

基于 DIL 的线控转向系统安全设计

陆俊文 施陆锴 高立臣

博世华域转向系统有限公司

摘要: 为了对线控转向系统 (SbW) 进行安全设计, 分析了线控转向的安全目标和故障类型, 并建立安全机制。归纳了软硬件模块故障在系统层级的失效, 利用驾驶员在环 (DIL) 系统注入故障, 模拟线控转向整车在发生故障时的表现, 以此验证安全机制的可靠性。针对转向盘操纵结构 (HWA) 非预期转向试验表明, 所建立的安全机制能确保车辆平稳运行。

关键词: 线控转向; 降级; 安全设计

0 前言

SbW 是转向系统的一种形式, 它取消了作为机械连接的中间轴, 通过线束传递电信号的方式使 HWA 和车轮转向执行器 (RWA) 实现联动, 赋予了底盘域更灵活的传动比和手感的变动能力。与传统的转向系统相比, SbW 实现了 HWA 和 RWA 的解耦。而这部分的差异, 给 SbW 提出了更高的安全以及可靠性要求。为了降低电子电气系统故障或错误引发的非预期风险, 根据强制标准 GB19765-2005 的要求, SbW 的设计和开发须根据功能安全 GB/T34590-2017, 从系统、硬件和软件各层面逐一分析并设计安全机制, 使得线控系统在故障发生情况下, 能够仍然可控且可合理降级进入设定的安全状态, 同时还需对这些安全机制进行大量测试和可靠性评判。

1 相关研究现状

李赛赛等提出了对转向系统安全机制在实车上进行单点故障注入, 并通过整车反应、车辆轨迹和方向盘手力矩进行功能安全主观评价。高乐、蒯家琛等提出了通过硬件在环 (HiL) 测试方法给电动助力转向系统 (EPS) 硬件进行了扭矩传感器和电机电流故障注入。李傲寒阐述利用 dSPACE 工具搭建了 HiL 系统台架对设计的硬件冗余和软件故障检测等安全机制进行故障注入和故障容错确认测试。由此可见, 安全机制设计后需要进行故障注入系统可靠性测试, 测试方法主要有两种: 实车和 EPS 电子电气系统 HiL。实车可控性测试针对低成熟度模块有较高的风险, 不定因素干扰过

大 (人为操控多变、路况因素不可控), 无法对安全机制进行可重复工况的客观评判。而 EPS 电子电气系统 HiL 只能针对子系统进行验证, 对于整体系统联动工况及驾驶环境下的可控性方面的评判有较大的局限。

因此, 基于半实物仿真的 DIL, 融合了实车及 HiL 的优点形成的半实物“人—车—环境”闭环系统, 在各种可重复且可编辑的不同场景工况下, 可以在自动注入故障后, 实时记录 SbW 的响应以及车辆观测值, 实现安全机制客观验证与高效迭代。

2 线控转向的安全分析

2.1 SbW 的安全目标

SbW 可划分为 HWA 和 RWA 两个子系统, 每个子系统由若干相关项构成。如图 1 所示, 显示了“人—车—环境”闭环中各相关项之间方向明确的数据传递, 其中: 1 表示驾驶员通过转向盘向驾驶员意图感知单元输入的基础信号 (包括: 角度、角速度和手力等); 2 表示反馈力矩执行单元向转向盘传递的手感力矩; 3 表示 HWA 通过信号处理控制单元传递给 RWA 的目标转角值; 4 表示 RWA 反馈测量数据给 HWA 用于计算手感; 5 表示 SbW 通过齿条、横拉杆和转向节等连接机构, 传递给转向车轮的转向角; 6 表示车载供电系统给 SbW 的供电; 7 表示车载通信数据; 8 表示车载报警数据; 9 表示传递给驾驶员的可视化或声音报警; 10 表示转向车轮与环境间 (如地面等) 交互的物理数据 (力、力矩等)。

以上相关项和数据传递表明了 SbW 系统的核心功能, 即执行 HWA 转角输入和反馈 RWA 力矩。基于危害分析和风险评估 (HARA) 分析, 可以得出 SbW 的

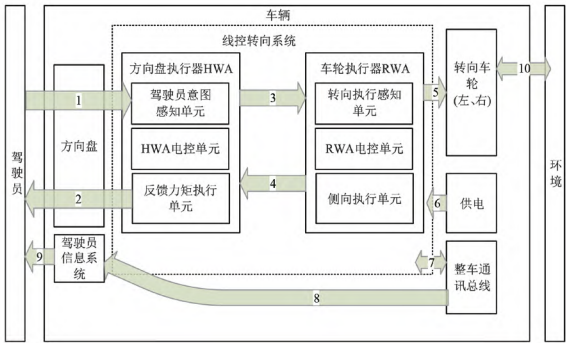


图1 SbW 的系统示意

异常表现并推导出最基本的安全目标，如表 1 所示。

2.2 基于 SbW 系统架构的故障分析

基于以上异常表现，可依据 SbW 系统架构进一步细分故障源，并推导其可能发生的故障形式。如图 2 所示，为由物理模块构成的系统架构示例，包括电控单元、执行电机、扭矩角度传感器、蜗杆小总成、机械限位组和机械连接组件等。其中，电控单元又由多

个模块构成，模块间传递信号包括驱动电机的 PWM，芯片间通信的 I2C、IPC 等。

结合系统架构和表 1 中的异常表现，罗列了如表 2 所示的部分物理模块故障形式所对应的异常表现。

2.3 SbW 系统安全机制的设计

SbW 由上下两个子系统组成，其安全机制也包含单个子系统本身和多子系统协同工作。其中，对于子系统本身的安全设计目的在于：(1) 尽可能把单点失效转换为多点失效；(2) 有监控和提示机制确保潜伏失效。因此，基于三层监控框架概念可以初步确定带有安全机制的子系统架构。如图 2 所示，其中不限于软件算法的异构、硬件模块检测、问答监控和锁步核等措施。另外，系统的机械模块的可靠性也需要考虑在安全设计中，以避免机械组件的损伤导致系统失稳而违背安全目标。

对于协同工作的安全机制，主要考虑某电控子系统失效，另外子系统如何确保整体进入安全状态。例

表 1 SbW 的异常表现、安全目标及安全状态

系统失效	安全目标	相关子系统	安全状态
转向盘 / 轮胎自转	SG1 系统应避免车辆在行驶过程中自动转向	HWA, SWA	仍能执行转向直到车辆安全状态 仍能提供手力反馈 仍能激活或维持剩余的转向冗余能力，或者实施缓解措施 隔离或关闭故障
转向丢失	SG2 系统应避免车辆在行驶过程中丧失转向能力	HWA, SWA	
转向卡滞	SG3 系统应避免车辆在行驶过程中方向盘非预期卡滞、 SG2 系统应避免车辆在行驶过程中丧失转向能力	HWA, SWA	
反馈力矩丢失	SG4 系统应避免车辆在行驶过程中丧失手感反馈力矩	HWA	
转向盘与车轮异步	SG5 系统应避免车辆在行驶过程中上下执行器不同步	HWA, SWA	

act [package] FunctionaNew[SbW 电控单元三层监控示例]

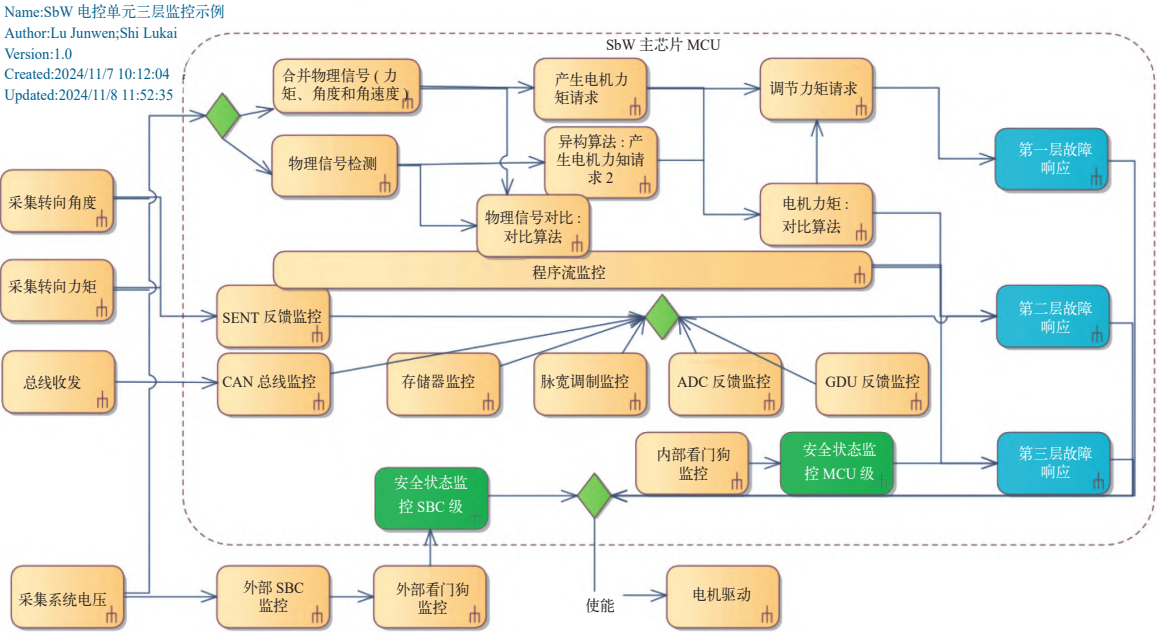


图2 基于三层监控的 HWA 软件架构示意

表 2 SbW 系统故障示例

物理模块	故障形式	导致的异常表现
扭矩传感器	值域(无效,偏差,超限等)、突变、振荡、卡滞、断开	所有异常表现
执行电机	突变、丢失、值域	所有异常表现
电机转子位置传感器	值域、突变、振荡、卡滞、断开	所有异常表现
私有总线	节点丢失、消息值域(无效,偏差,超限等)	丢失转向能力、丢失反馈能力、上下转向不同步
蜗轮蜗杆(HWA)	间隙,卡滞	丢失反馈能力、上下转向不同步

如 HWA 非预期自转向情况下,SWA 的转向角度直接切换来自实车总线请求等。

3 线控转向安全机制确认

为了验证当故障发生后,系统内的安全机制是否能有效地进行处理,基于故障注入的降级及可控性验证是常用方法之一。SbW 的故障注入验证主要考虑故障的覆盖程度、故障注入的运行工况和安全机制的判定标准。

3.1 SbW 的故障注入等效法则

SbW 的硬件元件数量繁多,每个元件又有较多的故障类型,例如仅电阻一项就可能有短路、断路以及温漂等故障。软件层面如校验错误、接收/发送失败和赋值偏差等故障,均可影响许多模块。因此,系统层面的验证按照单个元件或功能的每个故障进行注入并

不现实。

基于系统架构分析不难发现许多故障在系统层级的表现近似甚至相同,因此,可将发生相同失效的故障归纳为失效等价类(FEC),每一种失效等价类可以用一种或两种效率高且复现性高的方式来代替,并赋予阶跃突变、振荡和卡滞这三种故障特性来模拟极端状况。本文是通过软件注入算法或基于继电器的硬件注入方式来实现故障全覆盖,如表 3 所示。

3.2 SbW 安全机制验证场景设计

考虑到 SbW 的验证场景无约束性,为了实现有限的验证场景,则依据发生概率选取最恶劣的场景。场景一般包括操控参数和工况。场景暴露概率是操控参数选取的主要依据。SbW 的操控参数使用曝光概率等级 E2 ~ E4,如表 4 所示。

类似地,基于车辆横向运动验证要求,SbW 的验证场景可以选取极限工况,例如蛇形绕桩、绕“8”行驶等。

结合操控参数和工况,可以形成数量有限且覆盖全面的 SbW 验证场景,如表 5 所示为例。

3.3 SbW 安全机制可控性客观判定机制的建立

SbW 安全机制通过可控性进行评判。可控性参数指标包括但不限于车辆质心横向位移、车辆质心侧向加速度、车辆质心的横摆角速度以及转向操控力等。

测试要求在不通知驾驶员的情况下,进行故障注入,并且记录参数指标并观察车辆是否仍然能按照横向轨迹要求行驶。主要步骤有如下:

表 3 SbW 故障等效示例

失效类型	潜在故障原因	涉及的元件	等效注入
执行电机力矩突降	电源供电突降 计算值溢出 执行电机驱动电路故障	电压转换模块 BSW、APP H 桥、GDU	方法 1:纯逻辑注入,软件模块“产生电机电力矩请求”中添加因子和偏差输入标定接口
			方法 2:软件控制硬件注入,相分离器开关输入接口,模拟 U/V/W 三相的不同开断组合
			方法 3:硬件注入,电机三相 U/V/W 输出引脚连接外部继电器,通过实时控制信号实现通断和短路
传感器值无效	磁体损坏 传感器接插件损坏 传感器输出开路	磁体、接插件、线束 传感器内部电路引线	方法:硬件注入,通过继电器对传感器输出信号进行开路、短路、地/高电平连接等
蜗轮蜗杆损坏	机械磨损,装配间隙,摩擦过大	蜗轮蜗杆间隙,调节装置	方法:纯逻辑注入,软件模块“产生电机电力矩请求”中添加噪声信号或偏差标定接口

表 4 曝光率等级 E2 ~ E4 的工况参数值示例

操控参数	E2	E3	E4
	(<1 % 的平均运行时间)	(1 ~ 10 % 的平均运行时间)	(>10 % 的平均运行时间)
车速 V_x	>180 km/h	>130 km/h	$\leq$ 130 km/h
侧向加速度 a_y	3.5 ~ 5 m/s ²	1.5 ~ 3.5 m/s ²	0 ~ 1.5 m/s ²

表 5 SbW 验证场景指标示例

工况名称	操控步骤概述	故障模式	失效源
直线行驶	以 $V_x=0\sim 200\text{ km/h}$ 在直线车道上保持直行	阶跃, 振荡	HWA/RWA
稳态圆周行驶	以 $a_y\geq 5\text{ m/s}^2$ 在半径为 80 m 的圆周车道上匀速行驶	阶跃, 振荡	RWA
蛇形绕桩	以 $a_y\geq 5\text{ m/s}^2$ 和 $V_x=60\text{ km/h}$ 通过标桩间距为 18m 的蛇形试验区域	阶跃, 卡滞	HWA/RWA
绕“8”行驶	以 $V_x=26\text{ km/h}$ 在半径为 9 m 的“8”字形车道上行驶	阶跃, 卡滞	HWA/RWA
双移线	以 $V_x=50\text{ km/h}$ 行驶, 进入标准双移线变道区域	阶跃, 卡滞	RWA

(1) 没有故障, 并在给定运行场景, 记录正常系统表现和数据。

(2) 关闭或规避安全机制, 在相同运行场景下, 基于可控性 C0 ~ C1 的要求确定故障持续时间以及故障的特性值边界, 例如手感模拟力阶跃跳变的最大幅值差, 转向卡滞时间长度等。

(3) 开启安全机制, 在相同运行场景下, 注入 (2) 确定的故障, 并记录数据。

(4) 结合 (1) ~ (3) 物理参数变化以及驾驶人主观感受, 判定是否可控。

4 基于 DIL 的 SbW 安全设计

低成熟度产品的安全机制设计与验证是设计开发中的重点, 开发阶段越是后期, 考虑的安全机制越全面, 相应测试条件也越严苛。因此, 基于半实物仿真的测

试方法孕育而生。相较于实车验证受到安全、条件等方面的局限, 半实物仿真的测试参数更易调校, 且故障注入精度更高, 形式更多元, 这将大大减少验证安全机制的时间。

4.1 SbW 的 DIL 系统基本架构

DIL 是把真实的 SbW、车辆及其运行环境仿真模型和驾驶员联系在一起, 如图 4 所示。

DIL 由转向盘输入装置、车轮转向负载模拟电机、转向节模拟器、转向系统硬点调节机构、控制柜及上位机组成。转向盘输入切换装置由带有离合器的空心轴电机组成, 可以提供角度或扭矩输入自动转向或 / 和驾驶人控制模式。装有角度传感器和扭矩传感器的转向盘输入装置采集输出角度和力矩并提供给实时系统, 拉杆负载电机配合转向节模拟器在横拉杆端动态施加齿条力或位移载荷, 横拉杆端的力传感器及位移传感

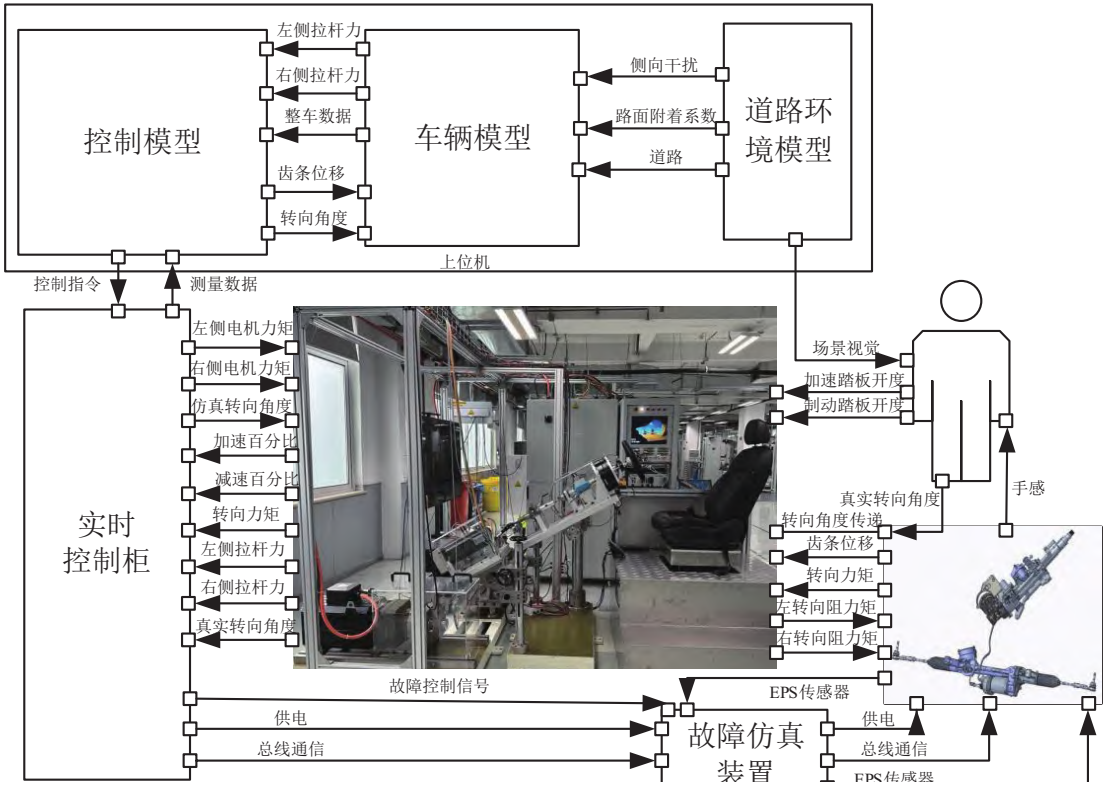


图 4 DIL 实时系统机电耦合集成示意

器实时采集拉杆力和拉杆位移。

DIL 系统中，HWA 的上管柱与转向盘输入装置相连，用来实现人或转向电机的转向运动输入。车轮执行器（SRA）的拉杆外球头和转向节模拟器相连，并由左右负载电机传递力。HWA 和 SRA 的供电接口与控制柜的可编程电源相连接，总线接口与上位机的实时总线通道相连并与模拟车辆节点进行交互。转向盘转向模拟电机、车轮转向负载模拟电机、可编程电源以及车辆模拟总线节点都由上位机基于仿真模型实时并行控制。

4.2 DIL 系统的故障注入模拟机制

根据等效故障的概念，DIL 主要是从硬件和软件两个方面对 SbW 实现故障注入。硬件故障注入主要针对 SbW 系统接口的物理故障，包括传感器接口、供电接口、总线接口和机械连接等。该单元在信号传输完整通路之中添加单个串联继电器和若干并联继电器，控制继电器的通断实现信号的短路和断路。

软件故障注入主要通过逻辑信号变化来仿真 SbW 系统失效表现，包括 SbW 的主动电机输出力矩请求、电机转子传感器输出、硬件信号故障和机械零部件失效物理信号故障等。其工作方式是根据硬件软件接口（HSI）进行逻辑信号阻拦或直接篡改等实现系统失效，故障特性如表 6 所示。

4.3 基于 DIL 的 SbW 故障自学习自动注入

基于实车的安全机制可控性验证存在较大的不确定因素，例如外界干扰、操控误差以及人为的随机性等。然而在 DIL 系统中，可以解决以上问题，使得不确定因素足够减少。其原理是根据可控性试验标准指标要求，针对当前的操控场景进行操控参数监控，一旦符合条件即触发故障注入，如图 5 所示。因此，由于试验标准一致，即使人为或全自动操控各不同，但仍能实现故障注入场景的一致性且可重复。例如指标要求中转向盘转角达到 90° 后 5 s 且车速保持为 200 km/h，DIL 系统可以根据虚拟驾驶场景中的操控参数，例如：车速稳定值、转向角度稳定值和持续时间等进行判断。

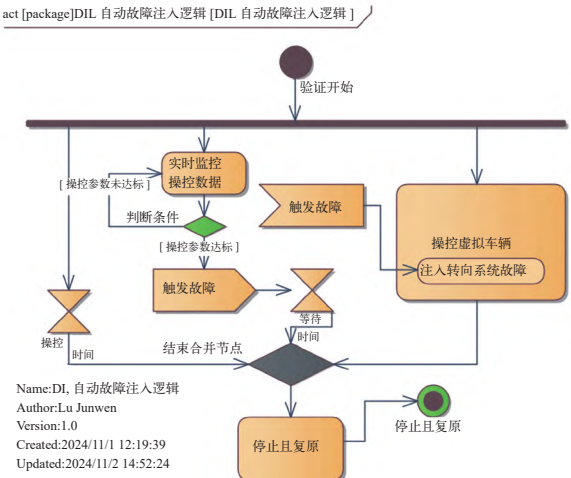


图 5 基于 DIL 故障自学习注入逻辑图

5 DIL 自转安全机制验证

结合表 1 和表 5，针对安全目标“SG1 系统应避免车辆在行驶过程中自动转向”，以 HWA 非预期转向为例，对其的安全机制进行分析和研究。

HWA 由于手感电机的力矩突变，导致发生非预期的自转向，此时，需要确保故障可以被正确隔离，以及系统降级并能使车辆达到安全状态过程中 SbW 仍然保持可控。

本文分别对直行和稳态绕圆场景工况，驾驶员在 DIL 中根据虚拟场景进行操控，故障自学习注入机制判断当前的虚拟车辆数据根据给定的条件进行自动触发且驾驶员不可预测。相同工况下对开启安全机制和关闭安全机制的产品进行两次观测，可控性观测数据如图 6 和图 7 所示。

在虚拟环境下，选取故障注入瞬间时刻，车辆相对车道的偏移情况如图 8 和图 9 所示。相同驾驶员的驾驶习惯下，在无安全机制的系统在力矩特性在 4 N·m 处 HWA 非预期自转使得车辆驶出车道，相同的故障和力矩特性下。在添加了安全机制后，即使 HWA 非预期自转，但车辆有较轻微的影响但立即切换总线数据使得车辆仍然可以保持在车道内。

表 6 基于 DIL 的故障模拟方法示例

故障特性	故障注入参数接口	方法
阶跃突变	起始值、终值、变化率、持续时间	故障（值域）从起始值以给定的变化率跳变至终值 故障（控制信号）数字量跳变
卡滞	终值、持续时间	故障（值域）保持终值至给定的卡滞时间
振荡干扰	幅值、频率、占空比、波形（方波），持续时间	故障（值域）以给定幅值与频率的 50 % 占空比的方波

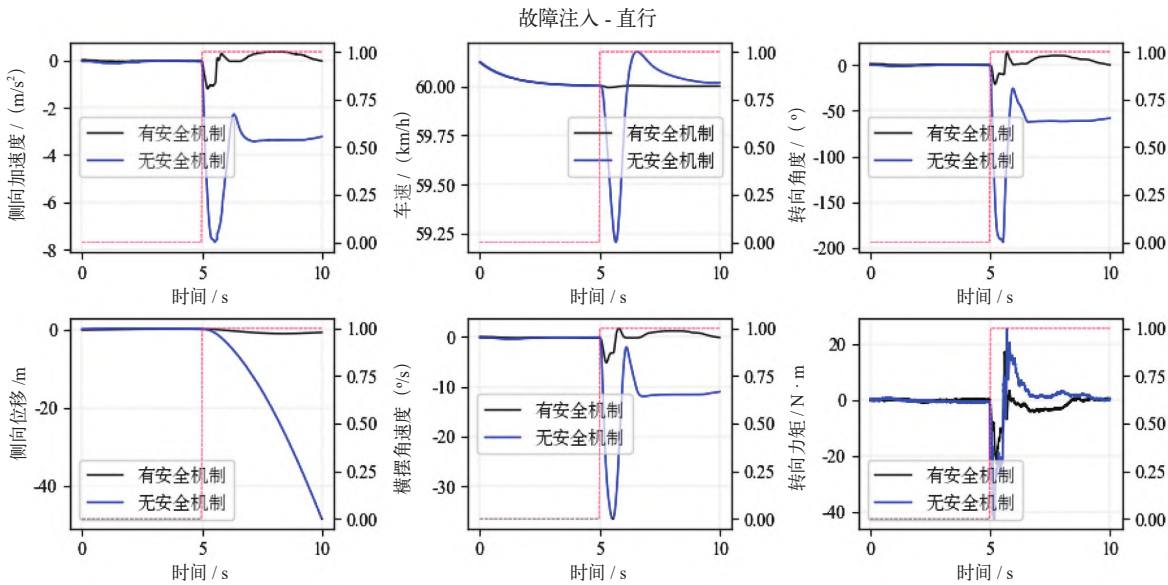


图6 直行工况下故障注入前后数据对比

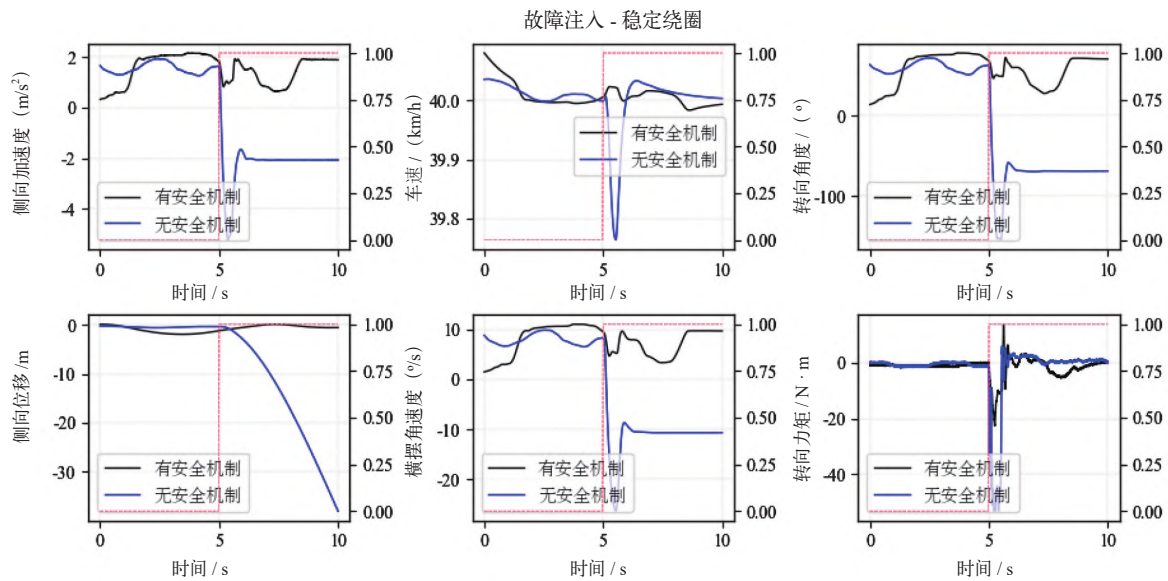


图7 稳态绕圈工况下故障注入前后数据对比

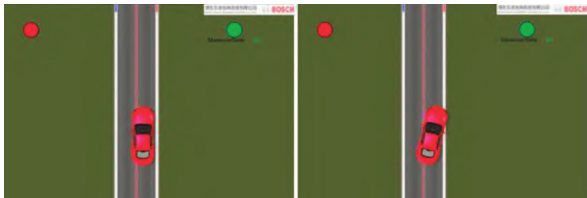


图8 直线工况下有无安全机制车道偏移对比

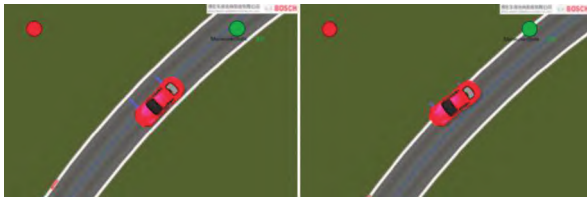


图9 稳态绕圈工况下有无安全机制车道偏移对比

6 结语

本文阐述了 SbW 从安全目标分析到安全机制设计和验证的过程，主要基于系统架构对可能存在的故障以及如何监控和消除该故障进行梳理，通过等效分析对故障和工况进行了有效区间的筛选，并在作者开发

的硬件在环 DIL 系统上，在开发过程中，对低成熟度的安全机制进行确认和优化。另外，DIL 不再只局限于系统合格性测试，还能在系统及安全设计和开发阶段，实现基于测试结果的产品开发。DIL 还能实现重复性高的故障自动化注入以及虚拟场景和可控标准的多元化开发，对“可控性”评价带来更客观的判断依据。

虚拟工况的真实性以及实车六自由度感受是DIL的一大难点,当前的研究在和不同车型实际数据对标仍在进行中,未来将会把实车六自由度进行解耦,并且使SbW的安全机制判定维度更加丰富。

参考文献

- [1] 《中国公路学报》编辑部. 中国汽车工程学术研究综述·2023[R]. 中国公路学报, 2023,36(11): 1-192.
- [2] 李赛赛, 梁东, 郭瑞玲, 等. 乘用车转向功能安全主客观测试评价方法[J]. 汽车实用技术, 2023.019.029: 149-155.
- [3] 高乐, 刘秋铮, 陈慧. EPS系统功能安全测试方法[J]. 电子技术与软件工程, 2020,06: 28-30.
- [4] 蒯家琛, 王伟, 温敏, 等. 基于硬件在环的EPS系统故障诊断及自动化测试[J]. 北京汽车, 2021,04: 44-47.
- [5] 李傲寒. 基于ISO26262的乘用车线控转向系统功能安全研究[D]. 长春: 吉林大学, 2024.
- [6] DIN 70065. Road Vehicle-Requirements for a "Steer-by-Wire(SbW)-System[S]. 2024.
- [7] E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units[S]. 2015.
- [8] ISO 15037-1-2019 Road Vehicles-Vehicles dynamics test methods Part 1:General conditions for passenger cars[S]. 2019.
- [9] ISO 4138-2021 Passenger cars - Steady-state circular driving behavior - Open-loop test methods[S]. 2021.
- [10] 国家市场监督管理总局, 中国国家标准化管理委员会. 乘用车紧急变线试验车道第1部分: 双移线 GB/T 40521.1-2021[S].2021.
- [11] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 汽车直线行驶稳定性试验方法 GB/T 41600-2022 [S]. 2022.
- [12] 陆俊文, 等. 一种多功能汽车转向系统在环测试试验台: ZL202223208540.8[P], 2023-06-16.
- [13] 高立臣, 等. 一种手自一体转向输入装置: ZL202322789716.1[P], 2024-05-17.



AMTS
Automotive
Manufacturing
Technology & Material
Show

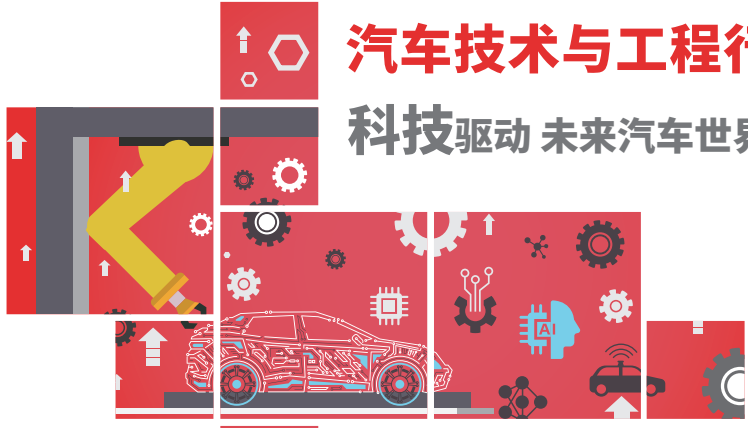
上海国际汽车制造技术与装备及材料展览会

Shanghai International Automotive Manufacturing Technology & Material Show

科技 Technology	材料 Materials	设计研发 Design and Development	工艺 Processing	装备 Equipment	质量 Quality	装配 Assembly	工程 Engineering
------------------	-----------------	-----------------------------------	------------------	-----------------	---------------	----------------	-------------------

SINCE
2004

2025.7.9-11
上海新国际博览中心
W1-W5, E1-E3馆
RX Hengjin
励进展览(上海)有限公司
www.shanghaiAMTS.com



汽车技术与工程行业盛会

科技驱动 未来汽车世界

一站式掌握汽车技术及工程
前沿技术与解决方案



预登记参观



立即扫码预登记
立省50元观展门票



添加AMTS & AHTE小秘书
获取更多展会信息