文章编号：0253-374X(2023)04-0616-07

DOI：10.11908/j.issn.0253-374x.21570

基于有限状态机的预期功能安全危害识别方法

熊　璐[1]，贾　通[1]，陈君毅[1]，邢星宇[1]，李　博[2]

（1. 同济大学 汽车学院，上海 201804；2. 武汉路特斯科技有限公司，湖北 武汉 430090）

摘要：针对自动驾驶系统危害与场景不可分割的特点，提出了一种基于有限状态机模型(FSM)的整车级预期功能安全危害识别方法。首先，明确危害事件组成要素；其次，将自动驾驶系统抽象为有限状态机模型以明确车辆状态和运行环境；最后，通过识别车辆状态与运行环境的冲突情况，系统性识别自动驾驶系统预期功能安全危害事件，减少对专家知识的依赖。为验证所提出方法的有效性，在某SAE L3级自动驾驶汽车上应用了该方法进行危害识别。结果表明，相较于系统理论过程分析(STPA)方法，有限状态机模型包含更加详细且系统化的环境信息，且由有限状态机模型直接输出危害事件要素，提高了危害识别的系统性。

关键词：自动驾驶；预期功能安全；功能安全；有限状态机；危害事件

中图分类号：U463.6　　**文献标志码**：A

Hazard Identification Method for Safety of the Intended Functionality Based on Finite State Machine

XIONG Lu[1], *JIA Tong*[1], *CHEN Junyi*[1], *XING Xingyu*[1], *Li Bo*[2]

(1. School of Automotive Studies, Tongji University, Shanghai 201804, China; 2. Wuhan Lotus Technology Co., Ltd., Wuhan 430090, China)

Abstract: Aimed at the dependence of hazards of the autonomous driving system (ADS) and scenarios, a method for identifying hazards of the safety of the intended functionality (SOTIF) at the vehicle level is proposed based on the finite state machine (FSM). First, the elements constituting hazardous events are specified. Then the FSM is adopted to abstract the ADS in combination with vehicle states and the operational environment. Finally, by identifying the conflicts between vehicle states and the operational environment, hazardous events of the ADS related to the SOTIF are systematically identified, which overcomes the overdependence on expert knowledge. The proposed method is applied to identify hazardous events on an SAE L3 autonomous vehicle to verify its effectiveness. The results show that compared with the system theoretic process analysis (STPA) method, the FSM model contains more detailed and systematic environmental information and the elements constituting the hazardous events are directly provided by the FSM model, which supports systematic identification of hazardous events.

Key words: autonomous driving; safety of the intended functionality(SOTIF); functional safety; finite state machine; hazardous events

随着自动驾驶技术的快速发展，其安全性要求越来越严格，从而对安全分析与验证方法提出更多挑战。自动驾驶汽车作为一个集环境感知、决策规划和运动控制为一体的复杂系统，不仅面临着传统因电控系统故障导致的功能安全问题[1-2]，同时也面临着预期功能安全问题。自动驾驶的预期功能安全问题源于运行环境和自身性能局限的共同作用，这造成安全分析与验证的困难性和复杂性远超功能安全。

业界将自动驾驶汽车在无故障或失效情况下仍无法实现预期功能的问题定义为预期功能安全问题[3]。现阶段对预期功能安全的研究仍不成熟，国际标准化组织针对预期功能安全问题，于2019年发布了ISO/PAS 21448《Road vehicles-safety of the intended functionality》[4]。该标准对自动驾驶车辆安全分析流程进行限定，主要包括系统规范与功能定义、危害识别和风险评估以及触发条件识别。其中危害识别和风险评估是最为重要的环节之一，需在概念阶段定性识别车辆潜在危害并进行风险评估，

收稿日期：2021-12-06
基金项目：国家重点研发计划(2021YFB2501205)
第一作者：熊璐(1978—)，男，教授，工学博士，主要研究方向为车辆系统动力学与控制。
E-mail：xiong_lu@tongji.edu.cn
通信作者：陈君毅(1980—)，女，讲师，工学博士，主要研究方向为自动驾驶汽车的测试和评价技术。
E-mail：chenjunyi@tongji.edu.cn

论文拓展介绍

并基于此对危害事件提出安全要求,为后续面向安全性设计和测试验证提供指导。

现有研究针对上述预期功能安全危害识别需求,多采用以下几种传统安全分析方法,包括故障树分析(fault tree analysis, FTA)、失效模式及效应分析(failure mode and effect analysis, FMEA)、危险与可操作性分析(hazard and operability analysis, HAZOP)等方法。FTA方法和FMEA方法认为事故是以特定时间顺序发生的离散事件造成的结果,以具体的系统失效或故障作为输入,由下而上或由上而下的构建自动驾驶系统事件链识别自动驾驶系统危害[5-6]。但此类方法针对自动驾驶系统存在明显局限,一方面高等级自动驾驶系统控制逻辑较为复杂,事件链的构建难度较大;另一方面,针对自动驾驶系统失效或故障的数据仍缺乏统一的定义,难以获取。HAZOP方法是一种基于系统偏差引导词的结构化和系统化分析方法,通过专家小组系统地辨识各种潜在预期功能偏差,分析各偏差的原因以识别相应的危害[7]。但该方法严重依赖于专家对系统的了解程度。

针对上述方法的局限,系统理论过程分析(systems-theoretic process analysis, STPA)被认为可以有效识别自动驾驶系统危害。STPA方法是一种基于系统理论事故模型与过程(systems theoretic accident model and process, STAMP)的安全分析方法,通过分析系统控制结构中的不安全控制行为识别系统潜在危害[8]。STPA方法有效地减少了对自动驾驶系统知识以及数据的依赖。至今,STPA方法在自动驾驶系统安全分析领域已有较多尝试[9-10],聚焦于控制行为异常以识别自动驾驶系统危害。以上研究可以证明传统STPA方法在自动驾驶系统上的有效性。但研究过程中发现,高等级自动驾驶系统控制结构较为复杂,STPA方法分析过程需以系统运行环境作为输入,分析全面性仍较难得到保证。

针对STPA方法分析全面性难以得到保证的问题,本文引入了包含自动驾驶系统车辆状态与运行环境的有限状态机模型(finite state machine,FSM),对危害事件重新进行定义,通过识别状态转移过程中的车辆状态与运行环境冲突情况,可获得包含运行环境与自身局限性两方面来源的危害事件。本文第1节主要描述基于有限状态机的危害识别方法,第2节为该方法在某自动驾驶汽车上的应用,第3节为总结和展望。

1　基于有限状态机的危害识别方法

传统危害识别方法引入运行场景信息时主观因素影响较大,使得系统全面地识别危害事件较为困难。因此,在现有危害识别方法的基础上,提出了基于有限状态机的危害识别方法,系统性引入运行环境。首先,与传统危害事件侧重点不同,本文对危害事件重新定义;其次,对有限状态机模型进行介绍;最后,基于自动驾驶系统危害与运行环境不可分割的特性,介绍了本文的危害分析方法,即通过识别自动驾驶系统在状态转移过程中的非预期行为全面识别系统危害事件。

1.1　危害事件定义

危害事件是危害识别环节的重要输出,虽然预期功能安全继续沿用了功能安全对危害事件的定义,但定义较为模糊,不利于系统化、规范化地识别危害场景,本文对危害事件内涵进行了明确。功能安全重点关注自动驾驶系统中与运行环境无关的电子电气系统故障,运行环境仅为判断危害后果的背景信息,但功能安全并未严格界定该运行环境的内涵,笼统地将车辆运行工况视为运行环境。而在预期功能安全中,运行环境既包含了触发性能局限的环境因素,同时也包含了组成危害的关键要素,对运行环境进行细化,一方面有利于构建自动驾驶系统潜在危害场景,同时也有利于进一步开展致因分析。

周堂瑞[10]在之前的研究过程中,结合已有危害事件的定义,如表1所示,定义了危害事件是使自动驾驶系统由安全状态转移至危险状态的事件。即在一定的环境条件和自车状态下,车辆非预期行为可能导致危害的事件。主要包括自车状态、一定环境条件和车辆非预期行为三个要素。上述三个要素涵盖危害事件的各个组成部分且使各个部分界限更加清晰。

表1　不同危害事件定义对比

Tab.1　Comparison of different definitions of hazardous event

	受伤害对象	环境条件	自车	危害行为
ISO 26262	运行场景	运行场景	运行场景	危害
Leveson[8]	恶劣环境条件	恶劣环境条件	系统状态	
Ericson[11]	目标物	危险因素	危险因素	触发机制
本文	一定环境条件	一定环境条件	自车状态	车辆非预期行为

1.2　有限状态机模型

为了将自动驾驶系统危害与运行环境有效结合,本文引入了有限状态机模型,有限状态机模型通过描述系统状态及其运行环境来建立系统模型。有

限状态机是一种常用的系统描述方式,作为一种离散输入、输出系统的数学模型,该模型通常包括以下几个部分:输入集合C,用于表示系统所接受的不同输入信息;输出集合S_{Tar},系统能够做出的有限响应集合;状态集合S,描述系统的不同状态;转移逻辑T,为状态机从一个状态转移到另一个状态的条件,通常是由当前状态和输入条件的共同作用组成[12]。图1即一个典型的有限状态机模型。

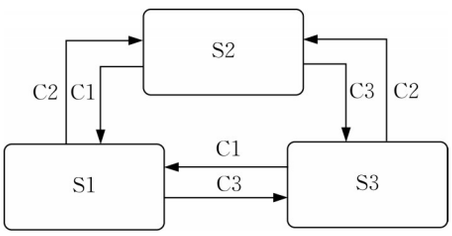

图1 典型有限状态机模型

Fig. 1 Typical finite state machine model

基于上述有限状态机的定义可知,有限状态机模型的引入使得自动驾驶系统描述更加清晰。状态转移过程中的当前状态S_{Cur}、输入集合C、环境条件与目标状态S_{Tar}之间的不匹配,与危害事件三要素一一对应,如图2所示。危害事件中的自车状态即当前状态S_{Cur},一定环境条件即状态转移过程中的输入条件,而车辆的非预期行为即输入的环境条件与所运行的目标车辆状态不匹配造成的行为。该不匹配本质即自动驾驶系统环境条件与车辆状态存在冲突,具体包括错误转入其他车辆状态、目标车辆状态行为不正确、目标车辆状态开启过早或过晚等。

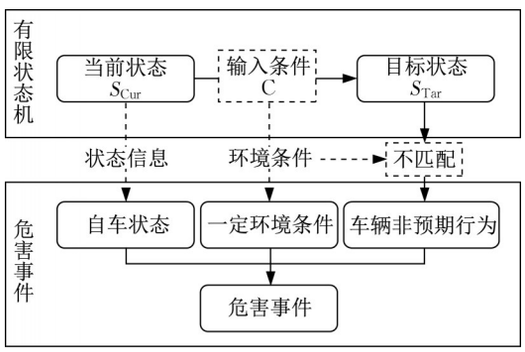

图2 有限状态机模型与危害事件对应关系

Fig. 2 Correspondence between FSM model and hazardous event

1.3 危害识别方法

通过将自动驾驶系统抽象为有限状态机模型,识别状态转移过程中车辆状态与环境条件冲突导致的非预期行为,通过判断车辆非预期行为是否会导致危害确定危害事件的三个要素,从而得出系统危害事件。并且可以基于危害事件构建测试用例,验证该危害事件。该方法的框架如图3所示。

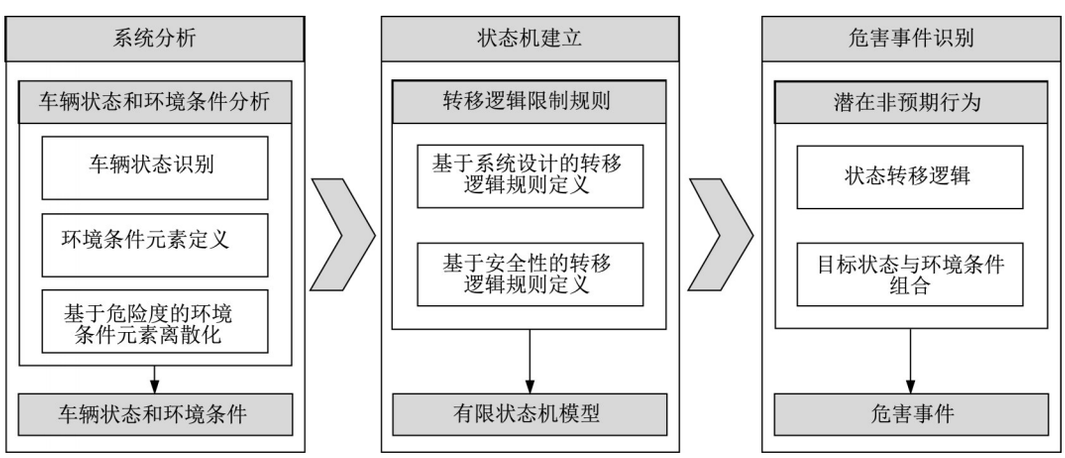

图3 危害识别方法框架

Fig. 3 Framework of hazard identification method

1.3.1 识别车辆状态与对应环境条件

首先,根据有限状态机模型定义,需将自动驾驶系统划分为有限个状态以及决定状态转移的环境条件。有限状态机模型在自动驾驶决策系统[13]、控制系统[14-15]和整车层面[16]均有应用。构建自动驾驶系统有限状态机模型即根据车辆约束、行驶规则、经验和交通法规等建立行为规则库,根据不同的环境信息划分车辆状态。根据系统定义的行为规则库和车辆状态划分,则可以输出车辆状态与其对应的环境信息。

此处需要说明的是,面向底层控制行为的有限状态机被直接用于系统开发[14-15],此类有限状态机模型关注车辆各部件状态,基于此识别的危害事件主要是由

功能失效导致的;面向功能层面的有限状态机关注整车状态而非部件状态[16],基于此识别的危害事件是主要由整车非预期行为导致的。本文所提出的危害识别方法对所有类型有限状态机模型均适用。

然后,识别决定车辆状态的环境条件。基于行为规则库输出的环境信息是决定车辆状态的语义信息。为保证自动驾驶系统在运行设计域内所遇见的全部场景均存在车辆状态响应,本文采用树状结构将语义层面的环境信息离散化、形式化生成环境条件元素,做全部环境条件元素的笛卡尔积形成环境条件。离散化原则可根据目标物和自车状态导致的运行环境危险度不同,采用不同的危险度模型。常用的危险度模型有碰撞时间(time-to collision, TTC)、车头时距(time headway, THW)等,图 4 即形式化表示的环境条件。

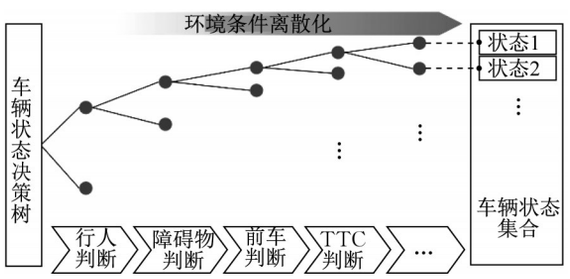

图 4　形式化表示的环境条件样例

Fig. 4　Example of formal environmental condition

1.3.2　建立系统有限状态机模型

部分车辆状态之间的转移将会导致违反交通规则或出现危险的情况,因此部分车辆状态之间存在转移逻辑限制。该转移逻辑限制主要包括两个方面。首先即根据交通规则、知识、经验定义的转移逻辑限制;另一方面是基于系统安全性要求设置的转移逻辑限制,禁止部分状态之间的转移。之后依据转移逻辑限制建立自动驾驶系统的有限状态机模型。

由于高等级自动驾驶系统过于复杂,可能存在多个相似的车辆状态。因此为了简化有限状态机模型,可以采用分层有限状态机模型(hierarchical finite state machine, HFSM),将具有相似转移逻辑的车辆状态建立子状态机,而顶层状态机表示大类车辆状态之间的转移逻辑,子状态继承顶层状态机的转移逻辑。对于分层有限状态机模型而言,满足系统顶层状态环境条件后,存在多个子状态响应该环境条件,为保证自动驾驶系统存在确定的动作行为,需对子状态环境条件进行规定,该转移规定也属于转移逻辑限制的一部分。

1.3.3　识别系统潜在危害事件

基于有限状态机模型得出完整状态转移逻辑集合,并系统性识别车辆状态与环境条件冲突导致的不安全控制行为。依据传统STPA方法,传统不安全控制行为(unsafe control action, UCA)分为UCA-1需要但未提供控制、UCA-2不需要但提供控制、UCA-3需要但提供控制行为错误、UCA-4错误的控制提供时间、UCA-5错误的控制持续时间5类,具体结果如表2所示。其中“需要”即满足执行车辆状态的环境条件,“不需要”则不满足执行车辆状态的环境条件,则由表2可知上述不安全控制行为均属于车辆状态与环境条件不匹配所导致的。

表2　传统不安全控制行为集

Tab. 2　Traditional unsafe control action set

被控对象	控制行为	
	提供控制	不提供控制
需要被控	UCA−3、UCA−4、UCA−5	UCA−1
不需要被控	UCA−2	安全

然而,上述不安全控制行为仅对开闭型控制行为是足够的,对于自动驾驶系统,其控制行为在一段时间内是连续变化的。显然,在现有的分类方法下UCA-4和UCA-5间是存在重合的。因此,本文提出通过分析环境条件与车辆状态间的冲突情况直接识别非预期行为,进而确定系统的潜在危害事件,涵盖了上述UCA-1至UCA-5的全部危害事件。

因此,可以在当前车辆状态S_{Cur}下,作目标车辆状态集合S_{Tar}与输入环境条件集合C的笛卡尔积,识别全部不安全控制行为集,记为U_{c}。即:

$$U_{\mathrm{c}}=S_{\mathrm{Tar}}\times C=\left\{\left(S_{\mathrm{Tar},i},C_{ij}\right)\mid i=0,1,2\cdots,k;\ j=1,2\cdots,l\right\} \tag{1}$$

式中:$S_{\mathrm{Tar},i}$为第i个目标车辆状态,0表示当前状态;C_{ij}为第i个目标车辆状态下第j个环境条件;k为目标车辆状态$S_{\mathrm{Tar},i}$个数;l为目标车辆状态$S_{\mathrm{Tar},i}$的环境条件个数。具体结果形式参见表3所示。这里需要说明的是,U1功能错误可能是由于自动驾驶系统电子电控系统失效或故障导致的,识别的危害事件属于功能安全范畴,而U2-U5是由于自动驾驶系统性能局限导致的,识别的危害事件属于预期功能安全范畴。

由危害事件定义可知,并非全部非预期行为均会导致事故,需存在危害作用对象才导致事故。因此,识别导致潜在危害的非预期行为及危害事件。

表3 不安全控制行为集

Tab. 3 Unsafe control action set

车辆目标状态S_{Tar}		状态转移条件C		
		当前状态环境条件	目标状态m环境条件	目标状态n环境条件
		C_0	C_m	C_n
$S_{Tar,0}$	当前状态	U1功能错误	U2错误保持	U2错误保持
$S_{Tar,m}$	目标状态m	U3错误开启	U1功能错误 U4开启过早 U5开启过晚	U3错误开启
$S_{Tar,n}$	目标状态n	U3错误开启	U3错误开启	U1功能错误 U4开启过早 U5开启过晚

2 在自动驾驶清扫车上的应用

为了验证本方法的有效性,将分别应用传统STPA方法和本文基于有限状态机的危害识别方法对某SAE L3级自动驾驶清扫车进行危害识别。清扫功能不涉及自动驾驶系统的安全问题,不作为分析对象,后续仅以SAE L3级自动驾驶汽车作为分析对象。

2.1 车辆状态与对应环境条件分析

该车辆存在手动驾驶和自动驾驶两种模式,但全程配备驾驶员进行监督或控制,并且仅在封闭园区内运行。其中自动驾驶模式目标为:在封闭园区内,车辆自主规划行驶路线行驶,在自主行驶过程中可识别并自主避让前方障碍物、行人等,其行驶目标以及其环境信息如表4所示。表中,GPS表示全球定位系统(global positioning system, GPS),基于GPS预定义了车辆在无路沿情况时的行驶轨迹。

表4 自动驾驶模式行驶目标与运行环境

Tab. 4 Driving objectives and environment of autonomous driving model

车辆功能	行驶目标	环境信息
车道保持	与路沿保持设定距离行驶	有路沿
GPS循迹	根据GPS信号规划路径行驶	无路沿,有稳定GPS信号
车辆停车	制动停车	无路沿,无稳定GPS信号
停车让行	识别前方行人,鸣笛并减速停车	车辆前方有行人
避障绕行	识别前方障碍物,绕行避障	车辆前方有障碍物

表4中的车辆功能属于面向功能层面的车辆状态,因此,可以采用该功能作为车辆状态。结合表4中环境信息,需明确有无行人或障碍物的环境条件元素。参考ISO 15622标准[17]对有无行人或障碍物的车头时距THW进行限定,之后做环境条件元素的笛卡尔积,得出全部车辆状态与环境条件,表5从车辆状态、环境条件和车辆预期行为对每个状态进行说明。

表5 分析对象各状态说明

Tab. 5 Description of each state of analysis object

编号	车辆状态	环境条件	车辆预期行为
S1	车辆停车	自动驾驶∩无路沿∩GPS信号不稳定	车辆安全减速至停车
S2_1	停车让行	①有路沿∩无行人∩有障碍物∩无换道空间 ②有路沿∩有行人 ③无路沿∩GPS信号稳定∩有行人 ④无路沿∩GPS信号稳定∩无行人∩有障碍物	车辆安全减速至停车避让前方障碍物或行人
S2_2	避障绕行	有路沿∩无行人∩有障碍物∩有换道空间	车辆与障碍物保持安全距离换道
S3_1	车道保持	有路沿∩无行人∩无障碍物	车辆与路沿保持设定距离和设定速度行驶
S3_2	GPS循迹	无路沿∩GPS信号稳定∩无行人∩无障碍物	车辆根据GPS信号按规划路线行驶

2.2 建立系统有限状态机模型

为满足自动驾驶系统的安全性要求,需根据交通规则与系统定义的转移逻辑限制对部分状态转移进行约束,具体细节如下:

(1)系统定义车辆仅可由车辆停车启动,且定义车辆停车进入自动驾驶其他状态时,需保证周围无障碍物或行人,故车辆停车状态仅可以转入车道保持与GPS循迹状态;

(2)由于GPS循迹状态控制精度低,系统定义禁止由GPS循迹转入避障绕行状态;

(3)停车让行与避障绕行可转入任意车辆状态。

接下来,梳理各状态之间的转移关系,建立系统分层有限状态机模型,如图5所示。分层状态机模型具体由S1车辆停车、S2主动避障和S3循迹三个顶层状态组成,包含5个具体子功能状态。

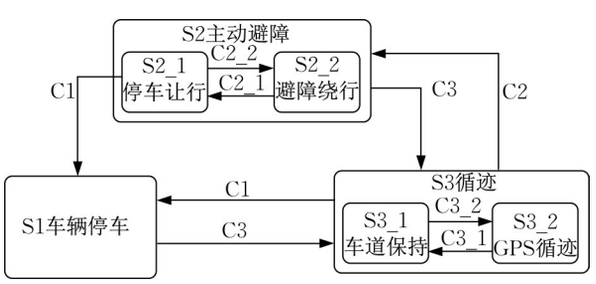

图5 分析对象的有限状态机模型

Fig. 5 FSM of analysis object

2.3 识别潜在危害事件

基于图5和表5识别该自动驾驶汽车的全部状态转移逻辑,作相同当前车辆状态的目标车辆状态S_{Tar}与

输入环境条件C的笛卡尔积,得到全部不安全控制行为导致的非预期行为,判断非预期行为是否会导致潜在危害,进而全面地识别潜在危害事件。本文以当前车辆状态S_{Cur}是S3_2 GPS循迹状态为例介绍危害识别过程。当前车辆状态S_{Cur}为S3_2 GPS循迹时,其目标车辆状态集S_{Tar}包括保持当前状态S3_2 GPS循迹、可转入状态S1车辆停车、S2_1停车让行和S3_1车道保持,其输入环境条件C为上述目标车辆状态的环境条件。具体结果即表6所示。

判断上述非预期行为是否会导致潜在事故得到潜在危害事件,其中部分车辆非预期行为不会导致车辆潜在危害事件,不作为后续分析。例如车辆非预期行为$S_{Tar,1}$车辆停车状态和$S_{Tar,2}$停车让行状态处于最小风险状态,当原因为U3错误开启、U4过早开启时不会导致潜在危害。此外$S_{Tar,2}$停车让行状态包含4个不同环境条件,分析最危险环境条件下的潜在危害。同理$S_{Tar,3}$车道保持状态也分析最危险环境条件下的潜在危害。

表6　S3-2 GPS循迹状态的非预期行为及潜在危害

Tab. 6　Unexpected behavior and potential hazards of S3_2 following GPS state

当前车辆状态S_{Cur}	输入环境条件C	目标车辆状态S_{Tar}(车辆非预期行为)	原因	潜在危害
S3_2	C_0	$S_{Tar,0}$	U1	偏离行驶轨迹,与路边障碍物发生碰撞
		$S_{Tar,1}$	U3	无
		$S_{Tar,2}$	U3	无
		$S_{Tar,3}$	U3	偏离行驶轨迹,与路边障碍物发生碰撞
	C_1	$S_{Tar,0}$	U2	与路边障碍物发生碰撞
		$S_{Tar,1}$	U1	偏离行驶轨迹,与路边障碍物发生碰撞
			U4	无
			U5	偏离行驶轨迹,与路边障碍物发生碰撞
		$S_{Tar,2}$	U3	无
		$S_{Tar,3}$	U3	偏离行驶轨迹,与路边障碍物发生碰撞
	C_2	$S_{Tar,0}$	U2	与行人或障碍物发生碰撞
		$S_{Tar,1}$	U3	无
		$S_{Tar,2}$	U1	与行人或障碍物发生碰撞
			U4	无
			U5	与行人或障碍物发生碰撞
		$S_{Tar,3}$	U3	与行人或障碍物发生碰撞
	C_3	$S_{Tar,0}$	U2	偏离行驶轨迹,与路边障碍物发生碰撞
		$S_{Tar,1}$	U3	无
		$S_{Tar,2}$	U3	无
		$S_{Tar,3}$	U1	与路沿发生碰撞
			U4	偏离行驶轨迹,与路边障碍物发生碰撞
			U5	偏离行驶轨迹,与路边障碍物发生碰撞

此外,表6中的当前车辆状态与输入环境条件组合即语义层面的功能场景,可结合自然驾驶数据等相关信息确定当前车辆状态与输入环境条件的参数以及参数范围,进而生成逻辑场景以及具体场景,用于测试验证上述危害事件。例如构建S3_2循迹状态转入S2_1停车让行状态的功能场景如下:车辆沿GPS信息循迹行驶,无循迹路沿,但GPS信号稳定,车辆前方存在行人横穿。测试验证行人在何种位置和速度横穿时导致车辆非预期行为。

综上所述,利用本文提出的基于有限状态机的危害识别方法共识别得到54项潜在整车级危害事件。

2.4　对比分析

本团队[9]基于传统STPA方法识别该自动驾驶汽车的整车级潜在危害事件,通过识别系统不安全控制行为从而识别车辆潜在危害,结果对比如下表7所示。

传统STPA方法与本文提出的方法主要包含以下4个方面的不同:

(1)分析对象方面:STPA方法大多从控制结构出发识别系统危害,若识别软件层面的危害,需对软件架构进行一定程度抽象与重构。而本文提出的方法从自动驾驶汽车有限状态机出发识别系统危害,危害事件涵盖软件和硬件两方面问题;

(2)危害事件来源方面:STPA方法识别危害事件存在较大主观随意性。而应用本文所提出的方法,危害事件由有限状态机直接输出,减少了主观因素的影响;

(3)危害事件数量方面:STPA方法识别的不安全控制行为须结合专家输入的环境条件才能够确认是否导致危害事件。而本文提出的方法通过判断车辆状态与环境条件是否存在冲突直接确定危害事件;

(4)后续生成场景方面:STPA方法没有办法直接

生成场景。而应用本文所提出的方法,自车状态和一定环境条件组合满足功能场景定义,因此可以生成测试场景验证危害事件的有效性。

表7 两分析方法应用结果对比

Tab. 7 Comparison of the results of two analysis methods

结果	方法	
	STPA方法	基于FSM的危害识别方法(本方法)
分析对象	控制结构	有限状态机
危害事件来源	基于专家知识	基于危害事件要素
危害事件数量	未知(需结合场景输入得出)	54
生成场景	不支持	支持自动化生成场景

3 总结和展望

本文针对自动驾驶系统预期功能安全危害事件识别方法展开研究。为解决危害事件分析没有涵盖运行环境影响的不足,本文引入了自动驾驶系统有限状态机模型,基于转移逻辑识别车辆状态与环境条件冲突导致的非预期行为,通过判断车辆非预期行为是否会导致事故识别潜在危害事件。在某自动驾驶汽车上应用上述方法,并对比现有STPA方法,验证了本文方法的有效性与优越性。

此外,在后续的研究中,将围绕以下方面展开:

(1)在验证潜在危害事件有效性方面,针对本文识别的潜在危害事件自动化构建危害事件测试场景,测试验证危害事件的有效性,定量识别各部件或系统的危害状态;

(2)在识别危害事件方面,将车辆状态和运行环境评定安全等级,匹配二者安全等级自动化识别危害事件。

作者贡献声明:

熊璐:论文修订与审核。

贾通:危害识别,文献资料收集与分析,论文撰写。

陈君毅:研究命题提出与构思,论文审核。

邢星宇:危害识别,文献资料分析,论文修订。

李博:文献资料收集,论文修订。

参考文献:

[1] 张云,李茹,焦伟赟,等.自动驾驶功能安全标准化研究[J].中国标准化,2020(11):109.
ZHANG Yun, LI Ru, JIAO Weiyun, *et al*. Research on standardization of functional safety of automated driving system [J]. China Standardization, 2020(11):109.

[2] International Organization for Standardization. ISO 26262 Road vehicles—Functional safety[S]. Gereva,Switzerland: ISO,2011.

[3] 毛向阳,尚世亮,崔海峰.自动驾驶汽车安全影响因素分析与应对措施研究[J].上海汽车,2018(1):33.
MAO Xiangyang, SHANG Shiliang, CUI Haifeng. Analysis and countermeasure of safety challenging factors for autonomous driving vehicles [J]. Shanghai Auto, 2018(1):33.

[4] International Organization for Standardization. ISO/PAS 21448: 2019 Road vehicles—Safety of the intended functionality [S]. Geneva,Switzerland: ISO, 2019.

[5] BUCHALI T, FOCK M, DOLD S, *et al*. Fault-tolerant architecture for an actuator concept in highly automated cars[C]// 2019 IEEE Vehicle Power and Propulsion Conference (VPPC). Hanoi:IEEE, 2019: 1-6.

[6] YANG J, WARD M, AKHTAR J. The development of safety cases for an autonomous vehicle: A comparative study on different methods[R].Kunshan: SAE, 2017.

[7] PAUL C, BENJAMIN L, WALTER S, *et al*. Validation of safety necessities for a Safety-Bag component in experimental autonomous vehicles [C]//2018 14th European Dependable Computing Conference (EDCC). Iasi:IEEE, 2018: 33-40.

[8] LEVESON N G. Engineering a safer world: Systems thinking applied to safety[M]. [S.l.]:The MIT Press, 2016.

[9] 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.
CHEN Junyi, ZHOU Tangrui, XING Xingyu, *et al*. Research on safety analysis method for autonomous vehicles based on STPA [J]. Automobile Technology , 2019(12): 1.

[10] 周堂瑞. 面向预期功能安全的自动驾驶汽车危害识别方法研究[D]. 上海:同济大学, 2020.
ZHOU Tangrui. Research on hazard identification method for safety of the intended functionality of autonomous vehicles [D]. Shanghai:Tongji University, 2020.

[11] ERICSON C A. Hazard analysis techniques for system safety[M]. Hoboken: John Wiley & Sons, 2005.

[12] 谭同超. 有限状态机及其应用[D]. 广州:华南理工大学, 2013.
TAN Tongchao. Finite state machine and its application [D]. Guangzhou:South China University of Technology, 2013.

[13] 熊璐,康宇宸,张培志,等.无人驾驶车辆行为决策系统研究[J].汽车技术,2018(8): 1.
XIONG Lu, KANG Yuchen, ZHANG Peizhi, *et al*. Research on behavior decision-making system for unmanned vehicle [J]. Automobile Technology, 2018(8): 1.

[14] URMSON C, ANHALT J, BAGNELL D, *et al*. Autonomous driving in urban environments: Boss and the urban challenge[J]. Journal of Field Robotics, 2008, 25(8): 425.

[15] ZIEGLER J, BENDER P, SCHREIBER M, *et al*. Making bertha drive—An autonomous journey on a historic route [J]. IEEE Intelligent Transportation Systems Magazine, 2014, 6(2): 8.

[16] MONTEMERLO M, BECKER J, BHAT S, *et al*. Junior: The stanford entry in the urban challenge[J]. Journal of field Robotics, 2008, 25(9): 569.

[17] International Organization for Standardization. Transport information and control system. Adaptive cruise control systems—Performance requirements and test procedures: ISO 15622—2010 [S]. Geneva, Switzerland: ISO, 2010.