·智能驾驶“人–车–环境”安全风险分析专题综述·

系统理论过程分析在自动驾驶安全分析中的应用综述*

张玉新[1]　吕周杭[1]　张淼[2]　胡宏宇[1]

（1.吉林大学汽车仿真与控制国家重点实验室，长春 130025；2.中国汽车技术研究中心有限公司汽车标准化研究院，天津 300300）

【欢迎引用】张玉新，吕周杭，张淼，等．系统理论过程分析在自动驾驶安全分析中的应用综述[J]．汽车文摘，2024(8)：17-25.

【Cite this paper】ZHANG Y X, LÜ Z H, ZHANG M, et al. A Review on Application of Systems Theoretic Process Analysis in Automated Driving Safety Analysis[J]. Automotive Digest (Chinese), 2024(8): 17-25.

【摘要】安全分析是汽车开发过程的重要一环，随着自动驾驶系统复杂性提升，传统安全分析方法面临着挑战。首先，将故障树分析（FTA）、故障模式与影响分析（FMEA）、危险与可操作性分析（HAZOP）这些传统安全分析方法，与系统理论过程分析方法（STPA）进行对比，重点阐述使用STPA进行自动驾驶系统安全分析的优势。其次，详细论述了STPA在自动驾驶功能安全、预期功能安全、信息安全及人机交互系统等重要领域的应用现状。最后，从拓展STPA分析方法、加强分析与验证闭环、扩大应用范围的角度对STPA在自动驾驶领域的应用进行了展望。

关键词：系统理论过程分析；自动驾驶；安全分析

中图分类号：U463.6；N941　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20230245

A Review on Application of Systems Theoretic Process Analysis in Automated Driving Safety Analysis

Zhang Yuxin[1], Lü Zhouhang[1], Zhang Miao[2], Hu Hongyu[1]

（1. Jilin University, State Key Laboratory of Automotive Simulation and Control, Changchun 130025; 2. Auto Standardization Research Institute, China Automotive Technology and Research Center Co., Ltd., Tianjin 300300）

【Abstract】Safety analysis is an integral part of the automotive development process, as the complexity of automated driving systems increases, traditional safety analysis methods are facing challenges. Firstly, the advantages and disadvantages of traditional analysis methods, such as Fault Tree Analysis (FTA), Failure Modes and Effect Analysis (FMEA), and Hazard and Operability (HAZOP), are compared with the System Theoretic Process Analysis (STPA), especially the advantages of STPA for the safety analysis of automated driving systems. Secondly, the current status of STPA applications in essential areas, such as Functional Safety, Safety of the Intended Functionality (SOTIF), Cyber Security, and Human Machine Interface (HMI), are discussed in detail. Finally, the application of STPA in automated driving is prospected from the perspectives of expanding the STPA analysis, integration of analysis and verification, and extending application areas.

Key words: System theoretic process analysis(STPA), Automated driving, Safety analysis

0　引言

随着科技的高速发展，汽车面临的安全问题也愈发丰富，主要集中在功能安全、预期功能安全、信息安全3个领域。为提高智能网联汽车产品性能和安全运行水平，推动智能网联汽车产业健康有序发展，工业和信息化部会同公安部组织起草了《关于开展智能网联汽车准入和上路通行试点工作的通知（征求意见稿）》[1]。该通知对企业安全保障能力做出了包括功能安全保障、预期功能安全保障、网络安全保障在内的能力要求。

在汽车开发流程中，安全性分析和验证是重要一环。传统的安全分析方法如故障树分析（Fault Tree Analysis，FTA）、故障模式与影响分析（Failure Modes

*基金项目：国家自然科学基金面上项目(52075213)；汽车标准化公益性开放课题(CATARC-Z-2022-01536)。

and Effect Analysis，FMEA）、危险与可操作性分析（Hazard and Operability，HAZOP）均存在局限性，无法充分应对预期功能安全和信息安全问题[2]，而由Leveson提出的系统理论过程分析（Systems Theoretic Process Analysis，STPA）方法由于其特有的系统视角，能够很好地解决上述问题。在此背景下，STPA方法在自动驾驶领域中的应用愈发增多。

目前，国内外学者针对STPA在自动驾驶领域应用的研究主要集中于STPA方法在自动驾驶系统中的应用，包括在不同领域如功能安全、预期功能安全、信息安全、人机交互的应用。本文首先通过对比法阐述了STPA方法用于自动驾驶系统安全分析的优势。其次，以STPA的实际应用为例，通过列举法介绍STPA在自动驾驶系统重要领域的应用现状，最后对其前景进行展望。

1　安全分析方法

1.1　“演绎”方法与“归纳”方法

“演绎”方法即假设系统以一定方式失效，通过推导找出哪些系统或组件的行为致使失效。演绎方法是从一般到个别的推理，能够缩小分析的范围，具有局部性的特点。“归纳”方法假设一个或多个组件的特定存在状态，通过安全分析确定该条件对系统的影响。在实际生产中，归纳方法通常受外界条件限制，因为对于大多数系统，很难去识别所有可能的系统危险或所有可能的组件故障模式[3]。

事件链模型以事件链的形式描述事故，将事故原因解释为发生在特定时间序列中的一系列离散事件，其优势在于能够直观地显示导致事故的系列事件[4]。Heinrich[5]提出的多米诺骨牌模型与Reason[6]提出的瑞士奶酪模型（Swiss Cheese Model, SCM）均属于事件链模型。目前，常用的事件链模型包括故障树分析（FTA）、故障模式与影响分析（FMEA）。

故障树分析（FTA）属于“演绎”方法，即通过该方法确定给定的系统状态如何发生，是一种“自上而下”的分析方法[3]，见图1。分析从故障树的顶部事件延展到故障树的叶子，进而分析得到在其环境中导致顶部事件发生的故障组合方式[7]，故障可以是与组件故障、人为错误或其他因素相关的事件。

故障模式和影响分析（FMEA）属于“归纳”方法，即通过该方法确定可能的系统状态，是一种“自下而上”的分析方法[3]，如图2所示。FMEA首先对系统进行分析，进而列出分析对象尽可能多的潜在故障模式，并对失效模式的原因、影响以及现有控制方法进行分析，最后根据严重程度（S）、暴露度（O）、可检测程度（D）的评价标准确定评价值，计算出风险优先级数（Risk Priority Number，RPN）[8]。FMEA也是评估系统可靠性的有效工具。

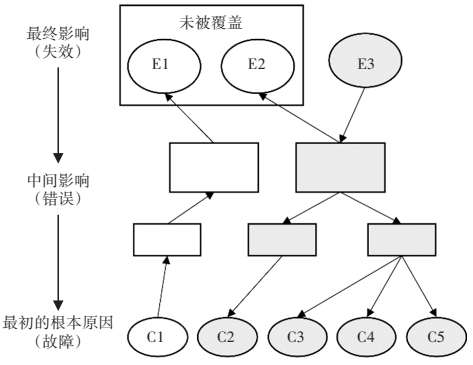

图1　自上而下的FTA方法

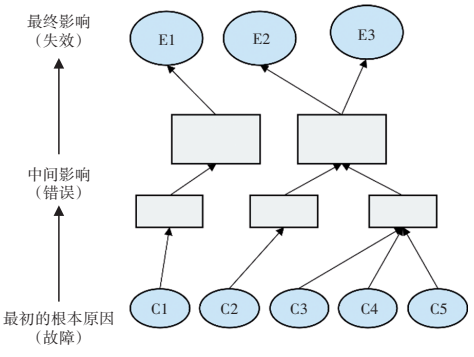

图2　自下而上的FMEA方法

除故障模式和影响分析（FMEA）外，安全分析领域内的“归纳”方法还有故障模式、影响及其诊断分析（Failure Modes Effects and Diagnostic Analysis，FMEDA）和事件树分析法（Event Tree Analysis，ETA）等。

1.2　“探索性”方法

“探索性”方法从系统不当行为（偏差）开始，探索可能的影响和可能的原因，HAZOP评估即属于“探索性”方法。也可以说，HAZOP评估介于“归纳”方法和“演绎”方法之间，因为HAZOP根据“演绎”方法假设顶部事件（偏差），随后遵循“归纳”方法探索系统行为[9]。

HAZOP是过程危险分析（Process Hazard Analysis，PHA）方法的一种[10]，通过引导词辅助列出系统及系统元素可能存在的与设计意图的偏差，假设系统存在不当行为，识别其可能导致的危害[11]。随后对每个节点中偏差的原因进行头脑风暴，并确定导致每个原因的事件序列[12]。

1.3　系统理论过程分析

系统理论过程分析（STPA）同样属于“探索性”方法，STPA是基于系统理论事故模型和过程（STAMP）

的危害分析方法。Leveson[13]描述了STPA和STAMP的原理，认为应将系统视为一个整体，关注组件交互而非仅关注单个组件的作用。安全分析的重心应从防止组件出现故障转变为通过施加安全约束完善控制过程[14]。

STPA将安全视为系统的控制问题。旨在通过识别不安全控制行为，找到因果场景，进而消除或控制系统中的危害，它可以应用于系统生命周期的任何阶段[15]。STPA的基本步骤包括定义STPA分析工作的目的和范围、建立分层控制结构、列出不安全控制行为、识别致因场景、提取安全需求[16]。现在，STPA广泛应用于各个行业，包括军事[17]、海事[18]、医疗[19]、航空[20]、核电[21]、智能交通[22]等领域，本文主要讨论的是STPA在自动驾驶领域的应用现状。

1.4 STPA与其他安全分析方法的比较

当使用FTA、FMEA等事件链模型进行安全分析时，分析人员将事故描述为一系列事件的结果。而随着技术的发展，自动驾驶系统愈发复杂，线性的事件链无法对其充分分析，经常会忽略事故的潜在原因[23]。

在FMEA中，系统功能应用被分配给子系统与组件，进而确定并分析失效模式和失效原因，计算风险优先级数(RPN)并进行风险等级排序。FMEA是聚焦于单个部件失效模式及其影响的归纳分析方法，更多考虑部件的可靠性，很少用于分析基于同一原因的故障或多个故障[24]。在一项对汽车前向避障系统的分析中，与STPA相比，FMEA能识别出更多的部件故障危害，而STPA的优势则在于寻找已识别危害的因果因素，比传统的危害分析方法考虑更多类型的危害原因[25]。

FMEA只能用于分析的后期，适合用于检查现有设计是否安全[26]。与开发流程后期对系统的迭代相比，在开发早期进行修改会降低成本并提高效率。STPA支持在系统开发早期的使用，也支持在开发流程中任意环节的迭代，在早期概念开发阶段就可以投入使用。

相较于FTA、FMEA，介于“归纳”方法和“演绎”方法之间的HAZOP分析包括对人为错误和其他组件影响的分析。但在HAZOP评估中，有时指导词和参数的不同组合可能会产生相同的偏差，这会导致研究效率的降低[27]。同时HAZOP通过演绎探索原因，不能准确得出导致偏差的所有原因的组合。基于以上原因，HAZOP仅适合用于简单的功能系统分析[24]。在对自动驾驶系统进行安全分析时，HAZOP中的引导词并不完全适用自动驾驶系统，HAZOP也不具备系统生成相关引导词的方法[28]，这种情况限制了上述方法在自动驾驶系统领域的应用[29]。

相较于FTA与FMEA等事件链模型，STPA将子系统交互、组件交互都纳入分析过程，其中的组件可能不存在失效。而传统的基于因果关系的事件链模型强调事件之间的线性关系，即每个事件都与前面的事件线性相关，无法考虑到组件交互对系统的影响[30]。随着系统越来越复杂，事件链无法满足分析需求，这正是STPA的系统视角的优势。Koelln[2]将STPA、FTA和FMEA方法用于自动驾驶汽车的安全分析，发现STPA能够识别大量的失效类型，并在分析中包括跨系统因素。除此之外，STPA可以纳入人为错误因素，这是FTA与FMEA不具备的，关于STPA在自动驾驶领域人机交互上的应用将在后续章节详细讨论。

对于自动驾驶相关的软件密集系统，STPA认为软件不会失效，有缺陷的需求(或实现)以及与系统其他部分的不安全交互才会导致危害发生[31]。因此对于软件密集系统，预防相关事故发生需要完整的软件行为安全相关需求/约束[30]。综上，使用STPA、FTA、FMEA、HAZOP对自动驾驶系统进行安全分析的效果对比如表1所示。

表1 不同安全分析方法的对比

评价维度	FTA	FMEA	HAZOP	STPA
关注组件间交互	差	差	中	优
关注部件可靠性	中	优	中	中
纳入人机交互	差	差	中	优
使用成本	低	低	高	高
复杂度	低	低	高	高
适用的开发阶段	设计	设计/生产	设计	设计/验证
纳入网络攻击	否	否	否	能
关注系统间交互	否	否	否	能
抽象/具体	具体	具体	抽象	抽象

2 STPA在自动驾驶系统中的应用

Shi[32]通过操作原理对驾驶自动化系统进行分类，包括信息提醒与警示类安全系统(如车道偏离预警、变道盲区预警系统、前方碰撞预警等)、持续车辆控制的驾驶自动化系统(如自适应巡航、高速公路自动驾驶、自主代客泊车等)、瞬时车辆控制的主动安全系统(如防抱死制动系统、电子稳定控制系统、自动紧急制动等)。上述系统均属于软件密集系统，适用于STPA方法，并存在许多应用实例。

2.1 STPA用于功能安全

在功能安全领域的应用中，将STPA与ISO 26262

中的危害分析和风险评估(Hazard Analysis and Risk Assessment,HARA)结合对自动驾驶系统进行系统的分析,如图3所示。

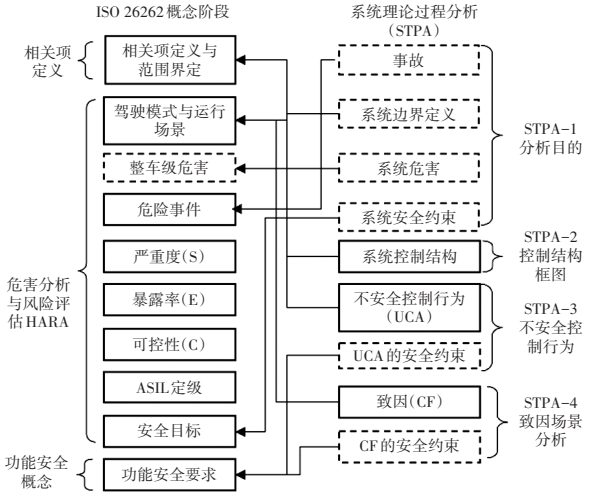

图3 STPA与HARA结合

周逢军[33]使用STPA对前向碰撞预警(Forward Collision Warning,FCW)系统进行安全分析,得出影响整车功能安全的主要事故类型与系统级危害类别。Sharma[34]使用STPA对自动紧急制动系统(Autonomous Emergency Braking,AEB)进行安全分析,通过分析与控制流程图相关的组件,确定不安全控制行为对应的场景和因果因素。马海涛[35]使用STPA对自动车道保持系统(Automated Lane Keeping System,ALKS)的人机交互系统进行安全分析,最终提出相应安全设计需求。

除了分析系统级别与组件级别的危害之外,STPA还可以从整车级别对自动驾驶汽车进行安全分析,进而细致划分不安全场景,制定不同级别的安全需求[36]。相较于传统的事件链模型,STPA对组件交互、系统交互的关注使其可以识别更多的致因场景[2]。Abdulkhaleq[37]使用STPA对全自动驾驶汽车进行安全分析,并认为STPA是推导安全约束的有效工具。

2.2 STPA用于预期功能安全

STPA在预期功能安全(SOTIF)流程中也有许多应用实例[38,39]。STPA步骤可以映射到SOTIF流程[40-42],二者存在很强的适配性,如图4所示。通过映射可以得到STPA的致因场景与SOTIF性能局限和触发条件之间的关系,并以此分析系统[42]。SOTIF流程旨在减少不安全的象限,即减少区域2和区域3并将它们移动到区域1。STPA可以通过安全分析揭示未知的不安全场景以减少区域3,Haixia[43]将STPA运用于高速公路领航(HighWay Pilot,HWP)的场景分析,将由未知场景导致区域3中潜在危险行为的概率降低到可接受水平。Shimizu[44]以自动紧急制动系统(AEB)为研究对象,提出了一个基于SOTIF的系统性能限制评估框架,结合STPA识别由于传感器攻击引起的危险场景,并评估场景中的性能限制。STPA还可以用于输出测试场景,SAE J3187以低速自动驾驶系统为研究对象,通过STPA得到的不安全控制行为与损失场景生成测试场景及其要素,生成的测试场景有助于提高自动驾驶系统的安全性[41]。

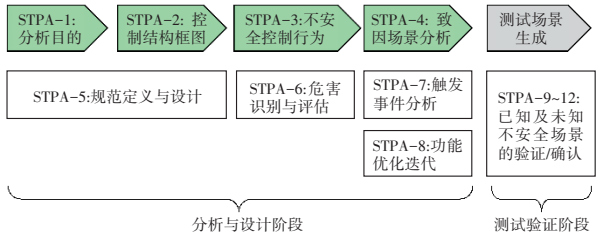

图4 STPA映射到SOTIF流程

2.3 STPA用于信息安全

STPA不仅可以用于功能安全分析和预期功能安全分析,还可以用于信息安全分析,信息的安全传输对于车辆整体安全有着关键作用[45]。为了保护软件密集系统免受外部攻击尤其是网络攻击的影响,Young和Leveson[46]提出了STPA的扩展STPA-sec,首次将信息安全问题纳入安全分析过程。在信息安全领域,STPA-sec具有传统安全分析方法不具备的优势。STPA-sec先定义损失,在安全评估开始时建立优先级,从系统功能的角度出发进行安全评估,将网络安全定义为战略问题,而非传统安全分析方法里的战术问题。并且,STPA-sec将外部攻击的产生归于系统结构缺陷,而非来自外部的事件,通过对系统结构的分析得出改进建议,进而通过这些设计上的更改,减少或者消除网络攻击的影响[47]。

Schmittner[48]提出了改进的STPA-sec,并将其用于分析混合动力汽车的电池管理系统。Friedberg[49]将STPA过程中的功能安全分析和STPA-sec过程中的信息安全分析集成到新的框架STPA-SafeSec中,并考虑二者的相互影响,扩大了STPA的适用范围。

2.4 STPA用于人机交互系统

STPA还可以用来分析自动驾驶系统与其他系统(例如交通参与者、环境、人类驾驶员)之间的各种交互,并为自动驾驶系统生成不同类型的安全需求[50]。France[51]提出了用于分析人机交互(Human Machine Interface,HMI)的人类控制器模型STPA-Engineering for Humans,可以用于识别与人类行为相关的场景。该模型包括控制动作选择、心智模型、心智模型更新

3部分，如图5所示。

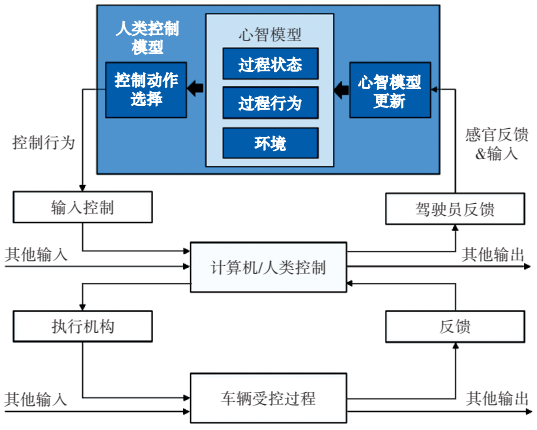

图5　控制结构中驾驶员的人类拓展模型

人机交互设计好坏与驾驶员执行驾驶任务的质量直接相关，在驾驶员驾驶车辆执行驾驶任务时，交互受各种内部和外部因素影响[52]。对汽车HMI的评价主要使用3个基本标准[53]：可用性[54]、注意力分散[55]和驾驶员可接受性[56]。以上的3个基本标准构成了车辆HMI的评价体系，HMI的设计也往往围绕着这3点展开。HMI通常使用听觉和视觉反馈方法向驾驶员提供旨在传达系统/车辆状态或潜在危害情况的信息。SAE J3187提出了第3种反馈方法“触觉”，并推荐在STPA方法的安全评估过程中使用触觉作为反馈方法[41]。STPA可以将驾驶员作为功能元素加入控制结构中，进而更系统地分析不安全控制行为和相关致因场景，得到相应安全需求并对车辆HMI进行更新，改善人机交互体验。将STPA应用于人机交互，可以使分析人员识别人类操作员对当前流程状态、行为和环境的认知，及其与心智模型更新的可能组合。这有助于分析人员识别未知事故的原因，同时方便向上追溯，增强了系统的可维护性[76]。

Koelln[57]将STPA用于分析SAE 4级的人机交互系统，通过在车辆系统范围内以及在更高层次上的人机界面中进行安全分析，从而明确事故原因。Chen[58]使用STPA对一款处于开发阶段的SAE 4级车辆中可能存在的不充分人机交互进行识别，说明了STPA在人机交互中的适用性。马海涛[35]以自动车道保持系统（ALKS）的人机交互系统为研究对象，将STPA分析得到的结果作为后续接管策略设计和接管界面设计的依据。

综上所述，STPA不仅可以用于提出自动驾驶系统整车级安全需求，还可以用于功能安全、预期功能安全、信息安全以及人机交互的设计与开发。该方法既可以满足多种开发需求，也具备应用于自动驾驶系统全周期开发的能力。

3　STPA的集成应用

系统视角使STPA在对自动驾驶系统的安全分析中具有独特的优势，如充分考虑系统交互与组件交互、可以纳入人为错误与外部干扰因素等。但作为一种安全分析方法，它在低层次部件失效的关注上仍有不足，也缺少对分析结果的验证过程。通过STPA与其他安全分析方法的集成、STPA分析阶段与验证阶段的集成，可以很好地对STPA的劣势进行补齐，使安全分析过程更加高效。STPA的集成应用总结如表2所示。

表2　STPA的集成应用

序号	STPA的集成应用方式	相对于单独使用STPA的优势	文献
1	STPA与FMEA的全步骤集成	在STPA基础上更关注具体部件的失效	[60]
2	使用HAZOP与STPA的UCA分析集成，定义整车级别的危害事件	使用HAZOP引导词扩充分析范围，获得更多的潜在车辆级危害	[42],[61],[62],[63]
3	使用STPA的致因场景与FMEA结合分析组件级别危害	得到了在分析单个组件时无法获得的危害	[61],[63]
4	综合STPA步骤4得到的因果场景和FTA的危险最小割集	更好地量化失效原因	[62]
5	综合STPA与HARA的分析流程	能够对风险进行评估，提出更具体的功能安全需求	[29],[64]
6	在STPA步骤后加入测试验证过程	验证STPA分析得到的安全需求是否有效	[65],[67],[68],[69]
7	建立STPA分析对象的模型	使系统的结构可视化，能够进一步验证STPA中得出的安全需求	[65],[66],[67],[70],[71]

3.1　STPA与其他安全分析方法集成

传统的安全分析方法如FTA、FMEA、HAZOP往往关注低层次部件的故障行为，这使其适用于简单的功能系统分析。STPA与传统的安全分析方法具有各自的优势，因此二者的结合可以使安全分析更加全面。

最简单的集成方法是使用STPA与其他安全分析方法分别对系统进行分析，最后结合分析结果，推导出系统的功能安全要求和附加安全要求[59]。还有的集成方法是将STPA与其他分析方法集成，例如冯浩[42]根据HAZOP引导词定义STPA的不安全控制行为。Chen[60]提出一种集成STPA与FMEA的方法STPAFT，集成后的方法保留了STPA的优势，还可以进行风险评估，能够获得更详细的因果因素，对系统的描述也更加清晰。

STPA也可以与多个安全分析方法集成，Capito[61]使用HAZOP和STPA步骤3分析车辆级危害，使用

FMEA和STPA步骤4分析车辆整体安全。刘逸恒[62]使用HAZOP和STPA对AEB系统分别进行整车级危险识别，综合STPA分析得到的因果场景和FTA的危险最小割集，最终得到主要失效成因结果。Christopher等[63]以通用常规液压制动系统为研究对象，使用HAZOP和STPA步骤3方法进行危害分析，输出车辆级别的危险列表，并根据ISO 26262定义为每个危险分配ASIL。随后使用FMEA和STPA步骤4进行安全分析并推导安全需求。

通过STPA与安全标准流程的集成，可以为每个危害事件分配ASIL等级，实现风险评估[64]。陈君毅[29]提出一种结合STPA方法与现有安全标准流程的自动驾驶汽车安全分析方法，并将该方法应用于SAE L3级自动驾驶清扫车的自动驾驶控制单元。Post[64]使用HARA对潜在风险级别进行分类，并用HARA识别车辆级危害，用STPA识别不希望出现的控制措施。

3.2 STPA分析阶段与验证阶段的集成

STPA往往存在着分析效果依赖于工作组成员经验、缺乏检查STPA分析效果的验证阶段等缺点，通过使用其他工具或增加流程，可以有效地改进安全分析流程，得到更好的分析效果。

首先是STPA与测试验证过程的集成，通过增加验证过程使STPA分析过程更加模式化，也使其分析效果更加直观，实现对STPA分析结果尤其是控制结构更改结果的应用与验证，有效提高安全分析的效率。Dakwat[65]将STPA与模型检验相结合，通过增加仿真和测试验证过程，补充对不安全控制行为的识别，并验证安全约束在减少危险场景上的有效性。Salehi等[66]将建模工具Event-B用于STPA步骤中，用以验证设计是否满足了安全需求。Abdulkhaleq[67]提出一个集成STPA与安全验证的流程，首先通过STPA导出车辆软件密集系统的安全需求，随后构建软件控制器的安全行为模型，最后进行包括软件测试和模型检查的安全验证。陈君毅[68]首先使用STPA对自动驾驶决策系统进行安全分析，随后对分析结果进行策略设计与试验验证，最终得到有效的安全策略并由此改进系统。郭菲菲[69]将STPA用于分析全自动泊车辅助系统，针对危害事件的触发条件改进系统结构，最后通过硬件在环测试（Hardware-In-the-Loop，HIL）和实车测试实现验证过程。

除了增加测试验证过程，还可以使用其他工具更好地利用STPA安全分析的结果。王克克[70]使用STPA对信息系统风险评估行为STAMP模型进行安全分析，得到各个系统的安全性指标，并采用改进的AHP算法筛选风险评估行为安全指标体系里的重要指标因素。对于STPA步骤2里建立的分层控制结构，也可以使用其他工具将其可视化，从而更好地分析不安全控制行为。Abdulkhaleq[71]通过构建一个有限状态机来建模系统的动态行为，将系统状态、控制动作和安全约束可视化，更好地识别并评估不安全控制行为。表2列出了STPA与其他安全分析方法和验证阶段集成的方法与具体作用。

综上所述，STPA不仅能与传统安全分析方法（如FMEA、HAZOP等）进行有效的集成，扩大应用范围和应用场景，进而提升安全分析效率；还可以与自动驾驶系统的验证过程进行集成，进而有机地连接自动驾驶系统开发的分析阶段与验证阶段，完成自动驾驶系统开发工作的闭环。通过综合利用STPA与相关分析与验证过程，可以提升系统开发效率和系统安全性。

4 总结和展望

自动驾驶系统属于软件密集系统，涉及“人-车-环境”多方面的影响因素。其失效模式除了功能安全领域的组件失效外，组件交互、人机交互、外部网络攻击、性能局限与功能不足的问题也与日俱增。STPA在预期功能安全和信息安全领域的适用性使其在自动驾驶领域具有应用前景，相较传统安全分析方法，STPA具有可以在安全分析全周期应用、用于整车开发、能发现更多组件交互问题、更好分析人为错误、应对外部网络攻击等优势。然而其也存在发现部件可靠性方面问题能力不优越、复杂度和成本高、缺乏后续验证过程等缺点。在总结STPA在自动驾驶领域的应用之后，现对其提出以下展望。

（1）衍生更全面的安全分析方法。在自动驾驶领域，单独使用STPA进行安全分析时会面临对部件可靠性相关的危害关注不足和方法抽象等问题。STPA可以通过与其他安全分析方法的组合应用提高其在功能安全领域的分析质量，与FTA、FMEA方法的集成也可以使分析可以更为具体，同时保留STPA的优势。未来可以以STPA为基础，结合特定安全分析方法形成一套新的集成二者优势的安全分析方法。

（2）形成分析与验证的闭环。使用STPA分析完毕之后，往往缺乏检查STPA分析效果的验证过程。将STPA与其他工具集成分析，包括测试验证过程的加入和对控制结构建模。验证过程即仿真和模型检验，测试过程包括软件测试、硬件在环测试（HIL）和实

车测试。可以对STPA分析效果进行直观的检验。同时还包括对控制结构建模等方法，使系统不再抽象，更好地识别不安全控制行为。未来可以通过将STPA与相应工具集成，形成安全分析与验证的完整链条。

（3）丰富STPA应用范围。STPA不仅可以用于自动驾驶系统的开发，还可以用于整车开发。由于STPA对系统间交互的关注和其能够适用于全开发流程，不断迭代更新，所以其在整车开发领域具有天然的优势。其在汽车开发中的应用前景不应仅限于单一系统，可以扩大其应用范围至全周期和全车开发。

参 考 文 献

[1] 工业和信息化部. 关于开展智能网联汽车准入和上路通行试点工作的通知（征求意见稿）[EB/OL]. (2022-11-02) [2023-05-18]. https://www. miit. gov. cn/gzcy/yjzj/art/2022/art_4ae46de7edee4a72adb611b3c67b9d6e.html.

[2] SCHMIDT S, KLLN G C, MICHAEL K. Comparison of Hazard Analysis Methods with Regard to the Series Development of Autonomous Vehicles[C]//2019 IEEE Intelligent Transportation Systems Conference (ITSC). Auckland, New Zealand: IEEE, 2019.

[3] U.S. Nuclear Regulatory Commission. Fault Tree Handbook [EB/OL]. (1981-01)[2024-06-13].https://www.nrc.gov/docs/ML1007/ML100780465.pdf.

[4] ZHANG Y, DONG C, GUO W, et al. Systems Theoretic Accident Model and Process (STAMP): A Literature Review [J]. Safety Science, 2021, 152(8): 105596.

[5] HEINRICH H.W. Industrial Accident Prevention: A Scientific Approach[M]. New York: McGraw-Hill, 1931.

[6] REASON J. Human Error[M]. Cambridge: Cambridge University Press, 1990.

[7] KABIR S. An Overview of Fault Tree Analysis and Its Application in Model-Based Dependability Analysis[J]. Expert Systems with Applications, 2017, 77(7): 114-135.

[8] WU Z, LIU W, NIE W. Literature Review and Prospect of the Development and Application of FMEA in Manufacturing Industry[J]. The International Journal of Advanced Manufacturing Technology, 2021, 112(1): 1409-1436.

[9] HOEPFFNER L. Analysis of the HAZOP Study and Comparison with Similar Safety Analysis Systems[J]. Gas Separation & Purification, 1989, 3(3): 148-151.

[10] Center for Chemical Process Safety. Guidelines for Process Safety Documentation[M/OL]. (1995-01-04) [2024-06-10]. https://onlinelibrary. wiley. com/doi/book/10.1002/97804709 38072.

[11] DUNJÓ J, FTHENAKIS V, VíLCHEZ A, et al. Hazard and Operability (HAZOP) Analysis: A Literature Review[J]. Journal of Hazardous Materials, 2009, 173(1-3): 19-32.

[12] BAYBUTT P. A Critique of the Hazard and Operability (HAZOP) Study[J]. Journal of Loss Prevention in the Process Industries, 2015, 33(1): 52-58.

[13] LEVESON N G. System Safety Engineering: Back to the Future[EB/OL]. (2002-06)[2024-06-10]. http://sunnyday.mit.edu/book2.pdf.

[14] LEVESON N G. A New Accident Model for Engineering Safer Systems[J]. Safety Science, 2004, 42(4): 237-270.

[15] LEVESON N G. A Systems Approach to Risk Management Through Leading Safety Indicators[J]. Reliability Engineering and System Safety, 2015, 136(4): 17-34.

[16] LEVESON N G, THOMAS J P. STPA Handbook[M/OL]. 2018[2024-06-10]. https://ocw. mit. edu/courses/16-63j-system-safety-spring-2016/661489367b4e73b373c72e8ebcac3d55_MIT16_63JS16_LecNotes13.pdf.

[17] STANTON N A, HARVEY C, ALLISON C K. Systems Theoretic Accident Model and Process (STAMP) Applied to a Royal Navy Hawk Jet Missile Simulation Exercise[J]. Safety Science, 2019, 113(3): 461-471.

[18] VENTIKOS N P, CHMURSKI A, LOUZIS K. A Systems-based Application for Autonomous Vessels Safety: Hazard Identification as a Function of Increasing Autonomy Levels [J]. Safety Science, 2020, 131(11): 104919.

[19] ESRA BAS. STPA Methodology in a Socio-Technical System of Monitoring and Tracking Diabetes Mellitus[J]. Applied Ergonomics, 2020, 89(4): 103190.

[20] SCARINCI A, QUILICI A, RIBEIRO D, et al. Requirement Generation for Highly Integrated Aircraft Systems Through STPA: An Application[J]. Journal of Aerospace Information Systems, 2019, 16(1): 9-21.

[21] REJZEK M, HILBES C. Use of STPA as a Diverse Analysis Method for Optimization and Design Verification of Digital Instrumentation and Control Systems in Nuclear Power Plants[J]. Nuclear Engineering & Design, 2018, 331 (5): 125-135.

[22] YAN F, TANG T, YAN H. Scenario Based STPA Analysis in Automated Urban Guided Transport System[C]//2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT). Birmingham: IEEE, 2016: 425-431.

[23] LEVESON N G. Engineering a Safer World: Systems Thinking Applied to Safety[M]. Cambridge: The MIT Press, 2016.

[24] SUN L, LI Y F, ZIO E. Comparison of the HAZOP, FMEA,

FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems[J]. ASME J. Risk Uncertainty Part B, 2022, 8(3): 031104.

[25] SULAMAN S M, BEER A, FELDERER M, et al. Comparison of the FMEA and STPA Safety Analysis Methods—A Case Study[J]. Software Quality Journal, 2019, 27(1): 349-387.

[26] FATTAHI R, TAVAKKOLI-MOGHADDAM R, KHALILZA-DEH M, et al. A Novel FMEA Model Based on Fuzzy Multiple-Criteria Decision-Making Methods for Risk Assessment[J]. Journal of Enterprise Information Management, 2020, 33(5): 881-904.

[27] BAYBUTT P. The Role of People and Human Factors in Performing Process Hazard Analysis and Layers of Protection Analysis[J]. Journal of Loss Prevention in the Process Industries, 2013, 26(6): 1352-1365.

[28] BAGSCHIK G, RESCHKA A, STOLTE T, et al. Identification of Potential Hazardous Events for an Unmanned Protective Vehicle[C]//2016 IEEE Intelligent Vehicles Symposium (IV). Gothenburg, Sweden: IEEE, 2016: 691-697.

[29] 陈君毅, 周堂瑞, 邢星宇, 等. 基于系统理论过程分析的自动驾驶汽车安全分析方法研究[J]. 汽车技术, 2019(12): 1-5.

[30] FLEMING C H, SPENCER M, THOMAS J, et al. Safety Assurance in NextGen and Complex Transportation Systems[J]. Safety Science, 2013, 55: 173-187.

[31] LEVESON N G. Safeware: System Safety and Computers [EB/OL]. ACM, 1995[2024-06-10]. http://sunnyday. mit. edu/book.html.

[32] SHI E, GASSER T M, SEECK A, et al. The Principles of Operation Framework: A Comprehensive Classification Concept for Automated Driving Functions[J]. SAE International Journal of Connected and Automated Vehicles, 2020, 3(1):27-37.

[33] 周逢军, 韩冰, 赵宪华, 等. 一种基于STPA的智能网联汽车系统安全分析方法[J]. 汽车零部件, 2021(7): 4.

[34] SHARMA S, FLORES A, HOBBS C, et al. Safety and Security Analysis of AEB for L4 Autonomous Vehicle Using STPA[C]//Workshop on Autonomous Systems Design (ASD 2019), 2019, 68: 1-13.

[35] 马海涛. 自动车道保持系统人机交互安全分析与评价[D]. 长春: 吉林大学, 2022.

[36] 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: 41-51.

[37] ABDULKHALEQ A, WAGNER S, LAMMERING D, et al. Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles[J/OL]. arXiv (2017-05-10) [2024-06-10]. https://arxiv. org/abs/1703.03657.

[38] ZHANG S, TANG T, LIU J. A Hazard Analysis Approach for the SOTIF in Intelligent Railway Driving Assistance Systems Using STPA and Complex Network[J]. Applied Sciences, 2021, 11(16): 7714.

[39] CHAAL M, BANDA O A V, GLOMSRUD J A, et al. A Framework to Model the STPA Hierarchical Control Structure of an Autonomous Ship[J]. Safety Science, 2020, 132(12): 104939.

[40] CZARNECKI K. On-Road Safety of Automated Driving System (ADS-Taxonomy and Safety Analysis Methods[J/OL]. (2018-07) [2024-06-10]. https://www. researchgate. net/publication/326546852_On-Road_Safety_of_Automated_Driving_System_ADS_-_Taxonomy_and_Safety_Analysis_Methods.

[41] SAE International. SAE J3187_202202: System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems [S/OL]. (2022-02-16)[2024-06-13]. https://www. sae. org/standards/content/j3187_202202/.

[42] 冯浩. 高速公路自动驾驶系统感知模块预期功能安全研究[D]. 长春: 吉林大学, 2022.

[43] HAIXIA L, LI J, PIMENTEL J, et al. Complete Safety Analysis of Known and Unknown Scenarios in Autonomous Vehicles Based on STPA Loss Scenarios[J/OL]. SAE Technical Paper, 2022[2024-06-13]. https://doi. org/10.4271/2022-01-7023.

[44] SHIMIZU K, SUZUKI D, MURAMATSU R, et al. Evaluation Framework for Performance Limitation of Autonomous Systems under Sensor Attack[C]// International Conference, SAFECOMP 2021. Berlin: Springer, 2021: 67-81.

[45] 曾珂瑜, 谢国琪, 李仁发. 面向智能网联汽车的系统理论过程分析研究[J]. 中国汽车, 2020(7): 4-10.

[46] YOUNG W, LEVESON N. Systems Thinking for Safety and Security[C]//Proceedings of the 29th Annual Computer Security Applications Conference, 2013: 1-8.

[47] SAHAY R, ESTAY D A S, MENG W, et al. A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS[J]. Computers & Security, 2023, 128(5): 103179.

[48] SCHMITTNER C, MA Z, PUSCHNER P. Limitation and

improvement of STPA-Sec for safety and security co-analysis[C]//Computer Safety, Reliability, and Security: SAFECOMP 2016 Workshops, 2016: 195-209.

[49] FRIEDBERG I, MCLAUGHLIN K, SMITH P, et al. STPA-SafeSec: Safety and Security Analysis for Cyber-physical Systems[J]. Journal of Information Security and Applications, 2016, 34: 183-196.

[50] ABDULKHALEQ A, BAUMEISTER M, BÖHMERT H, et al. Missing no interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems[J]. International Journal of Safety Science, 2018, 2(1): 115-24.

[51] FRANCE M E. Engineering for humans: A New Extension to STPA[D]. Cambridge: Massachusetts Institute of Technology, 2017.

[52] LEPLAT J. Task Analysis and Activity Analysis in Situations of Field Diagnosis[M]//Human Detection and Diagnosis of System Failures. Berlin: Springer, 1981: 287-300.

[53] FRANÇOIS M, OSIURAK F, FORT A, et al. Automotive HMI Design and Participatory User Involvement: Review and Perspectives[J]. Ergonomics, 2017, 60(4): 541-552.

[54] NIELSEN J. The Usability Engineering Life Cycle[J]. Computer, 1992, 25(3): 12-22.

[55] LEE J D, YOUNG K L, REGAN M A. Defining Driver Distraction[M]. Handbook of Traffic Psychology. Norfolk, VA, USA: Academic Press, 2008: 31-40.

[56] ADELL E. Acceptance of Driver Support Systems[C]// Proceedings of the European Conference on Human Centered Design For Intelligent Transport Systems, 2010, 2: 475-486.

[57] KLLN G C, MICHAEL K, SCHMIDT S. Comparison of the Results of the System Theoretic Process Analysis for a Vehicle SAE Level Four and Five[C]//2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). Rhodes, Greece: IEEE, 2020.

[58] CHEN S, KHASTGIR S, BABAEV I, et al. Identifying Accident Causes of Driver-Vehicle Interactions Using System Theoretic Process Analysis (STPA)[C]//2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Toronto, ON, Canada: IEEE, 2020.

[59] BREWER J, BECKER C, POLLARD J, et al. Functional Safety Assessment of a Generic Automated Lane Centering System and Related Foundational Vehicle Systems[R/OL]. (2018-08-01)[2024-06-10]. https://rosap.ntl.bts.gov/view/dot/37076.

[60] CHEN L, JIAO J, ZHAO T. A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA[J]. Applied Sciences, 2020, 10(21): 7400.

[61] CAPITO L, REDMILL K A. Methodology for Hazard Identification and Mitigation Strategies Applied to an Overtaking Assistant ADAS[C]//2021 IEEE International Intelligent Transportation Systems Conference (ITSC). Indianapolis, IN, USA: IEEE, 2021: 3972-3977.

[62] 刘逸恒. 基于预期功能安全的AEB系统设计与验证[D]. 长春: 吉林大学, 2022.

[63] CHRISTOPHER B, DAVID A, JOHN B. Functional Safety Assessment of a Generic, Conventional, Hydraulic Braking System with Antilock Brakes, Traction Control, and Electronic Stability Control [R/OL]. (2018-08-01)[2024-06-13]. https://rosap.ntl.bts.gov/view/dot/37210.

[64] POST K, DAVEY C K. Integrating SOTIF and Agile Systems Engineering[J/OL]. SAE Technical Paper, (2019-04-02) [2024-06-13]. https://www. sae. org/publications/technical-papers/content/2019-01-0141/.

[65] DAKWAT A L, VILLANI E. System Safety Assessment Based on STPA and Model Checking[J]. Safety science, 2018, 109: 130-143.

[66] SALEHI FATHABADI A, SNOOK C, DGHAYM D, et al. Designing Critical Systems Using Hierarchical STPA and Event-B[C]// 9th International Conference, ABZ 2023. Switzerland: Springer, 2023: 220-237.

[67] ABDULKHALEQ A, WAGNER S, LEVESON N. A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA[J]. Procedia Engineering, 2015, 128: 2-11.

[68] 陈君毅, 刘力豪, 周堂瑞, 等. 城市自动驾驶决策系统安全分析与策略设计[J]. 同济大学学报(自然科学版), 2020, 48(12): 1810-1817.

[69] 郭菲菲, 赵永飞, 付金勇 等. 全自动泊车辅助系统的预期功能安全开发研究[C]//中国汽车工程学会. 2020中国汽车工程学会年会论文集(4). 北京: 机械工业出版社, 2020: 545-551.

[70] 王克克, 郭莉丽, 郎静宏. 基于STAMP模型的风险评估行为安全指标体系[J]. 计算机工程与科学, 2022, 44(8): 1372-1381.

[71] ABDULKHALEQ A, WAGNER S. Integrating State Machine Analysis with System-Theoretic Process Analysis [EB/OL]. 2013[2024-06-10]. https://subs. emis. de/LNI/Proceedings/Proceedings215/501.pdf.

（责任编辑　明慧）