文章编号:1674-8190(2016)03-309-07

综合火/飞/推控制系统复杂任务的 STAMP 建模和 STPA 分析

胡剑波,郑磊

(空军工程大学 装备管理与安全工程学院,西安 710051)

摘 要:随着系统复杂性的日益增高,人为操作失误引起的系统任务失败呈增加的态势,传统的 FTA、FMEA 等基于线性事件链模型的分析方法已不能满足分析人为操作不当导致的系统危险,采用基于系统理论的过程分析方法,对作战飞机综合火/飞/推控制(IFFPC)系统中人为操作不当引起的潜在危险进行安全性分析。首先建立作战飞机 IFFPC 系统的 STAMP 模型,进而生成作战飞机 IFFPC 系统的 STPA 分析模型,最后根据提出的五类引起任务失败的原因因素,详细地进行作战飞机 IFFPC 系统不安全控制作用(UCA)的因素识别。结果表明:所采用的基于系统理论过程的分析方法弥补了传统安全性分析方法存在的缺陷,有效地解决了传统的 FTA、FMEA 等安全性分析方法不能很好地解决人为危险因素的问题,为含有人工控制器的复杂系统的安全性分析提供了一种新的思路。

关键词:综合火/飞/推控制系统;安全性分析;人工控制器;STPA 模型;危险因素识别

中图分类号:X949 **文献标识码**:A **DOI**:10.16615/j.cnki.1674-8190.2016.03.007

STAMP Modeling and STPA Analysis for Complex Tasks of Integrated Fire, Flying and Propulsion Control Systems

Hu Jianbo, Zheng Lei

(College of Material Management and Safety Engineering, Air Force Engineering University, Xi'an 710051, China)

Abstract: With the system's complexity increasing, the accidents caused by human errors are increasing. Traditional analysis methods, such as FTA(Fault Tree Analysis) and FMEA(Failure Mode and Effects Analysis) that based on the linear chain of events, can not identify the system risks caused by human errors. So the system-theoretic process analysis method is used to identify the potential risks of the combat aircraft's integrated fire, flying and propulsion control(IFFPC) system caused by human errors. Firstly, a STAMP model of the combat aircraft's IFFPC system is established, then the STPA analysis model of the combat aircraft's IFFPC system is built. In the end, according to the five kinds factors of failed mission, the risk factors of the combat aircraft's IFFPC system's unsafe control action(UCA)are identified. The result shows that, the STPA method makes up for the weaknesses of traditional analysis methods, and effectively solves the problem that the traditional analysis methods, such as FTA and FMEA based on the linear chain of events, can not identify the system risks caused by human errors. The method laid a solid foundation for the further safety analysis.

Key words: integrated fire, flying and propulsion control systems; safety analysis; manual controller; STPA model; identify risk factors

0 引 言

随着技术的进步,系统的复杂性日益增高,人为差错原因引起的事故越来越多,急需从控制的角度来分析和研究人为因素是如何引起事故的。同

收稿日期:2016-04-19; **修回日期**:2016-06-11

通信作者:胡剑波,jian_bo_h@163.com

时，人工控制器在复杂系统中的地位越来越重要。一是复杂系统为了追求高效率，通常运行在系统边界状态，这对人工控制器性能提出了严酷要求，稍有不慎，就会导致事故发生；二是信息技术被大量应用于复杂系统，其信息量大、关联性强，这对人工控制器能否正确地理解和解释这些信息带来了难度，若理解或者解释不正确，就会导致事故；三是人工控制器的上下文关联因素多，容易导致所做动作不符合顺序和时机要求，从而引起事故的发生。

传统的安全性分析方法，例如 FTA、FMEA，已经在实际应用中遇到了大量难题[1]，且未能有效地考虑人工控制器。例如，2009 年法国航空 447 坠毁事件有力地证明了传统安全性分析方法存在一定的缺陷[2]。法国民用航空安全性调查机构(BEA)的调查结论是：坠毁的原因集中在机组人员的“故障”上，可能是因为“提供了不合适的控制输入”，“识别其偏离飞行路径的时间太晚了”，或者“不能”诊断停车情形，结果缺少使飞机恢复飞行的输入。但是这一坠毁事件的实际原因依然令人深思，包括系统性因素、操作杆布局方式以及反馈等。可见，难以通过 FMEA 或者 FTA 等分析方法来得到上述结论。类似案例很多，例如 Turkish 航空公司的 1951 航班事故[3]，尽管在荷兰安全性委员会的报告结论中没有直接涉及人为差错，但提到的设备故障组合、不合理设计的自动化装置以及较差的机组资源管理等均与人工控制器有关。上述案例表明，除非在复杂系统的安全性分析中有更好的分析技术来综合地分析人为控制器，否则类似的事故还会发生。通过对以往的飞行事故案例进行分析，总结出有效的分析技术应具备如下特点：

①这种分析技术必须是系统的。将人当作系统的重要组成，从系统的角度来考虑安全性，对于识别的危险源，要运用系统建模的方法来刻画危险源的发生机理、传递过程和约束关系，从而得到有效的控制方法，并落实到设计和运行要求中。

②这种分析技术必须是完整的。将人当作系统的重要组成，从系统状态观测、状态可控制的角度来考虑安全性，在危险源识别、分析和控制中，必须考虑尽可能多的环境因素、外部干扰和内部各组成的可能状态，提出完整的安全性解决方案。

③这种分析技术必须是可行的。将人当作系统的重要组成，从人的自身能力、系统其他组成能力的角度来考虑安全性，在危险源识别、分析和控制中，合理配置系统的传感器、显示器和执行器，确保提出的安全性解决方案切实可行。

在相关的文献中，已经关注并开始研究存在的问题。J. R. Boyd[4] 利用反馈控制原理，建立了军队指挥系统的人工控制器模型，指出了人工控制决策模块、信息反馈对于任务失效的重要影响。J. Rasmussen[5] 利用人类认知的能力、规则和知识架构，提出了基于反馈控制原理的人工控制器 SRK 模型，构建了低层技能回路、中间层规则回路和高层知识回路，指出了技能回路不良、规则不全、知识不足对于任务失效的重要影响。L. T. Cameron[6] 在分析了人类认知生态心理模型及相关要素的基础上，结合文献[4]和[5]，利用 Nancy G. Leveson[7] 提出的基于系统理论的事故模型和过程(STAMP)及基于系统理论的过程分析(STPA)，综合运用分层结构化模型和反馈控制原理，提出了一种人工控制器的 STPA 方法。可见，对于含有人工控制器的复杂系统，系统理论、控制理论是分析和控制其安全性的有效途径。

本文在文献[4-6]的基础上，采用基于系统理论的过程分析方法，以作战飞机 IFFPC 系统的复杂任务为研究对象，建立含有人工控制器的 STAMP 模型，进行 STPA 分析，并将其应用于作战飞机 IFFPC 系统的任务失效分析中，以期为今后进一步的安全性分析研究奠定基础。

1 IFFPC 系统的 STAMP 模型

STAMP 模型运用系统理论和控制理论，将安全性问题当作系统的一种涌现特性。系统安全性被视为建立在组件之间相互作用和环境基础上的一种特性，STAMP 继承了涌现性、层次性、可控性等系统概念，并在系统中施加安全性约束[8]。与将事故视为起源于初始原因事件的线性传递相比，STAMP 认为事故是由于不合理的控制和系统开发以及设计和运行阶段安全性相关约束的不合理施加所致[9-10]。

参考文献[11-12]，结合 STAMP 相关理论，构建军用飞机 IFFPC 系统的 STAMP 模型，如图 1 所示。利用该 STAMP 模型，可揭示全新的事故因果关系模型。本文所研究的事故泛指不能预期完成任务。位于低层的发动机和飞机机体各自具

有两个相对独立的控制系统,但必然通过飞机动力学模型和运动学模型而相互关联。位于上层的火力控制系统,向人工控制器提供任务控制指令,而人工控制器又向火力控制系统提供反馈信息;这些控制指令可以直接送向飞机运动控制系统和发动机控制系统,也可直接接受来自飞机运动控制系统、发动机控制系统的反馈信息。最重要的人工控制器位于中间层,既要向两个低层控制系统施加控制信号,又要及时接受来自低层传感器的状态反馈信息,同时需要综合判断两个低层的运行态势,综合火力控制要求、运行环境等信息,进行统一协调。为了实现 IFFPC 系统分层控制,应用任务约束、控制作用、反馈以及过程模型,其层次结构清晰。在层次结构中的每个层次均可当作一个负责向其下方层次强制任务约束的控制器。从控制理论上来看,控制器需要四个必要条件:目标条件(任务约束)、作用条件(控制作用)、可观测性条件(反馈)及模型条件(过程模型)。STAMP 定义了四类必须消除或者控制的不安全控制作用,以阻止事故发生:①安全性要求的控制作用不提供或者跟不上;②提供了导致危险性的不安全控制作用;③潜在的安全控制作用提供得太晚、太早,或次序不符合要求;④安全控制作用停止得太快或者作用得太久。

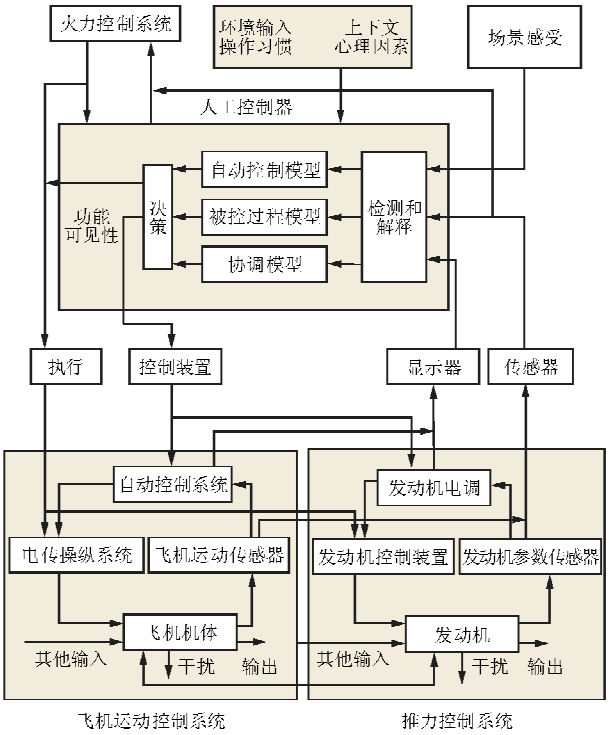

图 1　IFFPC 系统分层控制结构模型

Fig. 1　Hierarchical control model of IFFPC system

2　IFFPC 系统的 STPA 模型

根据图 1 所示的 IFFPC 系统的 STAMP 模型,结合 IFFPC 系统的决策过程,得到 IFFPC 系统的 STPA 模型,如图 2 所示。

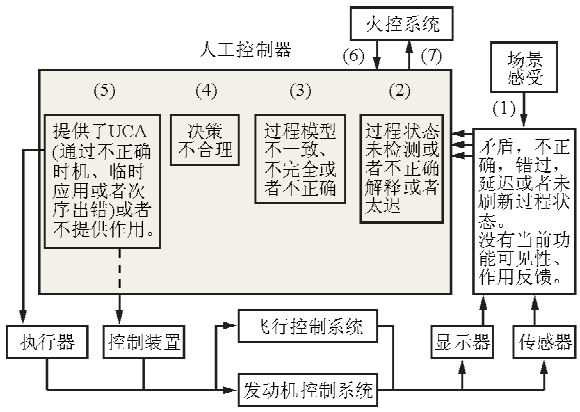

图 2　人工控制器 STPA 分析

Fig. 2　STPA analysis of the manual controller

2.1　人工控制器

从图 2 可以看出,人工控制器包含有五类不同的事故原因因素。这五类事故原因因素直接起源于“反馈”、人的认知(“检测与解释”、“意向模型”、“决策”),以及作用的“提供”等不同阶段。

第一类,用(1)表示,为反馈自身的相关缺陷。它包含显示器、传感器以及场景感受等所有反馈。在反馈到达人工控制器之前,要分析反馈是否存在,对于可能的 UCA(不期望控制作用),需指出反馈是否矛盾、错误、错过、延时或者未刷新。第一类事故原因因素有可能来自于与可见功能和 UCA 相关的事故原因因素。

第二类,用(2)表示,为有缺陷的反馈检测和解释。为了获得系统安全性,人工控制器必须准确地检测和解释实际存在的过程状态。任何通过反馈进行的不正确过程状态检测和解释,在出现相关的最差环境条件时,就会导致事故发生。

第三类,用(3)表示,为不一致过程模型。过程模型是人员认知的意向模型,包括被控过程(发动机、飞机本体等)的意向模型、自动控制器(飞行自动控制器、发动机电调)的意向模型以及两者协调的意向模型,是飞行员通过学习飞行手册等技术资料和通过大量实际操作建立的知识模型。当过程模型与实际过程不一致时,就会导致事故发生。

第四类，用(4)表示，为有缺陷的决策。这种事故原因是由于底层部件故障导致的决策与实际情况不符。当决策与实际情形不匹配时，就会导致事故发生。

第五类，用(5)表示，为导致UCA的不合理提供或者不提供应有的功能。不合理功能或者不提供应有的功能与反馈之间存在着内在联系，且内在联系可能是导致不安全控制作用的关键所在。

2.2 火力控制系统

图2中的(6)为火力控制系统向人工控制器下达的任务指令(给定的飞行高度、速度和方位)不合理、过时或者错误。属于第一类。

图2中的(7)为人工控制器向火力控制系统提供的反馈不合理，丢失或延时。属于第四类或者第五类。

2.3 低层控制系统

在图1所示的STAMP模型中，存在着两个低层控制系统，即飞行控制系统和发动机控制系统。这些控制系统均为一般反馈控制回路。建立的控制回路的STPA模型如图3所示，图中的①为不合理反馈，属于第一类；②为不合理控制算法，属于第二类；③为不一致过程模型，属于第三类；④为错误控制输入或者外部信息，可导致决策错误，属于第四类。

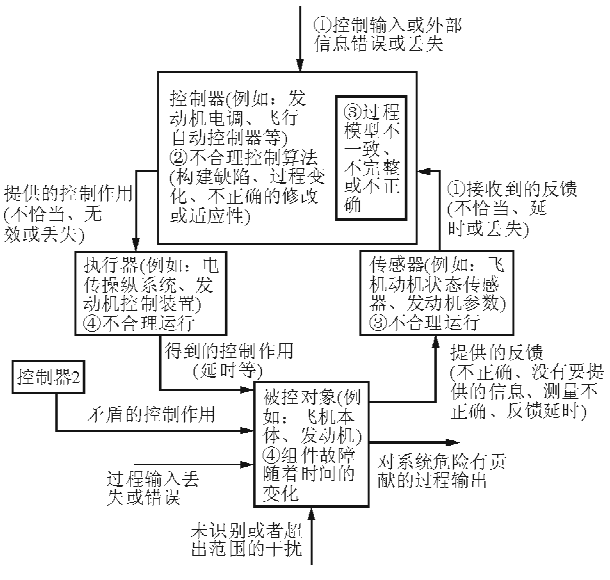

图3 控制回路的STPA模型

Fig. 3 STPA model of the control loop

3 IFFPC的STPA分析

3.1 基本步骤

STPA(系统理论过程分析)[13]是一种基于STAMP事故模型的危险性分析方法，是一种从上到下的系统工程方法，整个过程可以分成以下相互交叉、反复迭代的五个部分：

(1) 确定要分析的事故或危险性：确定分析的事故或者系统级危险性，即在开始STPA分析之前，要识别与必须控制的系统安全性要求相联系的潜在事故和相关的系统级危险性。

(2) 建立系统层次结构模型：确定分析对象的层次结构系统模型，绘制功能控制结构，包括组件之间的约束、反馈关系，以及由控制器、执行器、传感器和被控对象组成的控制回路。

(3) 识别潜在的不安全控制作用：依据STAMP中定义的四类不安全作用，识别可导致一个或多个所定义事故或者危险性的各个不安全控制作用。

(4) 构建安全性要求和约束：根据所识别的危险性控制作用，生成系统行为和组件行为的安全性要求和约束。

(5) 确定每个潜在危险控制作用的发生机理因素：检查安全控制结构的每个控制回路，识别揭示危险控制作用或者其他违反安全性约束的潜在原因因素及主要的机理因素。

鉴于上文已经建立了STAMP模型，并且STPA的重点在于安全性分析，并不是开展安全性设计，于是分析中不涉及安全性要求和约束的构建。下文将以“在飞机平台状态不满足武器发射条件的情形下，火控系统企图发现并截获目标”为任务失效源，分析该失效源对应的不期望控制作用UCA，并识别每个UCA原因因素。

3.2 引起失效的UCA识别

3.2.1 过程状态层次

根据STAMP模型，首先需确保飞机在发现并截获目标时具备发射条件，同时火控指令必须得到机长或者地面指挥中心的许可，而且在发现与截获的过程中其飞行路径不能受气象条件、地方威胁的影响。为此，高层需要考虑三组状态，即PS1(发射条件)、PS2(火控指令)和PS3(空域模型)。

每个高层 PS 所对应的低层 PS 如表 1 所示。

表 1　过程状态层次

Tabel 1　Process state level

层次	状　态		
高层 PS	1.发射条件 满足或不满足	2.指令许可 认可或不认可	3.空域模型 清空或不清空
低层 PS	1.1 飞机姿态角(Y/N) 1.2 飞行马赫数(Y/N) 1.3 飞行高度(Y/N) 1.4 发动机推力(Y/N) 1.5 飞机操纵能力(Y/N)	没　有	3.1 敌方威胁(Y/N) 3.2 天气影响(Y/N)

每个高层 PS 过程有两种基本状态:满足或者不满足。只有当高层 PS 过程状态的条件都满足时,才能开始或继续 IFFPC,若任何一个高层 PS 过程状态不满足,则不能开始或继续 IFFPC。任何一个高层 PS 过程状态只有其对应的低层 PS 过程状态都满足时才会满足。

3.2.2　UCA

通过以上的过程状态层次分析,按照 IFFPC 开始和持续两种情况,给出 UCA。所选择失效源对应的 UCA 如表 2 所示。

表 2　失效源对应的 UCA

Tabel 2　Corresponding UCA of the failure source

控制作用	UCA
开始 IFFPC	当发射条件(PS1)不满足时,开始 IFFPC 当指令许可(PS2)不满足时,开始 IFFPC 当空域清空(PS3)不满足时,开始 IFFPC
继续 IFFPC	当 PS1 不合适时,继续 IFFPC 违反 PS2 命令,继续 IFFPC 空域不满足 IFFPC 时,继续 IFFPC

3.3　引起 UCA 的事故原因因素识别

根据上述五类因素,结合过程状态层次框架分析,分别列出分析结果,如表 3 所示。

表 3　五类不同因素分析结果

Tabel 3　Five different factors' analysis results

危　险	UCA	过程模型联系	五类不同因素的分析结果				
			(1)矛盾,不正确,错过,延迟或者未刷新过程状态; 没有提供功能/作用反馈。	(2)过程状态未检测或解释不正确、太迟	(3)过程模型不一致、不完整、不正确	(4)决策不合理	(5)不合理提供
在飞机平台状态不满足武器发射条件的情形下,火控系统企图发现并截获目标。	一开始 IFFPC,当不满足 PS1/PS2/PS3 一继续 IFFPC,当不满足 PS1/PS2/PS3	扩展原因因素	PS1 的任何一条: —不正确或者遗漏 —没在适当的时间内刷新 —相互矛盾,使 PS1 含糊不清 PS2: —不正确或遗漏 —没有在适当时间内提供 —不再有效 PS3: —不正确或者遗漏 —没有在给定的时间内刷新 —相互矛盾,导致 PS3 含糊不清 PS1、PS2、PS3 相互矛盾。	PS1 的任何一条或其他改变或者更新 —没有检测到 —没有被正确地理解,导致 PS1 的不正确或矛盾理解 —检测和正确解释的时间太长 —检测和正确理解需要很多注意力。 PS2 或者任何改变/更新 —违反指令许可,没有正确检测或者解释。 —没有检测到许可,解释为许可。 PS3 —未检测到 —解释不正确,导致理解不正确或者相互矛盾 —正确检测和解释的时间太长 —正确检测和解释需要很多注意力 PS1、PS2、PS3 相互矛盾。	飞行员相信: —PS1 满足,实际上不满足 —PS2 满足,实际上不满足 —PS3 满足,实际上不满足	PS1 生成故障,不合理 PS2 生成故障,不合理 PS3 生成故障,不合理 传感器故障 执行器故障 发动机故障 飞控系统故障	飞行员不合适地提供了 IFFPC 开始和 IFFPC 继续指令,并且飞行员没有依据反馈信息意识到这一不适合指令。

第一类事故原因因素。主要表现因高层状态信息不正确、错误、及高层状态信息之间的矛盾导致的事故。针对高层过程状态 PS1，其相对应的任一反映飞机姿态的低层反馈信息都可能不正确、遗漏或没有在适当时间内刷新，并且有可能各个低层状态的反馈信息间会产生冲突，IFFPC 各个设备间也会产生冲突，因此对应的 PS1 高层状态就会模糊不清。类似的这种状况也会在 PS2 和 PS3 各自的高层过程状态和低层过程状态出现。另外一种反馈信息原因因素产生于 PS1、PS2 和 PS3 各个高层过程状态信息的冲突，这将会导致错误的意向模型和决策。传统安全性分析方法对于这类事故原因因素中的状态信息不正确、错误可以有效地进行分析，但是对于状态信息之间矛盾所导致的事故却不能有效地解决。例如，当 PS2 中的指令得到许可，但是 PS1 的发射条件不满足，同时 PS3 的空域模型没有清空，飞行员将不能正确地执行发射指令。

第二类事故原因因素。主要指由于过程更新的延时及其不正确解释导致的事故。这类原因因素的分析遵循于第一类原因因素的分析模式，从其相关的高层过程状态和低层过程状态出发。例如，任一 PS1 低层过程状态的改变在有限的时间内有可能没有被识别或者解释不正确，因此会花费大量的注意力，导致对高层过程状态不准确或相互冲突的理解。针对这类事故原因，传统的安全性分析方法只能对反馈信息的正确与否进行分析，而对其理解的正确与否并不能进行有效的分析，如果忽略对其理解不正确这一原因因素，则有可能会导致飞行员过程模型的错误，进而导致错误的开始或继续 IFFPC。

第三类事故原因因素。这类事故原因因素是由于飞行员错误的将不满足的条件判断为满足。区别于以上两种原因因素，这类事故原因因素是以高层过程状态的抽象为中心，主要表现在飞行员对高层状态信息的理解，当飞行员的理解与实际状态不相符时，就会导致事故。传统的安全性分析方法对这类由于逻辑错误引起的事故不能进行有效地分析。此外，表 3 中的三种事故原因因素为或逻辑，任何一种的理解与实际状况不符，都将会导致事故。在今后的系统设计中，对于复杂的多高层状态信息的系统，加强逻辑的简化将会减轻相关操作人员的负担，增强操作人员对系统实际状态的理解能力，从而减少人为错误，增加系统的安全性。

第四类事故原因因素。这类事故原因因素主要由于传感器、执行器、发动机、飞控系统等相关设备的故障造成飞行员的决策与实际情形不匹配。决策与实际情况不匹配的原因主要是由于设备的故障，而并非系统的逻辑错误和飞行员的理解错误。传统的安全性分析方法可以分析出因为这些设备故障导致的事故，值得注意的是，这只是引起事故的原因之一。

第五类事故原因因素。这类事故原因因素主要指飞行员不适当的开始或继续 IFFPC，同时没有通过反馈来及时调整这一错误动作。对于这种情况，如果是由于错误的反馈信息导致的飞行员的错误操作，可用传统的安全性分析方法进行分析；如果反馈信息正确，是由于某些外部干扰信息的影响导致的飞行员错误操作，传统的安全性分析方法将不能进行相应的分析。

上述分析的五类事故原因因素都直接或间接的与人为因素密切相关。从分析手段上看，不再将人为差错以概率的形式来体现，而是基于提出的 STPA 控制模型，对决策过程中的相关问题进行具体化的描述，根据火/飞/推控制系统的不同状态、周围环境等上下文信息着重对人为差错产生的事故原因进行分析；从分析结果上看，不是简单的给定人为差错的概率，而是得出导致人为差错的具体原因。与传统的安全性分析方法相比，本文所采用的方法在分析人为因素所导致的事故时，将人为差错的原因具体化，在改进火/飞/推控制系统结构、减少人为差错等方面具有实际意义。

4 结 论

(1) 本文应用的基于系统理论过程的分析方法有效地解决了传统的 FTA、FMEA 等基于线性事件链模型的安全性分析方法不能很好地解决人为危险因素的问题，通过作战飞机 IFFPC 系统的 STAMP 模型及 STPA 分析方法，结合 IFFPC 系统的三种可能状态，详细地描述了人工控制器包含的五类事故原因因素。

(2) 与传统安全性分析方法相比，将分析的重点从基于线性事件链模型的相关问题转移到基于系统理论的过程控制问题，主要对控制过程中潜在

的危险原因因素进行分析,找出危险源头,并通过规范和限制人的控制行为来确保任务的完成,弥补了传统安全性分析方法存在的缺陷,为含有人工控制器的复杂系统的安全性分析提供了一种新的思路。

参考文献

[1] 秦彦磊,陆愈实,王娟. 系统安全分析方法的比较研究[J]. 中国安全生产科学技术,2006,2(3):64-67.
Qin Yanlei, Lu Yushi, Wang Juan. Contrast research of system safety analysis methods[J]. Journal of Safety Science and Technology, 2006, 2(3): 64-67. (in Chinese)

[2] Kaiser J, Vernaleken C. Civil aviation[M]. Berlin: Springer Berlin Heidelberg, 2013: 135-158.

[3] Selles J W. Crashed during approach, Boeing 737-800, near amsterdam schiphol airport[EB/OL]. (2009-02-25)[2016-04-19]. http://catsr.ite.gmu.edu/SYST460/TA1951_AccidentReport.pdf.

[4] Boyd J R. The essence of winning and losing[EB/OL]. (2010-08-10)[2016-04-19]. https://www.researchgat-e.net/publication/247868527_The_Essence_of_Winning_and_Losing.

[5] Rasmussen J. Skills, rules, and knowledge: signals, signs, and symbols, and other distinctions in human performance models[J]. IEEE Transactions on Systems, Man and Cybernetics, 1983, 13(3): 257-266.

[6] Cameron L T. Extending the human-controller methodology in systems-theoretic process analysis(STPA)[D]. Cambridge: MIT, 2014.

[7] Nancy G Leveson. Engineering a safer world: systems thinking applied to safety[D]. Cambridge: MIT, 2012.

[8] 刘杰,阳小华,余童兰,等. 基于STAMP模型的核动力蒸汽发生器水位控制系统安全性分析[J]. 中国安全生产科学技术,2014,10(5):78-83.
Liu Jie, Yang Xiaohua, Yu Tonglan, et al. Safety analysis on control system for water level of steam generator in nuclear power plant based on STAMP model[J]. Journal of Safety Science and Technology, 2014, 10(5): 78-83. (in Chinese)

[9] Nancy G Leveson. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42(4): 237-270.

[10] 郑磊,胡剑波. 基于STAMP/STPA的机轮刹车系统安全性分析[J/OL]. 航空学报,http://www.cnki.net/kcms/detail/11.1929.V.20160606.1616.008.html.
Zheng Lei, Hu Jianbo. Safety analysis of wheel brake system based on STAMP/STPA[J/OL]. Acta Aeronautica et Astronautica Sinica, http://www.cnki.net/kcms/detail/11.1929.V.20160606.1616.008.html. (in Chinese)

[11] 宋述杰,张怡哲,邓建华. 火/飞/推综合控制系统及其仿真平台研究[J]. 飞行力学,2007,25(1):30-33.
Song Shujie, Zhang Yizhe, Deng Jianhua. Study on an integrated fire/flight/propulsion control system and its digital simulation/design plaform[J]. Flight Dynamics, 2007, 25(1): 30-33. (in Chinese)

[12] 张怡哲. 火力/飞行/推进控制系统综合研究[D]. 西安:西北工业大学,2001.
Zhang Yizhe. Study of integrated flight/fire/propulsion control system[D]. Xi'an: Northwestern Polytechnical University, 2001. (in Chinese)

[13] Nancy G Leveson. An STPA primer[EB/OL]. (2013-08-01)[2016-04-19]. http://sunnyday.mit.edu/STPA-Primer-v0.pdf.

作者简介:

胡剑波(1965—),男,博士,教授。主要研究方向:先进控制理论与应用、安全性工程、信息系统工程。

郑　磊(1987—),男,博士研究生。主要研究方向:安全性工程、飞行器适航性管理与验证。

(编辑:赵毓梅)