智能汽车系统功能安全保障机制的现状与展望

罗通强，刘坚坚，赵炳根，邱旭波，李仰光，吕 晨

（比亚迪汽车工业有限公司，广东，深圳 518118）

摘 要：随着高阶智能网联汽车的快速发展，其安全性引发了广泛关注，现阶段功能安全保障机制是国内外的研究热点。各国针对车辆安全性能逐步制定了相应的标准，国际标准化组织也不断完善功能安全（ISO 26262）和预期功能安全（ISO 21448）标准。因此，大多数汽车产品的安全目标，尤其是与自动驾驶相关的智能底盘系统（线控制动与线控转向执行机构）都可归类为汽车安全完整性等级中的D级别。基于行业研究资料总结了系统安全架构冗余机制，分析和梳理了不同自动驾驶等级的故障运行安全架构以及功能安全降级策略，展望了将ISO 21448引入ISO 26262标准的融合思路，以有效避免因车辆的E/E系统错误和执行器性能不足而引发的事故，为车辆安全行驶提供保障。

关键词：智能汽车；功能安全；冗余机制；域控制器

中图分类号：U461.91 **文献标志码：**A **DOI：**10.3969/j.issn.2095–1469.2024.06.01

Current Status and Future Outlook of System Functional Safety Mechanisms in Intelligent Vehicles

LUO Tongqiang，LIU Jianjian，ZHAO Binggen，QIU Xubo，LI Yangguang，LYU Chen

（BYD Auto Industry Company Limited，Shenzhen 518118，Guangdong，China）

Abstract: With the rapid development of advanced intelligent connected vehicles, their safety has become a widespread concern. Currently, the mechanisms to ensure functional safety are a major research focus both domestically and internationally. Countries are gradually establishing standards for vehicle safety performance, and the International Organization for Standardization (ISO) continues to refine the Functional Safety (ISO 26262) and Safety of the Intended Functionality (ISO 21448) standards. On this basis, the safety objectives of most automotive products, especially intelligent chassis systems related to autonomous driving, such as brake-by-wire and steer-by-wire actuators, are classified under Automotive Safety Integrity Level D (ASIL D). This paper summarizes industry research on redundancy mechanisms in system safety architecture, analyzes and organizes fail-operational safety architecture across different levels of autonomous driving, and examines functional safety degradation strategies. Finally it discusses the potential for integrating ISO 21448 into the ISO 26262 standard to effectively prevent accidents due to errors in the vehicle's Electronic/Electrical (E/E) systems and insufficient actuator performance, thereby providing stronger assurance for safe vehicle operation.

Keywords: intelligent vehicles; functional safety; redundancy; domain control unit

收稿日期：2024–10–14 **改稿日期：**2024–10–28

基金项目：国家重点研发计划项目（2023YFB2504500）

参考文献引用格式：

罗通强，刘坚坚，赵炳根，等.智能汽车系统功能安全保障机制的现状与展望[J].汽车工程学报，2024，14(6)：921–933.

LUO Tongqiang，LIU Jianjian，ZHAO Binggen，et al.Current Status and Future Outlook of System Functional Safety Mechanisms in Intelligent Vehicles[J].Chinese Journal of Automotive Engineering，2024，14(6)：921–933.(in Chinese)

近年来，智能网联汽车（Intelligent Connected Vehicles，ICVs）尤其是高级驾驶辅助系统（Advanced Driver Assistance Systems，ADAS）和全自动驾驶（Advanced Driving，AD）技术的革新，显著提升了行驶安全性。其中，智能汽车域控制器作为核心技术架构之一，发展迅猛，行业竞相加大研发投入[1-3]，以期在激烈的市场竞争中抢占技术创新高地。然而，随着全自动驾驶技术的推进，伴随而来的是新的安全考量。为了解决这一问题，中国、美国、欧洲等国家和地区的NCAP（New Car Assessment Program）都针对新车安全性能逐步制定了相应的测试规范[4-6]，国际标准化组织也不断完善功能安全（ISO 26262）和预期功能安全（ISO 21448）标准。

功能安全ISO 26262描述了由E/E故障和车辆中的随机硬件失效导致的危害[7]；预期功能安全ISO 21448描述了由于系统功能不足或人员误用导致的危害[8]。这意味着在故障发生时，系统可以主动关闭从而达到失效安全（Fail-Safe），或者以降级模式来运行达到失效运行（Fail-Operational）。

自动驾驶汽车控制器的复杂性体现在汽车和ADAS/AD系统的电气化[9]。随着电气化程度的提高，系统所需要的安全技术水平也随之提高。ASIL（Automotive Safety Integrity Level）等级的定义是为了对失效后带来的风险进行评估和量化以达到安全目标，ASIL分为QM、A、B、C、D五个等级，其中，ASIL D是最高的汽车安全完整性等级，对功能安全的要求最高，ISO 26262中也证实了将分解方法应用于安全关键系统的可实施性。适当的功能安全分解具有将顶级安全要求的ASIL等级降低为冗余安全要求的优点，该分解方法能减轻开发人员负担。但使用ASIL分解需要冗余安全要求具备独立性，因此，这些安全要求必须分配给足够独立的架构元素。为了应用安全目标分解策略，ISO 26262要求执行相关失效分析（Dependent Failure Analysis，DFA），从而为分解的功能部件之间足够的独立性提供依据[10]。

在智能网联汽车的系统设计中，冗余机制作为关键安全支柱，遵循功能安全与预期性功能安全双重考量。根据国际汽车自动化分级标准，智能网联汽车必须具备对自动驾驶系统故障的精细识别能力，包括系统故障行为的自动识别和持续运行能力的验证。当前L3级的自动驾驶存在显著的局限性，即在系统故障时，驾驶员的即时人工干预是受限的；而对于L4级以上的智能网联汽车，驾驶员不再被视为动态安全的备份参与者。因此，为了满足法规要求与提升乘客安全保障，必须开发出在驾驶员不在临时接管模式下的高可靠性和自主应急系统设计。这一研究着重于系统的鲁棒性设计，以确保在非人为操作期间的无缝切换运行。其设计旨在确保在关键子系统（如制动或转向）出现故障导致的自主操作中断时，能依赖冗余系统实现故障应对策略，如通过自动切换至备份路径，确保车辆能在非正常运行状态下安全地导向应急停车区域或安全区域，从而最大程度地降低潜在风险。这一策略通过精心的系统设计，保障了车辆在失效条件下的应急响应与安全处置。

汽车行业正在积极研究相关冗余安全技术，以提高自动驾驶技术的安全性[11-12]。随着自动驾驶水平的提高，与车辆驾驶安全相关的关键判断正在从驾驶员转移到车辆[13]。由于这些变化，许多部件和功能都与事故预防和安全相关[14-15]。德国汽车工业联合会推出了系统供应商和零部件供应商的产品开发和管理的生命周期模型，以确保车辆的安全[16-17]。然而，丰田公司总结发现，零部件供应商所生产的产品的质量控制是有限度的[18]。此外，文献[19]～[20]中特斯拉的案例也证实了摄像头传感器的识别错误会导致事故发生。

本文基于国内外大量文献和研究资料总结了微控制器、ECU级以及整车域控制器的安全架构冗余机制，然后系统地分析和梳理了不同自动驾驶等级的故障运行安全架构以及功能安全降级策略，最后展望了将ISO 21448引入ISO 26262标准的融合过程，该研究工作可以有效避免因车辆的E/E系统错误和执行器性能不足而引发的事故，为车辆安全行驶提供保障[21-22]。

1 ADAS/AD 系统的全链条安全体系现状

智能汽车通过感知传感器检测行人和环境，包括静态和动态物体。目前应用于自动驾驶汽车的感知传感器有摄像头、雷达、激光雷达、超声波传感器和 DGPS [23-24]。多传感器融合后的数据将进行滤波（例如卡尔曼滤波器或贝叶斯滤波器），然后对物体进行检测和分类，并预测后续场景 [25]。在下一步中，自动驾驶系统将执行路径规划。在对路况进行分析和解释后，会做出有关紧急制动、紧急转向和正常驾驶功能的决策 [26]。

保持系统故障运行的关键一步是检测处理链中所有潜在的故障原因并降低其发生的可能性 [27-28]。传统的硬件故障模式在 ISO 26262 的第 5 部分中被定义 [7]。针对此类传统故障的安全机制已经在 ADAS/AD 系统中实施，但它们不足以保证车辆安全。系统的硬件指标可以通过遵循半导体安全手册中描述的参数来实现。除了现有的安全措施外，还应根据 ISO 21448（SOTIF）制定和解决用于改进技术缺陷以提高性能的 SOTIF 措施 [8]。图 1 显示了智能汽车全流程的安全保障机制，从智能汽车的传感器到执行器，必须采用故障运行架构进行设计。

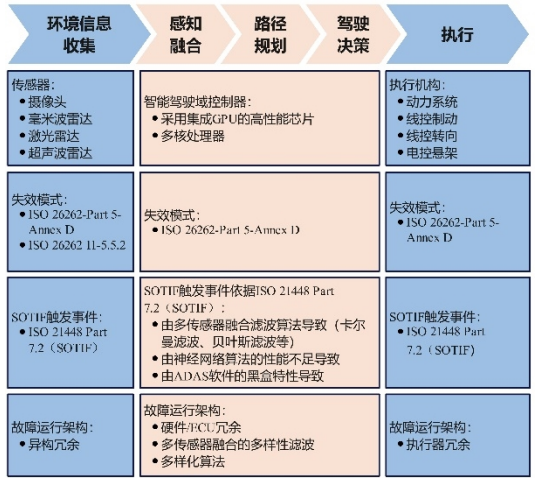


图 1　智能汽车安全架构处理链

1.1　域控制器安全架构的冗余机制

智能汽车的风险最小化策略可以最小化或防止此类系统发生故障。一方面，可以通过减少运行时间或故障率来实现风险最小化策略；另一方面，通过开发系统安全架构机制（比如故障安全架构或故障运行架构）来确保风险最小化策略。故障安全架构由传感器、电子控制单元和执行器构成，通过各种诊断功能对系统进行监控，当系统发生故障时，系统执行最小风险策略。表 1 总结了智能汽车 ADAS 控制器中冗余架构的主要类型。

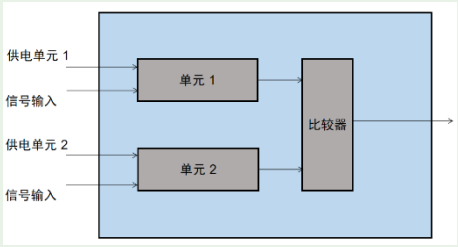
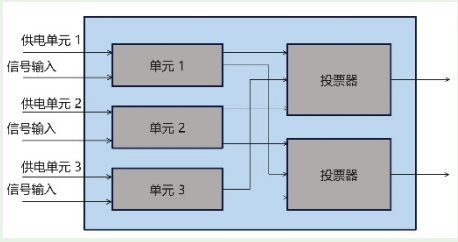
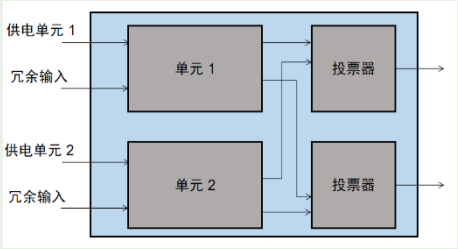
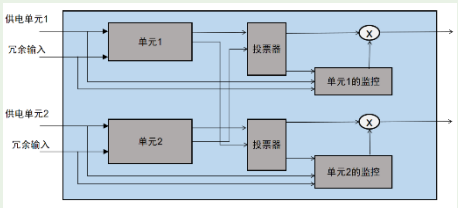
当系统发生故障时，并非总是可以关闭系统。故障操作架构的系统要求可以实现多样化的冗余或同质冗余。多样性是通过两个或多个不同的硬件和软件应用程序来实现的，这些应用程序可能会基于不同的标准，由不同的公司或团队开发。表 1 中的第 1 行为 1-out-of-2（1oo2）故障操作安全架构 [29]，是由两个独立的处理单元组成，这些处理单元能独立地控制执行器。如果一个处理单元发生故障，系统仍然可以运行。

表 1 中第 2 行的安全架构为 2-out-of-3（2oo3）故障运行架构，这种架构方案也称为三重模块化冗余（TMR）。图中的 3 个单元需要冗余计算并且彼此间相互独立，在功能计算中使用不同的输入信号和电源是非常重要的。通过计算结果的比较，如果至少两个计算单元具有相同的结果，则输出为真。如果其中一个单元发生故障，则系统可以继续使用其余两个单元。

与 2oo3 架构相比，2-out-of-2（2oo2）系统的实现更容易，如表 1 中第 3 行所示。如果两个组件之一在两个通道之一中发生故障，则系统在剩余的一个通道中可以继续使用。但在这种情况下，系统不再是故障运行状态。只运行一个通道的安全关键系统在一定的时间段内是可行的，但是并不能做到全功能冗余。

2oo2 DFS 架构由两个不同的子系统组成 [30]。该架构中，每个子系统有独立的监控功能，作为故障安全系统对子系统自身的错误进行检测（Fail-Safe，FS）。表 1 中第 4 行是基于 2oo2 DFS 架构开发的故障操作安全架构 2-out-of-2 性能诊断（2oo2 PD）。该方法的主要原理是将来自冗余或多样性冗余单元的结果进行对比，如果结果一致则这些结果

表 1 智能汽车冗余架构类型

冗余架构类型	架构示意图
1-out-of-2(1oo2)	
2-out-of-3(2oo3)	
2-out-of-2(2oo2)	
2-out-of-2 PD(2oo2 PD)	

直接用于控制执行器。如果结果不一致，则由监控功能检测并隔离有缺陷的单元。当故障单元被禁用时，系统由正常运行的单元控制，此时，系统可以保持故障运行状态。

1.2 具有多核处理器的域控制器的故障运行架构

当系统停用可能会导致发生危险情况（或系统停用违反了一个或多个安全目标），就有必要开发容错安全机制，以保证系统至少能在发生故障时进行紧急操作。本文列举的故障运行系统在微控制器和 ECU 级别的相关研究中均有涉及[31]，但是并未广泛应用于整车域控制器领域。典型的故障运行架构为 2oo3 系统（如表 1 中第 2 行），从传感器到执行器由 3 个完全独立的冗余元件组成，对应的 3 种不同路径会相互检查，以确保在发生故障的情况下找到并隔离有缺陷的路径。当故障发生时，域控制器的功能同样可以由其他两个残余路径正常运行。

在电动汽车和自动驾驶技术对多核处理器的使用需求增加的同时，主机厂会试图减少车辆中 ECU 的数量。图 2 显示了具有多核处理器的域控制器的故障运行架构解决方案。该方案的主要特点是使用第 2 个处理器作为故障处理器或计算核心的备份。在每个处理器中冗余计算和安全相关的关键功能，并将结果进行比较。如果结果不相等，则将这些结果与来自其他处理器的结果进行比较，以分析故障路径，然后系统可以主动使用剩余的正确运行路径。这种方法优势在于冗余核心内的故障操作架构可以增加系统的可用性。

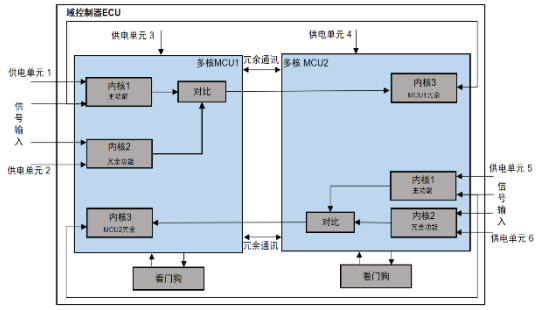


图 2　具有多核处理器的域控制器的故障运行架构

2　ADAS/AD 控制器的故障运行安全体系

故障运行系统对于自动驾驶汽车来说是必不可少的一部分。L3 级自动驾驶车辆需要在短时间内对故障进行操作，直到驾驶员能对接管车辆控制权的请求作出反应。具有 L4 和 L5 级的自动驾驶车辆必须在整个行驶周期内安全且无故障运行。该等级的自动驾驶即使在特殊情况下，比如 ADAS/AD 系统由于系统故障而停用时，车辆在施工区单车道或隧道内限速行驶仍有可能保证驾驶员的安全。安全性是驾驶员接受全自动驾驶汽车的一个重要因素，因此，自动驾驶汽车必须具有容错性功能，即从传感器到执行器应具备多重冗余功能。

由于传感器收集的数据用于后期在高性能电子控制单元内进行数据计算和分析，当前具有多核处理器的传统 ECU 的处理能力和内存不足以进行 L3 级以上的 ADAS/AD 系统功能计算。高性能芯片是执行全自动驾驶汽车计算的必要部分，AD 域的 ECU 由一个高性能芯片和一个传统安全的多核微控制器组成。通常，高性能芯片不仅可以用于处理复杂的传感器数据，而且可以执行复杂的感知和决策算法。传统的多核微控制器可以根据来自于高性能芯片的信息实现对执行器的控制。

以下章节系统地分析和梳理了不同自动驾驶等级的故障运行安全架构以及功能安全降级策略，架构的选择取决于测试用例。控制器域 ECU 的故障运行架构取决于驾驶系统的可用性，在 L3 级的自动驾驶时，机器与驾驶员交互的情况下需要保持系统故障运行的时间很短，这与在 L4 和 L5 级无人驾驶状态下确保系统处于故障运行状态是不同的。

2.1　自动驾驶域的故障运行安全架构

根据美国汽车工程师学会（SAE International）的自动驾驶等级划分，L3 代表的是“部分自动化”（Partial Automation）。在 L3 级别汽车系统能执行某些驾驶任务，如在特定的预定义条件下（如高速公路的特定车道）实现自动巡航和导航，但仍然需要驾驶员保持注意力并随时准备接管驾驶。在这种状态下，车辆可以在没有人类驾驶员干预的情况下进行大部分驾驶操作，但驾驶员应对可能的接管请求保持警觉。此外，如果系统遇到超出预设场景的情况，如交通状况变化，需要驾驶员立即接管驾驶。对于 L4 和 L5 级的自动驾驶，当发生系统故障时，自动驾驶汽车必须能保证达到安全状态。因此，L3 级车辆的系统降级策略与 L4 和 L5 级不同。L4 和 L5 级的自动驾驶车辆必须配备可以使用的故障运行冗余系统以作为 ADAS 的后备系统。由于系统对可靠性的要求，需要至少有 2oo2D 的硬件安全架构，或者是 2oo3 的硬件安全架构。图 3～5 所示的域控制器安全架构方案基于以下 4 个条件：

（1）控制器的架构具备实现独立处理不同传感器信号的能力；

（2）域控制器内的高性能芯片可实现对功能的冗余计算，并向多核微控制器提供两个独立的冗余通讯信号；

（3）高性能芯片需要具备信号冗余传输和电源冗余供应的能力；

（4）看门狗必须监控各个高性能芯片以检测它们是否正常运行。

图 3 为面向 L3 级自动驾驶的故障运行安全架构。当前的自动驾驶域控制器可以由 GPU 或 CPU 和一个多核处理器组成。在高性能芯片处理的过程中，首先根据 ISO 26262-5 中的要求对传感器信号进行独立监控，从而检测出传感器故障，如超出测量范围、偏移、振荡等。此后，根据 ISO 21448 中第 7 条监控传感器信号的传感特性，如 EMC 干扰、精度等。传感器数据的处理也是在高性能芯片中完成，以便在不同 GPU 中冗余地实现传感器信息的融合。路径的决策是在高性能芯片或在多核微控制

器中执行。若图 3 中的高性能芯片发生故障，多核芯片可以为高性能芯片的关键功能作为冗余备份。多核处理器还具有雷达等传感器接口实现部分功能的冗余，以便在高性能芯片发生故障的情况下使车辆进入安全状态。

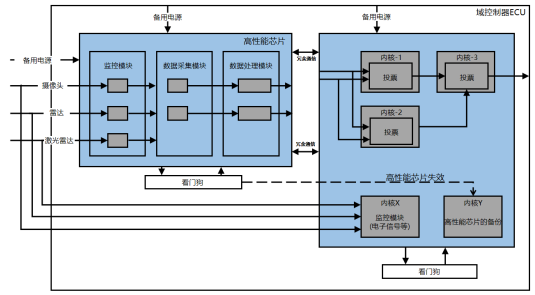


图 3　L3 级自动驾驶的故障运行安全架构

图 4 为域控制器内采用 2oo2D 架构的方案。与图 3 中的安全架构相比，第 2 个高性能芯片可以实现对功能和算法的冗余计算，计算结果通过多核 MCU 中的投票器相互比较。此外，每个高性能芯片都具有自诊断能力，若结果不相等，则很容易检测到故障路径。在该情况下，系统通过使用正确的路径保持故障运行状态。在结果不相等的情况下，如果无法确定错误路径，则系统不再处于故障运行状态，必须关闭以达到故障安全状态。

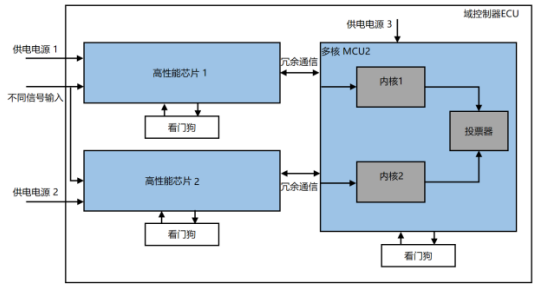


图 4　故障运行安全架构：2oo2D 方案

图 5 为域控制器 ECU 内三重冗余的架构设计。与 2oo2D 安全架构相比，该架构具有更高的冗余性能。在投票器内可以比较 3 个独立路径以检测故障路径。该域控制器内存在 3 个高性能芯片，若其中一个或者两个发生故障，系统都会处于故障运行的状态。若 3 个高性能芯片同时发生故障，则系统必须关闭以处于故障安全的状态。

图 6 展现了高性能芯片内 ADAS 功能和算法的故障运行处理机制。图中的高性能芯片由 GPU 和

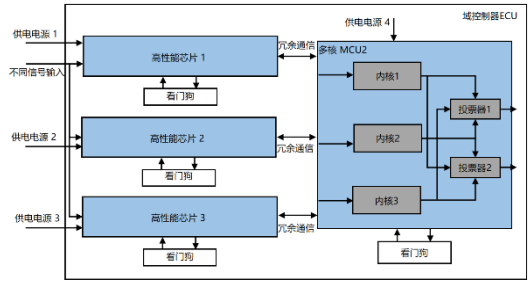


图 5　故障运行安全架构：2oo3D 方案

CPU 组成，两者共同构建了故障运行处理架构。CPU 首先对传感器的信号进行诊断。随后将感知、路径规划和驾驶策略的功能和算法在相互冗余的 GPU 中进行执行。两个相互冗余 GPU 中的结果在 CPU2 中对比，从而确保了多重冗余能力。最后在多核处理器中对高性能芯片的输出进行比较，如图 3～5 所示。

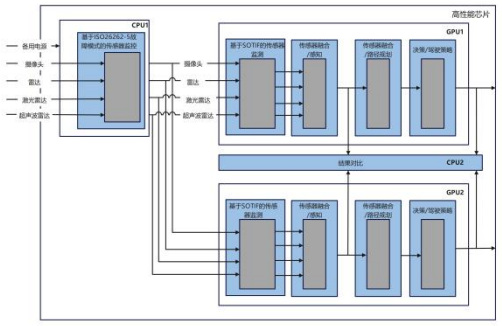


图 6　高性能芯片内的故障运行处理机制

综上所述，本文针对特定条件的自动驾驶级别提出了最适合的安全架构。图 3 中的架构适用于 L3 级的自动驾驶系统，因为 L3 级自动驾驶系统的冗余度要求低且在该情况下驾驶员可以被视为 ADAS/AD 系统的后备。图 4 和图 5 中的安全架构适用于 L4 级和 L5 级的自动驾驶车辆，因为此类系统对安全性和冗余度要求更高。如果对系统安全性要求较低，例如车辆仅在机场等受限区域使用时，可以选择图 3 中的安全架构。在研究合适的安全架构时，还有许多其他因素需要考虑，例如测试用例和成本等。

2.2　ADAS/AD 系统的功能安全降级策略

底盘系统的线控化和自动驾驶系统的发展应用使车辆系统变得更加安全。ISO 26262 标准提供了

将分解方法应用于安全关键系统开发的可能性，特别是ASIL D级功能安全系统。适当的分解具有降低源自安全目标的顶级安全要求的优点，但ASIL分解需要安全要求的冗余，需要分配给足够独立的架构元素。

ISO 26262—Part 9中第5条提到了分解方法的以下要求：

（1）作为一项基本原则，ASIL分解需要安全要求具有冗余性，且分配给充分独立的架构要素；

（2）如果架构要素不是充分独立的，则冗余要求和架构要素继承初始的ASIL等级；

（3）使用同构冗余（通过复制设备或复制软件）的情况下，考虑到硬件和软件的系统性失效，不能降低ASIL等级，除非相关失效的分析提供了存在充分独立性或潜在共因指向安全状态的证据。因此，同构冗余因缺少要素间的独立性，通常不足以降低ASIL等级。

对于传统的汽车系统架构，相关学者已成功将ISO 26262国际功能安全标准的第9部分——尤其是关于失效模式及影响分析（Failure Mode and Effects Analysis，FMEA）的分解方法，适配于那些被归类为ASIL D级别的复杂系统。这种策略旨在将系统设计的优化纳入到高级安全标准框架内，确保在面临潜在故障时，能提供一套系统级的故障操作规程，通过预先设计的冗余策略和风险缓解机制，确保在ASIL D级的严苛要求下，系统的可靠性和安全性得到有效提升。这种方法论的实施，旨在提升整体安全性能并遵循国际安全规范的最佳实践。如图7所示，该概念中的域ECU提供了所需的足够独立的架构元素[32-33]。

3　自动驾驶功能安全融合设计的展望

3.1　ISO 21448方法论的局限性

对于汽车电子电气系统而言，流程是安全性保障的基础，汽车线控化、智能化需解决功能安全、预期功能安全和信息安全问题[34]，相关标准随之推出，而标准的实施和产品的认证均以符合标准的

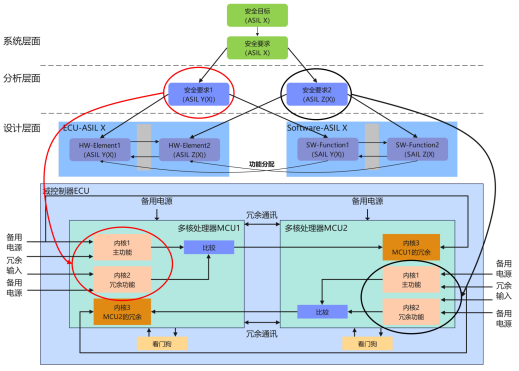


图7　域控制器ECU内的ASIL分解方案

开发流程为依托。

汽车电子工业界从2008年开始致力于IEC61508在汽车上的运用，随后于2011年正式发布了汽车功能安全标准，其内容包括：危害识别与评估、功能安全概念、系统安全概念、软硬件安全概念、验证与确认、生产、运行与维护报废等，贯穿于产品开发流程的各个阶段，与传统汽车开发流程具有较好的融合性。功能安全流程的实施需部分新的方法和相应的工具进行支撑，包括HARA、HAZOP、STPA等[35]。

功能安全旨在避免由E/E系统功能失效导致的不可接受的风险，主要是针对系统性失效/随机硬件失效导致的风险分析和控制[36]。对于智能汽车或智能底盘，在没有出现电子电器系统失效时，由于设计上的功能不足或总成的性能局限性（如轮胎在地面上的附着能力），也会导致其产生相应的风险，但此部分并不属于ISO 26262的范畴。为了弥补ISO 26262的局限，预期功能安全标准应运而生[37]。

最初ISO 21448要成为ISO 26262的一个章节，但因为在没有系统失效的情况下保证安全这个概念非常复杂，预期功能安全（SOTIF）便成为一个独立的标准，该标准将风险划分为4个区域，分别为可知安全场景、可知危险场景、不可知安全场景和不可知危险场景，SOTIF的目标就是在开发阶段通过各种手段尽可能减小不可知危险场景的范围，如图8所示[38]。2019年1月，ISO 21448：2019 Road vehicles — Safety of the intended functionality发布；

2019年5月，ISO 21448工作组草案（WD）中已将该国际标准的范围拓展至L1-L5级自动驾驶车辆系统；2020年又新增了运行阶段、场景库、GSN、地图、V2X等内容。与功能安全相比，预期功能安全流程中各项开发活动更加抽象，活动开展对软件工具的依赖更强，与传统开发流程的融合难度也更大。预期功能安全流程定义8项活动，包括定义和设计、危害识别和风险评估、识别功能不足及其触发条件、降低SOTIF风险的功能性修改、SOTIF检验和验证策略定义、已知潜在危害场景评估、未知场景探究和评价，以及制定SOTIF释放标准[39-42]。上述活动难以在明确的研发阶段完成，使其在与其他开发流程的融合方面面临很大困难。

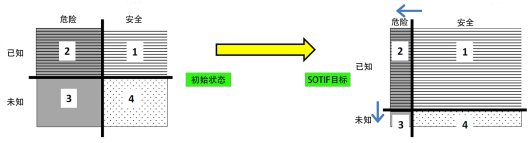


图8 SOTIF对象及目标

随着智能网联汽车的发展，信息安全也成为了必须考虑的安全性问题，汽车网络安全也面临新的挑战，相关学者需要努力通过新的工程方法和特殊技术手段来应对车辆整个生命周期中出现的威胁、风险管理、安全设计、意识和汽车网络安全问题。因此，安全可靠的智能网联汽车生产和设计已成为行业焦点。在解决汽车网络安全的问题上，尽管可以借鉴其他领域的经验，但是，汽车行业所面临的“专属挑战”仍不可避免。于是，汽车行业意识到需要通过特定的行业标准来解决汽车网络安全问题并保护个人资产。国际标准化组织（ISO）和美国汽车工程师学会（SAE）近期联合起草发布了“ISO/SAE DIS 21434道路车辆-汽车网络安全工程”国际规范。从汽车行业的角度来看，该标准就产品开发和整个供应链设计的安全性方面达成了共识，具体目标分为3点：

（1）确定一个结构化的流程，以确保信息安全设计；

（2）降低成功攻击的可能性，减少损失；

（3）提供清晰的方法，以帮助车企应对全球行业共同面对的信息安全威胁。

功能安全、预期功能安全和信息安全的开发流程活动对应关系如图9所示，这些研发活动最终将融入整车的开发流程中，新增活动的内容及其特点将深刻影响总体研发流程的形态，也对研发活动的组织管理提出了新要求。重塑研发流程是智能汽车/智能底盘研发体系进化的重要趋势。

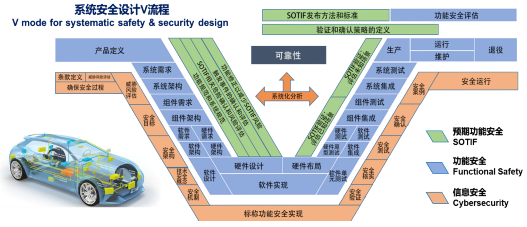


图9 功能安全、预期功能安全和信息安全的开发流程活动

为了确保具有自动驾驶相关功能的车辆的安全性，ISO 21448应适用于相关零部件和系统[43-44]。ISO于2019年宣布了预期功能的安全性（ISO 21448），以防止未包含在ISO 26262中的性能局限性和无意引发的风险。宝马[45]、百度[46]等公司尝试在产品开发方面将SOTIF引入其产品全生命周期安全开发流程；大陆集团[47]、ANSYS[48]、欧盟项目[49]和NHTSA[50]在产品安全分析评估方面尝试引入安全分析工具，从而进行了SOTIF分析评估实践。以上都在SOTIF实践方案中进行的探索。在SOTIF安全验证确认方面，欧盟[51]及其延伸项目VVM[52]、SetLevel[53]、日本SAKURA[54]项目以及中国智能网联汽车联盟预期功能安全工作组等都在实践中与SOTIF进行了结合。

在以往的安全分析方法中，往往通过将系统分解为更小的组件，单独检查和分析每个组件，然后将分析结果按照系统架构组合起来，以便理解系统的危害。通过这样简单的分解，工程师将一个大系统分解为若干个小的组件，并假设事故是由组件故障引起的，在分析了组件故障后，再将组件的故障融入到整个系统当中。这种分解法只适用于相互独立的子系统，当今智能驾驶车辆系统的复杂性大大增加，各子系统间甚至是各个大的系统之间也存在着必然的联系，分解法的安全分析在该系统中会存在明显的不足。系统的组成不仅仅是系统要素的简单叠加，还包括系统要素间的交互作用。业界依次

建立了 STPA、HARA、FTA 等安全分析工具及安全分析方法，通过将这些分析工具与分析方法融入进 V 型开发的流程中，将故障模型从组件故障扩展到更复杂的流程和系统组件之间的不安全交互。这种基于模型的开发流程可以加强智能驾驶车辆设计的安全性，具体的开发流程如图 10 所示。在涉及车辆功能安全、预期功能安全以及网络安全的开发流程中，首先对整体系统进行危险分析、风险评估（FuSa 和 SOTIF 分析工具为 HARA，网络安全分析工具为 TARA），建立功能事件树；接着对各个系统进行安全需求分析，建立各自的失效树以及受攻击树，最后通过将各个安全需求分解成技术手段需求，引入汽车安全完整性等级 ASIL，设计失效模式和影响分析。

然而，如图 11 所示的功能安全概念的开发仅由车辆制造商执行。此外，ISO 26262 明确将概念

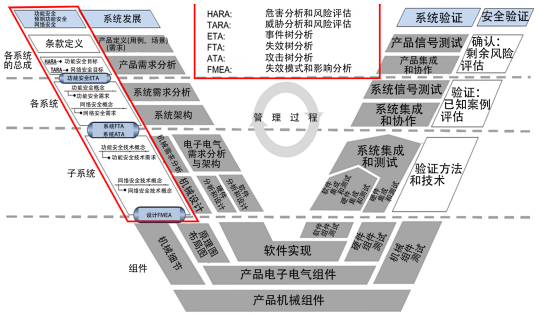


图 10　引入 HARA 等安全分析工具的系统 V 型设计路线

阶段和系统开发阶段分开，但 ISO 21448 确认整个过程阶段是混合的。在现有流程中，因为软、硬件开发与测试阶段仅使用整车开发中提供的有限信息，很难确认开发过程是否朝着正确的方向前进，这使开发与测试阶段在引入 ISO 21448 时处于被动状态。事实上，ISO 21448 应与 ISO 26262 并用，并形成一个完整的 V 流程，使制造商和供应商能以相同的概念进行开发，以满足开发自动驾驶汽车相关技术的安全要求。

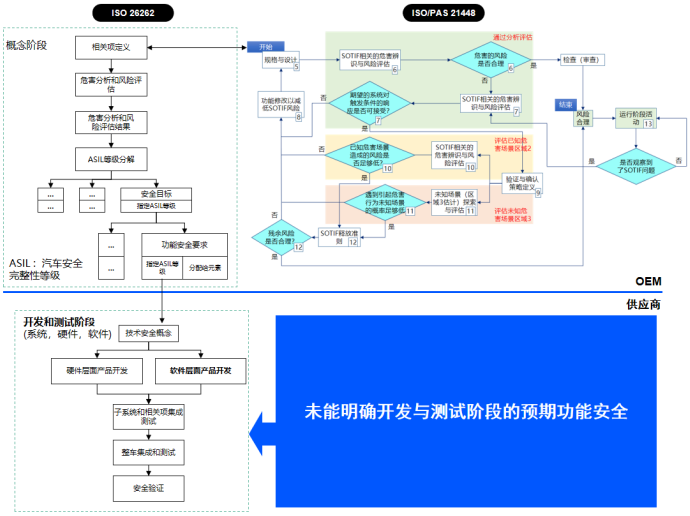


图 11　传统的 ISO 21448 与 ISO 26262 开发流程

3.2　ISO 26262 与 ISO 21448 的融合设计开发流程

为了开发符合 ISO 21448 安全性的系统软件与硬件，系统软、硬件的开发必须与主机厂一起参与实际产品开发相关的 ISO 21448 流程。本文提出了一种融合 ISO 26262 和 ISO 21448 的开发流程，如图 12 所示。文中所提出的流程可应用于 ISO 21448 流程的概念阶段和开发阶段，供应商在参与开发与测试阶段的角色与图 12 中的 ISO 26262 和 ISO 21448 融合开发不同。本文提出的 ISO 21448 的应用过程见表 2。该过程是为了澄清通过执行输出的具体性、测试用例和源自 ISO 21448 的安全目标来定义不明确的情况和场景情况。

表 2 中定义了在这种情况下可能发生风险的详细因素和与之相关的风险源，以便根据风险设定安全目标。图 12 中改进的过程可以作为系统 HARA 分析的先决条件，通过对顶层系统的假设来定义相关系统，并对车辆运动等相关事项进行部分假设。

此外，系统简化并整合了最终系统中可能出现的问题以得出结果。当通过图 12 中的循环结构重复相同的工作时，该流程可以通过重复使用现有结果来达到节省时间的目的。

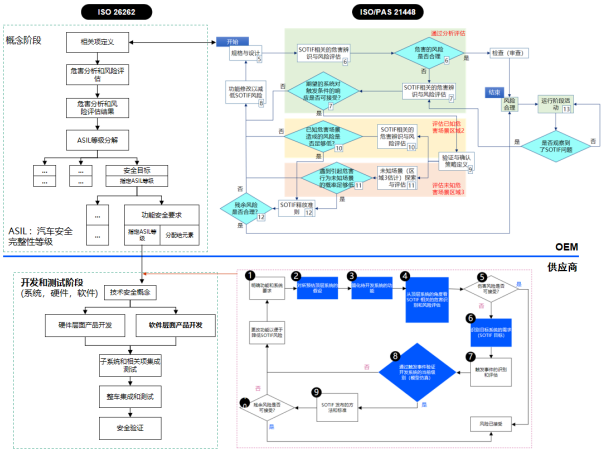


图 12 ISO 21448 与 ISO 26262 融合的开发流程

表 2 ISO 21448 流程分析

No.	阶段	细节内容
1	明确系统功能和要求	要定义场景的开发要求，通过考虑 ISO 26262 和 ISO 21448 来定义功能安全要求和系统功能要求。
2	假设对顶层系统的预估	基于测试用例和场景，需要假设开发系统对顶层系统（车辆）的影响。
3	简化待开发系统的功能	为了分析风险，将具有代表性的情况划分为几个特征并得出简化后的结果。
4	确认与 ISO 21448 相关的风险原因，并评估风险是否可接受	与 ISO 21448 目标相关的风险可通过系统功能、简化的结果和更高的系统假设进行评估。
5	确定风险是否可接受	系统的风险源是否可以接受通过上一步的推导结果来决定。
6	减除开发系统的要求	通过上一步的推导结果建立系统的安全目标。
7	触发事件的识别和评估	该过程可用于分析影响系统性能的因素，以及导致系统性能下降的不良条件。
8	通过触发事件验证概念阶段	将第 2 阶段的场景和第 7 阶段的触发事件应用到所开发的系统中并进行验证。
9	确定 ISO 21448 分配的方法和标准	
10	确定剩余风险是否可接受	

4 总结与展望

本文详尽剖析了基于微控制器、ECU、多核处理器中域控制器 ECU 开发的安全冗余架构和故障运行处理机制，并深入探讨了目前的 ADAS/AD 系统中安全相关的技术与 SOTIF 技术融合方面可能存在的不足，通过对 ADAS/AD 域控制器 ECU 故障运行架构的研究，展望了如何设计合适的 ISO 26262 与 ISO 21448 融合设计开发流程。通过对智能汽车安全关键领域的深入梳理和客观评估，为优化 ADAS/AD 系统设计的综合安全策略提供了理论框架，旨在驱动更高级别的安全性提升和发展趋势的探索。综合研究现状的不足与发展趋势，总结如下。

（1）丰富场景数据库与实虚融合提升驾驶测试的可信度与安全性。场景数据库作为仿真测试的基石，其内容的丰富性和对现实场景的高度模拟能力直接决定了测试结果的可信度。在智能汽车技术研发的开发性测试与认证性验证中，实虚融合的验证方法被广泛采用，旨在通过结合实际与虚拟世界，解决自动驾驶路测数据匮乏的难题，以实现互补性的验证，从而提升测试的全面性和有效性。这种策略旨在提升智能驾驶系统的鲁棒性和安全性，为技术成熟度与法规适应性提供强有力的支持。

（2）E/E 系统标准待完善，测试技术亟待升级。智能汽车对汽车的安全性提出新要求。传统汽车开

发验证经过百年积累，制定了标准工况开展验证，机械系统潜在的安全失效问题基本解决。E/E 系统功能安全虽有标准，但由于依赖于流程和内部规范，企业尚未完全掌握，且自动驾驶汽车的预期功能安全控制仍缺乏实施标准。功能安全和预期功能安全都需要复杂的测试验证方法支撑，传统机电系统验证技术亟待升级换代。

（3）系统级性能验证体系需覆盖全生命周期，确保安全性能稳定。全生命周期的系统级性能验证体系亟须搭建。由于车辆的动力学性能会随着驾驶时间发生变化，传统的车辆性能试验往往只是针对新车进行，性能衰退的影响只能在长期的道路试验中发现（转向系统松旷、制动器磨损，性能下降），而性能下降会导致安全问题，需要进行考核验证，这也给自动驾驶系统带来了巨量的测试验证需求。因此，随着 ISO 26262 和 ISO 21448 的深化，更系统化的安全设计方法，从系统级到组件级的端到端全方位安全设计考量更加迫切。

参考文献（References）

[1] FORD.A Matter of Trust：Ford Safety Assessment Report for Self-Driving Vehicle Development[EB/OL].(2018-08-16)[2018-08-18]. https://media. ford. com/content/fordmedia/fna/us/en/news/2018/08/16/a-matter-of-trust-ford-releases-safety-assessment-report.html.

[2] GM.Self-Driving Safety Report[EB/OL].[2018-08-18]. https://www.gm.com/mol/selfdriving.html.

[3] WAYMO.Waymo Safety Report[EB/OL].[2018-08-18]. https://waymo.com/safety/.

[4] PEREIRA N Q, CALLANGH B.A Comparison New Car Assessment Program NCAP Requirements and Procedures Around the World[C]//SAE Technical Papers, 2013-36-0499, 2013.

[5] HOBBS C A, MCDONOUGH P J. Development of the European New Car Assessment Programme (Euro NCAP)[J].Regulation, 1998, 44(3): 2439-2453.

[6] PAINE M, PAINE D, CASE M, et al.Trends with ANCAP Safety Ratings and Real-World Crash Performance for Vehicle Models in Australia [C]//Proceeding of 23rd International Technical Conference on the Enhanced Safety of Vehicles, May 27-30, 2013, Seoul, Korea (South).2013: 1794-1801.

[7] ISO FDIS 26262 (2nd Edition) : Road Vehicles-Functional Safety[S].Geneva: ISO, 2018.

[8] ISO 21448: Safety of the Intended Functionality [S]. Geneva: ISO, 2018.

[9] Autoindustrie Treibt Chipnachfragean [EB/OL]. [2017-01-30]. http://www. pwc. de/automobil-industrie/auto-industrie-treibt-chipnachfrage-an.html.

[10] HIP-HOPS, Automated Fault Tree, FMEA and Optimisation Tool[EB/OL].[2018-12-10].http://www.hiphops.eu/index.php/the-manual.

[11] MBOWA K, AIGBAVBOA C, AKINSHIPE O, et al. An Overview of Key Emerging Technologies Transforming Public Transportation in the Fourth Industrial Revolution Era [C]// International Conference on Engineering for Sustainable World: ICESW 2020, Aug.10-14, 2020, Ota, Nigeria.Bristol: IOP Publishing, 2021: 1696-1705.

[12] KIM M J, YU S H, KIM T H, et al.On the Development of Autonomous Vehicle Safety Distance by an RSS Model Based on a Variable Focus Function Camera [J]. Sensors, 2021, 21(20): 1-11.

[13] NARAYANAN A.Ethical Judgement in IntelligentControl Systems for Autonomous Vehicles [C]//2019 Australian & New Zealand Control Conference (ANZCC), Nov.27-29, 2019, Auckland, New Zealand.Piscataway NJ: IEEE, c2019: 231-236.

[14] KÖLBL M, LEUE S. Automated Functional Safety Analysis of Automated Driving Systems [C]//Formal Methods for Industrial Critical Systems: 23rd International Conference, FMICS 2018, Sept. 3-4, 2018, Maynooth, Ireland.Heidelberg: Springer, 2018: 35-51.

[15] BIRCH J, RIVETT R, HABLI I, et al. Safety Casesand Their Role in ISO 26262 Functional Safety Assessment [C]//Proceedings of the 32nd International Conference on Computer Safety, Reliability, and Security, 2013.New York: Springer-Verlag, 2013: 154-165.

[16] LIM G T, LEE J.On a Method to Analyze and Verify the Functional Safety of ISO 26262 Based on Systems Engineering Framework [J]. Journal of the Korea Safety Management and Science, 2013, 15(3): 61-69.

[17] FINKBEINER M, KRINKE S, OSCHMANN D, et al. Data Collection Format for Life Cycle Assessment of the German Association of the Automotive Industry (VDA) [J].The International Journal of Life Cycle Assessment, 2003, 8(6): 379-381.

[18] COLE ROBERT E.What Really Happened to Toyota?[J]. MIT Sloan Management Review, 2011, 52(4): 29.

[19] BANKS V A, PLANT K L, STANTON N A.Driver Error or Designer Error: Using the Perceptual Cycle Model to

Explore the Circumstances Surrounding the Fatal Tesla Crash on 7th May 2016[J]. Safety Science, 2018, 108: 278-285.

[20] JENSSEN G D, MOEN T, JOHNSEN S O. Accidents with Automated Vehicles—Do Self-Driving Cars Need a Better Sense of Self ?[C]//Proceedings of the 26th ITS World Congress, Singapore.2019: 21-25.

[21] JEON S H, CHO J H, JUNG Y, et al. Automotive Hardware Development According to ISO 26262[C]// 13th International Conference on Advanced Communication Technology (ICACT2011), Feb. 13-16, 2011, Gangwon, Korea (South). Piscataway NJ: IEEE, c2011: 588-592.

[22] SCHNELLBACH A, GRIESSNIG G.Development of the ISO 21448[C]//Systems, Software and Services Process Improvement: 26th European Conference, EuroSPI 2019, Sept. 18-20, 2019, Edinburgh, UK. Heidelberg: Springer, 2019: 585-593.

[23] 李茂月,陈月,徐光岐.基于入位基准线的避死区自动泊车路径规划[J].中国机械工,2019,30(1):53-63.
LI Maoyue, CHEN Yue, XU Guangqi. Automatic Parking Path Planning for Dead Zone Avoidance Based on Entry Baselines[J]. China Mechanical Engineering, 2019, 30(1): 53-63.(in Chinese)

[24] 熊璐,严森炜,余卓平,等.基于库位跟踪的自动泊车决策规划系统[J].汽车技术,2018(8):18-26.
XIONG Lu, YAN Senwei, YU Zhuoping, et al. Decision Making and Planning System of Autonomous Parking Based on Closed-Loop Update of Parking Spot[J]. Automobile Technology, 2018(8): 18-26.(in Chinese)

[25] 李克强,戴一凡,李升波,等.智能网联汽车(ICV)技术的发展现状及趋势[J].汽车安全与节能学报,2017,8(1):1-14.
LI Keqiang, DAI Yifan, LI Shengbo, et al. State-of-the-Art and Technical Trends of Intelligent and Connected Vehicles[J]. Journal of Automotive Safety and Energy, 2017, 8(1): 1-14.(in Chinese)

[26] 余卓平,韩伟,徐松云,等.电子液压制动系统液压力控制发展现状综述[J].机械工程学报,2017,53(14):1-15.
YU Zhuoping, HAN Wei, XU Songyun, et al. Review on Hydraulic Pressure Control of Electro-Hydraulic Brake System[J]. Journal of Mechanical Engineering, 2017, 53(14): 1-15.(in Chinese)

[27] 荣芩,吴晓东,许敏.基于ISO标准的道路车辆线控转向系统的功能安全概念设计[J].汽车安全与节能学报,2018,9(3):250-257.
RONG Qin, WU Xiaodong, XU Min. Functional Safety Concept Design for Steer-by-Wire System of Road Vehicle Based on the ISO[J]. Journal of Automotive Safety and Energy, 2018, 9(3): 250-257.(in Chinese)

[28] 吴志红,陆科,朱元.车用电机控制器功能安全及主动短路分析[J].同济大学学报(自然科学版),2018,46(9):1298-1305.
WU Zhihong, LU Ke, ZHU Yuan. Analysis of Active-Short-Circuit of Permanent Magnet Synchronous Mot or in Electric Vehicles[J]. Journal of Tongji University (Natural Science), 2018, 46(9): 1298-1305.(in Chinese)

[29] International Electrotechnical Commission. IEC61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems[Z].2005.

[30] KOHN A, SCHNEIDER R, VILELA A, et al. Architectural Concepts for Fail-Operational Automotive Systems[C]// SAE Technical Papers, 2016-01-0131, 2016.

[31] KOHN A, KASMEYER M, SCHNEIDER R, et al. Fail-Operational in Safety-Related Automotive Multi-Core Systems[C]//10th IEEE International Symposium on Industrial Embedded Systems (SIES), June 8-10, 2015, Siegen, Germany. Piscataway NJ: IEEE, c2015: 1-4.

[32] KOOPMAN P, WAGNER M. Toward a Framework for Highly Automated Vehicle Safety Validation[C]//SAE Technical Papers, 2018-01-1071, 2018.

[33] LUO Yaping, SABERI A K, VAN DEN BRAND M. Safety-Driven Development and ISO 26262[M]//Automotive Systems and Software Engineering: State of the Art and Future Trends, 2019: 225-254.

[34] 宗长富,李刚,郑宏宇,等.线控汽车底盘控制技术研究进展及展望[J].中国公路学报,2013,26(2):160-176.
ZONG Changfu, LI Gang, ZHENG Hongyu, et al. Study Process and Outlook of Chassis Control Technology for X-by-Wire Automobile[J]. China Journal of Highway and Transport, 2013, 26(2): 160-176.(in Chinese)

[35] XING Xingyu, ZHOU Tangrui, CHEN Junyi, et al. A Hazard Analysis Approach Based on STPA and Finite State Machine for Autonomous Vehicles[C]// 2021 IEEE Intelligent Vehicles Symposium (IV), July 11-17, 2021, Nagoya, Japan. Piscataway NJ: IEEE, c2021: 150-156.

[36] LURIE O, MILLER J. Hazard Analysis and Risk Assessment Beyond ISO 26262: Management of Complexity Via Parametrization[C]//SAE Technical Papers, 2018-01-1067, 2018.

[37] KHATUN M, GLAP M, JUNG R. Scenario-Based Extended Hara Incorporating Functional Safety and SOTIF for Autonomous Driving[C]//Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference, Nov. 1-

5，Venice，Italy.2020：53−59.
[38] SCHWALB E. Analysis of Safety of the Intended Use (SOTIF)[R]. National Highway Traffic Safety Administration，2019.
[39] HEJASE M，BARBIER M，OZGUNER U，et al. A Validation Methodology for the Minimization of Unknown Unknowns in Autonomous Vehicle Systems [C]//2020 IEEE Intelligent Vehicles Symposium (IV)，Oct. 19−Nov. 13，Las Vegas，NV，USA. Piscataway NJ：IEEE，c2020：114−119.
[40] BAGSCHIK G，MENZEL T，MAURER M. Ontology Based Scene Creation for the Development of Automated Vehicles[C]//2018 IEEE Intelligent Vehicles Symposium (IV)，June 26−30，2018，Changshu，China. Piscataway NJ：IEEE，c2018：1813−1820.
[41] HUANG An，XING Xingyu，ZHOU Tangrui，et al. A Safety Analysis and Verification Framework for Autonomous Vehicles Based on the Identification of Triggering Events[C]//SAE Technical Papers，2021−01−5010，2021.
[42] DING Wenhao，CHEN Baiming，LI Bo，et al.Multimodal Safety-Critical Scenarios Generation for Decision-Making Algorithms Evaluation[J].IEEE Robotics and Automation Letters，2021，6(2)：1551−1558.
[43] SARI B，DAS A. Extending SOTIF Application for Higher Automated Driving[R]. SAE International：WCX 18：SAE World Congress Experience，Detroit，USA，2018.
[44] SARI B.SOTIF for Higher Automated Driving[R]. Safe. Tech Conference 2018，München，Germany，2018.
[45] BMW.BMW Safety Assessment Report[Z].BMW Group，2020.
[46] Baidu.Apollo Pilot Safety Report[Z].2018.
[47] ABDULKHALEQ A，LAMMERING D，WAGNER S，et al.A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles[J].Procedia Engineering，2017，179(Supplement C)：41−51.
[48] KAISER B. An Integrative Solution Towards SOTIF and AV Safety[R].IQPC SOTIF Conference，2019.
[49] WILLEMSEN D，SCHMEITZ A，FUSCO M. Enabling Safe Multibrand Platooning for Europe [Z]. European Commission，2018.
[50] BECKER C，BREWER J C，YOUNT L. Safety of the Intended Functionality of Lane-Centering and Lane-Changing Maneuvers of a Generic Level 3 Highway Chauffeur System [R]. National Highway Traffic Safety Administration，2020.
[51] JUNIETZ P，WACHENFELD W，KLONECKI K，et al. Evaluation of Different Approaches to Address Safety Validation of Automated Driving [C]//2018 21st International Conference on Intelligent Transportation Systems (ITSC)，Nov. 4−7，2018，Maui，HI，USA. Piscataway NJ：IEEE，c2018：491−496.
[52] NEUROHR C，WESTHOFEN L，BUTZ M，et al. Criticality Analysis for the Verification and Validation of Automated Vehicles [J]. IEEE Access，2021，9：18016−18041.
[53] STEIMLE M，WEBER N，MAURER M. Toward Generating Sufficiently Valid Test Case Results：A Method for Systematically Assigning Test Cases to Test Bench Configurations in a Scenario-Based Test Approach for Automated Vehicles[J].IEEE Access，2022，10：6260−6285.
[54] JACOBO A，NOBUYUKI U，KUNIO Y，et al. Development of a Safety Assurance Process for Autonomous Vehicles in Japan [C]//Proceedings of International Conference on Enhanced Safety of Vehicles，June 10−13，2019，Eindhoven，The Netherlands. 2019：1103−1120.

作者简介

罗通强（1988−），男，广东廉江人，硕士，工程师，主要研究方向为整车系统集成和人因分析。
Tel：18666287979
E-mail：53191436@qq.com

通信作者

李仰光（1993−），男，广东汕尾人，硕士，工程师，主要研究方向为整车智能化和人因分析。
Tel：13751736976
E-mail：liyangguang123@126.com