文章编号:1674-8190(2020)04-508-09

STPA 与 ARP4761 中的安全性分析方法对比研究

崔利杰[1],田宇[2],丛继平[3],马涛[4]

(1.空军工程大学 装备管理与无人机工程学院,西安 710051)

(2.中国人民解放军 95655 部队,成都 611530)

(3.空军工程大学 研究生院,西安 710051)

(4.空军工程大学 信息与导航学院,西安 710051)

摘 要:STPA 是一种自顶向下的系统工程方法,可用于对复杂系统进行安全性分析,但目前对该方法的应用流程尚不具体,未表明其与传统安全性分析方法的异同,无法很好地体现出该方法的先进性和适用性。通过对比分析 STPA 方法与 ARP4761 中提供的安全性分析过程,说明 STPA 方法对于军用标准 GJB900A-2012 的符合性,指出其不足之处,并在功能控制结构、不安全控制行为识别、致因分析三个方面提出改进措施,提供符合现代飞机高技术特性的、值得借鉴的理论方法和流程指南,形成复杂航空产品乃至军用飞机系统级安全性设计流程,加深理论与实践的融合,可为 STPA 方法的进一步发展完善提供借鉴和参考。

关键词:STPA 方法;ARP4761;GJB900A-2012;安全性分析

中图分类号:[X949] **文献标识码**:A

DOI:10.16615/j.cnki.1674-8190.2020.04.008 **开放科学(资源服务)标识码(OSID)**:

A Comparative Study on the Safety Analysis Methods of STPA and ARP4761

CUI Lijie[1], TIAN Yu[2], CONG Jiping[3], MA Tao[4]

(1. College of Equipment Management and UAV Engineering, Air Force Engineering University, Xi'an 710051, China)

(2. Unit 95655 of the Chinese People's Liberation Army, Chengdu 611530, China)

(3. Graduate College, Air Force Engineering University, Xi'an 710051, China)

(4. College of Information and Navigation, Air Force Engineering University, Xi'an 710051, China)

Abstract: STPA (systems theoretic process analysis) is a kind of system engineering method, which can be used for the complex system to analyze its safety. However at present, the method is not in practical use and cannot well reflect the advanced nature and applicability of the method. By analyzing and comparing the STPA method with the analysis process in ARP4761, the conformity of STPA to GJB900A-2012 general requirements for equipment safety work is analyzed, which reflects the great advantages and applicability of STPA method and discovers its shortcomings. Some improvement measures are proposed in building functional control structure, identifying unsafe control behaviors and analyzing causes. The conclusion and proposed method can provide the theoretical and process guidance which is in line with the high-tech characteristics of modern aircraft and worthy of reference for the system-level safety design of complex aviation products. It deepens the integration of theory and practice, and provides reference for the further improvement of STPA method.

Key words: STPA method; ARP4761; GJB900A-2012; safety analysis

收稿日期:2019-10-09; **修回日期**:2019-11-21

基金项目:国家自然科学基金(71401174)

通信作者:丛继平,2039507399@qq.com

引用格式:崔利杰,田宇,丛继平,等. STPA 与 ARP4761 中的安全性分析方法对比研究[J]. 航空工程进展,2020,11(4):508-516.

CUI Lijie, TIAN Yu, CONG Jiping, et al. A comparative study on the safety analysis methods of STPA and ARP4761[J]. Advances in Aeronautical Science and Engineering, 2020, 11(4): 508-516. (in Chinese)

0 引　言

现代飞机是一个具有多功能的复杂系统,呈现出相互关联、信息融合、人机结合、软硬件耦合的发展趋势,这使得影响飞机运行安全的因素增加、安全因素之间的关联性增强,导致事故模型的构建和安全性分析变得更为困难。ARP4761 中描述的传统危害分析方法用来分析软件密集型系统的安全性,其有效性正逐渐降低。

国内外提出了多种针对软件密集型复杂系统安全性的分析模型和方法,例如,J. Rasmussen[1] 提出的跨学科研究风险管理建模的风险管理框架、E. Hollnagel 等[2] 针对社会技术系统提出的功能共振分析法、Hong Sheng 等[3-4] 提出的应用于评估轴承退化程度的基于 WP-EMD 和 SOM 网络的特征提取模型等。2004 年,N. G. Leveson[5] 提出了用于对危险致因进行分析的系统理论过程分析方法(System Theoretic Process Analysis,简称 STPA)。STPA 是一种自顶向下的系统工程方法,它注重于从危险入手,对系统的各部件以及各部件之间的相互作用进行分析。

目前,基于 STPA 的安全性分析已被应用于各个领域。在软件分析方面,让涛[6] 提出了一种基于 STPA 的软件安全性分析与验证方法;甘旭升等[7] 成功地将 STPA 危险分析方法应用于 ATSA-ITP 设计中。在具体的复杂系统中,刘朝晖等[8] 对数字化反应堆紧急停堆系统应用 STPA 方法进行安全性分析;王琳[9] 提出了基于 STPA 的复杂机载系统安全性分析方法;曹顺安等[10] 实现了直升机燃油系统运行的危险性分析。在交通系统运作中,王洁宁等[11] 提出了基于 STPA 的空管运行系统安全分析方法;刘金涛[12] 提出了基于 STPA 的需求阶段的高速列车运行控制系统安全分析方法;刘宏杰等[13] 完成了基于 STPA 方法的平交道口安全需求分析;A. L. Dakwat 等[14] 总结了基于 STPA 的系统安全分析和模型检验。在军用领域,胡剑波等[15-16] 进行了综合火/飞/推控制系统复杂任务的 STPA 分析,以及基于 STAMP/STPA 的机轮刹车系统安全性分析,拓宽了 STPA 方法的应用领域。相比于其他方法,STPA 分析运用系统与控制理论,更多地考虑系统组件间的相互作用对系统整体安全性的影响。因此,对于高耦合复杂系统来说,该方法能够更加全面、准确地识别其安全性需求,对提升系统的安全性水平具有重要意义。随着安全学科领域的不断发展,安全性分析方法也在不断改进。突出表现为:致因机理从基于链式/树型事故因果模型向基于系统的、网络式的致因分析方法转变,危险源识别从传统的事后被动分析方法向创新的事前主动判别型危险源体系转变[17]。

目前基于系统理论和控制模型的安全性分析方法已在软件应用、系统设计等方面有了实践成果,但运用 STPA 理论分析的流程并不细致具体,未表明其与传统的安全性分析方法有何异同,也无法证明其得出的安全性需求是否完备,不能很好地体现出该方法的先进性和适用性。因此,本文将 STPA 方法与 ARP4761 中提供的安全性分析过程从潜在事故因果模型、评估结果(输出)、分析过程等方面进行比较研究,并对照 GJB900A－2012《装备安全性工作通用要求》分析其对于军用标准的符合性,来体现 STPA 方法的优势与符合性,并针对在分析过程中发现的一些不足之处,提出改进方法。

1 安全性分析方法

1.1 ARP4761 中的安全性分析方法

ARP4761 论述了民航飞机适航合格审定的安全性评估指南和方法,在考虑飞机运行环境的基础上,介绍了飞机级安全性评估的流程、方法和工具。安全性评估过程包括安全性需求分析以及为飞机研制进行的相关验证活动[18]。

ARP4761 流程由三个部分组成:功能危害分析(FHA)、初步系统安全分析(PSSA)和系统安全分析(SSA),这些工作在研究系统的每个相关抽象级别(或层次级别)上执行。飞机研制中的安全性评估过程简述如图 1 所示[19]。

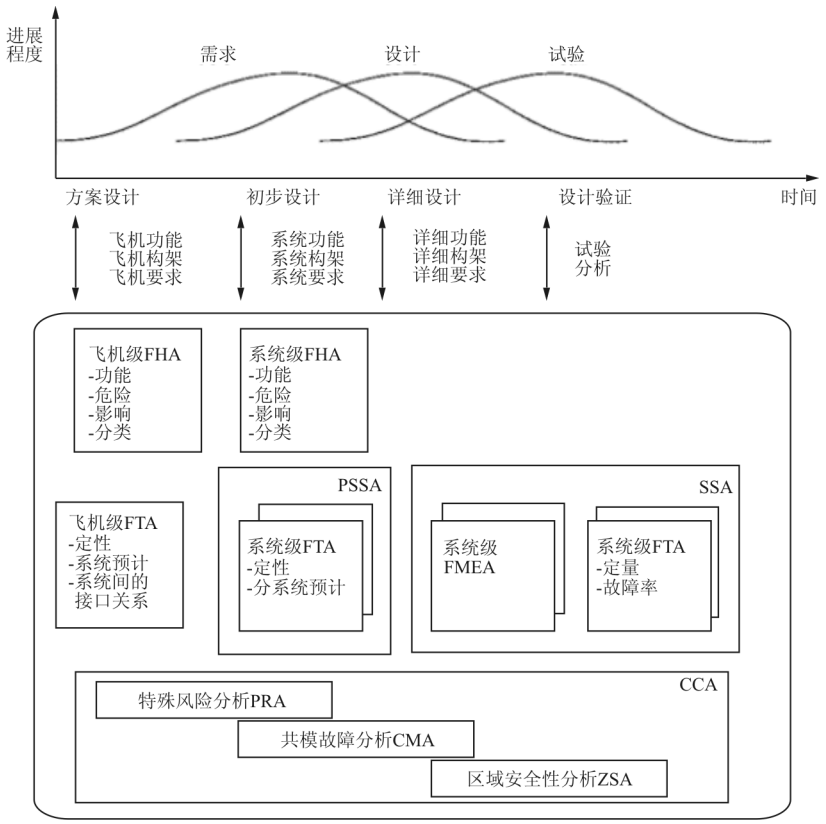

图 1 安全性评估过程

Fig. 1 Safety assessment process

故障和概率风险评估是 ARP4761 中描述的主要方法。针对飞机的安全性评估工作,使用基于故障的风险分析技术。分析的目标主要是定量的结果,定性分析只用于无法得到或不合适得到概率之处。

故障树分析(FTA)、关联图分析(DD)和马尔可夫分析(MA)是自上而下的分析技术,可持续向下分析到设计的详细层次。在 FHA 识别故障状态之后,FTA/DD/MA 作为初步系统安全分析的一部分,用来确定导致故障状态的较低层次的单个故障或组合故障。

故障模式与影响分析(FMEA)是一种系统的、自上而下的识别系统、单元与功能的故障模式并确定其对上层影响的方法。FMEA 可以在系统的任一层次(例如功能、零件等)上进行,通常用来分析单一故障的影响。

共因分析(CCA)是对共因失效进行定性和定量分析的工具,可以用来检验系统间是否满足独立性要求,分析共因失效条件下对系统失效的概率[10]。共因失效分析得出故障模式以及一些外部事件所能引起的灾难性的或危险的故障后,必须避免导致灾难性的故障后果的共因事件;而对于危险的故障后果,这些共因事件发生的概率必须控制在给定的概率之内。

总体来说,ARP4761 中安全性分析方法的共同特点如下:

(1) 假设事故是由部件故障和故障链引起的;

(2) 关注组件故障、常见原因/模式故障;

(3) 考虑组件之间有限的(主要是直接的)功能交互;

(4) 安全性等同于可靠性;

(5) 分析中不包括飞行员和其他操作人员,对人为因素进行了分类,但未对其进行处理;

(6) 可从概念形成阶段开始迭代系统工程。

1.2 STPA 安全性分析方法

在 STPA 中,控制问题被认为是导致系统发生危险的原因,其中控制问题是指未对系统各组件之间的交互、系统外部的干扰、系统部件的失效进行安全有效的控制。

STPA 方法是基于 STAMP(Systems Theoretic Accident Modeling and Processes)对已辨识的系统危险进行致因分析,即以控制为中心点,以系统中不安全的控制行为为着力点,对系统部件间的控制关系用分层的控制结构进行描述。通过过程模型,对不安全控制行为进行分类分析,找到系统危险核问题发生的根本原因,然后根据问题发生的原因可以衍生出对应的安全性需求(即安全约束)。通常认为,只有违反相应的安全性需求(安全约束)时,系统才会发生事故。

STPA 分析的危险包含设计错误、组件影响、造成事故的社会、组织和管理因素,特别是与软件、人为因素和操作方面相关的危险。总之,STPA 的目标是识别导致事故的详细场景,以便在设计中消除或控制它们,而不只是机电组件的故障或显示可靠性目标是否达到要求。

STPA 理论首先针对控制行为进行分类,并将不安全的控制行为总结为四种类型:(1)没有提供控制行为;(2)提供了产生危险的控制行为;(3)过早或过晚提供安全控制行为;(4)提供的控制行为作用时间过短或过长。

STPA 的过程可分为四个主要步骤:(1)定义分析目标,进行目标对象的系统级分析;(2)建立对象的功能控制结构;(3)识别潜在的不安全控制行为,分析单个组件的安全性需求;(4)分析不安全控制行为的致因,确定系统潜在的安全性需求:致因情景不仅包括组件故障,还包括其他因素,例如系统组件之间的直接和间接交互(可能没有"出现问题"),确定的致因情景作为开发系统和组件新的安全需求和约束基础。

2　STPA 方法与现有标准对比

STPA 方法较之于 ARP4761 安全性分析过程,更适应高度复杂、软件密集系统的安全性分析。GJB900A 提出的相关安全性工作项目,尤其是在软件安全性分析上,STPA 方法表现出了极强的适用性。

2.1　STPA 与 ARP4761 对比分析

ARP4761 没有考虑危险因素与人为因素(HF)的相互影响,而 STPA 则将人作为系统的一部分进行分析,识别潜在模式的影响类型,以及由于实际自动控制状态与飞行员的心理模型之间不同步而可能产生的危险。STPA 的目标与其他危险分析方法的相似之处在于:它试图确定系统危险是如何发生的,以便通过修改系统设计来消除或减轻危险。然而,其目标不是像 ARP4761 那样推导出概率需求,而是识别在设计或操作中需要消除或减轻的危险场景(危险被定义为系统安全工程中的危险,即系统状态或条件集,当与某些最坏的环境条件相结合时,将导致事故或损失事件)。总结 STPA 分析过程与 ARP4761 提供的分析评估过程在不同方面的主要差异,如表 1 所示。

表 1　STPA 与 APR4761 的差异

Table 1　Difference between STPA and APR4761

类　别	ARP4761 安全性分析过程	STPA 危险分析过程
事故过程模型	假设事故是由部件故障和故障链引发。	假设事故是由于对系统组件的行为和交互的约束执行不当造成的。
	关注组件故障、常见原因/模式故障。	重点关注组件之间的控制和交互,包括组件之间正常的交互以及单独的组件故障。
	考虑组件之间有限的(主要是直接的)功能交互。	识别组件之间的直接和间接不安全的功能关系。
	安全性与可靠性相似。	安全性被视为与可靠性不同的(有时是相互冲突的)系统特性。
目　标	安全评估。	危害分析。
	主要是定量,以显示符合相关适航标准的要求。 定性分析(例如 CCA)用于无法得到或不合适得到概率之处。	定性。目标是确定潜在的危害原因(进行危害分析),而不是安全评估。生成功能性(行为)安全要求,识别导致危害的系统和组件设计缺陷。

续表

类 别	ARP4761 安全性分析过程	STPA 危险分析过程
结 果	产生系统和部件的概率故障(可靠性)要求。	生成功能安全要求。
	可能性分析。	识别导致危害的设计缺陷。
	可能性(和严重性)分析。	最严重情况分析。
操作员在分析中的作用	除了作为物理系统组件故障的缓冲外,分析中不包括飞行员和其他操作人员。ARP4761 对人为因素进行了分类,但未对其进行处理。	飞行员和操作人员作为系统和分析的组成部分。
软件在分析中的作用	不为软件分配故障概率。	软件与其他任何控制器、硬件或人一样,通过设计来保证直接分析软件行为对危害的影响。
	假设需求是完整且一致的。	软件和其他组件生成功能安全需求,以消除或控制与软件行为相关的系统危害。
	安全评估只考虑由于需求实现错误而导致的故障。	考虑所有的软件行为(不仅仅是“故障”),以确定可能导致的系统危险。
操作在分析中的作用	除发电装置的安装和维护要求外,一般不包括其他操作。	操作和整体安全管理系统被包括在内。
过 程	从飞机功能和功能丧失开始。	从危险和损失开始。
	未完全从概念形成阶段开始迭代的系统工程过程。	可从概念形成阶段开始迭代的系统工程过程。

从表 1 可以看出:STPA 识别出了 ARP4761 中的安全性分析容易忽略的危险,特别是与软件、人为因素和操作相关的危险。

STPA 的目标是识别导致事故的详细场景,以便在设计中消除或控制危险,而不是显示可靠性目标是否达到要求。ARP4761 在分析之后的验证过程仍是必要的,以确保提供的需求得到充分验证。

在飞机复杂性和软件控制日益增加的过程中,过去简单、自动化程度较低的设计已逐渐被淘汰,航空领域的安全学需要采用新的方法来应对新的变化。ARP4761 中描述的传统安全评估过程忽略了造成飞机事故的部分重要原因,因此,需要创建和使用更全面的方法来评估安全性,分析更多类型的因果因素,并将软件和人为因素直接集成到评估中;同时需要不断探索 STPA 以及其他新的安全性分析方法的潜力,进而对 STPA 进行改进或扩展。

2.2 STPA 在 GJB900A 中的适用性

GJB900A 规定了装备寿命周期内开展安全性工作的一般要求和工作项目。本节将分析 STPA 方法是否符合和支持我军目前使用的这一安全标准中的相关工作项目。

(1) 安全性工作项目对照分析

①初步危险分析(工作项目 302):

STPA 可以(并且正在)用于 PHA。它包括工作项目 302 中提到的所有因素。传统的危险分析方法,如人工、软件、接口、组件之间的交互、模式、运行环境和约束等,对上述因素的处理往往存在不足,而 STPA 提供了确定消除或减轻危险措施所需的信息。

除了简单地识别危险之外,STPA 还确定了它们的因果情景。能在早期消除设计决策错误(根据系统安全设计优先),而不必在后期的详细决策阶段更改设计方案(撤销设计决策的返工代价高昂)。设计师们正在使用 STPA 作为他们早期设计工作的一部分,以帮助他们在无法逆转一些基本的设计决策之前做出提高安全性和网络安全性的决策。

②系统危险分析(工作项目 304):

STPA 通过生成系统和组件安全需求,确定它们产生的原因,并使用因果场景生成详细的设计和操作需求来支持这项任务。

一旦 STPA 确定了不安全控制行动(详细危险)的因果场景,如果不能完全消除危险,则确定如何验证和进行验证是很简单的。验证包括人工测试模拟器生成场景。此外,基于模型的开发系统可以使用不安全控制动作(详细的危险)来生成模型,并从这些正式的模型中生成软件测试数据,以确保危险软件行为的测试覆盖率。通过加强流程模型控制将要求与安全控制结构连接起来。

STPA 方法是一个自顶向下的危险分析工具,它可以包含所有子系统。在 STAMP 和 STPA 中,子系统危险分析是一般系统分析的一部分。STPA 识别危险和因果场景,这些场景可能涉及子系统行为,导致系统危险。因果情景中的信息(与任何危险分析技术一样)可以用于协助设计师确定设计缓解措施。与许多传统的危险分析技术不同,STPA 不仅考虑故障,还考虑设计错误、定时错误、无意中起作用或在错误的条件下起作用等。STPA 亦考虑人作为系统的一个组成部分,这与工作项目 304.2 任务描述中所要求相一致。

STPA 将系统危险分析、子系统危险分析、功能危险分析和系统中的系统危险分析集成到一个过程中,并生成所有这些任务所需的信息。

③使用与保障危险分析(工作项目 305):

STAMP 安全控制结构可以包括操作控制结构,采用 STPA 进行使用与保障危险分析是可行的。在现有文献中,STPA 已被用于操作飞行测试的安全性。使用与保障安全规划应从概念发展阶段开始,以便将作业安全纳入系统设计。STPA 可以支持这种提前性分析。

④安全性验证(工作顶目 401):

如工作项目 302 所述,从已确定的因果场景生成测试和演示具有可行性。

⑤安全性评价(工作项目 402):

与其他危险分析技术一样,STPA 以危险、潜在原因以及减轻或控制它们的形式向评价工作提供输入,但是作为一种危险分析技术,它也只能为这一过程提供输入,而关于每个危险和风险接受决策的最终决策则超出了 STPA 的范围。

此外,STPA 与传统的危险分析方法的不同之处在于,它提供了关于危险人员和软件行为的信息。有关如何预防这些危险的具体设计决策由分析提供,并在最终的安全性评估中使用,而不是简单地讨论软件的严格程度或人为错误的可能性。

在生成危险管理评估报告上,STPA 同样以确定的危险(包括不安全的控制行动)、潜在原因、消除或减轻危险的建议以及为减轻危险而创建的任何控制的形式向本报告提供了输入。实际的风险评估决策超出了风险分析技术的要求范围。

STAMP、STPA 和 CAST(基于系统论的因果分析)可以提供对任务 303 和 304 的支持,方法是提供危险的原因,并使用它们来帮助开发测试用例。STPA 还协助将系统安全流程进行更新。使用最初应用 STPA 时创建的安全控制结构,可以将更改定位到结构中,以便只需要检查那些受影响的部分,以确定更新是否引入或影响了危险因素。

总体来看,STPA 完全符合 GJB900A 相关要求。STPA 是一个自顶向下的系统危险分析方法,可用于风险分析任务(工作项目 300 系列)。它识别危险并生成:①系统和组件安全和网络安全需求;②消除或减轻识别危险所需的信息。STAMP 控制结构提供了记录关于系统结构和任务中描述的需求等大量信息的方法。STPA 建模和分析可以从概念开发阶段开始,以帮助设计师对基本的架构设计和开发问题进行决策,从而消除或减轻危险。有特定的因果情景可以帮助确保 PHA 不会在没有因果信息的情况下,通过过早的可能性评估,错误地对重要的危险进行分类。STPA 满足工作项目 304(系统危险分析)中强调的在项目早期获取安全相关信息的需要。随着决策的制定,分析可以以迭代的方式进行细化,生成的信息还可以用于验证设计和活动。

(2) STPA 与软件安全性分析

GJB900A 关于软件安全性工作特别规定了工作项目 600 系列,依据前文的分析过程以及对比,可以得出在软件安全性工作中,STPA 方法可直接或间接地协助下列工作,对这些活动所列的大部分任务提供帮助:

①识别软件相关的危害(软件对系统级危害);

②识别可能导致危险软件行为的因果场景;

③向设计软件以消除危险软件行为的人员和设计系统以减轻任何潜在危险软件行为的人员提供信息;

④创建文档和模型(即安全控制结构),以便就危害、不安全控制行动、不安全控制行动的原因、对控制器的安全关键反馈、环境威胁(包括网络安全威胁)以及正在考虑的系统内和更大系统内的协调和沟通进行沟通和共同理解;

⑤进行软件安全危害分析;

⑥跟踪危害及其后果,以及在危害日志中选择控制策略;

⑦跟踪软件体系结构中的系统级危险;

⑧识别对安全至关重要的软件功能和组件,以及对安全至关重要的反馈和沟通要求;

⑨支持软件测试和验证活动;

⑩生成关键指标，以识别软件或系统中的更改何时可能导致危险。

可以看出，由于软件安全性工作较强的结构性和程序性要求，基于自顶向下的系统工程的 STPA 方法更适合于软件密集型系统的安全性分析。

3 STPA 方法的改进

STPA 方法是一个自顶向下、持续迭代的过程，适用于复杂的系统生成功能安全要求，识别导致危害的设计缺陷。STPA 方法的优势总结如下：

（1）能够分析高度复杂的系统；

（2）能够在系统研发早期介入；

（3）能够分析软件和人为因素；

（4）能够识别大型复杂系统中容易忽略的系统功能；

（5）能够结合过程模型实现基于模型的系统工程；

（6）相对于传统危险分析方法，危险识别更全面。

STPA 可以用于系统生命周期的任一阶段，为系统设计、研制、运行等过程提供确保安全性约束执行必须的信息。但 STPA 方法仍存在一些不足之处需要改进：

（1）目前，研究运用的 STAMP 模型一般是基于主观描述建立系统功能控制结构等，模型建立的思路不清晰，层次不分明，未突出重点，其准确性受人的分析能力影响较大；

（2）在 STPA 方法中，过程模型的要素分解不够详细，分析控制过程中的不安全控制行为容易造成混乱，没有体现与分析实际相关的关键性信息；

（3）对于不安全控制行为的致因分析只是因果关系的向上追溯，缺乏具体的逻辑关系和方法步骤，分析工作量大，分析结果的完整性及准确性受人对系统的主观认知、分析能力等的影响较大。

因此，本节针对分析过程中发现的 STPA 方法以上三个不足，尝试提出一些方法上的改进以供商榷。

3.1 创建功能控制结构的改进

创建功能控制结构的改进，主要是从结构物理功能层次性划分的角度深入。根据优化依据划分出多级控制层、信息层的输入/反馈/输出、执行层等。整个研究对象中，不被其他控制器控制、发出初始指令的控制器划分为一级控制层，操作人员一般为一级控制层。上级的控制层直接控制下级控制层。如果需要建立的模型非常复杂，同层中就可以分析多个控制器的相互作用。如多一个系统能发挥不同级别的功能，它对应包含的控制器就分属于多个控制级。每一级的控制层都可能直接影响执行层。信息层就是同级之间、不同级之间的控制器的输入、输出、反馈信息。新的功能控制结构的建立过程如图 2 所示。

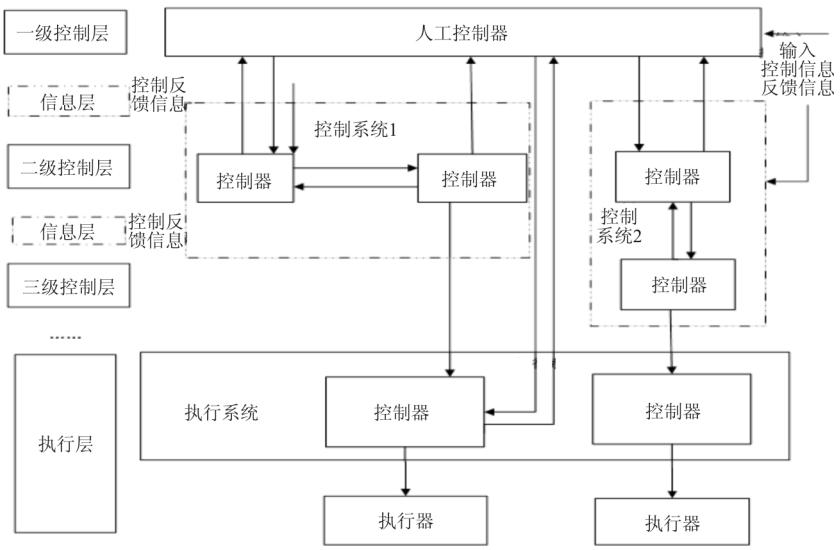

图 2 分层功能控制结构的建立

Fig. 2 Establishment of hierarchical function control structure

3.2　UCAs 识别过程的改进

STPA 方法的第三步是分析致因情景,识别潜在的不安全行为(Unsafe Control Actions,简称 UCAs)。这一步骤的主要方法是基于对过程模型的分析。改进后的过程模型如图 3 所示。

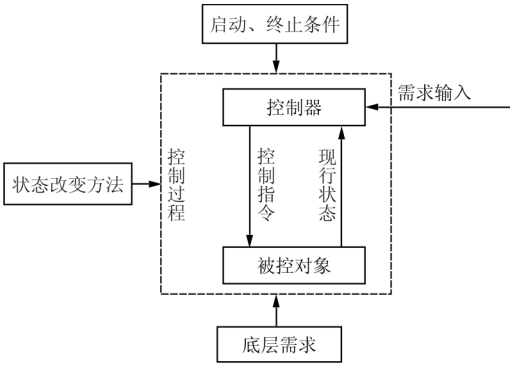

图 3　过程模型

Fig. 3　Process model

改进前的过程模型要素分解不够详细,不利于分析得出控制过程中的不安全控制行为,体现在分析实际相关的关键性信息不足。改进后体现与分析实际相关的关键性信息,明确输入和输出,状态的前后改变,这样可以从每一步骤的分析来找出不安全控制行为。

3.3　UCAs 致因分析的改进

STPA 方法完成针对单一的控制行为分析后,主要是根据控制反馈模型向后追溯因果场景来生成潜在需求,但并未说明采用何种逻辑、方法来向后追溯。因为在复杂系统安全性问题中,不安全控制行为往往是由于子系统关联产生的。因此可以从两个 UCAs 之间的相互影响来分类分析致因的产生。

(1) UCAs 的组合影响:当一个 UCA 发生的同时,发生了另一个与之相关 UCA,使得其影响增大或者削弱,这类问题统称为不安全控制行为的组合问题。考虑不安全控制行为的影响强度,不涉及 UCAs 提供时间及作用的长短时,UCAs 的共同作用的影响如表 2 所示。

表 2　UCAs 的组合影响

Table 2　UCAs combination impact

UCA-1	UCA-2	组合结果	组合影响
较弱	较弱	弱	……
较弱	较强	可能效果抵消	……
较强	较强	强	……

(2) UCAs 发生先后的影响:进行复杂系统安全性分析时,需要分析两个 UCAs 的作用先后影响。即考虑两个不安全控制行为在一个较短时间内,作用的次序不同对系统的影响。此处的较短时间被定义为在上一个不安全控制行为仍然作用的时间内。先后作用的次序不同,造成的影响也不同的这类问题。假设 UCA1 和 UCA2 是两个存在功能联系的不安全控制行为,那么 UCA1 和 UCA2 间的作用次序关系有三种情况:①UCA1 先发生;②UCA2 先发生;③UCA1 和 UCA2 同时发生。(UCA1 和 UCA2 造成不同影响的情形)。

(3) UCAs 之间的因果影响:当两种 UCAs 由于涉及到共同的物理功能等情况时,存在一定的因果联系,那么需要分析二者的交互影响,及在分析其中一个不安全控制行为的致因时,由于该不安全控制行为是另一个 UCA 产生的因素,那么此致因也同样是另一个 UCA 的致因。

通过对分层功能控制结构的优化使得系统的层次结构、信息交互更加清楚,进行实质内容的扩展以及结构上的优化,为后续分析步骤提供引导,有助于更复杂系统模型的建立,按照层级间的联系进行分析,有助于分析出潜在的不安全控制行为;通过对识别过程的改进,提出改进的过程模型,可以从每一步骤的分析来找出不安全控制行为。增添了底层需求,包括液压源、电源等,可以为多系统间的分析提供帮助;通过对致因分析方法的改进,按照一定逻辑方法分析控制行为所有可能原因,缩短分析时间,提高了分析过程的效率,从 STPA 方法三个主要方面优化了方法实施步骤。

4　结　论

(1) 本文通过将 STPA 方法与 ARP4761 标准进行对比,表明 STPA 方法的优越性,并通过对 STPA 方法的功能控制结构、不安全控制行为识别、致因分析三个方面进行结构和逻辑上的改进,使 STPA 方法更适用于复杂航空产品的系统安全性设计,为提高复杂航空产品的安全性提供理论支撑,拓宽了 STPA 的应用领域,而且对于 STPA 方法的改进措施也促进了其理论的进一步更新完善。

(2) 本文仅是对 STPA 安全性分析方法的理论研究,今后的研究会将该方法应用于具体的安全性分析工作中,进一步验证 STPA 方法的先进性。

参考文献

[1] RASMUSSEN J. Risk management in a dynamic society: a modelling problem[J]. Safety Science, 1997, 27(2/3), 183-213.

[2] HOLLNAGEL E. 功能共振分析方法：复杂社会－技术系统建模[M]. 田瑾，译. 北京：国防工业出版社，2015.
HOLLNAGEL E. Fram: the functional resonance analysis method modelling complex socio－technical systems[M]. Translated by TIAN Jin. Beijing: National Defense Industry Press, 2015. (in Chinese)

[3] HONG Sheng, ZHOU Zheng, ZIO E, et al. Condition assessment for the performance degradation of bearing based on a combinatorial feature extraction method[J]. Digital Signal Processing, 2014, 27: 159-166.

[4] HONG Sheng, ZHOU Zheng, ZIO E, et al. An adaptive method for health trend prediction of rotating bearings[J]. Digital Signal Processing, 2014, 35: 117-123.

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

[6] 让涛. 一种基于 STPA 的软件安全性分析与验证方法[J]. 电子世界，2016(5)：135-136.
RANG Tao. A STPA-based software security analysis and verification method[J]. Electronic World, 2016(5): 135-136. (in Chinese)

[7] 甘旭升，崔浩林，刘卫东，等. STPA 危险分析方法及其在 ATSA-ITP 设计中的应用[J]. 中国安全科学学报，2015(5)：80-86.
GAN Xusheng, CUI Haolin, LIU Weidong, et al. STPA hazard analysis method and its application in ATSA-ITP design[J]. Chinese Journal of Safety Science, 2015(5): 80-86. (in Chinese)

[8] 刘朝晖，陈智，吴志强，等. STPA 方法在数字化反应堆紧急停堆系统安全性分析中的研究与应用[J]. 核动力工程，2015，36(s2)：157-161.
LIU Zhaohui, CHEN Zhi, WU Zhiqiang, et al. Research and application of STPA method in safety analysis of digital reactor emergency shutdown system[J]. Nuclear Power Engineering, 2015, 36(s2): 157-161. (in Chinese)

[9] 王琳. 基于 STPA 的复杂机载系统安全性分析方法研究[D]. 南京：南京航空航天大学，2017.
WANG Lin. Research on security analysis method of complex airborne system based on STPA[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2017. (in Chinese)

[10] 曹顺安，陈捷宇，胡宁. 基于 STPA 的直升机燃油系统运行危险分析[J]. 质量与可靠性，2017(6)：23-27.
CAO Shun'an, CHEN Jieyu, HU Ning. Risk analysis of helicopter fuel system operation based on STPA[J]. Quality and Reliability, 2017(6): 23-27. (in Chinese)

[11] 王洁宁，孙晓萌. 基于 STPA 空管运行系统安全分析方法研究[J]. 武汉理工大学学报，2017，39(12)：49-55.
WANG Jiening, SUN Xiaomeng. Research on safety analysis method based on STPA air traffic management system [J]. Journal of Wuhan University of Technology, 2017, 39(12): 49-55. (in Chinese)

[12] 刘金涛. 基于 STPA 的需求阶段的高速列车运行控制系统安全分析方法研究[D]. 北京：北京交通大学，2015.
LIU Jintao. Research on safety analysis method of high speed train operation control system based on STPA demand stage[D]. Beijing: Beijing Jiaotong University, 2015. (in Chinese)

[13] 刘宏杰，唐涛，金夏垚，等. 基于 STPA 方法的平交道口安全需求分析[J]. 北京交通大学学报，2018，42(2)：84-90.
LIU Hongjie, TANG Tao, JIN Xiayao, et al. Analysis of safety requirements for level crossings based on STPA method[J]. Journal of Beijing Jiaotong University, 2018, 42(2): 84-90. (in Chinese)

[14] DAKWAT A L, EMILIA V. System safety based on STPA and model checking[J]. Safety Science, 2018(11): 130-143.

[15] 胡剑波，郑磊. 综合火/飞/推控制系统复杂任务的 STAMP 建模和 STPA 分析[J]. 航空工程进展，2016，7(3)：309-315.
HU Jianbo, ZHENG Lei. STAMP modeling and STPA analysis of complex tasks of integrated fire/fly/push control system[J]. Advances in Aeronautical Science and Engineering, 2016, 7(3): 309-315. (in Chinese)

[16] 郑磊，胡剑波. 基于 STAMP/STPA 的机轮刹车系统安全性分析[J]. 航空学报，2017，38(1)：246-256.
ZHENG Lei, HU Jianbo. Safety analysis of wheel brake system based on STAMP/STPA[J]. Acta Aeronautica et Astronautica Sinica, 2017, 38(1): 246-256. (in Chinese)

[17] LEVESON N, FLEMING C, THOMAS J, et al. A comparison of SAE ARP 4761 and STPA safety assessment processes[C]// Engineering Systems for Safety: Twenty-third Safety-critical Systems Symposium (SSS 15). Bristol, UK: SAE, 2015: 55-78.

[18] SAE. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: SAE ARP4761[S]. USA: SAE, 1996.

[19] ALBERICO D, BOZARTH J, BROWN M. Software system safety handbook[M]. Patuxent River, USA: Joint Services Software Safety Committee, 1999.

作者简介：

崔利杰(1979－)，男，博士，副教授。主要研究方向：航空安全、系统可靠性与优化。

田　宇(1997－)，男，学士，助理工程师。主要研究方向：航空安全。

丛继平(1997－)，男，硕士研究生。主要研究方向：航空安全。

马　涛(1980－)，男，硕士，副教授。主要研究方向：通信与信息系统。

(编辑：马文静)