民用航空与安全工程

文章编号：2095-1248(2024)06-0070-11

改进的STPA方法及其在复杂系统安全性分析中的应用

陈 磊

（沈阳航空航天大学 安全工程学院，沈阳 110136）

摘要： 提出一种使用功能属性（functional attribute，FA）及有向交互标签（directional interaction tag，DIT），对基于系统思维的过程分析（system-theoretic process analysis，STPA）方法所涉及的层次化控制结构模型（hierarchical control structure model，HCSM）进行拓展与改进的方法。通过该方法构建层次化功能控制结构及交互模型（hierarchical functional control structure and interaction model，HFCSIM），完成对STPA的实质性提升与完善。通过这一改进，STPA中HCSM的构建没有严谨的具体形式，以及组件间交互信息不完整且过于依赖“头脑风暴”和难以保障模型一致性等问题得以解决，并从根本上确保了分析结果的系统性、完整性和正确性。最后以飞机机轮刹车系统为例，验证了该改进方法的有效性。

关键词： 功能属性；有向交互标签；层次化功能控制结构及交互模型；STPA；安全性分析

中图分类号： X949 **文献标志码：** A

DOI： 10. 3969/j. issn. 2095-1248.2024.06.008

A modified STPA method and its application in safety analysis of complex system

CHEN Lei

（College of Safety Engineering，Shenyang Aerospace University，Shenyang 110136，China）

Abstract：A method of expanding and improving the hierarchical control structure model（HCSM）of system-theoretic process analysis（STPA）using functional attribute（FA）and directional interaction tag（DIT）was proposed. Based on this method，the hierarchical functional control structure and interaction model（HFCSIM）of the system and essential improvement to STPA was obtained. Through this modification，issues such as the lack of specific methods and forms follow，incomplete interaction information between components，excessive reliance on “Brainstorming” and the difficulty in ensuring model consistency could be solved，and the systematicness，completeness and correctness of the analysis results could be fundamentally ensured. Finally，the effectiveness of the modified method was validated by taking the aircraft wheel braking system as an example.

Key words：functional attribute；directional interaction tag；hierarchical functional control structure

收稿日期： 2024-04-26

基金项目： 辽宁省教育厅高等学校基本科研项目（项目编号：LJKZ0169）

作者简介： 陈磊（1981-），女，辽宁沈阳人，讲师，博士，主要研究方向：复杂系统安全性分析，E-mail：zheermao1005@163.com。

and interaction model；STPA；safety analysis

STPA是以基于系统思维的事故模型及分析过程（system-theoretic accident modeling and process，STAMP）为基础的危险分析技术[1]。它将安全视为控制问题，并使用层次化的安全控制结构HCSM来描述系统。当组件之间的不安全交互、外部干扰和（或）组件故障未得到充分控制时，就会发生事故。它的出现弥补了传统安全分析方法在识别软件及系统的设计错误和缺陷，特别是组件间异常交互等潜在危险元素及事故场景方面存在的严重不足。目前，STPA已在各领域得到广泛应用[2]。这足以证明，它能够在分析过程中应对复杂性带来的影响，并通过增强对系统和风险的理解来减少事故的发生[3]。

近年来，学者们对STPA的改进工作大致可以概括为两类：第一类为对STPA的形式化描述，如文献[4]形式化定义了不安全控制动作（unsafe control actions，UCA），并用真值计算方法自动识别UCA。文献[5]延续了文献[4]的方法。文献[6]对STPA的形式化是体现在对时间相关UCA的描述上。文献[7]使用了有限状态机的静态信息，以人工方式描述系统信息。第二类仅用STPA作为获取安全需求的手段，再利用形式化工具验证系统是否满足这些安全需求，如文献[8—9]先通过STPA获取安全需求，再利用NuSMV识别系统的控制缺陷。文献[10]将STPA与模型检测工具SPIN相结合，实现安全分析与验证的无缝对接。文献[11]用Event-B建立形式化模型来验证STPA提出的需求。文献[12—15]将STPA与UPPAAL相结合，对不安全控制动作及损失场景进行识别。两类改进都通过形式化的手段提高了分析效率，一定程度上降低了主观性分析，但都没有对STPA方法进行本质性的改进。而STPA的不足主要体现在HCSM上。其问题主要有：（1）建模过程不够详细且缺乏系统性和完整性；（2）在不同的分析者间或不同的分析阶段，HCSM的一致性和连续性很难维持，在本质上影响分析的正确性和结果的有效性。

针对上述问题，本文提出一种使用功能模块（functional module，FM）、功能属性FA及有向交互标签DIT对HCSM进行拓展和改进的方法，用以建立系统的层次化功能控制结构及交互模型HFCSIM。这个方法能够解决用STPA的HCSM在构建过程中无严谨的具体形式可参照，从而导致模型及交互信息不完整，模型主观性强及模型一致性难以得到保障的问题，在根本上确保分析结果的系统性、完整性和正确性。

1　STPA方法

STPA主要有3个步骤：（1）建立分析所需的工程基础，包括确定系统可能发生的事故、导致事故的系统级危险及构建HCSM。（2）识别导致危险的UCA。STPA将不安全的控制动作分为4类，它们分别是未提供控制动作、提供了不正确的控制动作、提供控制动作的时序错误及控制动作持续的时间过长或过短。（3）通过分析HCSM的每个组成部分及它们之间的交互行为，确定导致UCA发生或安全约束（safety constraint，SC）被违反的原因[16]。

2　STPA方法的改进

为描述简便，本文提出的改进的STPA方法将在下文中记为MSTPA（modified STPA）。MSTPA与STPA的主要区别体现在MSTPA对HCSM的改进上，即构建HFCSIM，除此之外的其余步骤均相同。以下将对HFCSIM的构建方法及过程进行详细的阐述。

2.1 层次化功能控制结构及交互模型HFCSIM的构建

2.1.1 功能模块的功能属性及有向交互标签

功能共振事故模型(functional resonance accident model,FRAM)是Hollnagel于2004年提出的事故模型[17],其通过含6个功能属性FA的模型,分析系统功能环节间的相互作用,研究系统内功能属性异变导致的危险因素的耦合与传播[18]。虽然FRAM对系统的功能属性FA进行了比较全面细致的划分,在事故模型建立方面较STPA指导性更强,易于维持模型的一致性和完整性,但FRAM在系统需求捕获、设计错误、组件间异常交互及故障识别方面的能力显著弱于STPA[19]。因此本文将借鉴FRAM对功能属性FA的划分,将其与STPA的HCSM建模过程相融合,从而在最大程度丰富HCSM对各组件间交互耦合关系描述的同时,最大限度降低主观性对模型产生的影响,最终使分析结果的完整性、一致性及正确性得到保障。

首先,将系统看做由若干个不同的功能模块FM组成。在STPA中,功能模块FM可分为控制器模块(controller,CT)、执行器模块(actuator,AT)、传感器模块(sensor,SE)和被控对象模块(controlled process,CPR)。然后,根据FRAM对6个功能属性FA的描述并结合STPA自身特点,对FM的功能属性FA从控制(control,C)、状态变量(state variable,SV)、反馈(feedback,FB)、保障(guarantee,G)及模型(model,M)等5个方面进行定义。

为详细描述各功能模块FM之间的交互耦合行为,需要在每个功能属性FA中进行更细致的有向功能标签DIT的划分。有向功能标签DIT是有名称、起点及终点的有向线,其功能是明确各功能模块FM间的交互耦合行为及方向,具体内容如下:

(1)每个功能模块FM的控制C属性包含该模块输出的控制行为(control action,CA)、来源于系统内部其他功能模块FM的输入控制命令(input control command,ICC)、来源于系统外其他通道的控制命令(external control command,ECC)。其中,ICC和ECC既是控制命令也是输入,CA是控制行为的同时也是输出,本研究范围内将其归为FM的控制属性。

(2)每个功能模块FM的状态变量SV属性包含系统状态变量(system state variable,SSV)和环境状态变量(environment state variable,ESV)。

(3)每个功能模块FM的反馈FB属性包含由较高层次收到的来源于较低层次的反馈(feedback from lower level,FFL)和由较低层次提供给较高层次的反馈信息(feedback to upper level,FTU)。

(4)每个功能模块FM的保障G属性是指功能执行所需的前提条件和资源,没有这些条件和资源,功能无法在其他属性都完备的情况下正常运行,因此称其为保障属性。前提(precondition,P)是指功能执行前必须具备的条件,在P(一个或多个)得以满足前功能是无法开始执行的,P可以被理解为在功能执行前,必须为“真”的系统状态或必须被证实的已经具备的某些条件;资源(resource,R)是功能执行所需或消耗的事物,即功能对输入进行处理以产生输出所必须的如硬件、软件、程序、人力及能源等。

(5)每个功能模块FM的模型M属性包含过程模型(process model,PM),其中包括对控制关系的描述。

功能模块FM的功能属性FA及对应的有向交互标签DIT如图1所示。

2.1.2 HFCSIM的构建

当给定某一系统时,HFCSIM的构建过程可以根据以下步骤来完成:(1)明确系统功能,确定系统的边界;(2)将系统按照内部功能划分为若干FM;(3)明确各个FM所在的层次及相互之间的关系;(4)确定每个FM所具备的

全部FA；(5) 确定每个FM的FA所包含的所有DIT的名称及方向，并将各FM连接起来，形成HFCSIM；(6) 对构建的HFCSIM进行梳理和检查，以确保其能够充分完整地体现系统整体功能及系统内各FM之间的交互耦合关系，如有缺失，则返回至第(4)步对模型进行修正和补充，直至模型正确且完整。步骤(4)—(6)会随设计过程的推进而不断迭代，初始的HFCSIM可能仅有简单的FM、FA及DIT，但随设计细节的不断完善，模型也会逐渐被细化，其DIT也将逐渐趋近完善，具体流程如图2所示。

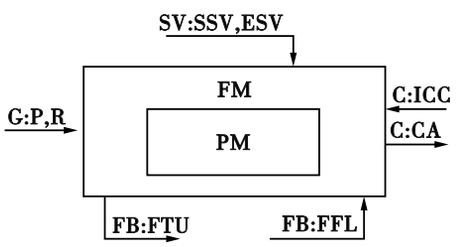

图 1　功能模块FM的功能属性FA及对应的有向交互标签DIT

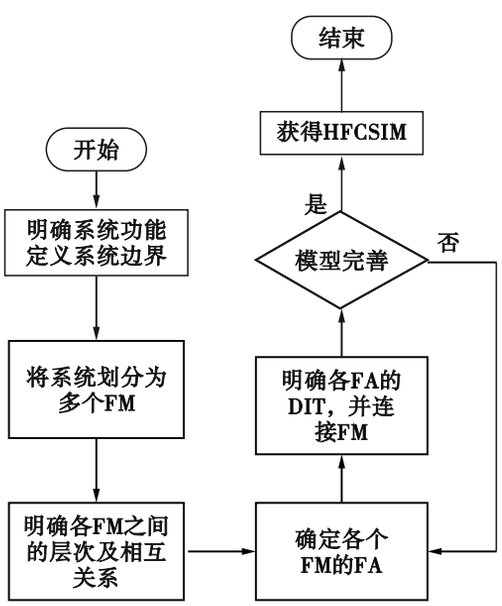

图2　HFCSIM建模流程图

2.2　基于功能属性FA及有向交互标签DIT的UCA及其致因分析

STPA方法认为，即便没有物理上的失效，组件间异常的交互也可能导致事故的发生。因此，HFCSIM对交互的体现程度将直接影响分析的深度和广度，进而影响结果的正确性和完整性。创建HFCSIM的目的除提高建模的可依据性，确保模型的一致性、完整性及正确性之外，另一个重要的目标就是通过DIT来细化和引导UCA及其致因的识别。

如上文所述FM的FA共分为5种，即控制C、反馈FB、状态变量SV、模型M和保障G。借鉴UCA的4种分类，结合每种FA中DIT的实际性质，并考虑标签的方向，将每种DIT的可能导致UCA的原因都进行分析分类，其具体内容如表1所示。

依据表1中的引导词，结合相应的HFCSIM，则可对UCA及其致因展开详细的分析。由于有DIT的存在，很容易维持分析的连续性及一致性，且不易因忽略信息导致分析的不完整和不正确。

3　MSTPA应用示例

3.1　SAE ARP4761机轮刹车系统

本文选取SAE ARP 4761中提供的经典案例机轮刹车系统(wheel brake system，WBS)为研究对象，对上述方法的应用进行阐述。

WBS与其他地面运动系统及更高层次的控制系统共享数据，由电子电气、液压、机械等多种组件集成，且无论是刹车系统控制单元(brake system control unit，BSCU)还是液压系统(hydraulic system，HS)都具备冗余；同时，WBS还是具备多重操作模式的人机交互系统，是典型的复杂系统。WBS安装在两个主起落架上，控制每个起落架上4对共8个机轮的刹车。其主要功能有地面减速制动、停留刹车、改变方向和空中刹车。WBS中液压回路子系统由正常模式线路(normal mode line，NML)和备用模式线路(alternate mode line，AML)组成。正常模式线路简称绿线路(green line，GL)，由绿色液压泵(green pump，GP)供压；

表1 以DIT为引导的UCA及其致因分析分类

序号	FA	DIT	不恰当/错误类型
1	C	CA	未提供该控制行为导致不安全状态
			提供了控制行为导致不安全状态
			控制行为提供的时机过早、过晚或顺序错误
			控制行为持续时间过长或结束过早
		ICC	该控制命令未被输入导致不安全状态
			该控制行为的输入导致不安全状态
			控制行为输入时机过早、过晚或顺序错误
			控制行为持续时间过长或结束过早
		ECC	该系统外部控制命令未被提供导致不安全状态
			提供了该系统外部控制行为导致不安全状态
			系统外部控制行为输入的时机过早、过晚或顺序错误
			系统外部控制行为持续时间过长或结束过早
2	M	PM	过程模型不正确
			过程模型不连续
			过程模型不完整
3	FB	FFL	需要时低层次未提供该反馈信息
			低层次提供的反馈信息不够准确
			低层次提供的反馈信息过晚，或持续时间过短
			低层次提供的反馈信息与实际情况不一致
			低层次提供的正确反馈信息被遗失
		FTU	需要时高层次未收到反馈信息
			高层次接收的反馈信息不够准确
			高层次接收到反馈信息过晚，或持续时间过短
			高层次接收到的反馈信息与实际情况不一致
			向高层次提供的正确的反馈信息被遗失
4	SV	SSV	需要时未提供该状态参数
			提供的状态参数不够准确
			提供状态参数的时间过晚或持续时间过短
			提供了与实际情况不一致的状态参数
			提供了正确的状态参数但被遗失
		ESV	需要时未提供该环境参数
			提供的环境参数不够准确
			提供状态参数的时间过晚或持续时间过短
			提供了与实际情况不一致的状态参数
			提供了正确的状态参数但被遗失
5	G	P	未提供该前提条件导致危险
			该前提条件的提供导致危险
			过早、过晚或以错误的顺序提供了前提条件
			前提条件维持的时间过长或过短
		R	未提供该资源导致危险
			资源提供的不恰当导致危险
			提供资源的时机过早或过晚
			资源持续的时间过长或过短

备用模式线路简称蓝线路(blue line，BL)，即由蓝色液压泵(blue pump，BP)或蓄压器(accumulator pump，ACCP)供压组成。两条线路上的液压泵可以为8个机轮提供刹车的压力。除液压泵外，液压回路主要由以下组件构成：隔离阀(isolation valve，ISV)、关断阀(shut-off valve，SV)、选择阀(selector valve)、计量伺服阀(metering servo valve，MV)等。

BSCU是WBS中唯一的数据组件。BSCU的一部分输入来自于更高级别的WBS，如自动刹车控制命令Autobrake，设置刹车减速率(deceleration rate，Dec_R)、飞机的地速(aircraft ground speed，AC_GS)及防滑命令(anti-skid)等，另一部分是液压子系统HS各液压线路的液压、工作模式的反馈及机轮的轮速(wheel speed，Wheel_S)。为了提高可靠性，BSCU内有2个相互独立的LRU(line-replaceable unit)，其中一个为另一个的备用。每个LRU内，均有监测(monitor，MON)和命令(command，CMD)两个单元模块。WBS系统的构成如图3所示。

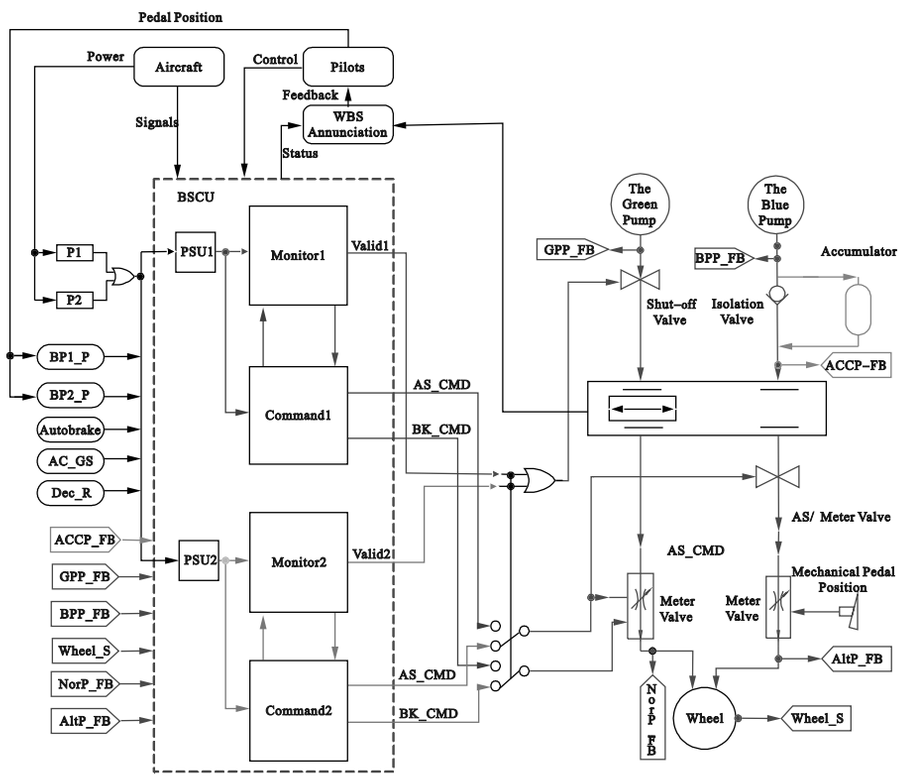

图3　WBS系统的构成

注：BP1_P：Braking Pedal 1 Position；BP2_P：Braking Pedal 2 Position；DecRate：Decelerate Rate；C_GS：AC Ground Speed；GPP_FB：Green Pump Pressure Feedback；BPP_FB：Blue Pump Pressure Feedback；ACCP_FB：Accelerator Pressure Feedback；Wheel_S：Wheel Speed；NorP_FB：Normal Mode Pressure eedback；AS-CMD：Anti-Skid Command；BK-CMD：Braking Command.AltP_FB：Alternate Mode Pressure Feedback。

3.2　基于MSTPA的安全分析过程

3.2.1　系统级事故及系统级危险的确定

根据MSTPA的分析步骤，首先对WBS系统地面刹车过程相关的系统级事故及诱发事故的系统级危险进行识别。根据WBS的系统功能及STPA中对事故的定义[1,16]，其可能引发的系统级事故有：(1)AC-1：飞机内或(及)飞机外部区域的相关人员的伤亡；(2)AC-2：飞机级或其他飞机的机体或子系统受损或完全被破坏；(3)AC-3：地面移动/固定的设备或设施受到碰撞受损或完全被破坏。

系统级危险则是指可能导致系统级事故

发生的一系列事件，因此，在WBS中会导致上述事故发生的系统级危险及其与系统级事故的对应关系为：(1)H-1：在飞机着陆(landing，LA)、中断起飞(rejected takeoff，RTO)过程中，刹车压力不足或刹车不及时，使制动不充分，无法充分减速，导致飞机冲出/偏离出跑道，对应事故AC-1、AC-2、AC-3；(2)H-2：飞机刹车失控使飞机与地面建筑物或其他设备设施发生碰撞，对应事故AC-1、AC-2、AC-3；(3)H-3：飞机刹车系统失效或由于不恰当的操作导致飞机未停靠在安全区域，妨碍其他飞机的正常运行，对应事故AC-1、AC-2；(4)H-4：因跑道或防滑系统等原因导致飞机机轮出现打滑、抱死等现象，使机轮爆胎，对应事故AC-1、AC-2。其中飞机冲出/偏离出跑道的事件属于导致事故的高风险事件[19]，因此本研究将以系统级危险H-1为例展开后续的分析。

3.2.2 HFCSIM的构建

在确定了系统级事故及相应的系统级危险后，下一步需要建立WBS人机交互系统的HFCSIM，为后续UCA及其致因的分析和识别打下基础。按照系统功能，可将整个WBS人机交互系统划分为4个FM，即机组人员Pilots、刹车控制单元BSCU、液压物理系统HS及机轮Wheels。其中，Pilots和BSCU为控制层，HS及Wheels为被控对象层。Pilots、BSCU、HS及Wheels所具备的FA及有向交互标签DIT如表2所示。根据表2中内容绘制WBS人机交互系统的HFCSIM，如图4所示。

表2 WBS系统的FM、FA及DIT

FM	序号	FA	DIT	内容	方向	备注
Pilots	1	C	CA	启用或解除Autobrake模式	Pilots→BSCU	5
	2			设置减速率(deceleration rate，Dec_Rate)		
	3			脚踏板电信号		
	4			启动或关闭BSCU		
	5			防滑命令		
	6			脚踏板机械位置	Pilots→HS	
	7			故障提示及警报		
	8			压力线路状态		
	9			NM/AM工作模式指示		
	10	FB	FFL	自动刹车设置指示	BSCU→Pilots	Input
	11			Autobrake状态指示		
	12			预设的减速率		
	13			BSCU启动或关闭提示		
	14			飞行阶段(taxing，landing，RTO(rejected takeoff))		
	15		SSV	其他刹车减速系统的状态参数	AC→Pilots	Input
	16	SV		飞机地速(AC ground speed，AC_GS)		
	17			飞机跑道长度	E→Pilot	Input，E=Environment天气影响能见度
	18		ESV	跑道状况		Input，湿滑、干燥、结冰等
	19			当前的飞行阶段		
	20	M	PM	Autobrake当前的状态	Pilots	Inside
	21			BSCU等WBS系统组件当前状态		

续表 2

FM	序号	FA	DIT	内容	方向	备注
BSCU	22	C	ICC	飞机地速 AC_GS	Pilots→BSCU	Input
	23			跑道的长度		
	24			其他地面减速系统当前状态		
	25			启用或解除 Autobrake 模式		
	26			设置减速率		
	27			脚踏板电信号		
	28			关闭或启动 BSCU		
	29		CA	对 BP 线路发布防滑命令	BSCU→HS	Output
	30			GP 中 SV 的开启		
	31			实施自动刹车（对 GP 线路发布自动刹车/防滑命令）		
	32			对BP线路发布防滑命令		
	33	SV	SSV	Autobrake 模式触发（扰流板伸出信号）	系统→BSCU	Input
	34			AC_GS		
	35	FB	FTU	故障检测结果	BSCU→Pilots	Output
	36			压力线路状态		
	37			NM/AM 工作模式指示		
	38			自动刹车设置指示		
	39			Autobrake 状态指示		
	40			当前减速率指示		
	41			BSCU 启动或关闭指示		
	42		FFL	轮速	Wheels→BSCU	Input
	43			GP/BP/ACC 的状态反馈	HS→BSCU	Input
	44			NM/AM/EM 工作状态反馈		
	45	M	PM	减速率	BSCU	Inside
	46			Autobrake 状态		
	47			飞机地速 AC_GS		
	48			轮速		
	49			刹车压力		
	50			防滑调节		
	51			液压线路状态		
	52			BSCU 自身状态		
	53	G	P	系统提供电源	系统→BSCU	Input
	54	C	CA	刹车/防滑压力调节	HS-Wheels	Output
	55		ICC	机组人员脚踏板机械位置	Pilots→HS	Input
HS	56			GP 中 SV 的开启	BSCU→HS	
	57			对 GP 线路发布刹车/防滑命令		
	58			对 BP 线路发布防滑命令		
	59	FB	FTU	GP/BP/ACC 的状态反馈	HS→BSCU	Output
	60			NM/AM/EM 工作状态反馈		
Wheels	61	C	ICC	刹车压力/防滑调节	HS→Wheels	Input
	62	FB	FTU	轮速	Wheels→BSCU	Output

3.2.3 UCA的识别

在建立HFCSIM后，接下来的步骤是对UCA进行识别。因本文着重研究的是WBS，且出于篇幅原因，将仅对BSCU的控制行为——实施自动刹车进行分析，根据STPA对UCA的4种分类可以识别出如表3所示的导致H-1的BSCU实施自动刹车相关的UCA。

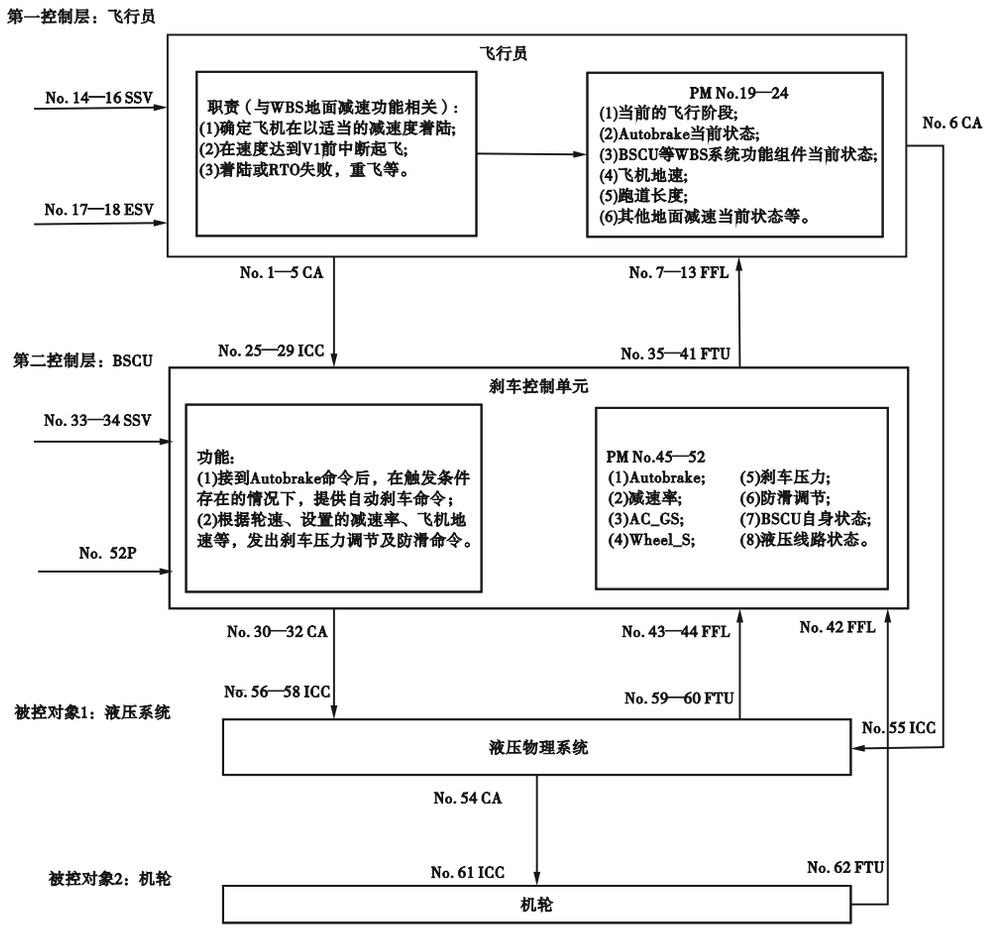

图4 WBS人机交互系统HFCSIM

表3 导致H-1的与BSCU实施自动刹车相关的UCA

控制器	控制动作	控制对象	UCA类型			
			未提供导致危险	提供导致危险	过早、过晚或错误的顺序提供导致危险	持续时间过长或过短
BSCU	实施自动刹车	HS	Landing/RTO阶段没有实施自动刹车操作，致使飞机未减速，冲出跑道。	自动刹车压力提供较小，飞机减速不足，最终冲出跑道。	机轮未触地就实施了自动刹车，致使飞机失控，机轮由于过热而起火。	自动刹车时，刹车持续时间过短，飞机未能充分减速，冲出跑道。
				自动刹车压力提供较大，机轮抱死、过载、过热、飞机失控。	RTO过程中，达到V1速度后才实施自动刹车，导致飞机冲出跑道。	
					飞机在落地一段时间后才实施自动刹车，导致飞机减速不够充分，最终冲出跑道。	

3.2.4　危险致因因素(casual factor，CF)的识别

在确定了导致H−1与BSCU实施自动刹车命令相关的UCA之后，应对导致UCA的危险致因因素进行分析识别。由于篇幅原因，本文仅对导致H−1与BSCU实施自动刹车命令相关的UCA之一“BSCU在飞机Landing/RTO阶段，未提供自动刹车操作，导致飞机无减速，冲出跑道”的致因进行分析。识别出UCA的致因因素如表4、表5所示。

表 4　以BSCU的DIT为引导的CF分析

UCA	FM	以DIT为引导的CF分析		
LA/RTO时未实施自动刹车控制命令，致使飞机未充分减速，冲出跑道。	BSCU	FA	DIT	CF
		C	ICC	机组人员未预置自动刹车命令
		M	PM	BSCU过程模型中有不正确/不一致/不连贯的部分轮速反馈不正确，导致BSCU认为飞机已停止运动
		FB	FFL	HS系统NLM线路压力状态反馈不正确，BSCU认为NLM线路失效
				地面减速扰流板未能正常伸出
		SV	SSV	地面减速扰流板伸出信息未正确传递给WBS系统
				飞机地速AC_GS输入数据错误
		G	R	BSCU断电

表 5　以BSCU组件错误/故障/失效为CF的分析

UCA	FM	组件错误/故障/失效		
LA/RTO时未实施自动刹车控制命令，致使飞机未充分减速，冲出跑道。	BSCU	BSCU的Autobrake命令输入通道出现Bug/受到电磁干扰，导致输入信息不完整		
		BSCU的两个MON监控错误，认为CMD失效导致NLM液压线路被切换至AM		
		BSCU的两个LRU同时失效	LRU1失效	LRU1的电子系统故障或LRU1断电
			LRU2失效	LRU2的电子系统故障或LRU2断电
		BSCU内部通信总线出现故障，导致传输的信息出现错误		
		选择开关卡死	选择开关卡死在两个命令单元输出的中间位置，导致BSCU无命令输出	
			选择开关卡死在LRU1输出位置但LRU1失效	LRU1电子系统故障或LRU1断电

4　结论

STPA是以STAMP理论为基础的危险分析技术，虽弥补了传统安全分析技术在应对现代复杂系统时的一些缺陷，但仍旧存在一些不足，如HCSM的构建规则不够明确，极易导致模型所包含的信息不完整，不同分析人员对模型理解的不一致，并最终导致分析结果不正确。

针对上述STPA的局限性，本文通过划分和建立系统的功能模块FM、功能属性FA及有向交互标签DIT，对STPA层次化控制结构模型HCSM进行了改进，形成了新的层次化功能控制结构及交互模型HFCSIM，弥补了STPA在

模型建立的过程中仅靠自然语言描述模型建立规则的不足，提高了模型信息的完整程度，可以在一定程度上保障分析过程中模型的一致性、完整性及正确性，从而提高分析结果的正确性和完整性，并通过对机轮刹车系统WBS的分析，验证了这一改进的有效性。

参考文献(References)：

[1] Leveson N G. Engineering a safer world: systems thinking applied to safety [M]. Cambridge: MIT Press, 2011.

[2] 林经源，何涛. 基于STPA与时序逻辑的CTCS-3级列控系统安全分析[J]. 兰州交通大学学报，2023，42(4)：80-90.

[3] Bjerga T, Aven T, Zio E. Uncertainty treatment in risk analysis of complex systems: the cases of STAMP and FRAM [J]. Reliability Engineering & System Safety, 2016, 156(5): 203-209.

[4] Thomas J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis [D]. Massachusetts: Massachusetts Institute of Technology, 2013.

[5] Suo D. Tool-assisted hazard analysis and requirement generation based on STPA [D]. Massachusetts: Massachusetts Institute of Technology, 2016.

[6] Asare P, Lach J, Stankovic J A. FSTPA-I: a formal approach to hazard identification via system theoretic process analysis [C]//2013 ACM/IEEE International Conference on Cyber-Physical Systems. Philadelphia: IEEE, 2013: 150-159.

[7] Abdulkhaleq A, Wagner S. Integrating state machine analysis with system-theoretic process analysis [J]. Software Engineering, 2013, 19(2): 501-514.

[8] 夏宇. 基于NuSMV和STPA的RBC交接场景安全分析方法研究[D]. 北京：北京交通大学，2018.

[9] Wang H L, Zhong D M, Zhao T D. Avionics system failure analysis and verification based on model checking [J]. Engineering Failure Analysis, 2019, 13(5): 373-385.

[10] Abdulkhaleq A, Wagner S. Integrated safety analysis using systems-theoretic process analysis and software model checking [C]//International Conference on Computer Safety, Reliability, and Security. Cham: Springer, 2015: 121-134.

[11] Howard G, Butler M, Colley J, et al. A methodology for assuring the safety and security of critical infrastructure based on STPA and Event-B [J]. International Journal of Critical Computer-Based Systems, 2019, 9(1/2): 56.

[12] Zhao C X, Dong L, Li H, et al. Safety assessment of the reconfigurable integrated modular avionics based on STPA [J]. International Journal of Aerospace Engineering, 2021, 21(1): 8875872.

[13] 钟德明，宫浩原，孙睿. 一种准确识别损失场景的STPA[J]. 北京航空航天大学学报，2023，49(2)：311-323.

[14] 李浩. 基于STAMP理论的机载显示系统安全性分析方法研究[D]. 天津：中国民航大学，2020.

[15] 王鹏，李浩，赵长啸，等. 基于STPA的机载平视显示系统安全性分析[J]. 电讯技术，2019，59(12)：1469-1476.

[16] Leveson N, Thomas J. STPA Handbook [EB/OL]. (2018-03-16) [2021-04-19]. https://psas.scripts.mit.edu/home/materials/.

[17] Hollnagel E, Goteman O. The functional resonance accident model [J]. Proceedings of cognitive system engineering in process plant, 2004, 20(3): 155-161.

[18] 张玥，帅斌，黄文成，等. 基于FRAM的铁路危险品运输事故演化机制研究[J]. 中国安全科学学报，2020，30(2)：171-176.

[19] 史思杨. 基于MB-STPA的飞机刹车系统安全性分析方法研究[D]. 天津：中国民航大学，2020.

(责任编辑：刘划　英文审校：曹依霏)