]	[0.277,0.307]	[0.307,0.335]	[0.335,0.355]	[0.335,0.385]	[0.085,0.323]	[0.323,0.352]	[0.352,0.381]	[0.381,0.4]	[0.4,0.431]	[0.117,0.397]	[0.397,0.426]	[0.426,0.455]
	0.248 – 0.453	[0.028,0.277]	[0.277,0.35]	[0.35,0.379]	[0.379,0.398]	[0.398,0.429]	[0.113,0.366]	[0.366,0.396]	[0.396,0.424]	[0.424,0.444]	[0.444,0.474]	[0.145,0.44]	[0.44,0.47]	[0.47,0.498]
	0.453 – 0.651	[0.067,0.364]	[0.364,0.394]	[0.394,0.422]	[0.422,0.442]	[0.442,0.472]	[0.148,0.41]	[0.41,0.439]	[0.439,0.468]	[0.468,0.487]	[0.487,0.518]	[0.179,0.483]	[0.483,0.513]	[0.513,0.541]
	0.651 – 0.788	[0.096,0.39]	[0.39,0.419]	[0.419,0.448]	[0.448,0.467]	[0.467,0.498]	[0.183,0.435]	[0.435,0.465]	[0.465,0.493]	[0.493,0.513]	[0.513,0.543]	[0.214,0.509]	[0.509,0.539]	[0.539,0.567]
	0.788 – 1	[0.118,0.433]	[0.433,0.463]	[0.463,0.491]	[0.491,0.511]	[0.511,0.541]	[0.203,0.479]	[0.479,0.508]	[0.508,0.537]	[0.537,0.556]	[0.556,0.587]	[0.235,0.553]	[0.553,0.582]	[0.582,0.61]
0.226-0.348	0 – 0.248	[0.067,0.323]	[0.323,0.352]	[0.352,0.381]	[0.381,0.4]	[0.4,0.431]	[0.152,0.368]	[0.368,0.398]	[0.398,0.426]	[0.426,0.446]	[0.446,0.476]	[0.183,0.442]	[0.442,0.472]	[0.472,0.5]
	0.248 – 0.453	[0.095,0.366]	[0.366,0.396]	[0.396,0.424]	[0.424,0.444]	[0.444,0.474]	[0.18,0.412]	[0.412,0.441]	[0.441,0.47]	[0.47,0.489]	[0.489,0.52]	[0.211,0.485]	[0.485,0.515]	[0.515,0.543]
	0.453 – 0.651	[0.129,0.409]	[0.409,0.439]	[0.439,0.467]	[0.467,0.487]	[0.487,0.517]	[0.215,0.455]	[0.455,0.485]	[0.485,0.513]	[0.513,0.533]	[0.533,0.563]	[0.243,0.529]	[0.529,0.558]	[0.558,0.587]
	0.651 – 0.788	[0.164,0.435]	[0.435,0.465]	[0.465,0.493]	[0.493,0.513]	[0.513,0.539]	[0.249,0.481]	[0.481,0.51]	[0.51,0.539]	[0.539,0.558]	[0.558,0.589]	[0.281,0.555]		
	0.788 – 1	[0.185,0.479]	[0.479,0.508]	[0.508,0.536]	[0.536,0.556]	[0.556,0.586]	[0.27,0.524]	[0.524,0.554]	[0.554,0.582]	[0.582,0.602]	[0.602,0.632]			
0.348-0.496	0 – 0.248	[0.103,0.377]	[0.377,0.407]	[0.407,0.435]	[0.435,0.455]	[0.455,0.485]	[0.188,0.423]	[0.423,0.452]	[0.452,0.481]	[0.481,0.5]	[0.5,0.531]	[0.219,0.497]		
	0.248 – 0.453	[0.131,0.421]	[0.421,0.45]	[0.45,0.479]	[0.479,0.498]	[0.498,0.529]	[0.216,0.466]	[0.466,0.496]	[0.496,0.524]				[0.54,0.57]	[0.57,0.598]
	0.453 – 0.651	[0.166,0.464]	[0.464,0.494]	[0.494,0.522]	[0.522,0.542]	[0.542,0.572]	[0.251,0.51]	[0.51,0.539]						
	0.651 – 0.788	[0.2,0.49]	[0.49,0.519]	[0.519,0.548]	[0.548,0.567]	[0.567,0.598]	[0.285,0.535]							
	0.788 – 1	[0.221,0.533]	[0.533,0.563]	[0.563,0.591]	[0.591,0.611]	[0.611,0.641]								
0.496-0.61	0 – 0.248	[0.146,0.42]	<escape>[0.42,0.449]	[0.449,0.477]	[0.477,0.									
	0.248 – 0.453	[0.174,0.463]	[0.463,0.493]	[0.493,0.521]	[0.521,0.541]	[0.541,0.571]	[0.26,0.509]	[0.509,0.538]	[0.538,0.567]	[0.567,0.586]	[0.586,0.617]	[0.291,0.582]	[0.582,0.612]	[0.612,0.64]
	0.453 – 0.651	[0.209,0.506]	[0.506,0.536]	[0.536,0.564]	[0.564,0.584]	[0.584,0.614]	[0.294,0.552]	[0.552,0.582]	[0.582,0.61]	[0.61,0.62]	[0.62,0.66]	[0.326,0.626]	[0.626,0.655]	[0.655,0.684]
	0.651 – 0.788	[0.244,0.532]	[0.532,0.562]	[0.562,0.59]	[0.59,0.61]	[0.61,0.64]	[0.329,0.578]	[0.578,0.607]	[0.607,0.636]	[0.636,0.655]	[0.655,0.686]	[0.361,0.651]	[0.651,0.681]	[0.681,0.709]
	0.788 – 1	[0.264,0.575]	[0.575,0.605]	[0.605,0.633]	[0.623,0.653]	[0.653,0.683]	[0.349,0.621]	[0.621,0.651]	[0.651,0.679]	[0.679,0.699]	[0.699,0.729]	[0.381,0.695]	[0.695,0.724]	[0.724,0.753]
0.61-1.0	0 – 0.248	[0.18,0.564]	[0.564,0.593]	[0.5930.622]	[0.622,0.641]	[0.641,0.672]	[0.265,0.609]	[0.609,0.639]	[0.639,0.667]	[0.667,0.687]	[0.687,0.717]	[0.297,0.683]	[0.683,0.713]	[0.713,0.741]
	0.248 – 0.453	[0.208,0.607]	[0.607,0.637]	[0.637,0.665]	[0.665,0.685]	[0.685,0.715]	[0.293,0.653]	[0.653,0.682]	[0.682,0.711]	[0.711,0.73]	[0.73,0.761]	[0.325,0.727]	[0.727,0.756]	[0.756,0.785]
	0.453 – 0.651	[0.243,0.651]		[0.68,0.709]	[0.709,0.728]	[0.728,0.759]	[0.328,0.696]	[0.696,0.726]	[0.726,0.754]	[0.754,0.774]	[0.774,0.804]	[0.359,0.44]	[0.44,0.8]	[0.8,0.828]
	0.651 – 0.788	[0.278,0.676]	[0.676,0.706]	[0.706,0.734]	[0.734,0.754]	[0.754,0.784]	[0.363,0.722]	[0.722,0.751]	[0.751,0.78]	[0.78,0.799]	[0.799,0.83]			
	0.788 – 1	<escape>[0.2												

接续上表

ECR	VHIR \ VCCR	VCR 0.42-0.604		VCR 0.604-0.759					VCR 0.759-1.0					
		0.639-0.773	0.773-1	0-0.184	0.184-0.412	0.412-0.639	0.639-0.773	0.773-1	0-0.184	0.184-0.412	0.412-0.639	0.639-0.773	0.773-1	
0-0.226	0 – 0.248	[0.455,0.474]	[0.474,0.505]	[0.168,0.459]	[0.459,0.488]	[0.488,0.517]	[0.517,0.536]	[0.536,0.567]	[0.211,0.556]	[0.556,0.585]	[0.585,0.614]	[0.614.0.633]	[0.633,0.664]	
	0.248 – 0.453	[0.498,0.518]	[0.518,0.548]	[0.196,0.502]	[0.502,0.532]	[0.532,0.56]	[0.56,0.58]	[0.58,0.61]	[0.239,0.599]					
	0.453 – 0.651	[0.541,0.561]	[0.561,0.591]	[0.23,0.546]	[0.546,0.575]	[0.575,0.604]	[0.604,0.623]	[0.623,0.654]	[0.274,0.643]	[0.643,0.672]	[0.672,0.7]	[0.7,0.72]	[0.72,0.75]	
	0.651 – 0.788	[0.567,0.587]	[0.587,0.617]	[0.265,0.571]	[0.571,0.601]	[0.601,0.629]	[0.629,0.649]	[0.649,0.679]	[0.308,0.668]	[0.668,0.698]	[0.698,0.726]	[0.726,0.746]	[0.746,0.776]	
	0.788 – 1	[0.61,0.63]	[0.63,0.66]	[0.286,0.615]	[0.615,0.644]	[0.644,0.673]	[0.673,0.692]	[0.692,0.723]	[0.329,0.712]	[0.712,0.741]	[0.741,0.769]	[0.769,0.789]	[0.789,0.82]	
0.226-0.348	0 – 0.248	[0.5,0.52]	[0.52,0.55]	[0.234,0.504]	[0.504,0.534]	[0.534,0.562]	[0.562,0.582]	[0.582,0.612]	[0.277,0.601]	[0.601,0.631]	[0.631,0.659]	[0.659,0.679]	[0.679,0.709]	
	0.248 – 0.453	[0.543,0.563]	[0.563,0.593]	[0.262,0.548]	[0.548,0.577]	[0.577,0.606]	[0.606,0.625]	[0.625,0.656]	[0.305,0.644]	[0.644,0.674]	[0.674,0.702]	[0.702,0.722]	[0.722,0.752]	
	0.453 – 0.651	[0.587,0.606]	[0.606,0.637]	[0.297,0.591]	[0.591,0.621]	[0.621,0.649]	[0.649,0.669]	[0.669,0.699]	[0.34,0.688]	[0.688,0.717]	[0.717,0.746]	[0.746,0.765]	[0.765,0.796]	
	0.651 – 0.788	[0.612,0.632]	[0.632,0.662]	[0.332,0.617]	[0.617,0.646]	[0.646,0.675]	[0.675,0.694]	[0.694,0.725]	[0.375,0.714]	[0.714,0.743]	[0.743,0.771]	[0.771,0.791]	[0.791,0.822]	
	0.788 – 1	[0.656,0.675]		[0.66,0.69]	[0.69,0.718]	[0.718,0.738]	[0.738,0.768]		[0.395,0.757]	[0.757,0.786]	[0.786,0.815]	[0.815,0.835]	[0.835,0.865]	
0.348-0.496	0 – 0.248	[0.555,0.574]		[0.27,0.559]	[0.559,0.588]	[0.588,0.617]	[0.617,0.636]	[0.636,0.667]	[0.313,0.656]	[0.656,0.685]	[0.685,0.714]	[0.714,0.733]	[0.733,0.764]	
	0.248 – 0.453	[0.598,0.618]	[0.618,0.648]	[0.299,0.602]	[0.602,0.632]	[0.632,0.66]	[0.66,0.68]	[0.68,0.71]	[0.342,0.699]					
	0.453 – 0.651	[0.642,0.661]	[0.661,0.692]	[0.333,0.646]	[0.646,0.675]	[0.675,0.704]	[0.704,0.723]	[0.723,0.754]	[0.376,0.743]	[0.743,0.772]	[0.772,0.801]	[0.801,0.82]	[0.82,0.851]	
	0.651 – 0.788	[0.667,0.687]	[0.687,0.717]	[0.368,0.671]	[0.671,0.701]	[0.7010.729]	[0.729,0.749]	[0.749,0.779]	[0.411,0.768]	[0.768,0.798]	[0.789,0.826]	[0.826,0.846]	[0.846,0.876]	
	0.788 – 1	[0.711,0.73]	[0.73,0.761]	[0.389,0.715]	[0.715,0.744]	[0.744,0.773]	[0.773,0.792]	[0.792,0.823]	[0.432,0.812]	[0.812,0.841]	[0.841,0.87]	[0.87,0.889]		
0.496-0.61	0 – 0.248	[0.597,0.617]	[0.617,0.647]	[0.314,0.601]	[0.601,0.63]1	[0.63,0.659]	[0.659,0.679]	[0.679,0.709]	[0.357,0.698]	[0.698,0.727]	[0.727,0.756]	[0.756,0.776]	[0.766,0.806]	
	0.248 – 0.453	[0.64,0.66]	[0.66,0.69]	[0.342,0.645]	[0.645,0.674]	[0.674,0.702]	[0.702,0.722]	[0.722,0.753]	[0.382,0.741]	[0.941,0.771]	[0.771,0.799]	[0.799,0.819]	[0.819,0.849]	
	0.453 – 0.651	[0.684,0.703]	[0.703,0.734]	[0.377,0.688]	[0.688,0.717]	[0.717,0.746]	[0.746,0.766]	[0.766,0.796]	[0.42,0.785]	[0.785,0.814]	[0.814,0.843]	[0.843,0.862]	[0.862,0.893]	
	0.651 – 0.788	[0.709,0.729]	[0.729,0.759]	[0.412,0.714]	[0.714,0.743]	[0.743,0.772]	[0.772,0.791]	[0.791,0.822]	[0.455,0.81]	[0.81,0.84]	[0.84,0.868]			
	0.788 – 1	[0.753,0.772]	[0.772,0.803]	[0.432,0.757]	[0.757,0.786]	[0.786,0.815]	[0.815,0.835]	[0.835,0.865]	[0.475,0.854]	[0.854,0.883]	[0.883,0.912]	[0.912,0.931]	[0.931,0.962]	
0.61-1.0	0 – 0.248	<escape>[0</escape></escape>.803,0.<esc									[0.872,0.9]	[0.90.92]	[0.92,0.95]	
	0.248 – 0.453	[0.785,0.804]	[0.804,0.835]	[0.376,0.789]	[0.789,0.818]	[0.818,0.847]	[0.847,0.866]	[0.866,0.897]	[0.419,0.886]	[0.886,0.915]	[0.915,0.944]	[0.944,0.963]	[0.963,0.994]	
	0.453 – 0.651	[0.828,0.848]	[0.848,0.878]	[0.411,0.832]	[0.832,0.862]	[0.862,0.89]	[0.89,0.91]	[0.91,0.94]	[0.454,0.93]	[0.93,0.959]		1	1	
	0.651 – 0.788	[0.854,0.873]	[0.873,0.904]	[0.445,0.858]	[0.858,0.887]	[0.887,0.916]	[0.916,0.935]	[0.935,0.966]	[0.488,0.955]	[0.955,0.984]	[0.984,1]	1	1	
	0.788 – 1	[0.897, 0.912]						[0.979.1]	[0.509,0.998]	[0.998,1]	1	1	1	



表XIV：OpenPilot 系统风险影响因素的数据分析

系统风险因素	风险评估值	风险评估计算详情
ECU耦合风险 (ECR)	ECR(OpenPilot)=[0.57293920,0.94365520]	OpenPilot 控制着车辆的主要部件，包括 ECM[1]，BCM[2]，SSM[3]，SCU[4]，PCM[5]，TCM[6]，TCU[7]，EPS[8]
车辆通信 风险（VCR）	VCR(OpenPilot)=[0.63848454,0.80522362]	OpenPilot 系统控制车辆的通信模块，包括车内、用户到车辆、车辆到车辆和车辆到基础设施通信。
车辆代码复杂度 风险（VCCR）	VCCR（OpenPilot）=[0.72454854,0.82819294]	OpenPilot 共包含 1684 个文件，其中有 234464 行代码，31925 行空白行和 34723 行注释
车辆历史风险 安全问题(VHIR)	VHIR(OpenPilot)=[0.47562178,0.56006950]	OpenPilot自2018年以来报告了175个缺陷（2018年13个、2019年51个、2020年61个、2021年31个，以及2022年19个）

[1]发动机控制模块，[2]制动控制模块，[3]安全系统模块，[4]座椅控制单元，[5]动力总成控制模块 [6]变速器控制模块，[7]远程信息处理控制单元，[8]电动助力转向控制模块

然后，使用上述车辆智能网联系统风险评估模型，与AVSDA[4] 漏洞测量工具、代码复杂度与损失测量工具[29]以及编码复杂度、代码耦合度与内聚度测量工具[25]，通过二分类方法，识别实验中的真正例(TP)、假正例(FP)、真负例(TN)和假负例(FN)文件，并测量每个模型的准确率、精确率和召回率。

上述结果如表 XV 所示。通过该表可以看出，所提出的 VSRQ 模型在准确率、精确率和召回率方面均优于其他方法。其中，我们提出的模型召回率为 73.43%，表明它能够快速定位车辆智能网联系统中的风险文件。我们提出的 VSRQ 模型准确率也高达 94.36%，这表明车辆系统识别和风险评估都相当可靠。由于模型采用了更全面的两阶段指标评估，VSRQ 模型在精确率方面也优于其他几种方法，精确率达到 37.60%。

最后，为进一步考察 VSRQ 的性能，我们还研究了平均指标比率与文件中记录的错误数量之间的关系，如图 8 所示。例如，VSRQ 将一个报告了 8 个漏洞的文件归为风险等级极高，并为其分配比率 1。如图 8 所示，VSRQ 确定的风险评级系数 VSR 与 OpenPilot 系统中错误文件里的缺陷数量有关；VSR 风险系数的值越大，缺陷文件中的缺陷就越多。与其他三组相比，可以看出，AVSDA[4] 模型的识别准确率不足，且未进行区间化；另外两组指标的[29],[25] 值则是随机选取的。

*3）VSRQ*模型方法的性能比较：随后，我们从分析过程和分析结果两个方面，将其与另外三种方法进行了比较，包括AVSDA[4],代码复杂度与代码变更测量工具 [29]，以及编码复杂度、代码耦合度与内聚度测量工具[25]。

根据实验过程分析，我们可以

表 XV：VSRQ 与其他模型的比较

	VSRQ	*AVSDA[4]*	*CCL[a] [29]*	*CCC[b][25]*
TN	1542	1517	1528	1483
TP	47	41	35	26
FN	17	23	29	38
FP	78	103	92	137
准确率	94.36%	92.52%	92.81%	89.61%
精确率	37.60%	28.47%	27.56%	15.95%
召回率	73.43%	64.06%	54.69%	40.63%

a 代码复杂度和损失测量 *b* 编码复杂度、代码耦合度和内聚性测量

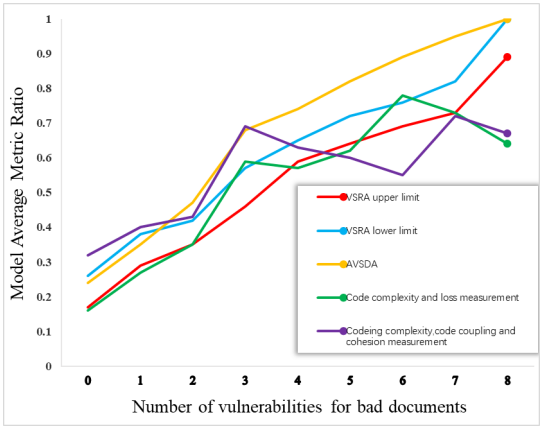


图 8：各风险评估模型的指标比率

由此可以推断，AVSDA 的 [4] 主要指标过于简单，且指标权重的设定过于随意，这往往导致无法识别漏洞。相比之下，代码复杂度与损失测量工具[29]以及代码复杂度、代码耦合度和内聚度测量工具 [25]仅分别对车辆智能网联系统的代码复杂度进行考察。而本文提出的 VSRQ 不仅考虑了对车辆系统构成风险的多指标影响因素，还引入了 FCA 方法来考察车辆系统影响因素与 ISO 26262 [14]评价标准之间的关系，但其考量方式极为简单，缺乏分析的合理性。FCA-I-FAHP 方法可用于

识别更高风险的车辆软件集成系统风险等级，并降低层次分析法的主观性。

我们比较了上述四种方法针对实验结果得出的风险分析结果。从表XIV和图 8可以推断，所提出的 VSRQ 模型在准确率、精确率和召回率方面优于其他方法。

VI. 结论

在本研究中，我们提出了一种用于定量评估车辆智能网联系统安保风险的方法，称为车辆智能网联系统风险评估（VSRQ）。VSRQ方法分为两个阶段。在分析车辆易受攻击部件的阶段，我们采用ECU耦合、通信风险、代码复杂度风险和车辆历史安全事件风险等风险评估类别，为其子影响因素建立安全度量方程。我们采用区间FAHP方法进行风险评估，根据易受攻击车辆部件的相对重要性及其对车辆损害的严重程度进行加权。随后，我们利用方程VSR对软件集成车辆系统中安全问题发生的可能性进行加权。我们构建了车辆软件系统安全风险矩阵集成模型，如图XIII所示。

然后，我们确定了车辆智能网联系统的三种状态——稳定、危急和危险，并针对每种状态提出了相应的安全纠正措施。研究结果表明，该评估方法能够以 94.36% 的准确率和 73.43% 的召回率识别漏洞。我们迫切希望研究更多情况，并在不同平台上尝试使用 VSRQ。此外，我们的车辆智能网联解决方案可用于评估特定车辆部件（如发动机系统）相关的风险。

参考文献

[1] O. Henniger，“Evita：具备入侵防护功能的汽车电子安全应用”，技术报告，*EVITA*，2011年。[2] Q. Hommes 和 V. Eikema，“ISO 26262《道路车辆—功能安全》草案的审查与评估”，SAE技术论文，技术报告，2012年。[3] M. M. Islam、A. Lautenbach、C. Sandberg 和 T. Olovsson，“汽车嵌入式系统的风险评估框架”，载于第*2*届*ACM*网络物理系统安全国际研讨会（*CPSS-2016*）论文集，2016年，第3–14页。[4] L. Moukahal、M. Zulkernine 和 M. Soukup，“AVSDA：自动驾驶汽车安全衰减评估”，载于第*17*届互联网与系统风险和安全国际会议（*CRiSIS-2022*）论文集。施普林格，2022年，第20–37页。[5] Z. Ying、M. Ma、Z. Zhao、X. Liu 和 J. Ma，“机会式自动驾驶汽车车队的基于信誉的领导者选举方案”，*IEEE*车辆技术汇刊，第71卷，3532，2021年4，3519号，第–页。[6] X. Feng、Q. Shi、Q. Xie 和 L. Wang，“P2BA：一种针对车载自组织网络中半可信路侧单元的隐私保护批量认证协议”，*IEEE*信息取证与安全汇刊，第16卷，第3888–3899页，2021年。[7] J. Guo、X. Li、Z. Liu、J. Ma、C. Yang、J. Zhang 和 D. Wu，“TROVE：一种利用强化学习的车载自组织网络情境感知信任模型”，*IEEE*物联网期刊，第7卷，第7期，第6647–6662页，2020年。[8] C. Gao、G. Wang、W. Shi、Z. Wang 和 Y. Chen，“自动驾驶安全：最新进展与挑战”，*IEEE*物联网期刊，第9卷，第10期，第7572–7595页，2021年。[9] G. D. L. Torre、P. Rad 和 K.-K. R. Choo，“无人驾驶汽车安保：挑战与未来研究机遇”，未来一代计算机系统，第108卷，第1092–1111页，2020年。[10] D. Zelle、C. Plappert、R. Rieke、D. Scheuermann 和 C. Krauß，“Threat-surf：一种用于汽车网络安全工程的自动化威胁面评估方法”，《微处理器与微系统》，第90卷，页码104461，2022年。[11] A. Behfarnia 和 A. Eslami，“使用贝叶斯防御图对自动驾驶汽车进行风险评估”，载于第88届IEEE车辆技术会议（VTC-Fall）论文集。IEEE，2018年，第1–5页。[12] J. Cui、L. Wei、H. Zhong、J. Zhang、Y. Xu 和 L. Liu，“车载自组织网络中的边缘计算：一种高效且保护隐私的协同下载方案”，IEEE通信领域精选期刊，第38卷，第6期，第1191–1204页，2020年。[13] Q. Kong、R. Lu、F. Yin 和 S. Cui，“基于区块链的车联网物联网中出行即服务隐私保护驾驶员监控”，IEEE车辆技术汇刊，第70卷，2021年4月，页码3799，第3788–页。[14] R. Palin、D. Ward、I. Habli 和 R. Rivett，“ISO 26262安全论证：合规性与保证”，载于第6届IET国际系统安全会议（IET ICSS-2011）论文集。IET，2011年。[15] G. Macher、C. Schmittner、O. Veledar 和 E. Brenner，“ISO/SAE DIS 21434汽车网络安全标准概述”，第12235卷，第123–135页，2020年。[16] D. K. Nilsson、P. H. Phung 和 U. E. Larson，“基于安全与网络安全特性的车辆电子控制单元分类”，载于《道路运输信息与控制—RTIC 2008及英国智能交通系统协会会员会议》，IET，2008年。[17] S. J. V. C. S. E. 委员会等，“信息物理车辆系统网络安全指南”，SAE国际，2016年。[18] S. Burton、J. Likkei、P. Vembar 和 M. Wolf，“汽车功能安全= 安全+ 网络安全”，载于第1届物联网安全国际会议（SECURIT-2012）论文集。ACM，2012年，第150–159页。[19] A. Bertolino、A. Calabro、D. F. Giandomenico、G. Lami、F. Lonetti、E. Marchetti、F. Martinelli、I. Matteucci 和 P. Mori，“网联汽车安全软件工程解决方案综述”，《软件质量期刊》，第26卷，第4期，第1223–1256页，2018年。[20] G. A. F. III，“汽车安全度量指标”，载于《安全、网络与物联网进展》。施普林格，2021年，第341–353页。[21] M. A. Razzaque、S. M. Cheraghi 等，“车载自组织网络中的安全与隐私：综述及未来方向”，载于《无线网络与安全》。施普林格，2013年，第107–132页。[22] A. Demba 和 D. P. M¨oller，“车车通信技术”，载于第18届IEEE电气与信息技术国际会议（EIT-2018）论文集。IEEE，2018年，第0459–0464页。[23] A. Zaabi、Y. Y. Chan 和 E. Damiani，“自动驾驶汽车安全：概念模型”，载于IEEE亚太交通电气化会议暨博览会（ITEC亚太-2019）论文集。IEEE，2019年。[24] Y. Shin、A. Meneely、L. Williams 和 J. A. Osborne，“评估复杂度、代码变更量和开发者活动度量指标作为软件漏洞的指示因素”，IEEE软件工程汇刊，第37卷，第6期，第772–787页，2011年。[25] I. Chowdhury 和 M. Zulkernine，“将复杂度、耦合度和内聚度指标用作漏洞的早期指示因素”，《系统架构期刊》，第57卷，第3期，第294–313页，2011年。[26] A. Boudguiga、A. Boulanger、P. Chiron、W. Klaudel、H. Labiod 和 J.-C. Seguy，“RACE：协同引擎风险分析”，载于第7届新技术、移动性与安全国际会议（NTMS-2015）论文集。IEEE，2015年，第1–5页。[27] J. Cui 和 B. Zhang，“VERA：一种适用于自动驾驶汽车的简化安全风险分析方法”，IEEE车辆技术汇刊，第69卷，第10期，第10 494–10 505页，2020年。[28] F. Fontana，“自动驾驶汽车与OpenPilot：框架完整概述”，2021年。[29] Y. Shin、A. Meneely、L. Williams 和 J. A. Osborne，“评估复杂度、代码变更量和开发者活动度量指标作为软件漏洞的指示因素”，IEEE软件工程汇刊，第37卷，第6期，第772–787页，2010年。